Cisco MDS 9000 シリーズ システム管理構成ガイド、リリース 9.x

最終更新：2025 年 5 月 19 日

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/

© 2025 Cisco Systems, Inc. All rights reserved.

目 次

はじめに：

はじめに xxiii

対象読者 xxiii

表記法 xxiii

マニュアルに関するフィードバック xxv

関連資料 xxv

通信、サービス、およびその他の情報 xxv

第 1 章

新機能および変更された機能に関する情報 1

第 2 章

システム管理の概要 3

Cisco Fabric Services 3

システムメッセージ 3

Call Home 4

スケジューラ 4

システム プロセスとログ 4

組み込まれている Event Manager 4

SNMP 5

RMON 5

パス トレース 5

ドメイン パラメータ 6

SPAN 6

Fabric Configuration Server 6

第 3 章

CFS インフラストラクチャの使用 7

CFS について 7

CFS を使用した Cisco MDS NX-OS 機能 7
CFS の機能 8
アプリケーションの CFS のイネーブル化 9
CFS プロトコル 9
CFS 配信のスコープ 9
CFS の配信モード 10
非協調型配信 10
協調型配信 10
無制限の非協調型配信 10
混合ファブリック内での CFS の接続性 10
ファブリックのロック 11
変更のコミット 11
CFS マージのサポート 12
IP を介した CFS 配信 12
CFS の静的 IP ピア 14
CFS リージョンの概要 15
注意事項と制約事項 16
デフォルト設定 16
CFS の設定 17
スイッチの CFS 配信のディセーブル化 17
変更のコミット 18
変更の破棄 18
設定の保存 18
ロック済みセッションのクリア 18
IP を介した CFS のイネーブル化 19
IPv4 を介した CFS の有効化または無効化 19
IP を介した CFS の IP マルチキャスト アドレスの設定 19
IPv4 を介した CFS のIP マルチキャストアドレスの構成 20
CFS の静的 IP ピアの構成 20
CFS リージョンの設定 22
CFS リージョンの作成 22

CFS リージョンへのアプリケーションの割り当て 22
別の CFS リージョンへのアプリケーションの移動 22
リージョンからのアプリケーションの削除 23
CFS リージョンの削除 24
CFS 設定の確認 24
CFS 配信ステータスの確認 25
アプリケーション登録スターテスの確認 25
CFS ロック ステータスの確認 26
IP を介した CFS 構成の確認 26
IP を介した CFS の IP マルチキャストアドレス構成の確認 27
静的 IP ピア構成の確認 27
CFS リージョンの確認 27
その他の参考資料 28

第 4 章 システムメッセージロギングの設定 29
システム メッセージ ロギングの概要 29
システム メッセージ ロギング 32
SFP 診断 33
出力されるシステム メッセージ ロギング サーバ ファシリティ 33
システム メッセージ ロギング設定の配信 34
ファブリックのロックの上書き 35
システム メッセージ ロギングの注意事項および制約事項 35
デフォルト設定 35
システムメッセージロギングの設定 36
システム メッセージ ロギングを設定するためのタスク フロー 36
メッセージ ロギングのイネーブル化またはディセーブル化 36
コンソール重大度の設定 37
モニタ重大度の設定 38
モジュール ロギングの設定 39
ファシリティ重大度の設定 40
オンボード ログ ファイルの構成 40

システム メッセージの送信元 ID の構成 41
システム メッセージ ロギング サーバの設定 42
システム メッセージ ロギングの配布の構成 42
変更のコミット 43
変更の破棄 43
ファブリックのロックの上書き 44
システム メッセージ ロギング情報の表示 44
その他の参考資料 50

第 5 章 **Call Home の設定 51**
Call Home の概要 51
Call Home の機能 52
Smart Call Home の概要 53
Smart Call Home の取得 54
Call Home 宛先プロファイル 55
Call Home アラート グループ 55
カスタマイズされたアラート グループ メッセージ 55
Call Home のメッセージ レベル機能 56
Syslog ベースのアラート 56
RMON ベースのアラート 56
HTTPS サポートを使用した一般的な EMail オプション 57
複数 SMTP サーバ サポート 57
電子メール ベースのアラート 58
定期的なインベントリ通知 58
重複するメッセージのスロットリング 58
Call Home 設定の配信 59
ファブリックのロックの上書き 59
Call Home ネーム サーバ データベースのクリア 59
EMC Email Home 遅延トラップ 59
イベント トリガ 60
Call Home メッセージ レベル 63

メッセージの内容 65
注意事項と制約事項 75
Call Home データベースのマージに関する注意事項 75
Call Home の設定に関する注意事項 75
デフォルト設定 76
Call Home の設定 77
Call Home を設定するためのタスク フロー 77
連絡先情報の設定 77
DCNM-SAN を使用したコンタクト情報の構成 78
Call Home 機能のイネーブル化 79
DCNM-SAN を使用した Call Home 機能の有効化 80
宛先プロファイルの設定 81
DCNM-SAN を使用した事前定義済み接続先プロファイルの構成 83
新規接続先プロファイルの構成 83
DCNM-SAN を使用した新規接続先プロファイルの構成 84
アラート グループと宛先プロファイルのアソシエート 85
DCNM-SAN を使用したアラート グループの関連付け 86
アラート グループ メッセージのカスタマイズ 87
DCNM-SAN を使用したアラート グループ メッセージのカスタマイズ 88
Call Home メッセージ レベルの設定 89
Syslog ベースのアラートの設定 89
DCNM-SAN を使用した Syslog ベースのアラートの構成 90
RMON アラートの設定 90
DCNM-SAN を使用した RMON アラートの構成 91
イベント トラップ通知の構成 92
一般的な EMail オプションの構成 92
DCNM-SAN を使用した一般的なEMail オプションの構成 93
HTTPS サポートの設定 93
トランスポート メソッドの有効化または無効化 94
HTTP プロキシ サーバの設定 95
DCNM-SAN を使用した HTTP プロキシサーバーの構成 96

Call Home ウィザードの設定 96
Call Home ウィザードを設定するためのタスク フロー 96
Call Home ウィザードの起動 97
SMTP サーバーおよびポートの構成 98
セキュアな電子メール アラートの構成 99
マルチ SMTP サーバー サポートの構成 100
定期的なインベントリ通知のイネーブル化 101
DCNM-SAN を使用した定期的なインベントリ通知の有効化 101
重複メッセージ スロットリングの構成 102
DCNM-SAN を使用した重複メッセージ スロットリングの構成 103
Call Home ファブリック配信のイネーブル化 103
Call Home 構成変更のコミット 104
Call Home 構成変更の破棄 104
DCNM-SAN を使用した Call Home ファブリック配信の有効化 105
ファブリックのロックの上書き 105
Call Home 通信テスト 105
DCNM-SAN を使用した Call Home 通信テスト 106
遅延トラップの設定 107
遅延トラップ機能の有効化 107
DCNM-SAN を使用した遅延トラップ機能の有効化 108
Cisco Device Manager を使用した遅延トラップのイネーブル化 108
イベント フィルタ通知の表示 109
Call Home コンフィギュレーションの確認 109
Call Home 情報の表示 109
遅延トラップ情報の表示 113
アラート グループのカスタマイズの確認 113
イベント通知トラップの確認 113
Call Home トランスポートの確認 114
Call Home のモニタリング 114
フルテキスト形式の Syslog アラート通知の例 114
XML 形式での syslog アラート通知の例 115

XML 形式の RMON 通知の例 118
Call Home のフィールドの説明 119
Call Home 一般 119
Call Home 宛先 120
Call Home SMTP サーバ 120
Call Home 電子メール セットアップ 120
Call Home アラート 121
Call Home ユーザ定義コマンド 121
遅延トラップ 122
Call Home プロファイル 122
イベント宛先アドレス 122
イベント宛先セキュリティ（詳細） 123
イベント フィルタ一般 123
イベント フィルタ インターフェイス 124
イベント フィルタ制御 124
その他の参考資料 125
Call Home の機能履歴 125

第 6 章 メンテナンス ジョブのスケジューリング 127
コマンド スケジューラについて 127
スケジューラの用語 127
コマンド スケジューラのライセンス要件 128
注意事項と制約事項 128
デフォルト設定 129
コマンド スケジューラの設定 129
コマンド スケジューラを設定するためのタスク フロー 129
コマンド スケジューラのイネーブル化 129
例 130
リモート ユーザ認証の設定 130
ジョブの定義 131
ジョブの削除 133

スケジュールの指定 133
例 134
一時的スケジュールの指定 135
スケジュールの削除 136
割り当てられたジョブの削除 136
スケジュール時刻の削除 137
実行ログの設定 137
実行ログ ファイルの内容のクリア 138
スケジューラ設定の確認 138
コマンド スケジューラの構成の確認 138
コマンド スケジューラの実行ステータスの確認 139
ジョブ定義の確認 139
実行ログ ファイルの内容の表示 139
実行ログ ファイルの内容のクリア 140
スケジューラのコンフィギュレーション例 140

第 7 章 システム ステータス モニタリング 143
システム ステータス モニタリングの機能履歴 143
システム ステータス モニタリングについての情報 144
オンライン ヘルス管理システム 144
ループバック テストの設定頻度 145
ループバック テストのフレーム長の設定 145
ハードウェア障害時の処理 146
テストの実行要件 146
特定モジュールのテスト 146
前回のエラー レポートのクリア 147
現在のステータスの説明 147
オンボード障害ロギング 148
デフォルト設定 149
システム ヘルスの設定 149
システムの正常性を構成するためのタスク フロー 149

システムの正常性開始の構成 150
ループバック テストの構成頻度の構成 151
ループバック テスト構成のフレーム長の構成 151
ハードウェア障害アクションの構成 151
テストの実行要件 152
前回のエラー レポートのクリア 153
内部ループバック テストの実行 153
外部ループバック テストの実行 154
Serdes ループバックの実行 156
オンボード障害ロギングの構成 156
スイッチの OBFL の構成 157
モジュールの OBFL の構成 158
モジュール カウンタのクリア 159
すべてのモジュールのカウンタのリセット 159
アラート、通知、およびカウンタのモニタリングの構成 160
CPU 使用率のモニタリング 160
RAM 使用量情報の取得 160
Rx および Tx トラフィック カウンタのモニタリング 160
インターフェイスのステータスのモニタリング 160
トランシーバしきい値のモニタリング 161
スーパバイザ スイッチオーバー通知の構成 162
CRC および FCS エラーを含むカウンタの構成 162
アラートの Call Home の構成 163
ユーザ認証失敗のモニタリング 163
コアの構成 163
カーネル コア収集の構成 164
コアの手動コピー 164
コアの自動コピー 165
コアの削除 165
例：コアの構成 165
システム ステータスのモニタリング構成の確認 166

システム ヘルスの表示 166
ループバック テスト構成のフレーム長の確認 169
スイッチの OBFL の確認 169
モジュールの OBFL の確認 169
カーネル コア収集の確認 169
自動コア コピーの確認 170
OBFL ログの表示 170
モジュール カウンタ情報の表示 171
システム プロセスの表示 171
システム ステータスの表示 174
プロセス障害ログの表示 176
その他の参考資料 177

第 8 章 組み込みイベント マネージャについて 179
EEM の機能の履歴 179
EEM について 180
EEM の概要 180
ポリシー 180
イベント文 182
アクション文 183
VSH スクリプト ポリシー 184
環境変数 184
EEM イベント相関 185
高可用性 185
EEM のライセンス要件 185
EEM の前提条件 185
注意事項と制約事項 185
デフォルト設定 186
Embedded Event Manager の設定 186
CLI によるユーザ ポリシーの定義 186
イベント文の設定 187

アクション文の設定 192
VSH スクリプトによるポリシーの定義 197
VSH スクリプト ポリシーの登録およびアクティブ化 197
ポリシーの上書き 198
環境変数の定義 199
EEM の設定確認 199
EEM の設定例 200
その他の参考資料 201

第 9 章 RMON の設定 203
RMON について 203
RMON 設定情報 204
Threshold Manager を使用した RMON 設定 204
RMON アラーム設定情報 205
デフォルト設定 205
RMON の設定 206
SNMP での RMON トラップの構成 206
RMON アラームの構成 206
RMON イベントの構成 207
RMON 設定の確認 208
その他の参考資料 209
RMON の機能履歴 209

第 10 章 オンライン診断の設定 211
オンライン診断について 211
オンライン診断機能の概要 211
ブートアップ診断 212
ヘルス モニタリング診断 213
オンデマンド診断 215
指定されたヘルスモニタリング診断でのリカバリ アクション 216
スーパーバイザの修正（リカバリ）アクション 217

高可用性 217
オンライン診断機能のライセンス要件 218
デフォルト設定 218
オンライン診断の設定 218
起動診断レベルの設定 218
利用可能なテストの一覧の表示 219
ヘルスモニタリング診断テストのアクティブ化 220
ヘルスモニタリング診断テストの非アクティブ化 221
オンデマンド診断テストの開始または中止 221
オンデマンド モードでのオンデマンド診断テストの開始 223
診断結果の消去 224
診断結果のシミュレーション 225
修正（リカバリ）アクションの有効化 225
オンライン診断の確認 226
オンライン診断のコンフィギュレーション例 227
その他の参考資料 227

第 11 章 スイッチ間リンク診断の構成 229
ISL 診断に関する情報 229
サポートされるプラットフォーム 229
注意事項と制約事項 230
遅延テスト 230
シングル ホップ トラフィック テスト 231
マルチホップ エンドツーエンド トラフィック テスト 232
ISL 診断の構成 233
Cisco MDS 9700 シリーズ スイッチでの遅延テストの構成 233
他のサポートされているプラットフォームでの遅延テストの構成 235
Cisco MDS 9700 シリーズ スイッチでのシングル ホップ トラフィック テストの構成 236
他のサポートされているプラットフォームでのシングル ホップ トラフィック テストの構成 238
Cisco MDS 9700 シリーズ スイッチでのマルチホップ トラフィック テストの構成 240

サポートされている他のプラットフォームでのマルチホップ トラフィック テストの構成 242
ISL 診断のデバッグ 245
その他の参考資料 245

第 12 章 Pathtrace の使用 247

第 13 章 SNMP の設定 249
SNMP セキュリティについて 249
SNMP バージョン 1 およびバージョン 2c 250
SNMP バージョン 3 250
SNMPv3 CLI のユーザ管理および AAA の統合 251
CLI および SNMP ユーザの同期 251
SNMPv3 サーバーの AAA 排他動作 252
スイッチ アクセスの制限 253
グループベースの SNMP アクセス 253
ユーザの作成および変更 253
AES 暗号ベースの機密保全 254
トラップ、通知、およびインフォーム 254
EngineID 255
スイッチの LinkUp/LinkDown 通知 255
LinkUp および LinkDown トラップ設定の範囲 256
デフォルト設定 256
SNMP の設定 257
SNMP スイッチの連絡先および場所の情報の割り当て 257
CLI から SNMP ユーザの構成 257
パスワードの作成または変更 259
SNMPv3 メッセージ暗号化の適用 259
SNMPv3 メッセージ暗号化のグローバルでの適用 260
SNMPv3 ユーザに対する複数のロールの割り当て 260
コミュニティの追加 261

SNMP トラップとインフォーム通知の設定 262
SNMPv2c 通知の設定 262
IPv4 を使用した SNMPv2c 通知の構成 262
IPv6 を使用した SNMPv2c 通知の構成 263
DNS ネームを使用した SNMPv2c 通知の構成 264
SNMPv3 通知の設定 264
IPv4 を使用した SNMPv3 通知の構成 264
IPv6 を使用した SNMPv3 通知の構成 265
DNS ネームを使用した SNMPv3 通知の構成 266
場所に基づく SNMPv3 ユーザの認証 266
SNMP 通知のイネーブル化 267
通知ターゲット ユーザの設定 269
スイッチの LinkUp/LinkDown 通知の構成 270
インターフェイスの Up/Down SNMP リンクステート トラップの設定 271
エンティティ（FRU）トラップの構成 272
AAA 同期時間の変更 273
SNMP の設定の確認 274
インターフェイスの SNMP リンクステート トラップの Up/Down の表示 274
SNMP トラップの表示 275
SNMP セキュリティ情報の表示 276
その他の参考資料 279

第 14 章 ドメイン パラメータの構成 281
ファイバ チャネル ドメインの概要 281
ドメインの再起動 282
ドメイン マネージャのすべての最適化 283
ドメイン マネージャの高速再起動 283
ドメイン マネージャのスケール再起動 284
ドメイン マネージャの選択的再起動 284
スイッチの優先度 284
fcdomain の開始 285

着信 RCF 285
マージされたファブリックの自動再構成 285
ドメイン ID 285
static または preferred ドメイン ID の指定 288
許可ドメイン ID リスト 288
許可ドメイン ID リストの CFS 配信 288
連続ドメイン ID の割り当て 288
ファブリックのロック 289
変更のコミット 289
ファブリックのロックのクリア 289
FC ID 289
永続的 FC ID 290
固定的 FC ID 設定 290
HBA の固有エリア FC ID の概要 290
固定的 FC ID の選択消去 291
注意事項と制約事項 291
デフォルト設定 291
ファイバ チャネル ドメインの設定 292
ドメインの再起動 292
ドメイン マネージャのすべての最適化を有効にする 293
ドメイン マネージャの高速再起動の有効化 294
ドメイン マネージャのスケール再起動の有効化 294
ドメイン マネージャの選択的再起動の有効化 295
スイッチ優先順位の構成 295
ファブリック名の構成 296
着信 RCF の拒否 296
自動再構成の有効化 297
ドメイン ID の設定 297
static または preferred ドメイン ID の指定 298
許可ドメイン ID リストの構成 299
許可ドメイン ID 配信のイネーブル化 299

変更のコミット 300
変更の破棄 300
連続ドメイン ID 割り当ての有効化 301
FC ID の設定 301
永続的 FC ID 機能の有効化 301
永続的 FC ID の構成 302
HBA に対する一意のエリア FC ID の設定 303
永続的 FC ID の消去 305
ファブリックのロックのクリア 306
FC ドメイン設定の確認 306
CFS 配信ステータスの表示 307
保留中の変更の表示 307
セッション ステータスの表示 307
fcdomain 情報の表示 307

第 15 章 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 313
SPAN について 313
SPAN ソース 314
IPS 送信元ポート 315
使用可能な送信元インターフェイス タイプ 315
送信元としての VSAN 316
SPAN セッション 316
フィルタの指定 317
SD ポートの特性 317
SPAN 変換動作 318
ファイバ チャネル アナライザによるトラフィックのモニタリング 320
SPAN を使用しないモニタリング 320
SPAN を使用するモニタリング 321
単一 SD ポートによるトラフィックのモニタ 321
SD ポート設定 322
FC トンネルのマッピング 323

VSAN インターフェイスの作成 323
リモート SPAN 323
RSPAN の使用の利点 324
FC トンネルと RSPAN トンネル 325
ST ポート設定 325
ST ポートの特性 326
明示的なパスの作成 326
注意事項と制約事項 327
Cisco MDS 9700 シリーズ スイッチの注意事項 327
SPAN 設定時の注意事項 327
VSAN を送信元として設定する場合の注意事項 328
フィルタを指定する場合の注意事項 329
RSPAN 設定時の注意事項 329
SPAN および RSPAN のデフォルト設定 330
SPAN の設定 331
SPAN の SD ポートの設定 331
SPAN モニタリング用 SD ポートの構成 331
SPAN セッションの構成 332
SPAN フィルタの構成 333
第 2 世代ファブリック スイッチ用の SPAN の設定 334
入力 SPAN セッションの構成 334
出力 SPAN セッションの構成 335
例 335
SPAN シリーズの一時停止および再アクティベート 336
フレームのカプセル化 336
SPAN を使用したファイバ チャネル アナライザの設定 337
338
トラフィックのモニタの用シングル SD ポートの構成 338
送信元スイッチの設定 339
VSAN インターフェイスの作成 339
FC トンネルの有効化 340

FC トンネルの開始 340
ST ポートの構成 341
RSPAN セッションの構成 341
すべての中間スイッチの設定 342
VSAN インターフェイスの設定 342
IP ルーティングの有効化 343
宛先スイッチの設定 343
VSAN インターフェイスの設定 343
SD ポートの構成 343
FC トンネルのマッピング 344
明示的なパスの作成 344
明示的パスのリファレンス 346
RSPAN トラフィックのモニタリング 346
SPAN 構成の確認 347
SPAN 情報の表示 348
RSPAN 情報の表示 349
RSPAN の設定例 352
単一の送信元と 1 本の RSPAN トンネル 352
単一の送信元と複数の RSPAN トンネル 353
複数の送信元と複数の RSPAN トンネル 353

第 16 章

Fabric Configuration Server の設定 355
FCS についての情報 355
FCS の重要性 356
デフォルト設定 357
FCS の設定 357
FCS 名の指定 357
プラットフォーム属性の登録 358
FCS 設定の確認 359
FCS 要素の表示 360
その他の参考資料 363

第 17 章 ファブリック モジュール エラー モニタリング 365

ファブリック モジュール エラー モニタリングの機能履歴 365

ファブリック モジュール エラー モニタリングについて 365

ファブリック モジュール エラー モニタリングのガイドラインおよび制限事項 366

ファブリック モジュール エラー モニタリングの構成 367

設定例 368

第 18 章 Port Pacing の構成 369

Port Pacing についての情報 369

注意事項と制約事項 369

Port Pacer の構成 370

ポート ペーシングの有効化 370

Port Pacing 構成の表示 370

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、関連マニュアルの入手方法についても説明します。次のセクションを含んでいます：

- 対象読者 （xxiii ページ）
- 表記法 （xxiii ページ）
- マニュアルに関するフィードバック （xxv ページ）
- 関連資料 （xxv ページ）
- 通信、サービス、およびその他の情報 （xxv ページ）

対象読者

このマニュアルは、Cisco MDS 9000 シリーズ スイッチの設置、構成、および維持に携わるネットワーク管理者を対象としています。

表記法

コマンドの説明では、次の表記法を使用しています。

表記法	説明
bold	太字の文字は、表示どおりにユーザが入力するコマンドおよびキーワードです。
italic	イタリック体の文字は、ユーザが値を入力する引数です。
[x]	省略可能な要素（キーワードまたは引数）は、角かっこで囲んで示しています。
[x | y]	いずれか1つを選択できる省略可能なキーワードや引数は、角カッコで囲み、縦棒で区切って示しています。

表記法	説明
{x | y}	必ずいずれか1つを選択しなければならない必須キーワードや引数は、波かっこで囲み、縦棒で区切って示しています。
[x {y | z}]	角かっこまたは波かっこが入れ子になっている箇所は、任意または必須の要素内の任意または必須の選択肢であることを表します。角かっこ内の波かっこと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。
`variable`	ユーザが値を入力する変数であることを表します。イタリック体が使用できない場合に使用されます。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。

例では、次の表記法を使用しています。

表記法	説明
`screen フォント`	スイッチが表示する端末セッションおよび情報は、スクリーンフォントで示しています。
太字の screen フォント	ユーザが入力しなければならない情報は、太字のスクリーンフォントで示しています。
イタリック体の *screen* フォント	ユーザが値を指定する引数は、イタリック体の screen フォントで示しています。
<>	パスワードのように出力されない文字は、山カッコ（<>）で囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

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 安全上の重要事項

「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。

これらの注意事項を保管しておいてください。

マニュアルに関するフィードバック

このマニュアルに関する技術的なフィードバック、または誤りや記載もれなどお気づきの点がございましたら、mds-docfeedback@cisco.comよりご連絡ください。ご協力をよろしくお願いいたします。

関連資料

Cisco MDS 9000 シリーズ スイッチ全体のマニュアル セットは、次の URL にあります:

https://www.cisco.com/c/en/us/support/storage-networking/mds-9000-nx-os-san-os-software/series.html

ドキュメント ロードマップ

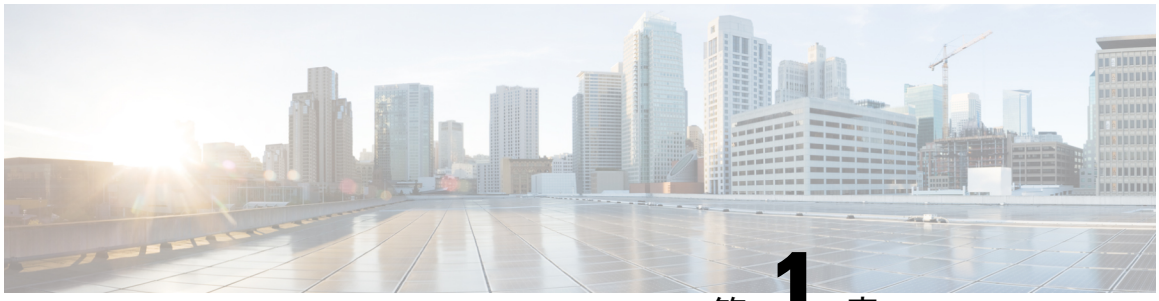
https://www.cisco.com/c/en/us/td/docs/storage/san_switches/mds9000/roadmaps/rel90.html

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。
- 重要な技術によって求めるビジネス成果を得るには、Cisco Services [英語] 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 [英語] 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 DevNet [英語] にアクセスしてください。
- 一般的なネットワーク、トレーニング、認定関連の出版物を入手するには、Cisco Press [英語] 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。

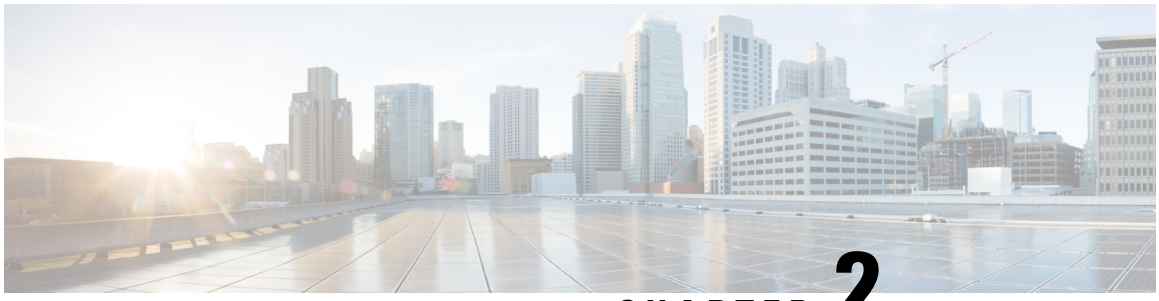
シスコのバグ検索ツール

Cisco バグ検索ツール（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。



第 1 章

新機能および変更された機能に関する情報



CHAPTER 2

システム管理の概要

システム管理機能を使用して、Cisco MDS NX-OS ソフトウェアを使用してスイッチをモニタおよび管理できます。そのような機能には、Call Home、SNMP、RMON、SPAN、および Embedded Event Manager（EEM）があります。

- Cisco Fabric Services, on page 3
- システムメッセージ, on page 3
- Call Home, on page 4
- スケジューラ, on page 4
- システム プロセスとログ, on page 4
- 組み込まれている Event Manager, on page 4
- SNMP, on page 5
- RMON, on page 5
- パス トレース （5 ページ）
- ドメイン パラメータ, on page 6
- SPAN, on page 6
- Fabric Configuration Server, on page 6

Cisco Fabric Services

Cisco MDS NX-OS ソフトウェアは、データベースを効率的に分散し、デバイスの柔軟性を高めるため、Cisco Fabric Services（CFS）インフラストラクチャを使用します。CFS により、ファブリック内のすべてのスイッチに設定情報を自動的に配信できるため、SAN のプロビジョニングが簡単になります。

CFS の構成については、CFS インフラストラクチャの使用, on page 7を参照してください。

システムメッセージ

システム メッセージは、Telnet、SSH、コンソール ポートのいずれかを通じてスイッチにアクセスするか、システム メッセージ ロギング サーバ上のログを参照することにより、リモートでモニタされます。ログ メッセージは、システム再起動後には消去されています。

システム メッセージ構成の詳細については、システムメッセージロギングの設定, on page 29を参照してください。

Call Home

Call Home は、重要なシステム イベントを電子メールで通知します。ポケットベル サービス、通常の電子メール、または XML ベースの自動解析アプリケーションとの適切な互換性のために、さまざまなメッセージのフォーマットが使用できます。この機能の一般的な用途としては、ネットワーク サポート技術者を直接ポケットベルで呼び出したり、ネットワーク オペレーション センター（NOC）に電子メールで通知したり、Technical Assistance Center で直接ケースを作成するために Cisco Smart Call Home サービスを使用することが挙げられます。

Call Home 構成の詳細については、Call Home の設定, on page 51を参照してください。

スケジューラ

Cisco MDS コマンド スケジューラ機能を使用すると、Cisco MDS 9000 ファミリのすべてのスイッチで、設定およびメンテナンス ジョブをスケジュールできます。この機能を使用して、一度だけ実行するジョブや定期的に実行するジョブをスケジュールできます。Cisco NX-OS コマンド スケジューラは、将来の指定した時刻に 1 つ以上のジョブ（CLI コマンドのセット）をスケジュールするための機構を提供します。ジョブは、将来の指定した時刻に一度だけ実行することも、定期的に実行することもできます。

Cisco MDS コマンド スケジューラ機能の構成については、メンテナンス ジョブのスケジューリング, on page 127 を参照してください。

システム プロセスとログ

スイッチの状態は、さまざまなシステムプロセスとログによってモニタできます。Online Health Management System（システム ヘルス）は、ハードウェア障害検出および復旧機能です。この Health Management System は、Cisco MDS 9000 ファミリの任意のスイッチング、サービス、スーパーバイザ モジュールの全般的な状態を確認します。

スイッチの正常性のモニタリングについては、システム ステータス モニタリング, on page 143を参照してください。

組み込まれている Event Manager

Embedded Event Manager（EEM）はデバイス上で発生するイベントをモニタし、構成に基づいて各イベントの回復またはトラブルシューティングのためのアクションを実行します。EEM は次の 3 種類の主要コンポーネントからなります。

- イベント文：別の Cisco NX-OS コンポーネントからモニタし、アクション、回避策、または通知が必要になる可能性のあるイベント。
- アクションステートメント：電子メールの送信やインターフェイスの無効化などの、イベントから回復するために EEM が実行できるアクション。
- ポリシー：イベントのトラブルシューティングまたはイベントからの回復を目的とした 1 つまたは複数のアクションとペアになったイベント。

EEM の構成については、組み込みイベント マネージャについて, on page 179を参照してください。

SNMP

簡易ネットワーク管理プロトコル（SNMP）は、ネットワーク デバイス間で管理情報をやり取りするためのアプリケーション層プロトコルです。すべての Cisco MDS 9000 ファミリ スイッチで、SNMPv1、SNMPv2c、および SNMPv3 の 3 つの SNMP バージョンが使用できます。CLI と SNMP は、Cisco MDS 9000 ファミリのすべてのスイッチで共通のロールを使用します。SNMP を使用して CLI で作成したロールを変更したり、その逆を行うことができます。

CLI ユーザーと SNMP ユーザーのユーザー、パスワード、ロールは、すべて同じです。CLI を通じて設定されたユーザは SNMP（たとえば、DCNM-SAN や Device Manager）を使用してスイッチにアクセスでき、その逆も可能です。

SNMP の構成については、SNMP の設定, on page 249 を参照してください。

RMON

RMON は、各種のネットワーク エージェントおよびコンソール システムがネットワーク モニタリング データを交換できるようにするための、Internet Engineering Task Force（IETF）標準モニタリング仕様です。RMON のアラームとイベントを使用し、Cisco SAN-OS Release 2.0(1b) 以降または Cisco Release NX-OS 4.1(3) 以降のソフトウェアが動作する Cisco MDS 9000 ファミリ スイッチをモニタできます。

RMON の構成については、RMON の設定, on page 203 を参照してください。

パス トレース

Pathtrace 機能は Traceroute 機能に基づいて構築されており、ファブリック内の 2 つのデバイス間のパスの各ホップで、入力および出力インターフェイス名、送受信されたフレームとエラーの数などのインターフェイスに関する情報を提供します。Pathtrace は、個々のスイッチに接続してファブリック ショートパス ファースト（FSPF）トポロジをホップごとにチェックしなくても、最短パスのエンドツーエンド ビューを提供します。

Pathtrace 機能の使用については、Pathtrace の使用 （247 ページ） を参照してください。

ドメイン パラメータ

ファイバ チャネル ドメイン（fcdomain）機能では、FC-SW-2 標準で記述されているように、主要スイッチ選択、ドメイン ID 配信、FC ID 割り当て、ファブリック再設定機能が実行されます。ドメインは VSAN 単位で設定されます。ドメイン ID を設定しない場合、ローカル スイッチはランダムな ID を使用します。

ファイバチャネル ドメイン機能の構成については、ドメイン パラメータの構成, on page 281 を参照してください。

SPAN

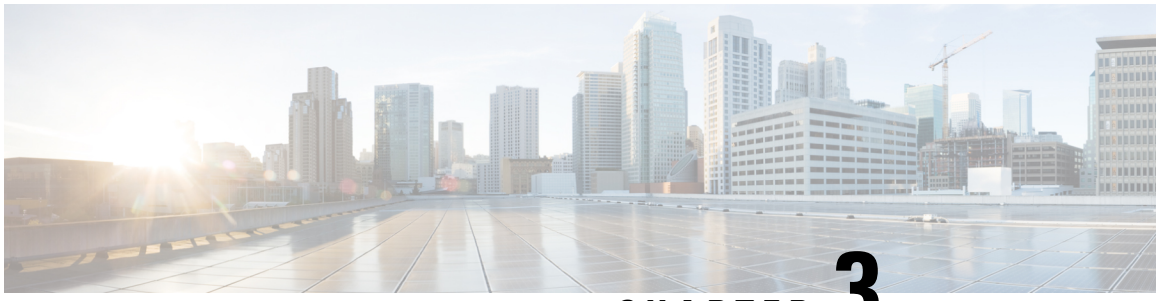
スイッチド ポート アナライザ（SPAN）機能は、Cisco MDS 9000 ファミリのスイッチ専用の機能です。SPAN は、ファイバ チャネル インターフェイスを通じてネットワーク トラフィックをモニタします。任意のファイバ チャネル インターフェイスを通るトラフィックは、SPAN 宛先ポート（SD ポート）という専用ポートに複製することができます。スイッチの任意のファイバ チャネル ポートを SD ポートとして設定できます。SD ポート モードに設定したインターフェイスは、標準データ トラフィックには使用できません。ファイバ チャネル アナライザを SD ポートに接続して、SPAN トラフィックをモニタできます。

SPAN 機能の詳細については、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, on page 313 を参照してください。

Fabric Configuration Server

Fabric Configuration Server（FCS）を使用すると、トポロジ属性を検出したり、ファブリック要素の設定情報リポジトリを維持したりすることができます。通常、管理アプリケーションは N ポートを通してスイッチの FCS に接続されます。Cisco MDS 9000 ファミリ スイッチ環境では、複数の VSAN がファブリックを構成し、VSAN ごとに 1 つの FCS インスタンスが存在します。

FCS の構成については、Fabric Configuration Server の設定, on page 355 を参照してください。



CHAPTER 3

CFS インフラストラクチャの使用

Cisco Fabric Service（CFS）は、ファブリック内で自動的に設定を同期化するための、共通のインフラストラクチャを提供します。CFS は、転送機能と、さまざまな共通サービスをアプリケーションに提供します。CFS はファブリック内の CFS 対応スイッチを検出したり、すべての CFS 対応スイッチのアプリケーション機能を検出したりできます。

- CFS について, on page 7
- 注意事項と制約事項, on page 16
- デフォルト設定, on page 16
- CFS の設定, on page 17
- CFS リージョンの設定, on page 22
- CFS 設定の確認, on page 24
- その他の参考資料, on page 28

CFS について

Cisco MDS 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、効率的なデータベース配信を実現し、デバイスの柔軟性を高めます。ファブリック内のすべてのスイッチに設定情報を自動的に配信できるため、SAN プロビジョニングが簡単になります。

複数の Cisco MDS NX-OS アプリケーションが、CFS インフラストラクチャを使用して、特定のアプリケーションのデータベースの内容を維持および配信します。

Cisco MDS スイッチの機能の多くでは、ファブリック内のすべてのスイッチで設定が同期している必要があります。ファブリック全体で設定を維持することは、ファブリックの一貫性を維持するうえで重要です。共通のインフラストラクチャがない場合、そのような同期を行うには、ファブリック内の各スイッチで手動で設定することになります。これは、退屈で誤りが起きやすい作業です。

CFS を使用した Cisco MDS NX-OS 機能

次の Cisco NX-OS の機能は、CFS インフラストラクチャを使用します。

- N ポート仮想化
- FlexAttach 仮想 pWWN
- NTP
- ダイナミック ポート VLAN メンバーシップ
- 分散デバイス エイリアス サービス
- IVR トポロジ
- SAN デバイス バーチャライゼーション
- TACACS+ および RADIUS
- ユーザおよび管理者ロール
- ポート セキュリティ
- iSNS
- Call Home
- Syslog
- fctimer
- SCSI フロー サービス
- Fabric Startup Configuration Manager（FSCM）を使用した、保存されたスタートアップ コンフィギュレーション
- 許可ドメイン ID リスト
- RSCN タイマー
- iSLB

CFS の機能

CFS には次の機能があります。

- CFS レイヤでクライアント/サーバー関係を持たないピアツーピア プロトコル。
- 3 つの配信スコープ
  - 論理スコープ：配信は、VSAN のスコープ内で発生します。
  - 物理スコープ：配信は、物理トポロジ全体におよびます。
  - 選択した VSAN セットを超える場合：Inter-VSAN Routing（IVR）などの一部のアプリケーションは、一部の特定の VSAN を超えた設定の配信を必要とします。これらのアプリケーションは、配信を制限する VSAN セットを CFS に指定できます。
- 3 つの配信モード。
  - 協調型配信：ファブリック内で同時に 1 つの配信だけが許可されます。
  - 非協調型配信：協調型配信が進行中である場合を除いて、ファブリック内で複数の同時配信を実行できます。
  - 無制限の非協調型配信：既存の協調型配信がある場合でも、ファブリック内で複数の同時配信が許可されます。無制限の非協調型配信は、他のすべての配信タイプの配信と同時に実行できます。
- ファブリック マージ イベント中（2 つの独立したファブリックのマージ中）に、アプリケーション設定のマージを実行するマージ プロトコルをサポートします。

アプリケーションの CFS のイネーブル化

すべての CFS ベースのアプリケーションでは、配信機能をイネーブルまたはディセーブルにできます。Cisco SAN-OS Release 2.0(1b) よりも前に存在していた機能では、配信機能がデフォルトでディセーブルになっており、配信機能を明示的にイネーブルにする必要がありました。

Cisco SAN-OS Release 2.0(1b) 以降、または MDS NX-OS Release 4.1(1) 以降で採用されているアプリケーションでは、配信機能がデフォルトでイネーブルになっています。

アプリケーションで配信が明示的にイネーブルにされていない場合は、CFS はそのアプリケーションの設定を配信しません。

CFS プロトコル

CFS 機能は、下位層の転送には依存しません。現在、Cisco MDS スイッチでは、CFS プロトコル レイヤはファイバ チャネル 2（FC2）レイヤの上に存在し、クライアントとサーバの関係がないピアツーピアのプロトコルになっています。CFS は FC2 転送サービスを使用して、他のスイッチに情報を送信します。CFS はすべての CFS パケットに対して独自の SW_ILS（0x77434653）プロトコルを使用します。CFS パケットはスイッチ ドメイン コントローラ アドレスで送受信されます。

CFS は、IP を使用して他のスイッチに情報を送信することもできます。

CFS を使用するアプリケーションは、下位層の転送をまったく認識しません。

CFS 配信のスコープ

Cisco MDS 9000 ファミリ スイッチ上のさまざまなアプリケーションが、さまざまなレベルで設定を配信する必要があります。

- VSAN レベル（論理スコープ）

  VSAN の範囲内で動作するアプリケーションは、設定の配信が VSAN に限定されます。アプリケーション例は、VSAN 内だけでコンフィギュレーション データベースを適用できる場合のポート セキュリティです。

- 物理トポロジ レベル（物理スコープ）

  アプリケーションは、複数の VSAN にまたがる物理トポロジ全体に設定を配信しなければならない場合があります。そのようなアプリケーションとしては、NTP や DPVM（WWN ベースの VSAN）が挙げられます。これらは VSAN とは無関係です。

- 選択されたスイッチ間

  アプリケーションは、ファブリック内の選択したスイッチ間だけで動作する可能性があります。アプリケーションの例としては、2 台のスイッチ間で動作する SCSI フロー サービスが挙げられます。

CFS の配信モード

CFS は、さまざまなアプリケーション要件をサポートするため、協調型配信と非協調型配信の、2 種類の配信モードをサポートしています。2 つのモードは相互に排他的です。常に 1 つのモードだけを適用できます。

非協調型配信

非協調型配信は、ピアからの情報と競合させたくない情報を配信する場合に使用されます。例としては、iSNS などのローカル デバイス登録が挙げられます。1 つのアプリケーションで、複数の非協調型配信が可能です。

協調型配信

協調型配信では、同時に 1 つのアプリケーション配信だけを実行できます。CFS はロックを使用してこの機能を実行します。ファブリック内のいずれかの場所にあるアプリケーションによってロックが取得されている場合、協調型配信を開始できません。協調型配信は、次の 3 段階で構成されています。

1. ファブリック ロックが取得されます。
2. 設定が配信され、コミットされます。
3. ファブリック ロックが解放されます。

協調型配信には、次の 2 種類があります。

- CFS によるもの：アプリケーションが介在することなく、アプリケーション要求に応じて CFS が各段階を実行します。
- アプリケーションによるもの：各段階がアプリケーションによって完全に管理されます。

協調型配信は、複数のスイッチから操作および配信が可能な情報を配信するのに使用されます。たとえば、ポート セキュリティの設定です。

無制限の非協調型配信

無制限の非協調型配信では、既存の協調型配信がある場合でも、ファブリック内で複数の同時配信が許可されます。無制限の非協調型配信は、他のすべての配信タイプの配信と同時に実行できます。

混合ファブリック内での CFS の接続性

CFS は、Cisco Nexus 5000 シリーズ スイッチ上や Cisco MDS 9000 スイッチ上でも動作するインフラストラクチャ コンポーネントです。混合ファブリック内のさまざまなプラットフォーム（Cisco Nexus 7000 シリーズ、Cisco Nexus 5000 シリーズ、Cisco MDS 9000 スイッチなど）は、相互に情報をやりとりすることができます。

CFSoIP と CFSoFC を使用して、各 CFS クライアントは他のプラットフォーム上で動作しているそれぞれのインスタンスと通信することもできます。定義されたドメインと配信スコープの

範囲内で、CFS はクライアントのデータと構成を他のプラットフォーム上で動作しているピアに配信できます。

3 種類すべてのプラットフォームで CFSoIP と CFSoFC の両方がサポートされています。ただし、Cisco Nexus 7000 シリーズと Cisco Nexus 5000 シリーズのスイッチでは、CFSoFC が動作するために、FC または FCoE プラグインおよび対応する設定が必要になります。Cisco MDS 9000 スイッチでは、両方のオプションがデフォルトで使用可能になっています。

Note 一部のアプリケーションは、異なるプラットフォーム上で動作しているそれらのインスタンスと互換性がありません。そのため、設定をコミットする前に、CFS 配信に関するクライアントの注意事項を注意深く読むことを推奨します。

Cisco Nexus 5000 シリーズと Cisco MDS 9000 スイッチに対する CFS の詳細については、『Cisco Nexus 5000 Series NX-OS System Management Configuration Guide』と『Cisco MDS 9000 Family NX-OS System Management Configuration Guide』をそれぞれ参照してください。

ファブリックのロック

CFS インフラストラクチャを使用する Cisco NX-OS 機能（またはアプリケーション）を初めて設定する場合、この機能は CFS セッションを開始して、ファブリックをロックします。ファブリックがロックされると、Cisco NX-OS ソフトウェアは、ロックを保持しているスイッチ以外のスイッチからこの Cisco NX-OS 機能への設定変更を許可せず、ロックされたステータスをユーザに通知するためのメッセージを発行します。設定変更は、該当アプリケーションによって保留データベースに保持されます。

ファブリックのロックが必要な CFS セッションを開始した後に、セッションが終了されなかった場合、管理者はセッションをクリアできます。ファブリックをロックしたユーザの名前は、再起動およびスイッチオーバーを行っても保持されます。（同じマシン上で）別のユーザーが設定タスクを実行しようとしても、拒否されます。

CFS ロック ステータスの確認については、CFS ロック ステータスの確認, on page 26 を参照してください。

変更のコミット

コミット操作により、すべてのアプリケーション ピアの保留データベースを保存し、すべてのスイッチのロックを解除します。

一般に、コミット機能はセッションを開始しません。セッションを開始するのは、ロック機能だけです。ただし、設定変更がこれまでに行われていなければ、空のコミットが可能です。この場合、コミット操作の結果として、ロックを取得し、現在のデータベースを配信するセッションが行われます。

CFS インフラストラクチャを使用して機能への設定変更をコミットすると、次のいずれかの応答に関する通知が届きます。

- 1 つ以上の外部スイッチが成功ステータスを報告：アプリケーションは変更をローカルに適用し、ファブリック ロックを解除します。
- どの外部スイッチも成功ステートを報告しない：アプリケーションはこのステートを失敗として認識し、ファブリック内のすべてのスイッチに変更を適用しません。ファブリック ロックは解除されません。

Note **feature commit** の完了後、機能の配信に参加しているすべてのスイッチで実行構成が変更されます。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。

CFS マージのサポート

アプリケーションは CFS を通して、設定をファブリック内で継続的に同期します。このような 2 つのファブリック間で ISL を起動すると、これらのファブリックがマージされることがあります。これらの 2 つのファブリック内の設定情報セットが異なっている時は、マージイベント中に調停する必要があります。CFS は、アプリケーション ピアがオンラインになるたびに通知を送信します。M 個のアプリケーション ピアがあるファブリックが N 個アプリケーション ピアがある別のファブリックとマージし、アプリケーションが通知のたびにマージ動作を行う場合は、リンク アップ イベントによりファブリック内で M*N 回のマージがトリガーされます。

CFS は、CFS レイヤでマージの複雑性に対処することで必要とされるマージ数を 1 つに減らすプロトコルをサポートしています。このプロトコルは、スコープ単位でアプリケーションごとに稼働します。プロトコルには、ファブリックのマージマネージャとしてそのファブリック内から 1 つのスイッチを選択する作業が伴います。その他のスイッチは、マージプロセスで何も役割を果たしません。

マージ時、2 つのファブリック内のマージマネージャは相互にコンフィギュレーション データベースを交換します。一方のアプリケーションが情報をマージし、マージが正常に行われたかどうかを判断し、結合されたファブリック内のすべてのスイッチにマージ ステータスを通知します。

マージに成功した場合、マージしたデータベースは結合ファブリック内のすべてのスイッチに配信され、新規ファブリック全体が一貫したステートになります。

IP を介した CFS 配信

ファイバ チャネルを介して到達できないスイッチを含むネットワークに対し、IP を介して情報を配信するように CFS を設定できます。IP を介した CFS 配信は次の機能をサポートしています。

- IP ネットワーク全体での物理的配信
- ファイバ チャネルまたは IP を介して到達可能なすべてのスイッチに配信が到達する、ハイブリッド ファイバ チャネルおよび IP ネットワークでの物理的配信。

Note スイッチはまずファイバ チャネルを介して情報を配信し、ファイバ チャネルでの最初の試みが失敗すると IP ネットワークを介して配信します。IP およびファイバ チャネルの両方を介した配信がイネーブルの場合、CFS は重複メッセージを送信しません。

- IP バージョン 4（IPv4）または IP バージョン 6（IPv6）を介した配信。

Note CFS は同じスイッチから IPv4 と IPv6 の両方を介しては配信できません。

- 設定可能なマルチキャスト アドレスを使用してネットワーク トポロジの変更を検出するキープアライブ メカニズム
- Cisco MDS SAN-OS Release 2.x との互換性
- 論理スコープ アプリケーションに対する配信は、VSAN の実装がファイバ チャネルに制限されているため、サポートされません。

Figure 1: ファイバ チャネル接続と IP 接続を持つネットワーク例 1, on page 13 に、ファイバ チャネル接続と IP 接続の両方を持つネットワークを示します。ノード A はファイバ チャネルを介してノード B にイベントを転送します。ノード B はユニキャスト IP を使用してノード C とノード D にイベントを転送します。ノード C はファイバ チャネルを介してノード E にイベントを転送します。

Figure 1: ファイバ チャネル接続と *IP* 接続を持つネットワーク例 *1*

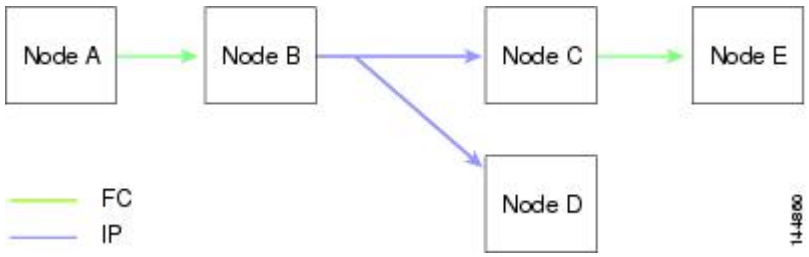


Figure 2: ファイバ チャネル接続と IP 接続を持つネットワーク例 2, on page 14 は、ノード D とノード E がファイバ チャネルを使用して接続されていることを除き、Figure 1: ファイバ チャネル接続と IP 接続を持つネットワーク例 1, on page 13 と同じです。ノード B にはノード C とノード D の IP 用配信リストがあるので、この例のすべてのプロセスは同じです。ノード D はすでにノード B からの配信リストに入っているため、ノード C はノード D に転送しません。

Figure 2: ファイバ チャネル接続と *IP* 接続を持つネットワーク例 *2*

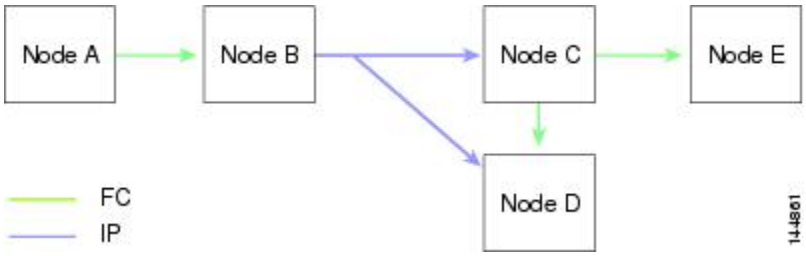
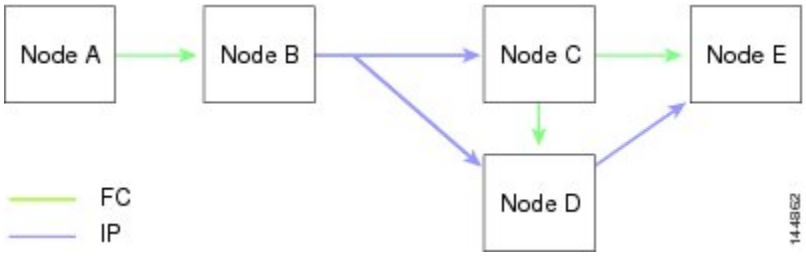


Figure 3: ファイバ チャネル接続と IP 接続を持つネットワーク例 3, on page 14 は、ノード D とノード E が IP を使用して接続されていることを除き、Figure 2: ファイバ チャネル接続と IP 接続を持つネットワーク例 2, on page 14 と同じです。ノード E はノード B からの配信リストに入っていないため、ノード C とノード D はイベントをノード E に転送します。

Figure 3: ファイバ チャネル接続と *IP* 接続を持つネットワーク例 *3*



CFS の静的 IP ピア

IP を介した CFS は、静的 IP ピアでも使用できます。この場合、IP マルチキャストを介したダイナミック検出は無効になり、CFS 配信は静的に構成されたピアでのみ実行されます。

CFS は、設定された IP アドレスのリストを使用して各ピアと通信し、ピア スイッチの WWN を学習します。ピア スイッチの WWN を学習した後、CFS はスイッチを CFS 対応とマークし、アプリケーションレベルのマージとデータベース配信をトリガーします。

一部のデバイスでは、マルチキャスト フォワーディングはデフォルトでディセーブルになっています。たとえば、IBM Blade シャーシでは、特に外部イーサネット ポートでマルチキャスト フォワーディングがディセーブルになっており、イネーブルにする方法はありません。N ポート バーチャライゼーション デバイスは、IP だけを転送メディアとして使用し、ISL 接続またはファイバ チャネル ドメインを持っていません。このようなデバイスは、CFS に静的 IP ピアを使用するとメリットがある場合があります。

次の MDS 9000 の機能では、IP を介した CFS 配信のために、スタティック IP ピア設定が必要です。

- N ポート バーチャライゼーション デバイスは、通信チャネルとして IP を持っています。これは、NPV スイッチに FC ドメインがないためです。NPV デバイスは、IP を介した CFS を転送メディアとして使用します。
- NPV 対応のスイッチだけをリンクする、CFS リージョン 201 上の FlexAttach 仮想 pWWN 配信。

CFS リージョンの概要

CFS リージョンは、物理配信スコープにおける所定の機能またはアプリケーションに対するスイッチのユーザ定義のサブセットです。SANが広い範囲におよぶ場合、物理プロキシミティに基づいてスイッチセット間で特定のプロファイルの配信をローカライズまたは制限しなければならない場合があります。MDS SAN-OS Release 3.2.(1) よりも前のバージョンでは、SAN 内のアプリケーションの配信スコープは、物理ファブリック全体におよんでおり、ファブリック内の特定のスイッチのセットに配信を制限する機能はありませんでした。CFS リージョンの機能では、CFS リージョンを作成することでこの制限を克服できます。CFS リージョンは、CFS機能またはアプリケーションに対する、ファブリック内の複数の配信アイランドです。CFS リージョンは、機能の構成の配信をファブリックにおけるスイッチの特定のセットまたはグループに制限するように設計されています。

Note CFS リージョンは、SAN 内の物理スイッチに対してだけ設定できます。CFS リージョンの設定は、VSAN では行えません。

Example CFS Scenario：Call Home は、ある状況が発生した場合や、何らかの異常が発生した場合にネットワーク管理者に対してアラートをトリガーするアプリケーションです。ファブリックが広い範囲におよび、ファブリック内のスイッチのサブセットを担当するネットワーク管理者が複数存在する場合、Call Home アプリケーションは、管理者のいる場所にかかわらずすべてのネットワーク管理者にアラートを送信します。Call Home アプリケーションは、メッセージ アラートを選択してネットワーク管理者に送信するために、CFS リージョンを実装してアプリケーションの物理スコープを調整するか絞り込む必要があります。

CFS リージョンは、0 ～ 200 の数字で識別されます。リージョン 0 はデフォルトのリージョンとして予約されており、ファブリック内のすべてのスイッチを含みます。1 ～ 200 のリージョンを設定できます。デフォルト リージョンでは下位互換性を維持しています。リリース 3.2(1) よりも前の SAN-OS が動作するスイッチが同じファブリック上にある場合、これらのスイッチを同期化する際に、リージョン 0 の機能だけがサポートされます。これらのスイッチを同期化する際、他のリージョンの機能は無視されます。

機能が移動される、つまり、機能が新しいリージョンに割り当てられると、機能のスコープはそのリージョンに制限されます。他のすべてのリージョンは、配信やマージの対象から外されます。機能へのリージョンの割り当ては、配信において初期の物理スコープよりも優先されます。

複数の機能の設定を配信するように CFS リージョンを設定できます。ただし、特定のスイッチでは、一度に特定の機能設定を配信するように設定できる CFS リージョンは 1 つだけです。機能を CFS リージョンに割り当てた場合、この設定を別の CFS リージョン内に配信できません。

注意事項と制約事項

ファブリック内のすべてのスイッチは CFS に対応している必要があります。Cisco MDS 9000 ファミリ スイッチは、Cisco SAN-OS Release 2.0(1b) 以降、または MDS NX-OS Release 4.1(1) 以降を実行している場合、CFS に対応しています。CFS に対応していないスイッチは配信を受信できず、ファブリックの一部が目的の配信を受信できなくなります。

CFS には、次の注意事項と制限事項があります。

- 暗黙的な CFS の使用：CFS 対応アプリケーションに CFS タスクを初めて発行した場合は、設定変更プロセスが開始し、アプリケーションによってファブリックがロックされます。
- 保留データベース：保留データベースはコミットされていない情報を保持する一時的なバッファです。データベースがファブリック内の他のスイッチのデータベースと同期するように、コミットされていない変更はすぐに適用されません。変更をコミットすると、保留データベースはコンフィギュレーション データベース（別名、アクティブ データベースまたは有効データベース）を上書きします。
- アプリケーション単位でイネーブル化またはディセーブル化される CFS 配信：CFS 配信ステートのデフォルト（イネーブルまたはディセーブル）は、アプリケーション間で異なります。CFS 配信がディセーブル化されたアプリケーションは、設定を配信せず、ファブリック内の他のスイッチからの配信も受信しません。
- 明示的な CFS コミット：大半のアプリケーションでは、新しいデータベースをファブリックに配信したりファブリック ロックを解放したりするために一時的なバッファ内の変更をアプリケーション データベースにコピーする明示的なコミット動作が必要です。コミット操作を実行しないと、一時的バッファ内の変更は適用されません。

デフォルト設定

Table 1: デフォルトの CFS パラメータ , on page 16 に、CFS 設定のデフォルト設定値を示します。

Table 1: デフォルトの ***CFS*** パラメータ

パラメータ	デフォルト
スイッチでの CFS 配信	イネーブル
データベース変更	最初の設定変更によって暗黙的にイネーブルにされる
アプリケーションの配信	アプリケーションごとに異なる
コミット	明示的な設定が必要
IP を介した CFS	ディセーブル
CFS の静的 IP ピア	ディセーブル

パラメータ	デフォルト
IPv4 マルチキャスト アドレス	239.255.70.83
IPv6 マルチキャスト アドレス	ff15:efff:4653

CFS の設定

ここでは、構成プロセスについて説明します。

スイッチの CFS 配信のディセーブル化

デフォルトでは、CFS 配信はイネーブルに設定されています。アプリケーションは、ファブリック内のアプリケーションが存在するすべての CFS 対応スイッチにデータと設定情報を配信できます。この設定が操作の通常モードです。

物理接続を維持したまま、スイッチで IP を介した CFS を含む CFS をグローバルに無効化し、CFS を使用するアプリケーションをファブリック全体への配信から隔離することができます。

Note スイッチで CFS がグローバルにディセーブルになっている場合、CFS 動作はスイッチに制限され、すべての CFS コマンドはスイッチが物理的に隔離されているかのように機能し続けます。

スイッチ上で CFS 配信をグローバルにディセーブルまたはイネーブルにするには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

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

IP を介した CFS を含む、スイッチ上のすべてのアプリケーションの CFS 配信をグローバルに無効化します。

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

スイッチの CFS 配信をイネーブルにします（デフォルト）。

変更のコミット

commit コマンドを入力すると、指定した機能の変更をコミットできます。

変更の破棄

設定変更を廃棄する場合、アプリケーションは保留データベースを消去し、ファブリック内のロックを解除します。中断とコミット機能の両方を使用できるのは、ファブリックロックが取得されたスイッチだけです。

指定した機能に対して **abort** コマンドを使用すると、その機能の変更を廃棄できます。

設定の保存

まだ適用されていない変更内容（保留データベースにまだ存在する）は実行コンフィギュレーションには表示されません。変更をコミットすると、保留データベース内の設定変更が有効データベース内の設定を上書きします。

Caution 変更内容は、コミットしなければ、実行コンフィギュレーションに保存されません。

CISCO-CFS-MIB には CFS 関連機能の SNMP 設定情報が含まれます。この MIB の詳細については、『*Cisco MDS 9000 Family MIB Quick Reference*』を参照してください。

ロック済みセッションのクリア

アプリケーションによって保持されているロックは、ファブリック内の任意のスイッチからクリアできます。この方法は、ロックが取得されクリアされない状況から復帰するために提供されています。

CFS ロックをクリアするには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **dpvm abort**

以前に構成ロックを取得したスイッチから構成を終了します。この方法は、ファブリック全体の CFS ロックをクリアします。

ファブリック全体の DPVM アプリケーションの CFS ロックをクリアします。

ステップ 3 switch(config)# **clear dpvm session**

ファブリック内の任意のスイッチからセッションをクリアします。

DPVM アプリケーションの CFS ロックをクリアします。

IP を介した CFS のイネーブル化

IPv4 を介した CFS の有効化または無効化

IPv4 を介した CFS を有効または無効にするには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **cfs ipv4 distribute**

スイッチのすべてのアプリケーションに対して IPv4 を介した CFS をグローバルでイネーブルにします。

ステップ 3 switch(config)# **no cfs ipv4 distribute**

```
This will prevent CFS from distributing over IPv4 network.
Are you sure? (y/n) [n] y
```

スイッチの IPv4 を介した CFS をディセーブルにします（デフォルト）。

IP を介した CFS の IP マルチキャスト アドレスの設定

同様のマルチキャスト アドレスを持つすべての CFS over IP 対応スイッチにより、1 つの CFS over IP ファブリックが構成されます。ネットワーク トポロジ変更を検出するためのキープアライブ メカニズムのような CFS プロトコル特有の配信は、IP マルチキャストアドレスを使用して情報を送受信します。

Note アプリケーション データの CFS 配信はダイレクト ユニキャストを使用します。

IP を介した CFS の IPv4 または IPv6 どちらかのマルチキャスト アドレス値を設定できます。デフォルトの IPv4 マルチキャストアドレスは 239.255.70.83 で、デフォルトの IPv6 マルチキャストアドレスは ff15:efff:4653 です。

IPv4 を介した CFS のIP マルチキャストアドレスの構成

IPv4 を介した CFS の IP マルチキャスト アドレスを構成するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **cfs ipv4 mcast-address 239.255.1.1**

```
Distribution over this IP type will be affected
Change multicast address for CFS-IP ?
```

IPv4 を介した CFS 配信の IPv4 マルチキャスト アドレスを設定します。有効な IPv4 アドレスの範囲は 239.255.0.0 ～ 239.255.255.255 および 239.192/16 ～ 239.251/16 です。

ステップ 3 switch(config)# **no cfs ipv4 mcast-address 239.255.1.1**

Example:

```
Distribution over this IP type will be affected
Change multicast address for CFS-IP ?Are you sure? (y/n)  [n] y
```

IPv4 を介した CFS 配信の デフォルトの IPv4 マルチキャスト アドレスに戻します。CFS のデフォルトの IPv4 マルチキャスト アドレスは 239.255.70.83 です。

CFS の静的 IP ピアの構成

IP を介した CFS 向けの静的 IP ピア アドレスを構成するには、次の手順に従ってください。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **cfs static-peers**

```
WARNING: This mode will stop dynamic discovery and rely only on the static peers. For
this mode to be in effect, at least one static peer will need to be configured.
Do you wish to continue? (y/n)  [n] y
```

switch(config-cfs-static)#

CFS 静的ピアの構成モードを開始し、マルチキャスト転送を使用したピアのダイナミック検出を無効化します。これを有効にするには、ステップ 3 で少なくとも 1 つの静的ピアを構成する必要があります。

ステップ 3 switch(config)# **no cfs static-peers**

```
WARNING: This will remove all existing peers and start dynamic discovery.
Do you wish to continue? (y/n)  [n] y
```

すべてのスイッチで、CFS の静的ピア検出を無効にし、マルチキャスト転送を使用したダイナミック ピア検出を有効にします。

ステップ 4 switch(config-cfs-static)# **ip address 1.2.3.4**

switch(config-cfs-static)#**ip address 1.2.3.5**

switch(config-cfs-static)# **end**

switch#

IP アドレスを静的ピア リストに追加し、スイッチを CFS 対応としてマークします。静的 IP ピア リストを表示するには、**show cfs static peers** コマンドを使用します。

ステップ 5 switch(config-cfs-static)# **no ip address 1.2.3.3**

switch(config-cfs-static)# **end**

静的ピア リストから IP アドレスを削除し、マルチキャスト転送を使用してスイッチをダイナミック ピア検出に移動します。

ステップ 6 switch# **show cfs static peers**

IP アドレス、WWN、および CFS 静的ピア要求のステータスを表示します。

- ディスカバリが進行中
- ローカル
- 到達可能
- 到達不能
- ローカル IP が存在しません
- 再検出と配布が無効になっています

Note
ローカル スイッチで IP アドレスと WWN を構成する必要があります。CFS がローカル スイッチ情報を受信しない場合、CFS はピア スイッチの検出を開始できません。

CFS リージョンの設定

CFS リージョンの作成

CFS リージョンを作成する手順は、次のとおりです。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **cfs region 4**

たとえば、ナンバー 4 のリージョンを作成します。

CFS リージョンへのアプリケーションの割り当て

スイッチでリージョンにアプリケーションを割り当てる手順は、次のとおりです。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **cfs region 4**

たとえば、ナンバー 4 のリージョンを作成します。

ステップ 3 switch(config-cfs-region)# **ntp**

switch(config-cfs-region)# **callhome**

アプリケーションを追加します。

別の CFS リージョンへのアプリケーションの移動

アプリケーションを別の CFS リージョンに移動できます。たとえば、NTP および Call Home アプリケーションを持つリージョン 1（元のリージョン）からリージョン 2（ターゲット リージョン）に移動できます。

アプリケーションを移動するには、次の手順を行います。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **cfs region 2**

リージョン 2 に入ります。

ステップ 3 switch(config-cfs-region)# **ntp**

switch(config-cfs-region)# **callhome**

元々リージョン 1 に属していたアプリケーションをリージョン 2 に移動するよう指定します。この例では、NTP および Call Home アプリケーションをリージョン 2 に移動します。

Note
同じリージョンにアプリケーションを複数回追加しようとすると、「Application already present in the same region.」というエラー メッセージが表示されます。

リージョンからのアプリケーションの削除

リージョンからのアプリケーションの削除は、アプリケーションをデフォルト リージョンのリージョン 0 に戻す場合と同じです。したがって、ファブリック全体がアプリケーションの配信の範囲になります。

リージョン 1 からアプリケーションを削除する手順は、次のとおりです。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **cfs region 1**

リージョン 1 に入ります。

ステップ 3 switch(config-cfs-region)# **no ntp**

switch(config-cfs-region)# **no callhome**

移動する、リージョン 1 に属するアプリケーションを削除します。

CFS リージョンの削除

リージョンの削除とは、リージョン定義を取り消すことです。リージョンを削除すると、リージョンによってバインドされているすべてのアプリケーションが解除されてデフォルト リージョンに戻ります。

たとえば、リージョン番号 4 というリージョンを削除する手順は、次のとおりです。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **no cfs region 4**

Example:

```
WARNING: All applications in the region wiil be  moved to default region.
Are you sure? (y/n)  [n]
```

リージョン 4 を削除します。

Note
ステップ 2 のあとに、「リージョン内のすべてのアプリケーションはデフォルト リージョンに移動されます。（All the applications in the region will be moved to the default region.）」という警告が表示されます。

CFS 設定の確認

CFS のコンフィギュレーション情報を表示するには、次の作業のいずれかを行います。

コマンド	目的
show cfs status	スイッチの CFS 配信ステータスを表示します。
show cfs application	CFS に現在登録されているアプリケーションを表示します。
show cfs lock	アプリケーションによって現在取得されているすべてのロックを表示します。
show cfs status	IP を介した CFS 構成の確認
show cfs region brief	CFS リージョンに関する簡単な情報を表示します。
show cfs region	CFS リージョンに関する詳細情報を表示します。

これらのコマンドの出力に表示される各フィールドの詳細については、『*Cisco MDS 9000 Family Command Reference*』を参照してください。

CFS 配信ステータスの確認

show cfs status コマンドを実行すると、スイッチの CFS 配信ステータスが表示されます。

```
switch# show cfs status
Distribution : Enabled
Distribution over IP : Disabled
IPv4 multicast address : 239.255.70.83
IPv6 multicast address : ff15::efff:4653
```

アプリケーション登録スターテスの確認

show cfs application コマンドは、CFS に現在登録されているアプリケーションを表示します。最初のカラムには、アプリケーション名が表示されます。2 番めのカラムは、アプリケーションの配信がイネーブルであるかディセーブルであるかを示します（enabled または disabled）。最後のカラムは、アプリケーションの配信範囲を示します（論理、物理、またはその両方）。

Note **show cfs application** コマンドは、CFS に登録されているアプリケーションのみを表示します。CFS を使用するコンディショナル サービスは、これらのサービスが稼働していなければ出力には示されません。

```
switch# show cfs application
-----------------------------------------------
 Application    Enabled   Scope
-----------------------------------------------
 ntp            No        Physical-fc-ip
 fscm           Yes       Physical-fc
 role           No        Physical-fc-ip
 rscn           No        Logical
 radius         No        Physical-fc-ip
 fctimer        No        Physical-fc
 syslogd        No        Physical-fc-ip
 callhome       No        Physical-fc-ip
 fcdomain       No        Logical
 fc-redirect    Yes       Physical-fc
 device-alias   Yes       Physical-fc
Total number of entries = 11
```

show cfs application name コマンドは、特定のアプリケーションの詳細を表示します。表示されるのは、イネーブル/ディセーブル ステート、CFS に登録されているタイムアウト、結合可能であるか（結合のサポートに対して CFS に登録されているか）、および配信範囲です。

```
switch# show cfs application name ntp
 Enabled        : Yes
 Timeout        : 5s
 Merge Capable  : Yes
```

```
 Scope          : Physical
 Region     : Default
```

CFS ロック ステータスの確認

show cfs lock コマンドを実行すると、アプリケーションによって現在取得されているすべてのロックが表示されます。このコマンドにより、アプリケーションごとにアプリケーション名とロックの取得範囲が表示されます。アプリケーション ロックが物理範囲で取得されている場合、このコマンドはスイッチ WWN、IP アドレス、ユーザ名、およびロック所有者のユーザ タイプを表示します。アプリケーションが論理範囲で取得されている場合、このコマンドはロックが取得された VSAN、ドメイン、IP アドレス、ユーザ名、およびロック所持者のユーザ タイプを表示します。

```
switch# show cfs lock
Application: ntp
Scope      : Physical
-------------------------------------------------------------------------
 Switch WWN               IP Address       User Name    User Type
-------------------------------------------------------------------------
 20:00:00:05:30:00:6b:9e  10.76.100.167    admin        CLI/SNMP v3
 Total number of entries = 1
Application: port-security
Scope      : Logical
-----------------------------------------------------------
 VSAN   Domain   IP Address       User Name    User Type
-----------------------------------------------------------
 1      238      10.76.100.167    admin        CLI/SNMP v3
 2      211      10.76.100.167    admin        CLI/SNMP v3
 Total number of entries = 2
```

show cfs lock name コマンドは、指定したアプリケーションに類似するロックの詳細情報を表示します。

指定アプリケーションのロック情報

```
switch# show cfs lock name ntp
Scope      : Physical
-------------------------------------------------------------------------
 Switch WWN               IP Address       User Name    User Type
-------------------------------------------------------------------------
 20:00:00:05:30:00:6b:9e  10.76.100.167    admin        CLI/SNMP v3
 Total number of entries = 1
```

IP を介した CFS 構成の確認

IP を介した CFS 構成を確認するには、 **show cfs status** コマンドを使用します。

```
switch# show cfs status
Distribution : Enabled
Distribution over IP : Disabled
```

```
IPv4 multicast address : 239.255.70.83
IPv6 multicast address : ff15::efff:4653
```

IP を介した CFS の IP マルチキャストアドレス構成の確認

IP を介した CFS の IP マルチキャストアドレス構成を確認するには、 **show cfs status** コマンドを使用します。

```
switch# show cfs status
Fabric distribution Enabled
IP distribution Enabled mode ipv4
IPv4 multicast address : 10.1.10.100
IPv6 multicast address : ff13::e244:4754
```

静的 IP ピア構成の確認

IP ピアの構成を確認するには、 **show cfs status** コマンドを使用します。

```
switch# show cfs status
Distribution: Enabled
Distribution over IP: Enabled - mode IPv4 (static)
IPv4 multicast address : 239:255:70:83
IPv6 multicast address : ff15::efff:4563
```

静的 IP ピア検出のステータスを表示するには、**show cfs static peers** コマンドを使用します。

```
switch# show cfs static peers
--------------------------------------------------------------
IP Address     WWN                          Status
--------------------------------------------------------------
192.0.2.4     00:00:00:00:00:00:00:00      Discovery in progress
192.0.2.5     20:00:00:0d:ec:06:55:b9      Reachable
192.0.2.6     20:00:00:0d:ec:06:55:c0      Local
```

CFS リージョンの確認

CFS リージョンを表示するには、次の作業を行います。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **show cfs region brief**

CFS リージョンに関する簡単な情報を表示します。

ステップ 3 switch(config)# **show cfs region**

CFS リージョンに関する詳細情報を表示します。

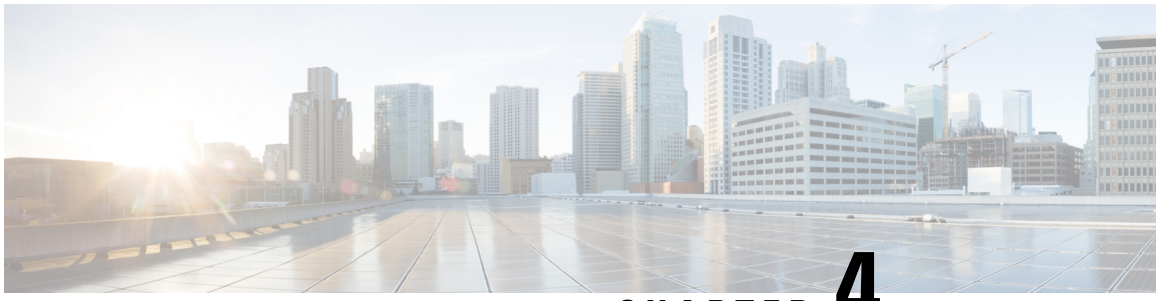
Note
CFS ピアを正常に形成するには、2 つの異なる管理スイッチに接続されている 2 つの異なるスイッチに共通の mcast IP を構成します。

その他の参考資料

CFS の実装に関する詳細情報については、次の項を参照してください。

MIB

MIB	MIB のリンク
• CISCO-CFS-CAPABILITY-MIB • CISCO-CFS-MIB	MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 http://www.cisco.com/en/US/products/ps5989/prod_technical_reference_list.html



CHAPTER 4

システムメッセージロギングの設定

この章では、Cisco MDS 9000 シリーズ スイッチでシステム メッセージ ロギングを構成する方法について説明します。

- システム メッセージ ロギングの概要, on page 29
- システム メッセージ ロギングの注意事項および制約事項, on page 35
- デフォルト設定, on page 35
- システムメッセージロギングの設定, on page 36
- その他の参考資料, on page 50

システム メッセージ ロギングの概要

システム メッセージ ロギング ソフトウェアでは、メッセージをログ ファイルに保存したり、メッセージを他のデバイスに転送したりできます。デフォルトでは、スイッチにより、正常だが重要なシステム メッセージがログ ファイルに記録され、それらのメッセージがシステム コンソールに送信されます。この機能には次の特徴があります。

- モニタリングおよびトラブルシューティングに使用するロギング情報を提供
- 取得したロギング情報のタイプが選択可能
- キャプチャされたロギング情報を適切に設定されたシステム メッセージ ロギング サーバに転送するために宛先サーバを選択可能。

Note 最初にスイッチを初期化するとき、初期化が完了するまでネットワークは接続されません。そのため、メッセージはシステム メッセージ ロギング サーバに数秒間リダイレクトされます。

ログ メッセージは、システム再起動後には消去されています。ただし、重大度が Critical 以下（レベル 0、1、2）の最大 100 個のログ メッセージは NVRAM に保存されます。

Table 2: 内部ロギング ファシリティ , on page 30 では、システム メッセージ ログでサポートされているファシリティの例について説明します。

Table 2: 内部ロギング ファシリティ

ファシリティ キーワード	[説明（Description）]	標準であるか、または Cisco MDS 固有であるか
acl	ACL マネージャ	Cisco MDS 9000 ファミリ固有
all	すべてのファシリティ	Cisco MDS 9000 ファミリ固有
auth	認証システム	標準
authpriv	認証（プライベート）システム	標準
bootvar	Bootvar	Cisco MDS 9000 ファミリ固有
callhome	Call Home	Cisco MDS 9000 ファミリ固有
cron	cron ファシリティまたは at ファシリティ	標準
daemon	システム デーモン	標準
fcc	FCC	Cisco MDS 9000 ファミリ固有
fcdomain	fcdomain	Cisco MDS 9000 ファミリ固有
fcns	ネーム サーバー	Cisco MDS 9000 ファミリ固有
fcs	FCS	Cisco MDS 9000 ファミリ固有
flogi	FLOGI	Cisco MDS 9000 ファミリ固有
fspf	FSPF	Cisco MDS 9000 ファミリ固有
ftp	File Transfer Protocol	標準
ipconf	IP 設定（IP configuration）	Cisco MDS 9000 ファミリ固有
ipfc	IPFC	Cisco MDS 9000 ファミリ固有
kernel	カーネル	標準
local0 to local7	ローカルに定義されたメッセージ	標準
lpr	ライン プリンタ システム	標準
mail	メール システム	標準
mcast	マルチキャスト	Cisco MDS 9000 ファミリ固有
module	スイッチング モジュール	Cisco MDS 9000 ファミリ固有
news	USENET ニュース	標準
ntp	NTP	Cisco MDS 9000 ファミリ固有

ファシリティ キーワード	[説明（Description）]	標準であるか、または Cisco MDS 固有であるか
platform	プラットフォーム マネージャ	Cisco MDS 9000 ファミリ固有
port	ポート	Cisco MDS 9000 ファミリ固有
port-channel	PortChannel	Cisco MDS 9000 ファミリ固有
qos	QoS	Cisco MDS 9000 ファミリ固有
rdl	RDL	Cisco MDS 9000 ファミリ固有
rib	RIB	Cisco MDS 9000 ファミリ固有
rscn	RSCN	Cisco MDS 9000 ファミリ固有
securityd	セキュリティ	Cisco MDS 9000 ファミリ固有
syslog	内部システム メッセージ	標準
sysmgr	システム マネージャ	Cisco MDS 9000 ファミリ固有
tlport	TL ポート	Cisco MDS 9000 ファミリ固有
user	ユーザ プロセス	標準
uucp	UNIX 間コピー プログラム	標準
vhbad	仮想ホスト ベース アダプタ デーモン	Cisco MDS 9000 ファミリ固有
vni	仮想ネットワーク インターフェイス	Cisco MDS 9000 ファミリ固有
vrrp_cfg	VRRP の設定	Cisco MDS 9000 ファミリ固有
vrrp_eng	VRRP エンジン	Cisco MDS 9000 ファミリ固有
vsan	VSAN システム メッセージ	Cisco MDS 9000 ファミリ固有
vshd	vshd	Cisco MDS 9000 ファミリ固有
wwn	WWN マネージャ	Cisco MDS 9000 ファミリ固有
xbar	クロスバー システム メッセージ	Cisco MDS 9000 ファミリ固有
zone	ゾーン サーバ	Cisco MDS 9000 ファミリ固有

Table 3: エラー メッセージの重大度 , on page 32 に、システム メッセージ ログでサポートされているシビラティ（重大度）を示します。

Table 3: エラー メッセージの重大度

level キーワード	レベル	説明	システム メッセージ定義
emergencies	0	システムが使用不可	LOG_EMERG
alerts	1	即時処理が必要	LOG_ALERT
critical	2	クリティカルな状態	LOG_CRIT
errors	3	エラー状態	LOG_ERR
warnings	4	警告状態	LOG_WARNING
notifications	5	正常だが注意を要する状態	LOG_NOTICE
informational	6	情報メッセージだけ	LOG_INFO
debugging	7	デバッグ メッセージ	LOG_DEBUG

Note エラー ログ メッセージ フォーマットの詳細については、『*Cisco MDS 9000 Family System Messages Reference* 』を参照してください。

システム メッセージ ロギング

システム メッセージ ロギング機能を使用すると、後で参照できるようにシステム メッセージをログに記録できます。この機能では、次のことができます。

- モニタリングおよびトラブルシューティングのためにロギング情報を提供します。
- ユーザが、キャプチャされたロギング情報のタイプを選択できます。
- ユーザは、キャプチャされたロギング情報をリモート ロギング サーバーに転送できます。

リアルタイムのデバッグおよびメッセージ管理を強化するために、メッセージにはタイム スタンプが付加されます。

デフォルトでは、スイッチにより、正常だが重要なシステム メッセージがオンボード ログファイルに記録され、それらのログ発生時にシステム コンソールに記録されます。オンボード ログファイルは循環型で、最大 1200 件のメッセージを保存できます。オンボード ログファイルに保存されているメッセージは、CLI を使用して表示できます。

システム メッセージは、ユーザのスイッチへのセッション中にリアルタイムで表示される場合があります。これにより、トラブルシューティング時にスイッチイベントをリアルタイムでモニタリングできます。セッションに表示されるメッセージの最小シビラティ（重大度）は構成可能です。

システム メッセージは、リモート ログ サーバーに記録される場合もあります。最大 3 つのリモート接続先を構成できます。これらは、IPv4 アドレスと IPv6 アドレスが混在している場合があります。デフォルトでは、リモート ロギングの接続先が構成されている場合、システム メッセージは UDP を使用して送信されます。

Tip 複数のデバイスからのシステム メッセージを比較できるようにするには、すべてのデバイスの時刻が正しいことを確認してください。これにより、複数のデバイスに関係する一連のイベントを理解することができます。デバイス クロックは、NTP を使用して同期できます。

各接続先に記録されるシステム メッセージは、ファシリティとシビラティ（重大度）に基づいてフィルタリングできます。

SFP 診断

SFP 障害に関連したエラー メッセージは、Syslog に書き込まれます。SFP 障害に関連したイベントについて Syslog をリッスンできます。次のパラメータについて、値（下限または上限アラーム）と警告がチェックされます。

- TX 電力
- RX 電力
- 温度
- 電圧
- 電流

SFP通知トラップは、デジタル診断モニタリング情報に基づいて、すべてのセンサーのアラームおよび警告のモニタリング パラメータの最新ステータスを示します。この通知は、インターフェイス内のトランシーバ上でセンサーのモニタリング パラメータが 1 つでもステータスを変化させると生成されます。

SFP 通知トラップ情報は、CISCO-INTERFACE-XCVR-MONITOR-MIB に格納されます。この MIB の詳細については、『*Cisco MDS 9000 Family MIB Quick Reference*』を参照してください。

出力されるシステム メッセージ ロギング サーバ ファシリティ

すべてのシステム メッセージには、ロギング ファシリティとレベルがあります。ロギング ファシリティは*where* を示し、レベルは *what* を示すものと考えることができます。

シングル システム メッセージ ロギング デーモン（syslogd）が、構成済みの **facility** オプションに基づいて情報を送信します。ファシリティが指定されていない場合、local7 がデフォルトの送信ファシリティとなります。

内部ファシリティの一覧はTable 2: 内部ロギング ファシリティ , on page 30 に記載されており、送信ロギング ファシリティの一覧はTable 4: 送信ロギング ファシリティ , on page 34に記載されています。

Table 4: 送信ロギング ファシリティ

ファシリティ キーワード	[説明（Description）]	標準であるか、またはCisco MDS 固有であるか
auth	認証システム	標準
authpriv	認証（プライベート）システム	標準
cron	cron ファシリティまたは at ファシリティ	標準
daemon	システム デーモン	標準
ftp	File Transfer Protocol	標準
kernel	カーネル	標準
local0 to local7	ローカルに定義されたメッセージ	標準（デフォルトは local7）
lpr	ライン プリンタ システム	標準
mail	メール システム	標準
news	USENET ニュース	標準
syslog	内部システム メッセージ	標準
user	ユーザ プロセス	標準
uucp	UNIX 間コピー プログラム	標準

システム メッセージ ロギング設定の配信

ファブリック内のすべての Cisco MDS スイッチで、ファブリック配信をイネーブルにできます。システム メッセージ ロギングを設定した場合、配信がイネーブルになっていると、その設定がファブリック内のすべてのスイッチに配信されます。

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。システム メッセージ ロギング サーバは、有効/保留データベース モデルを使用して、設定をベースにコマンドを保存またはコミットします。設定の変更を確定すると、有効データベースが保留データベースの設定変更で上書きされ、ファブリック内のすべてのスイッチで設定が同じになります。構成変更を加えたあと、変更内容をコミットする代わりに終了すると、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。CFS アプリケーションの詳細については、CFS インフラストラクチャの使用, on page 7 を参照してください。

ファブリックのロックの上書き

システム メッセージ ロギングで作業を行い、変更の確定か廃棄を行っ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 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。

システムメッセージロギングの注意事項および制約事項

システム メッセージ ロギング構成が異なる 2 つのファブリックを CFS とマージする場合は、次のガイドラインに従ってください。

- マージされた構成は、ファブリック内のスイッチごとに存在する受信された構成を結合したものになることに注意してください。
- マージされた構成に、最大で 3 つの固有システム メッセージ ロギング サーバーしか含まれないことを確認してください。

Caution マージされた構成に含まれるサーバーが 3 台を超えると、そのマージは失敗します。

CFS マージの詳細な概念については、CFS マージのサポート, on page 12 を参照してください。

デフォルト設定

Table 5: システム メッセージ ログのデフォルト設定値 , on page 35 に、システム メッセージ ロギングのデフォルト設定を示します。

Table 5: **システム メッセージ ログのデフォルト設定値**

パラメータ	デフォルト
コンソールへのシステム メッセージ ロギング	Critical 重大度のメッセージに対してイネーブル
セッションへのシステム メッセージ ロギング	ディセーブル
オンボード ロギング ファイルのサイズ	4194304 バイト。
オンボード ロギング ファイル名	メッセージ

パラメータ	デフォルト
リモート サーバー機能	local7
リモート ロギングの接続先	設定されていません。
非セキュアなリモート サーバーの宛て先ポート	UDP 514
セキュアなリモート サーバーの宛て先ポート	TCP 6514
CA 証明書	装着されていません。

システムメッセージロギングの設定

システム ロギング メッセージは、デフォルトの（または設定された）ロギング ファシリティと重大度に基づいてコンソールに送信されます。

システム メッセージ ロギングを設定するためのタスク フロー

システム メッセージ ロギングを設定するには、次の手順を実行します。

Procedure

ステップ 1 メッセージ ロギングをイネーブルまたはディセーブルにします。
ステップ 2 コンソール シビラティ（重大度）レベルを構成します。
ステップ 3 モニタ重大度を設定します。
ステップ 4 モジュール ログのシビラティ（重大度）レベルを構成します。
ステップ 5 ファシリティ重大度を設定します。
ステップ 6 オンボード ログ ファイルを構成します。
ステップ 7 システム メッセージ ロギング サーバを設定します。
ステップ 8 システム メッセージ ロギングの配布を構成します。

メッセージ ロギングのイネーブル化またはディセーブル化

コンソールへのロギングをディセーブルにしたり、特定された Telnet セッションまたは SSH セッションへのロギングをイネーブルにできます。

- コンソールセッションへのロギングをディセーブルまたはイネーブルにすると、その状態は将来のすべてのコンソール セッションに適用されます。セッションを終了して新しいセッションに再度ログインした場合、状態は保持されます。
- TelnetセッションまたはSSHセッションへのロギングをイネーブルまたはディセーブルにした場合、その状態はそのセッションだけに適用されます。セッションを終了して新しいセッションに再度ログインした場合、状態は保持されません。

TelnetセッションまたはSSHセッションのロギング状態をイネーブルまたはディセーブルにするには、次の手順を実行します。

Procedure

ステップ 1 switch# **terminal monitor**

Telnet または SSH セッションへのロギングを有効にする。

Note
コンソール セッションへのロギングは、デフォルトで有効になっています。

ステップ 2 switch# **terminal no monitor**

Telnet または SSH セッションのロギングを無効にします。

Note
Telnet または SSH セッションは、デフォルトで無効になっています。

コンソール重大度の設定

コンソールセッションに対するロギングがイネーブルになっている場合（デフォルト）、コンソールに表示されるメッセージの重大度を設定できます。コンソールロギングのデフォルトの重大度は 2（Critical）です。

Note コンソールのボー レートが 9600 ボー（デフォルト）の場合、現在の Critical（デフォルト）ロギング レベルが維持されます。コンソールロギング レベルを変更しようとすると、必ずエラーメッセージが生成されます。ロギング レベルを上げる（Critical よりも上に）には、コンソールのボー レートを 38400 ボーに変更する必要があります。

コンソールセッションのシビラティ（重大度）レベルを構成するには、次の手順に従ってください。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **logging console 3**

レベル 3（エラー）でコンソール ロギングを構成します。シビラティ（重大度）レベルが 3 以上のロギング メッセージがコンソールに表示されます。

ステップ 3 switch(config)# **no logging console**

コンソール ロギングを工場出荷時のデフォルトのシビラティ（重大度）レベル2（クリティカル）に戻します。シビラティ（重大度）レベルが 2 以上のロギング メッセージがコンソールに表示されます。

モニタ重大度の設定

モニタ セッションに対するロギングがイネーブルになっている場合（デフォルト）、モニタに表示されるメッセージの重大度を設定できます。モニタ ロギングのデフォルトの重大度は 5（notifications）です。

モニタ セッションのシビラティ（重大度）を構成するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **logging monitor 3**

レベル 3（エラー）でモニタ ロギングを構成します。シビラティ（重大度）レベルが 3 以上のロギング メッセージがモニタに表示されます。

ステップ 3 switch(config)# **no logging monitor**

モニタ ロギングを工場出荷時のデフォルトのシビラティ（重大度）5（notifications）に戻します。シビラティ（重大度）レベルが 5 以上のロギング メッセージがコンソールに表示されます。

モジュール ロギングの設定

各モジュールに対するロギングを、特定の重大度レベルで有効または無効にできます。

Cisco MDS 9000 NX-OS リリース 9.4(3) 以降、ライン カードからのカーネル システム ログはスーパーバイザ モジュールに記録されます。この機能は、次の Cisco MDS 9700 シリーズ ラインカードでサポートされています。

- DS-X9448-768K9
- DS-X9648-1536K9
- DS-X9748-3072K9
- DS-X9334-K9

Table 6: デフォルトの重大度設定：

コマンド	デフォルト値
logging module	5
logging module kernel	2

モジュールのロギングを有効または無効にし、シビラティ（重大度）レベルを構成するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **logging module 1**

すべてのモジュールのレベル 1（アラート）でモジュール ロギングを構成します。

ステップ 3 （オプション）switch(config)# **logging module**

スイッチのすべてのモジュールのモジュール ロギングをデフォルトのレベル 5 に構成します。

ステップ 4 （オプション）switch(config)# **logging module kernel**

logging module kernel コマンドを有効にします。

スイッチのすべてのモジュールのモジュール カーネル ロギングをデフォルトのレベル 2 に構成します。

ステップ 5 （オプション）switch(config)# **logging module kernel 1**

重大度を構成します。

ステップ 6 （オプション）switch(config)# **no logging module**

モジュール ロギングを無効にします。

ステップ 7 （オプション）switch(config)# **no logging module kernel**

ロギング モジュール カーネルを無効にします。

ファシリティ重大度の設定

ロギング ファシリティのシビラティ（重大度）レベルを構成するには（Table 2: 内部ロギング ファシリティ , on page 30 を参照）、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **logging level kernel 4**

レベル 4（warning）で、カーネル ファシリティに関する Telnet または SSH ロギングを構成します。その結果、重大度レベルが 4 以上のロギング メッセージが表示されます。

ステップ 3 switch(config)# **no logging level kernel 4**

カーネル ファシリティの Telnet または SSH ロギングをデフォルトのシビラティ（重大度）レベル 6（情報）に戻します。

Note
show logging info コマンドを使用して、Table 2: 内部ロギング ファシリティ , on page 30 にリストされているファシリティのデフォルトのロギング レベルを表示します。

オンボード ログ ファイルの構成

デフォルトでは、スイッチにより、正常だが重要なシステム メッセージがログ ファイルに記録され、それらのメッセージがシステム コンソールに送信されます。ログ メッセージは、システム再起動後には消去されています。ロギング メッセージは生成時にログ ファイルに保存できます。必要に応じてこのファイルの名前を設定したり、そのサイズを制限できます。デフォルトのログ ファイル名は messages です。

ファイル名の最大文字数は 80 文字で、ファイル サイズの範囲は 4096 ～ 4194304 バイトです。

ログ メッセージをファイルに送るには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **logging logfile messages 3**

シビラティ（重大度）レベル 3 以上のエラーまたはイベントに関する情報のログを、messages という名前のデフォルトのログ ファイルに構成します。

ステップ 3 switch(config)# **logging logfile ManagerLog 3**

デフォルト サイズ 10,485,760 バイトを使用して、シビラティ（重大度） レベル 3 以上の errors または events の情報を ManagerLog という名前のファイルに記録するように構成します。

ステップ 4 switch(config)# **logging logfile ManagerLog 3 size 3000000**

シビラティ（重大度） レベル 3 以上の errors または events の情報を ManagerLog という名前のファイルに記録するように構成します。サイズの構成により、ファイル サイズを 3,000,000 バイトに制限しています。

ステップ 5 switch(config)# **no logging logfile**

ログファイルへのメッセージのロギングを無効にします。

logging logfile コマンドを使用して、ログ ファイルの名前を変更できます。

ログ ファイルの場所は変更できません。**show logging logfile** および clear logging logfile コマンドを使用して、このファイルの内容を表示および削除できます。**dir log:** コマンドを使用して、ロギング ファイルの統計を表示できます。 **delete log:** コマンドを使用して、ログ ファイルを削除できます。

追加のコピー シンタックスを使用して **copy log:** コマンドを使用して、ログファイルを別の場所にコピーできます。

システム メッセージの送信元 ID の構成

リモート Syslog サーバーに送信されるシステム メッセージでホスト名、IP アドレス、またはテキスト文字列を指定するには、次の手順を実行します。

手順

ステップ 1 switch# **configure**

構成モードに入ります。

ステップ 2 switch(config)# **logging origin-id** {**hostname** | **ip** *address* | **string** *word*}

リモート Syslog サーバーに送信されるシステム メッセージでホスト名、IP アドレス、またはテキスト文字列を指定します。

システム メッセージ ロギング サーバの設定

最大 3 台のシステム メッセージ ロギング サーバを設定できます。ログ メッセージを UNIX システム メッセージ ロギング サーバに送るには、UNIX サーバ上でシステム メッセージ ロギング デーモンを設定する必要があります。特権ユーザとしてログインし、次の手順に従います。

Procedure

ステップ 1 次の行を /etc/syslog.conf ファイルに追加します。

local1.debug /var/log/ myfile .log

Note
local1.debug および **/var/log/***myfile***.log** の間には必ず 5 個のタブ文字を追加してください。詳細な例については、/etc/syslog.conf ファイルのエントリを参照してください。

スイッチは、指定されたファシリティ タイプと重大度に基づいて、メッセージを送信します。**local1** キーワードは、UNIX のロギング ファシリティを使用することを指定します。スイッチからのメッセージは、ユーザ プロセスによって生成されます。**debug** キーワードで、記録する状況のシビラティ（重大度）を指定します。スイッチからのすべてのメッセージを受信するように UNIX システムを設定できます。

ステップ 2 UNIX シェル プロンプトに次のコマンドを入力して、ログ ファイルを作成します。

$ touch /var/log/ myfile .log

$ chmod 666 /var/log/ myfile .log

ステップ 3 次のコマンドを実行して、システム メッセージ ロギング デーモンに新しい変更を読み込ませます。

$ kill -HUP ~cat /etc/syslog.pid~

システム メッセージ ロギングの配布の構成

システム メッセージ ロギング サーバー構成のファブリック配布を有効にするには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

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

システム メッセージ ロギング サーバー構成をファブリック内のすべてのスイッチに配布できるようにし、ロックを取得して、今後のすべての構成変更を保留中のデータベースに保存します。

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

ファブリック内のすべてのスイッチに対するシステム メッセージ ロギング サーバー構成の配布を無効（デフォルト）にします。

変更のコミット

システム メッセージ ロギング サーバーの構成変更をコミットするには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

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

構成の変更をファブリック内のすべてのスイッチに配布し、ロックを解除して、保留中のデータベースに加えられた変更で有効なデータベースを上書きします。

変更の破棄

システム メッセージ ロギング サーバーの構成変更を廃棄するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **logging abort**

保留中のデータベースのシステム メッセージ サーバーの構成変更を廃棄し、ファブリック ロックを解除します。

ファブリックのロックの上書き

管理者特権を使用して、ロックされたシステム メッセージ ロギング セッションを解除するには、**clear logging session** コマンドを使用します。

```
switch# clear logging session
```

システム メッセージ ロギング情報の表示

システム メッセージ ロギング情報を表示するには、次の作業のいずれかを行います。

コマンド	目的
show logging	現在のシステム メッセージ ロギングを表示します。
show logging nvram	NVRM ログの内容を表示します。
show logging logfile	ログ ファイルを表示します。
show logging level	ロギング ファシリティを表示します。
show logging info	ロギング情報を表示します。
show logging last 2	ログ ファイルの最後の数行を表示します。
show logging module	スイッチング モジュールのロギング ステータスを表示します。
show logging monitor	モニタ ロギング ステータスを表示します。
show logging server	サーバ情報を表示します。

これらのコマンドの出力に表示される各フィールドの詳細については、『*Cisco MDS 9000 Family Command Reference*』を参照してください。

show logging コマンドを使用して、現在のシステム メッセージ ロギングの構成を表示します。例 現在のシステム メッセージ ロギング, on page 45 ～ リモート ロギング サーバー情報, on page 50 を参照してください。

Note **show logging** コマンドを使用すると、スイッチで構成されているロギング レベルがデフォルトのレベルと違う場合にだけ出力が表示されます。

現在のシステム メッセージ ロギング

次の例は、現在のシステム メッセージ ロギング設定とオンボード ログ ファイルの内容を表示します。

```
switch# show logging

Logging console:                enabled (Severity: critical)
Logging monitor:                enabled (Severity: debugging)
Logging linecard:               enabled (Severity: debugging)
Logging server:                 enabled
{172.20.102.34}
        server severity:        debugging
        server facility:        local7
{10.77.202.88}
        server severity:        debugging
        server facility:        local7
{10.77.202.149}
        server severity:        debugging
        server facility:        local7
Logging logfile:                enabled
        Name - messages: Severity - debugging Size - 4194304
Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
kern                    6                       6
user                    3                       3
mail                    3                       3
daemon                  7                       7
auth                    0                       7
syslog                  3                       3
lpr                     3                       3
news                    3                       3
uucp                    3                       3
cron                    3                       3
authpriv                3                       7
ftp                     3                       3
local0                  3                       3
local1                  3                       3
local2                  3                       3
local3                  3                       3
local4                  3                       3
local5                  3                       3
local6                  3                       3
local7                  3                       3
vsan                    2                       2
fspf                    3                       3
fcdomain                2                       2
module                  5                       5
sysmgr                  3                       3
zone                    2                       2
vni                     2                       2
ipconf                  2                       2
ipfc                    2                       2
xbar                    3                       3
fcns                    2                       2
fcs                     2                       2
acl                     2                       2
tlport                  2                       2
port                    5                       5
flogi                   2                       2
port_channel            5                       5
```

```
wwn                     3                       3
fcc                     2                       2
qos                     3                       3
vrrp_cfg                2                       2
ntp                     2                       2
platform                5                       5
vrrp_eng                2                       2
callhome                2                       2
mcast                   2                       2
rdl                     2                       2
rscn                    2                       2
bootvar                 5                       2
securityd               2                       2
vhbad                   2                       2
rib                     2                       2
vshd                    5                       5
0(emergencies)          1(alerts)       2(critical)
3(errors)               4(warnings)     5(notifications)
6(information)          7(debugging)
Feb 14 09:50:57 switchname %TTYD-6-TTYD_MISC: TTYD TTYD started
Feb 14 09:50:58 switchname %DAEMON-6-SYSTEM_MSG: precision = 8 usec
...
```

show logging nvram コマンドを使用して、NVRAM に保存されているログ メッセージを表示します。シビラティ（重大度）レベルが Critical 以下（レベル 0、1、2）のログ メッセージだけが NVRAM に保存されます。

NVRM ログの内容

次の例は、NVRM ログの内容を表示します。

```
switch# show logging nvram

Jul 16 20:36:46 switchname %KERN-2-SYSTEM_MSG: unable to alloc and fill in a
new mtsbuf (pid=2209, ret_val = -105)
Jul 16 20:36:46 switchname %KERN-2-SYSTEM_MSG: unable to alloc and fill in a
new mtsbuf (pid=2199, ret_val = -105)
Jul 16 20:36:46 switchname %KERN-2-SYSTEM_MSG: unable to alloc and fill in a
new mtsbuf (pid=2213, ret_val = -105)
Jul 16 20:36:46 switchname %KERN-2-SYSTEM_MSG: unable to alloc and fill in a
new mtsbuf (pid=2213, ret_val = -105)
...
```

ログ ファイル

次の例は、オンボード ログ ファイルを表示します。

```
switch# show logging logfile

Jul 16 21:06:50 %DAEMON-3-SYSTEM_MSG: Un-parsable frequency in /mnt/pss/ntp.drift
Jul 16 21:06:56 %DAEMON-3-SYSTEM_MSG: snmpd:snmp_open_debug_cfg: no snmp_saved_dbg_uri
;
Jul 16 21:06:58 switchname %PORT-5-IF_UP: Interface mgmt0 is up
Jul 16 21:06:58 switchname %MODULE-5-ACTIVE_SUP_OK: Supervisor 5 is active
...
```

コンソール ロギング ステータス

次の例は、コンソール ロギング ステータスを表示します。

```
switch# show logging console

Logging console:                enabled (Severity: notifications)
```

ロギング ファシリティ

次の例は、各スイッチ ファシリティのログ レベルを表示します。

```
switch# show logging level

Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
kern                    6                       6
user                    3                       3
mail                    3                       3
daemon                  7                       7
auth                    0                       7
syslog                  3                       3
lpr                     3                       3
news                    3                       3
uucp                    3                       3
cron                    3                       3
authpriv                3                       7
ftp                     3                       3
local0                  3                       3
local1                  3                       3
local2                  3                       3
local3                  3                       3
local4                  3                       3
local5                  3                       3
local6                  3                       3
local7                  3                       3
vsan                    2                       2
fspf                    3                       3
fcdomain                2                       2
module                  5                       5
sysmgr                  3                       3
zone                    2                       2
vni                     2                       2
ipconf                  2                       2
ipfc                    2                       2
xbar                    3                       3
fcns                    2                       2
fcs                     2                       2
acl                     2                       2
tlport                  2                       2
port                    5                       5
flogi                   2                       2
port_channel            5                       5
wwn                     3                       3
fcc                     2                       2
qos                     3                       3
vrrp_cfg                2                       2
ntp                     2                       2
platform                5                       5
```

```
vrrp_eng                2                       2
callhome                2                       2
mcast                   2                       2
rdl                     2                       2
rscn                    2                       2
bootvar                 5                       2
securityd               2                       2
vhbad                   2                       2
rib                     2                       2
vshd                    5                       5
0(emergencies)          1(alerts)       2(critical)
3(errors)               4(warnings)     5(notifications)
6(information)          7(debugging)
```

ログ情報

次の例は、現在のシステム メッセージ ロギング設定を表示します。

```
switch# show logging info

Logging console:                enabled (Severity: critical)
Logging monitor:                enabled (Severity: debugging)
Logging linecard:               enabled (Severity: debugging)
Logging server:                 enabled
{192.168.1.34}
        server severity:        debugging
        server facility:        local7
{192.168.1.88}
        server severity:        debugging
        server facility:        local7
{192.168.1.149}
        server severity:        debugging
        server facility:        local7
Logging logfile:                enabled
        Name - messages: Severity - debugging Size - 4194304
Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
kern                    6                       6
user                    3                       3
mail                    3                       3
daemon                  7                       7
auth                    0                       7
syslog                  3                       3
lpr                     3                       3
news                    3                       3
uucp                    3                       3
cron                    3                       3
authpriv                3                       7
ftp                     3                       3
local0                  3                       3
local1                  3                       3
local2                  3                       3
local3                  3                       3
local4                  3                       3
local5                  3                       3
local6                  3                       3
local7                  3                       3
vsan                    2                       2
fspf                    3                       3
fcdomain                2                       2
module                  5                       5
```

```
sysmgr                  3                       3
zone                    2                       2
vni                     2                       2
ipconf                  2                       2
ipfc                    2                       2
xbar                    3                       3
fcns                    2                       2
fcs                     2                       2
acl                     2                       2
tlport                  2                       2
port                    5                       5
flogi                   2                       2
port_channel            5                       5
wwn                     3                       3
fcc                     2                       2
qos                     3                       3
vrrp_cfg                2                       2
ntp                     2                       2
platform                5                       5
vrrp_eng                2                       2
callhome                2                       2
mcast                   2                       2
rdl                     2                       2
rscn                    2                       2
bootvar                 5                       2
securityd               2                       2
vhbad                   2                       2
rib                     2                       2
vshd                    5                       5
0(emergencies)          1(alerts)       2(critical)
3(errors)               4(warnings)     5(notifications)
6(information)          7(debugging)
```

ログ ファイルの最後の数行

次の例は、ログ ファイルの最後の数行を表示します。

```
switch# show logging last 2

Nov 8 16:48:04 switchname %LOG_VSHD-5-VSHD_SYSLOG_CONFIG_I: Configuring console from
pts/1 (171.71.58.56)
Nov 8 17:44:09 switchname %LOG_VSHD-5-VSHD_SYSLOG_CONFIG_I: Configuring console from
pts/0 (171.71.58.72)
```

スイッチング モジュールのロギング ステータス

次の例は、スイッチング モジュールのロギング ステータスを表示します。

```
switch# show logging module


Logging linecard:                enabled (Severity: debugging)
```

モニタ ロギング ステータス

次の例は、モニタ ロギング ステータスを表示します。

```
switch# show logging monitor

Logging monitor:                 enabled (Severity: information)
```

リモート ロギング サーバー情報

次の例は、構成されたリモート ロギング サーバー情報を表示します。

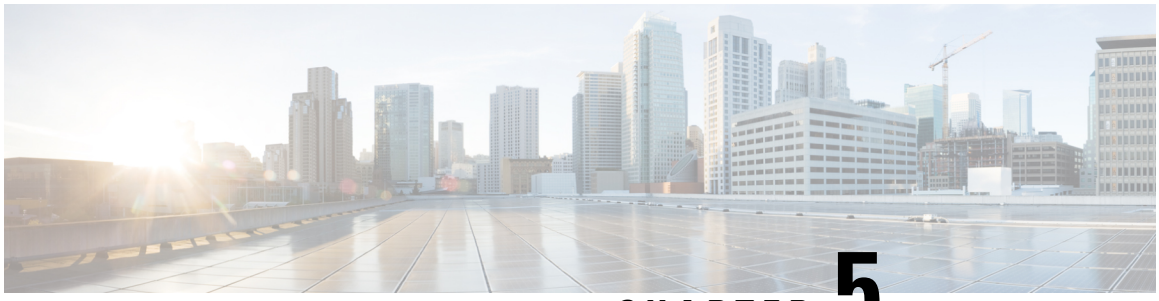
```
switch# show logging server
Logging server:                  enabled
{192.168.113.1}
        server severity:         notifications
        server facility:         local7
        server VRF:              default
        server port:             55552
        server transport:        secure
{192.168.106.50}
        server severity:         notifications
        server facility:         local7
        server VRF:              default
        server port:             55551
        server transport:        secure
{192.168.229.220}
        server severity:         notifications
        server facility:         local7
        server VRF:              default
        server port:             55552
```

その他の参考資料

システム メッセージ ロギングの実装に関する詳細情報については、次の項を参照してください。

MIB

MIB	MIB のリンク
• CISCO-SYSLOG-EXT-MIB • CISCO-SYSLOG-MIB	MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 http://www.cisco.com/en/US/products/ps5989/prod_technical_reference_list.html



CHAPTER 5

Call Home の設定

Call Home は、重要なシステム イベントを電子メールで通知します。ポケットベル サービス、通常の電子メール、または XML ベースの自動解析アプリケーションとの適切な互換性のために、さまざまなメッセージのフォーマットが使用できます。

Note Cisco Autonotify は、Smart Call Home と呼ぶ新機能にアップグレードされています。Smart Call Home は、Autonotify に比べて機能が大幅に改良されており、シスコの製品レンジ全体にわたって使用できます。Smart Call Home の詳細については、Smart Call Home のページ（http://www.cisco.com/go/smartcall/）を参照してください。

この章は、次の項で構成されています。

- Call Home の概要, on page 51
- 注意事項と制約事項, on page 75
- デフォルト設定, on page 76
- Call Home の設定, on page 77
- Call Home ウィザードの設定, on page 96
- Call Home コンフィギュレーションの確認, on page 109
- Call Home のモニタリング, on page 114
- Call Home のフィールドの説明, on page 119
- その他の参考資料, on page 125
- Call Home の機能履歴, on page 125

Call Home の概要

Call Home は、メッセージ スロットリング機能を備えています。定期的なインベントリ メッセージ、ポート syslog メッセージ、および RMON アラート メッセージが、配信可能な Call Home メッセージのリストに追加されます。必要に応じて、Cisco Fabric Services アプリケーションを使用して、Call Home 設定を、ファブリック内の他のすべてのスイッチに配信することもできます。

Call Home サービスでは、重要なシステム イベントに関する電子メール ベースの通知が提供されます。ポケットベル サービス、通常の電子メール、または XML ベースの自動解析アプリケーションとの適切な互換性のために、さまざまなメッセージのフォーマットが使用できます。

一般的な機能として次のものがあります。

- ポケットベルによるネットワーク サポート技術者の呼び出し
- ネットワーク オペレーション センターへの電子メールの送信
- Technical Assistance Center の直接ケースの提出

Call Home 機能は、Cisco MDS 9000 シリーズ スイッチと Cisco Nexus 5000 シリーズ スイッチから直接利用できます。複数の Call Home メッセージが提供され、それぞれに個別の宛先があります。事前に定義されたプロファイルに加えて、独自の接続先プロファイルを定義できます。各接続先プロファイルには最大 50 件の電子メール アドレスを構成できます。柔軟なメッセージの配信オプションとフォーマット オプションにより、個別のサポート要件を簡単に統合できます。

Call Home 機能には、次の利点があります。

- スイッチ上のトリガー イベント用に事前に定義された一連の固定のアラート。
- 関連するコマンドの自動的な実行と出力の添付。

Call Home の機能

Call Home 機能は、Cisco MDS 9000 シリーズ スイッチと Cisco Nexus 5000 シリーズ スイッチから直接利用できます。複数の Call Home プロファイル（*Call Home* 接続先プロファイル とも呼びます）が提供され、それぞれに個別の接続先があります。事前に定義されたプロファイルに加えて、独自の宛先プロファイルを定義できます。

Call Home 機能では、シスコまたは別のサポート パートナーによるサポートも利用できます。柔軟なメッセージの配信オプションとフォーマット オプションにより、個別のサポート要件を簡単に統合できます。

Call Home 機能には、次の利点があります。

- スイッチ上の固定の事前に定義されたアラートおよびトリガー イベント。
- 関連するコマンドの自動的な実行と出力の添付。
- 複数のメッセージ フォーマット オプション
  - ショート テキスト：ポケットベルまたは印刷形式のレポートに最適。
  - プレーン テキスト：人間が読むのに適した形式に完全整形されたメッセージ情報。
  - XML：Extensible Markup Language（XML）と、Messaging Markup Language（MML）と呼ぶ Document Type Definitions（DTD）を使用した、機械で読み取り可能なフォーマット。MML DTD は、Cisco.com の Web サイト http://www.cisco.com/ で公開されて

います。XML 形式は、シスコ Technical Assistance Center とのやり取りの中でも使用されます。

- 複数のメッセージ宛先への同時配信が可能。各宛先プロファイルには最大50件の電子メール宛先アドレスを設定できます。
- システム、環境、スイッチング モジュール ハードウェア、スーパーバイザ モジュール、ハードウェア、インベントリ、syslog、RMON、テストなど、複数のメッセージ カテゴリ。
- お使いのデバイスから直接、またはHTTPプロキシサーバやダウンロード可能な転送ゲートウェイ（TG）を介した、セキュアなメッセージ転送。TG集約ポイントは、複数のデバイスをサポートする場合またはセキュリティ要件によって、デバイスをインターネットに直接接続できない場合に使用できます。

Note Cisco MDS リリース 7.3(0)D1(1) 以降、すべてのアラートはタイプ「環境」、およびサブタイプ「マイナー」に分類されます。

- SUP_FAILURE、POWER_SUPPY_FAILURE、LINECARD_FAILURE アラートは、タイプ「環境」、およびサブタイプ「メジャー」に分類されます。

Smart Call Home の概要

Smart Call Home は、Cisco SMARTnet Service のコンポーネントであり、選択したシスコ デバイス上での予防的診断、リアルタイム アラート、パーソナライズされた Web ベースのレポート機能を提供します。

Smart Call Home は、デバイスから送信された Call Home メッセージを解析し、シスコ カスタマーサポートへの直接通知パスを提供することにより、システムの問題を迅速に解決します。

Smart Call Home には、次の機能があります。

- 連続的なデバイスのヘルス モニタリングとリアルタイム診断アラート。
- 使用しているデバイスからの Call Home メッセージの分析と、必要に応じた自動的なサービス リクエストの生成と適切な TAC チームへの送信。これには、すばやい問題解決のための詳細な診断情報が含まれます。
- Call Home メッセージと推奨事項、すべての Call Home デバイスのコンポーネントと設定情報への Web アクセス。関連付けられた Field Notice、セキュリティアドバイザリ、およびサポート終了日情報にアクセスできます。

。

Table 7: Smart Call Home の Autonotify と比較した利点 , on page 54 に Smart Call Home の利点の一覧を示します。

Table 7: Smart Call Home の Autonotify と比較した利点

機能	Smart Call Home	Autonotify
簡単な登録	登録処理が大幅に簡素化されます。デバイス シリアル番号や連絡先情報を知っている必要はありません。デバイスからメッセージを送信することで、シスコの手動の介入なしにデバイスを登録できます。手順の概要については www.cisco.com/go/smartcall を参照してください。	各シリアル番号をデータベースに追加するようにシスコに依頼する必要があります。
推奨事項	Smart Call Home は、SR が提起された問題や、SR が該当しないものの、お客様による対処が必要となる可能性がある、既知の問題に対する推奨事項を提供します。	Autonotify は、一連の障害状況に対する SR を提起しますが、それらの対する推奨事項は提供しません。
デバイス レポート	デバイス レポートには、完全なインベントリと設定の詳細が含まれています。使用可能になると、これらのレポートの情報は Field Notice、PSIRT、EoX 通知、設定のベスト プラクティス、およびバグにマッピングされます。	数
履歴レポート	履歴レポートは、メッセージとその内容を探すために使用できます。これには、過去 3 か月の間に送信されたすべてのメッセージに対する、show コマンド、メッセージ処理、分析結果、推奨事項とサービス リクエスト番号が含まれます。	基本的なレポートが使用できますが、メッセージの内容は含まれていません。
ネットワーク要約レポート	カスタマーネットワーク内のデバイスとモジュールの構成の要約を示すレポート（Smart Call Home に登録されているデバイスが対象です）。	数
シスコ デバイスのサポート	デバイスのサポートはシスコの製品レンジ全体に拡張されます。サポートされている製品の表については、www.cisco.com/go/smartcall を参照してください。	Smart Call Home への移行を推進するため、2008 年 10 月に廃止されました。

Smart Call Home の取得

シスコと直接サービス契約を結んでいる場合は、Smart Call Home サービスに登録することで、Technical Assistance Center から自動的なケース生成を受け取ることができます。

次の項目を登録する必要があります。

- ご使用のスイッチの SMARTnet 契約番号
- 電子メール アドレス
- お使いの Cisco.com ID

Smart Call Home の詳細と、クイック スタート コンフィギュレーションおよび登録手順については、次の場所にある Smart Call Home のページを参照してください。

http://www.cisco.com/go/smartcall/

Call Home 宛先プロファイル

宛先プロファイルには、アラート通知に必要な配信情報が入っています。宛先プロファイルは、一般にネットワーク管理者によって設定されます。

アラート グループを使用して、（定義済みまたはユーザ定義の）宛先プロファイルで受信される Call Home アラートのセットを選択できます。アラート グループは、Call Home アラートの事前に定義されたサブセットであり、Cisco MDS 9000 シリーズと Cisco Nexus 5000 シリーズのすべてのスイッチでサポートされています。Call Home アラートはタイプごとに別のアラート グループにグループ化されます。ネットワークの必要性に応じて、1 つ以上のアラート グループを各プロファイルに関連付けることができます。

Call Home アラート グループ

アラート グループは、事前に定義された Call Home アラートのサブセットで、Cisco MDS 9000 シリーズと Cisco Nexus 5000 シリーズのすべてのスイッチでサポートされています。アラート グループを使用することで、（定義済みまたはユーザ定義の）宛先プロファイルで受信される Call Home アラートのセットを選択できます。Call Home アラートが、接続先プロファイル内の電子メールの宛先に送信されるのは、その Call Home アラートが、その接続先プロファイルに関連付けられているいずれかのアラート グループに属する場合だけです。

定義済みの Call Home アラート グループを使用して、スイッチに特定のイベントが発生したときに通知メッセージを生成できます。定義済みのアラート グループは、特定のイベントが発生した際に追加の **show** コマンドを実行したり、定義済みの **show** コマンド以外からの出力を通知したりするようにカスタマイズできます。

カスタマイズされたアラート グループ メッセージ

アラート グループは、事前に定義された Call Home アラートのサブセットで、Cisco MDS 9000 シリーズと Cisco Nexus 5000 シリーズのすべてのスイッチでサポートされています。アラート グループを使用することで、（定義済みまたはユーザ定義の）宛先プロファイルで受信される Call Home アラートのセットを選択できます。定義済みの Call Home アラート グループは、スイッチ上で特定のイベントが発生したときに通知メッセージを生成します。定義済みのアラート グループをカスタマイズして、特定のイベントが発生したときに、show コマンドを追加で実行できます。

これらの追加の **show** コマンドの出力は、定義済みの **show** コマンドの出力とともに、通知メッセージに格納されます。

Call Home のメッセージ レベル機能

Call Home のメッセージ レベル機能を使用すると、緊急度に基づいてメッセージをフィルタできます。各宛先プロファイル（定義済みおよびユーザ定義）は、Call Home メッセージ レベルしきい値に関連付けられます。緊急度しきい値よりも値が小さいメッセージは送信されません。Call Home の重大度は、システム メッセージ ロギングの重大度とは異なります。

Syslog ベースのアラート

特定の syslog メッセージを Call Home メッセージとして送信するようにスイッチを設定できます。これらのメッセージは、宛先プロファイルとアラート グループ マッピングの間のマッピング、および生成された Syslog メッセージの重大度に基づいて送信されます。

Syslog ベースの Call Home アラートを受信するには、宛先プロファイルと Syslog アラート グループを関連付けて（現在は syslog-group-port という 1 つの Syslog アラート グループだけが存在する）、適切なメッセージ レベルを設定する必要があります。

syslog-group-port アラート グループは、そのポート ファシリティの syslog メッセージを選択します。Call Home アプリケーションは、syslog のシビラティ（重大度）を対応する Call Home のシビラティ（重大度）にマッピングします（Table 8: イベント トリガ , on page 60を参照）。たとえば、Call Home メッセージ レベルに対してレベル 5 を選択すると、レベル 0、1、2 の syslog メッセージが Call Home ログに追加されます。

syslog メッセージが生成されるたびに、Call Home アプリケーションは、宛先プロファイルとアラート グループ マッピングの間のマッピングに従い、生成された syslog メッセージの重大度に基づいて、Call Home メッセージを送信します。Syslog ベースの Call Home アラートを受信するには、接続先プロファイルと Syslog アラート グループを関連付けて（現在は syslog-group-port という 1 つの Syslog アラート グループだけが存在する）、適切なメッセージ レベルを構成する必要があります（Table 8: イベント トリガ , on page 60を参照）。

Note Call Home は、メッセージ テキストで Syslog メッセージ レベルを変更しません。Call Home ログ内の syslog メッセージ テキストは、『*Cisco MDS 9000 Series System Messages* Reference』の記載どおりに出力されます。

RMON ベースのアラート

RMON アラート トリガーに対応する Call Home 通知を送信するようにスイッチを設定できます。RMON ベースの Call Home メッセージのメッセージ レベルは、すべて NOTIFY（2）に設定されます。RMON アラート グループは、すべての RMON ベースの Call Home アラートに対して定義されます。RMON ベースの Call Home アラートを受信するには、宛先プロファイルを RMON アラート グループに関連付ける必要があります。

HTTPS サポートを使用した一般的な EMail オプション

Call Home の HTTPS サポートは、HTTP と呼ばれる転送方式を提供します。HTTPS サポートはセキュアな通信で使用され、HTTP はノンセキュアな通信で使用されます。Call Home 宛先プロファイルに対し、HTTP URL を宛先として設定できます。URL リンクは、セキュア サーバでもノンセキュア サーバでも構いません。HTTP URL を使用して設定された宛先プロファイルでは、Call Home メッセージは、HTTP URL リンクにポストされます。

Note Call Home HTTP 設定は、NX-OS Release 4.2(1) 以降が動作するスイッチに、CFS を通じて配信できます。Call Home HTTP 設定は、配信不可能な HTTP 設定をサポートしているスイッチには配布できません。NX-OS Release 4.2(1) よりも前のバージョンが動作しているスイッチでは、HTTP 設定は無視されます。

複数 SMTP サーバ サポート

Cisco MDS NX-OS および Cisco NX-OS 5000 シリーズ スイッチは、Call Home 用に複数の SMTP サーバーをサポートします。各 SMTP サーバーには 1 ～ 100 の優先順位が構成されており、1 が最高の優先順位、100 が最低です。優先順位を指定しない場合、デフォルト値の 50 が使用されます。

Call Home に対して最大 5 つの SMTP サーバを設定できます。サーバーは優先順位に基づいて接続されます。最も優先順位の高いサーバーが最初に接続されます。メッセージが送信できない場合、制限に達するまでリスト内の次のサーバーが接続されます。2 つのサーバーの優先順位が同じ場合は、先に構成された方が最初に接続されます。

優先度の高い SMTP サーバーに障害が発生すると、他のサーバーに接続されます。メッセージの送信中に遅延が発生する場合があります。最初の SMTP サーバー経由でメッセージを送信する試みが成功した場合、遅延は最小限に抑えられます。異なる SMTP サーバーで失敗した試行の数に応じて、遅延が増加する場合があります。

Note 新しい構成プロセスは、古い構成とは関係ありません。ただし、SMTP サーバーが古いスキームと新しいスキームの両方を使用して構成されている場合、古い構成が最優先されます。

複数の SMTP サーバーは、リリース 5.0(1a) 以降を実行する任意の MDS 9000 シリーズ スイッチ、Cisco Nexus 5000 シリーズ スイッチ、および Cisco Nexus 7000 シリーズ スイッチで構成できます。

新しい構成は、複数の SMTP サーバーを持つスイッチにのみ配布されます。ファブリック内の古いスイッチは、CFS 経由で受信した新しい構成を無視します。

CFS が有効になっている混合ファブリックでは、NX-OS リリース 5.0 を実行しているスイッチは新しい機能を構成し、新しい構成を CFS 経由でファブリック内のリリース 5.0 を持つ他のスイッチに配布できます。ただし、NX-OS リリース 4.x を実行している既存のスイッチがリリー

ス 5.0 にアップグレードされた場合、アップグレード時に CFS マージがトリガーされないため、新しい構成はそのスイッチに配布されません。アップグレードには2つのオプションがあります。

- ファブリック内のすべてのスイッチがそれらをサポートしている場合にのみ、新しい構成を適用します（推奨オプション）
- 新しい構成を持つ既存の NX-OS リリース 5.0 スイッチから空のコミットを実行します。

複数の SMTP サーバーのサポートを構成するには、 複数の SMTP サーバーのサポートを参照してください。

電子メール ベースのアラート

Cisco MDS NX-OS は、デフォルトの転送方式として SMTP（電子メール）を使用したアラートの配信をサポートしています。スイッチは、1 つまたは複数のリモート SMTP サーバーに接続する SMTP クライアントです。接続は暗号化されていない場合と暗号化されている場合があります。

リモート SMTP サーバーへの接続が TCP ポート 25 に構成されている場合、電子メール アラートは暗号化されていない接続を介してクリア テキストで送信されます。

リモート SMTP サーバーへの接続が TCP ポート 465 に設定されている場合、接続は暗黙的な TLS で確立され、電子メール アラートも暗号化されます。接続が TCP ポート 587 で行われる場合、接続は明示的な TLS（STARTTLS 方式）で行われ、電子メールアラートも暗号化されます。

電子メールのユーザー認証は、暗号化された配信ではオプションであり、電子メールのユーザー名とパスワードが構成されている場合にのみ実行されます。構成されていない場合、電子メールはやはり暗号化され、セキュアな接続で配信されますが、リモート SMTP サーバーでのユーザー認証は実行されません。このような場合、リモート SMTP サーバーは、ユーザー認証をバイパスし、暗号化のみを適用するように構成する必要があります。

電子メール認証と暗号化を構成するには、 セキュアな電子メール アラートの構成を参照してください。

定期的なインベントリ通知

スイッチ上で現在イネーブルかつ動作中のすべてのソフトウェア サービスの一覧と、ハードウェアインベントリ情報とともに、定期的にメッセージを送信するようにスイッチを設定できます。インベントリは、スイッチを停止せずに再起動するたびに変更されます。

重複するメッセージのスロットリング

同じイベントに対して受信する Call Home メッセージの数を制限するために、スロットリング メカニズムを設定できます。短時間のうちにスイッチから何度も同じメッセージが送信される場合、重複する多数のメッセージであふれることがあります。

Call Home 設定の配信

ファブリック内のすべての Cisco MDS 9000 シリーズ スイッチと Cisco Nexus 5000 シリーズ スイッチに対して、ファブリック配信を有効にできます。Call Home を設定した場合、配信がイネーブルになっていると、その設定がファブリック内のすべてのスイッチに配信されます。ただし、スイッチ プライオリティと Syscontact 名は配信されません。

スイッチで配信をイネーブルにしてから初めてコンフィギュレーション コマンド操作を入力するとき、ファブリック全体が自動的にロックされます。Call Home アプリケーションは、設定の変更を保存または確定するために、有効および保留データベース モデルを使用します。設定の変更を確定すると、有効データベースが保留データベースの設定変更で上書きされ、ファブリック内のすべてのスイッチで設定が同じになります。構成変更を加えたあと、変更内容をコミットする代わりに終了すると、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。CFS アプリケーションの詳細については、CFS インフラストラクチャの使用, on page 7 を参照してください。

Note スイッチ プライオリティと Syscontact 名は配信されません。

ファブリックのロックの上書き

Call Home で作業を行い、変更の確定か廃棄を行っ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 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。

Call Home ネーム サーバ データベースのクリア

Call Home ネーム サーバ データベースが一杯になると、新しいエントリを追加できなくなります。デバイスがオンラインになることはできません。ネーム サーバ データベースをクリアするには、データベース サイズを増やすか、使用していないデバイスを削除してクリーンアップを実行します。合計 20,000 個のネーム サーバ エントリがサポートされています。

EMC Email Home 遅延トラップ

DCNM-SAN は、EMC E-mail Home XML 電子メール メッセージを生成するように構成できます。SAN-OS Release 3.x およびそれよりも前のリリースでは、DCNM-SAN はインターフェイス トラップを受信し、EMC E-mail Home 電子メール メッセージを生成します。リンク トラップは、インターフェイスがアップからダウンに移行する場合、またはその逆の場合に生成され

ます。たとえば、サーバーのリブートがスケジュールされている場合、リンクがダウンし DCNM-SAN が電子メール通知を生成します。

Cisco NX-OS Release4.1(3) には、生成される電子メール メッセージの数を減らすために、遅延トラップを生成する機能が備わっています。この方法は、サーバーのリブートをフィルタし、無駄な EMC E-mail Home 電子メール メッセージの生成を回避します。NX-OS Release 4.1(3) では、ユーザは既存の機能か、もしくはこの新しい遅延トラップ機能を選択できます。

イベント トリガ

ここでは、Call Home のトリガー イベントについて説明します。トリガー イベントは複数のカテゴリにわかれており、各カテゴリには、イベントが発生したときに実行される CLI コマンドが割り当てられています。転送されるメッセージにはコマンド出力が含まれます。Table 8: イベント トリガ , on page 60 はトリガー イベントをリストしています。

Table 8: イベント トリガ

イベント	アラート グループ	イベント名	説明	Call Home メッセージ レベル
Call Home	システムおよび CISCO_TAC	SW_CRASH	ソフトウェア プロセスがステートレス再起動を伴ってクラッシュしました。サービスの中断を示します。	5
Call Home	システムおよび CISCO_TAC	CRASH_PROC	ソフトウェア プロセスがステートレス再起動を伴ってクラッシュしました。サービスの中断を示します。	5
Call Home	システムおよび CISCO_TAC	SW_SYSTEM_INCONSISTENT	ソフトウェアまたはファイル システムで不整合が検出されました。	5
Call Home	環境および CISCO_TAC	TEMPERATURE_ALARM	温度センサーが、温度が動作しきい値に達したことを示しています。	6
	環境および CISCO_TAC	POWER_SUPPLY_FAILURE	電源が障害になりました。	6
	環境および CISCO_TAC	FAN_FAILURE	冷却ファンが障害になりました。	5

イベント	アラート グループ	イベント名	説明	Call Home メッセージ レベル
Call Home	ラインカード ハードウェアおよび CISCO_TAC	LINECARD_FAILURE	ラインカード ハードウェアが障害になりました。	7
	ラインカード ハードウェアおよび CISCO_TAC	POWER_UP_DIAGNOSTICS_FAILURE	ラインカード ハードウェアの電源投入診断に失敗しました。	7
Call Home	ラインカード ハードウェアおよび CISCO_TAC	PORT_FAILURE	インターフェイス ポートのハードウェア障害。	6
Call Home	ラインカード ハードウェア、スーパーバイザ ハードウェア、および CISCO_TAC	BOOTFLASH_FAILURE	ブート コンパクト フラッシュ カードの障害。	6
Call Home	スーパーバイザ ハードウェアおよび CISCO_TAC	NVRAM_FAILURE	スーパーバイザ ハードウェア上の NVRAM のハードウェア障害。	6
Call Home	スーパーバイザ ハードウェアおよび CISCO_TAC	FREEDISK_FAILURE	スーパーバイザ ハードウェア上の空きディスク スペースがしきい値未満。	6
Call Home	スーパーバイザ ハードウェアおよび CISCO_TAC	SUP_FAILURE	スーパーバイザ ハードウェアの動作失敗。 **Note** アクティブなスーパーバイザが削除されると、スイッチオーバーが発生します。このイベントの Call Home 通知は送信されません。	7
		POWER_UP_DIAGNOSTICS_FAILURE	スーパーバイザ ハードウェアの電源投入診断に失敗しました。	7
Call Home	スーパーバイザ ハードウェアおよび CISCO_TAC	INBAND_FAILURE	インバンド通信パスの障害。	7

イベント	アラート グループ	イベント名	説明	Call Home メッセージ レベル
Call Home	スーパーバイザ ハードウェアおよび CISCO_TAC	EOBC_FAILURE	イーサネット アウトオブバンド チャネル通信障害。	6
Call Home	スーパーバイザ ハードウェアおよび CISCO_TAC	MGMT_PORT_FAILURE	管理イーサネット ポートのハードウェア障害。	5
	ライセンス	LICENSE_VIOLATION	使用中の機能のライセンスがなく、猶予期間の後にオフになります。	6
インベントリ	インベントリおよび CISCO_TAC	COLD_BOOT	スイッチの電源が投入され、コールド ブート シーケンスにリセットされます。	2
		HARDWARE_INSERTION	シャーシに新しいハードウェアが挿入されました。	2
		HARDWARE_REMOVAL	シャーシからハードウェアが除去されました。	2
テスト	テストおよび CISCO_TAC	TEST	ユーザがテストを生成しました。	2
ポート syslog	Syslog グループ ポート	SYSLOG_ALERT	ポート ファシリティに対応する syslog メッセージ。	2
RMON	RMON	RMON_ALERT	RMON アラート トリガー メッセージ。	2

Call Home メッセージ レベル

Table 9: イベント カテゴリと実行されるコマンド

[イベントカテゴリ（Event Category）]	説明	実行されるコマンド
システム show module show version show tech-support platform show tech-support sysmgr show hardware show sprom all	装置の動作に必要なソフトウェア システムの障害によって生成されたイベント。	**show tech-supportshow system redundancy status**
環境 show module show version show environment show logging logfile | tail -n 200	電源、ファン、温度アラームなどの環境センシング要素に関連するイベント。	**show moduleshow environment**
ラインカード ハードウェア show module show version show tech-support platform show tech-support sysmgr show hardware show sprom all	標準またはインテリジェント ラインカード ハードウェアに関連するイベント。	**show tech-support**
スーパーバイザ ハードウェア show module show version show tech-support platform show tech-support sysmgr show hardware show sprom all	スーパーバイザ モジュールに関連するイベント。	**show tech-support**

[イベントカテゴリ（Event Category）]	説明	実行されるコマンド
インベントリ show module show version show hardware show inventory show system uptime show sprom all show license usage	インベントリ ステータスは、ユニットがコールド ブートされる場合や、FRUが挿入または除去されたときに提供されます。これは、重大ではないイベントと見なされ、情報はステータスと資格設定に使用される	**show version**
テスト show module show version	ユーザがテスト メッセージを生成しました。	**show version**

Call Home メッセージ（syslog アラート グループに対して送信）には、Call Home メッセージ レベルにマッピングされた syslog 重大度があります（Syslog ベースのアラート, on page 56を参照）。

ここでは、Cisco MDS 9000 シリーズと Cisco Nexus 5000 シリーズのスイッチを 1 つ以上使用する場合の Call Home メッセージの重大度について説明します。Call Home メッセージ レベルは、イベント タイプごとに事前に割り当てられています。

重大度の範囲は 0 ～ 9 で、9 の緊急度が最も高くなっています。各 syslog レベルには、Table 10: 重大度と syslog レベルのマッピング , on page 64 に示すように、キーワードと対応する syslog レベルがあります。

Note Call Home は、メッセージ テキストで Syslog メッセージ レベルを変更しません。Call Home ログ内の syslog メッセージ テキストは、『*Cisco MDS 9000 Series System Messages* Reference』の記載どおりに出力されます。

Note Call Home のシビラティ（重大度）は、システム メッセージ ロギングのシビラティ（重大度）と同じではありません（『*Cisco MDS 9000 Series System Messages* Reference』を参照）。

Table 10: **重大度と *syslog* レベルのマッピング**

Call Home レベル	使用されるキーワード	Syslog レベル	説明
Catastrophic (9)	**Catastrophic**	該当なし	ネットワーク全体の破滅的な障害。

Call Home レベル	使用されるキーワード	Syslog レベル	説明
Disaster (8)	**Disaster**	該当なし	ネットワークに重大な影響が及びます。
Fatal (7)	**Fatal**	緊急（0）	システムが使用不可能な状態。
Critical (6)	**Critical**	アラート（1）	クリティカルな状態、ただちに注意が必要。
Major (5)	**Major**	重要（2）	重大な状態。
Minor (4)	**Minor**	エラー（3）	軽微な状態。
Warning (3)	**Warning**	警告（4）	警告状態。
Notify (2)	**Notification**	通知（5）	基本的な通知および情報メッセージです。他と関係しない、重要性の低い障害です。
Normal (1)	**Normal**	情報（6）	標準状態に戻ることを示す標準イベントです。
Debug (0)	**Debugging**	デバッグ（7）	デバッグ メッセージ。

メッセージの内容

スイッチ上で次の連絡先情報を設定できます。

- 連絡先担当者の名前
- 連絡先担当者の電話番号
- 連絡先担当者の電子メール アドレス
- 交換部品の送付先の住所（必要な場合）
- サイトが展開されているネットワークのサイト ID
- お客様とサービス プロバイダーの間のサービス契約を識別するコンタクト ID

Table 11: ショート テキスト メッセージ , on page 66 に、すべてのメッセージ タイプのショート テキスト フォーマット オプションを示します。

Table 11: ショート テキスト メッセージ

データ項目	説明
デバイス ID	設定されたデバイス名
日時スタンプ	起動イベントのタイム スタンプ
エラー判別メッセージ	起動イベントの簡単な説明（英語）
アラームの緊急度	エラー レベル（システム メッセージに適用されるエラー レベルなど）

Table 12: 対処的イベント メッセージ フォーマット , on page 66、Table 13: インベントリ エラー メッセージのフォーマット , on page 69、およびTable 14: ユーザが生成したテスト メッセージのフォーマット , on page 72 に、プレーンテキスト メッセージおよび XML メッセージに含まれる情報を示します。

Table 12: 対処的イベント メッセージ フォーマット

データ項目（プレーンテキストおよび XML）	説明（プレーンテキストと XML）	XML タグ（XML に限る）
タイム スタンプ	ISO 時刻表記によるイベントの日付とタイムスタンプ： *YYYY-MM-DDTHH:MM:SS*。 **Note** UTC からの時間帯または夏時間（DST）オフセットは、すでに適用済みです。T は、ハードコードされた時刻の区切りです。	/mml/header/time - ch:EventTime
メッセージ名	メッセージの名前。具体的なイベント名のリストはイベント トリガ, on page 60に示されています。	/mml/header/name
メッセージ タイプ	「Call Home」を指定。	/mml/header/type - ch:Type
メッセージ グループ	「reactive」を指定。	/mml/header/group
重大度	メッセージの重大度（Table 10: 重大度と syslog レベルのマッピング , on page 64 を参照）。	/mml/header/level - aml-block:Severity
送信元 ID	ルーティングのための製品タイプ	/mml/header/source - ch:Series

データ項目（プレーンテキストおよび XML）	説明（プレーンテキストと XML）	XML タグ（XML に限る）
デバイス ID	メッセージを生成するエンド デバイスの Unique Device Identifier（UDI）。メッセージがファブリック スイッチ専用でない場合、このフィールドは空白になります。フォーマットは、*type@Sid@serial* です。各項目の意味は次のとおりです。 • *type* は、バックプレーン SEEPROM から取得した製品モデル番号です。 • **@** 区切り文字です。 • *Sid* は C で、シリアル ID をシャーシ シリアル番号として特定します。 • *serial* は、Sid フィールドによって識別される番号です。 例：DS-C9509@C@12345678	/mml/ header/deviceId
カスタマー ID	任意のサポート サービスによって、連絡先情報またはその他の ID に使用される、オプションのユーザ設定可能フィールド。	/mml/header/customerID - ch:CustomerId
連絡先 ID	任意のサポート サービスによって、連絡先情報またはその他の ID に使用される、オプションのユーザ設定可能フィールド。	/mml/header/contractId - ch:ContractId>
サイト ID	シスコが提供したサイト ID または別のサポート サービスにとって意味のあるその他のデータに使用されるオプションのユーザ設定可能なフィールド	/mml/header/siterId - ch:SiteId

データ項目（プレーンテキストおよび **XML**）	説明（プレーンテキストと **XML**）	**XML** タグ（**XML** に限る）
Server ID	メッセージがファブリック スイッチから生成される場合、そのスイッチの Unique Device Identifier（UDI）。 フォーマットは、*type@Sid@serial* です。各項目の意味は次のとおりです。 • *type* は、バックプレーン SEEPROM から取得した製品モデル番号です。 • **@** 区切り文字です。 • *Sid* は C で、シリアル ID をシャーシ シリアル番号として特定します。 • *serial* は、Sid フィールドによって識別される番号です。 例：DS-C9509@C@12345678	/mml/header/serverId - -blank-
メッセージの説明	エラーを説明する短い文章。	/mml/body/msgDesc - ch:MessageDescription
装置名	イベントが発生するノード。これは、デバイスのホスト名です。	/mml/body/sysName - ch:SystemInfo/Name
担当者名	イベント発生中のノードに関する問題の問い合わせ先の担当者名。	/mml/body/sysContact - ch:SystemInfo/Contact
[連絡先電子メール（Contact email）]	このユニットの連絡先である人物の電子メールアドレス。	/mml/body/sysContacte-mail - ch:SystemInfo/Contact email
連絡先電話番号	このユニットの連絡先である人物の電話番号	/mml/body/sysContactPhoneNumber - ch:SystemInfo/ContactPhoneNumber
住所	このユニットに関連した RMA 部品の送付先住所を格納しているオプションのフィールド。	/mml/body/sysStreetAddress - ch:SystemInfo/StreetAddress
モデル名	スイッチのモデル名。製品シリーズ名の一部である固有モデルです。	/mml/body/chassis/name - rme:Chassis/Model
シリアル番号	ユニットのシャーシのシリアル番号	/mml/body/chassis/serialNo - rme:Chassis/SerialNumber
シャーシの部品番号	シャーシの最上アセンブリ番号	/mml/body/fru/partNo - rme:chassis/Card/PartNumber
シャーシのハードウェア バージョン	シャーシのハードウェア バージョン。	/mml/body/chassis/hwVersion - rme:Chassis/HardwareVersion

データ項目（プレーンテキストおよび XML）	説明（プレーンテキストと XML）	XML タグ（XML に限る）
スーパーバイザモジュールのソフトウェア バージョン	トップ レベル ソフトウェア バージョン。	/mml/body/fru/swVersion - rme:chassis/Card/SoftwareIdentity
影響のある FRU の名前	イベント メッセージを生成する、影響のある FRU の名前。	/mml/body/fru/name - rme:chassis/Card/Model
影響のある FRU のシリアル番号	影響のある FRU のシリアル番号。	/mml/body/fru/serialNo - rme:chassis/Card/SerialNumber
影響のある FRU の製品番号	影響のある FRU の製品番号。	/mml/body/fru/partNo - rme:chassis/Card/PartNumber
FRU スロット	イベント メッセージを生成している FRU のスロット番号。	/mml/body/fru/slot - rme:chassis/Card/LocationWithinContainer
FRU ハードウェア バージョン	影響のある FRU のハードウェア バージョン。	/mml/body/fru/hwVersion - rme:chassis/Card/SoftwareIdentity
FRU ソフトウェア バージョン	影響のある FRU 上で動作しているソフトウェア バージョン。	/mml/body/fru/swVersion - rme:chassis/Card/SoftwareIdentity
Command output name	実行されたコマンドの正確な名前。	/mml/attachments/attachment/name - aml-block:Attachment/Name
添付ファイルの種類	コマンド出力を指定します。	/mml/attachments/attachment/type - aml-block:Attachment type
MIME タイプ	通常は、テキスト、プレーン、符号化タイプのいずれか。	/mml/attachments/attachment/mime - aml-block:Attachment/Data encoding
コマンド出力テキスト	自動的に実行されるコマンドの出力 Table 9: イベント カテゴリと実行されるコマンド , on page 63）。	/mml/attachments/attachment/atdata - aml-block:Attachment/Data

Table 13: インベントリ エラー メッセージのフォーマット

データ項目（プレーンテキストと XML）	説明（プレーンテキストと XML）	XML タグ（XMLのみ）
タイム スタンプ	ISO 時刻表記によるイベントの日付とタイムスタンプ： *YYYY-MM-DDTHH:MM:SS*。 **Note** UTC からの時間帯または夏時間（DST）オフセットは、すでに適用済みです。T は、ハードコードされた時刻の区切りです。	/mml/header/time - ch:EventTime

データ項目（プレーンテキストと XML）	説明（プレーンテキストと XML）	XML タグ（XMLのみ）
メッセージ名	メッセージの名前。「Inventory Update」となります。具体的なイベント名については、イベント トリガ, on page 60を参照してください。	/mml/header/name
メッセージ タイプ	具体的には「インベントリの更新」。	/mml/header/type - ch-inv:Type
メッセージ グループ	具体的には「proactive」。	/mml/header/group
重大度	インベントリ イベントの重大度はレベル2です（Table 10: 重大度と syslog レベルのマッピング , on page 64を参照）。	/mml/header/level - aml-block:Severity
送信元 ID	シスコでのルーティングのための製品タイプ。具体的には「MDS 9000」。	/mml/header/source - ch-inv:Series
デバイス ID	メッセージを生成するエンドデバイスの Unique Device Identifier（UDI）。メッセージがファブリック スイッチ専用でない場合、このフィールドは空白になります。フォーマットは、*type@Sid@serial* です。各項目の意味は次のとおりです。 • *type* は、バックプレーン SEEPROM から取得した製品モデル番号です。 • **@** 区切り文字です。 • *Sid* は C で、シリアル ID をシャーシ シリアル番号として特定します。 • *serial* は、Sid フィールドによって識別される番号です。 例：DS-C9509@C@12345678	/mml/ header /deviceId
カスタマー ID	任意のサポート サービスによって、連絡先情報またはその他の ID に使用される、オプションのユーザ設定可能フィールド。	/mml/header/customerID - ch-inv:CustomerId
連絡先 ID	任意のサポート サービスによって、連絡先情報またはその他の ID に使用される、オプションのユーザ設定可能フィールド。	/mml/header/contractId - ch-inv:ContractId>
サイト ID	シスコが提供するサイト ID で使用されるオプションのユーザ設定可能フィールドか、他のサポート サービスにとって意味のあるその他のデータ。	/mml/header/siterId - ch-inv:SiteId

データ項目（プレーンテキストと XML）	説明（プレーンテキストと XML）	XML タグ（XMLのみ）
Server ID	メッセージがファブリック スイッチから生成される場合、そのスイッチの Unique Device Identifier（UDI）。 フォーマットは、*type@Sid@serial* です。各項目の意味は次のとおりです。 • *type* は、バックプレーン SEEPROM から取得した製品モデル番号です。 • **@** 区切り文字です。 • *Sid* は C で、シリアル ID をシャーシ シリアル番号として特定します。 • *serial* は、Sid フィールドによって識別される番号です。 例：DS-C9509@C@12345678	/mml/header/serverId - -blank-
メッセージの説明	エラーを説明する短い文章。	/mml/body/msgDesc - ch-inv:MessageDescription
デバイス名	イベントが発生するノード。	/mml/body/sysName - ch-inv:SystemInfo/Name
担当者名	イベント発生中のノードに関する問題の問い合わせ先の担当者名。	/mml/body/sysContact - ch-inv:SystemInfo/Contact
[連絡先電子メール（Contact email）]	このユニットの連絡先である人物の電子メール アドレス。	/mml/body/sysContacte-mail - ch-inv:SystemInfo/Contact email
連絡先電話番号	このユニットの連絡先である人物の電話番号	/mml/body/sysContactPhoneNumber - ch-inv:SystemInfo/ContactPhoneNumber
住所	このユニットに関連した RMA 部品の送付先住所を格納しているオプションのフィールド。	/mml/body/sysStreetAddress - ch-inv:SystemInfo/StreetAddress
モデル名	ユニットのモデル名。製品シリーズ名の一部である固有モデルです。	/mml/body/chassis/name - rme:Chassis/Model
シリアル番号	ユニットのシャーシのシリアル番号	/mml/body/chassis/serialNo - rme:Chassis/SerialNumber
シャーシの部品番号	シャーシの最上アセンブリ番号	/mml/body/fru/partNo - rme:chassis/Card/PartNumber
シャーシのハードウェア バージョン	シャーシのハードウェア バージョン。	/mml/body/fru/hwVersion - rme:chassis/Card/SoftwareIdentity

データ項目（プレーンテキストと XML）	説明（プレーンテキストと XML）	XML タグ（XMLのみ）
スーパーバイザ モジュールのソフトウェア バージョン	トップ レベル ソフトウェア バージョン。	/mml/body/fru/swVersion - rme:chassis/Card/SoftwareIdentity
FRU name	イベント メッセージを生成する、影響のある FRU の名前。	/mml/body/fru/name - rme:chassis/Card/Model
FRU s/n	FRU のシリアル番号。	/mml/body/fru/serialNo - rme:chassis/Card/SerialNumber
FRU 製品番号	FRU の製品番号。	/mml/body/fru/partNo - rme:chassis/Card/PartNumber
FRU スロット	FRU のスロット番号。	/mml/body/fru/slot - rme:chassis/Card/LocationWithinContainer
FRU ハードウェア バージョン	FRU のハードウェア バージョン。	/mml/body/fru/hwVersion - rme:chassis/Card/SoftwareIdentity
FRU ソフトウェア バージョン	FRU 上で動作しているソフトウェア バージョン。	/mml/body/fru/swVersion - rme:chassis/Card/SoftwareIdentity
Command output name	実行されたコマンドの正確な名前。	/mml/attachments/attachment/name - aml-block:Attachment/Name
添付ファイルの種類	コマンド出力を指定します。	/mml/attachments/attachment/type - aml-block:Attachment type
MIME タイプ	通常は、テキスト、プレーン、符号化タイプのいずれか。	/mml/attachments/attachment/mime - aml-block:Attachment/Data encoding
コマンド出力テキスト	イベント カテゴリに従って自動的に実行されるコマンドの出力（イベント トリガ, on page 60を参照）。	/mml/attachments/attachment/atdata - aml-block:Attachment/Data

Table 14: ユーザが生成したテスト メッセージのフォーマット

データ項目（プレーンテキストおよびXML）	説明（プレーンテキストと XML）	XML タグ（XMLのみ）
タイム スタンプ	ISO 時刻表記によるイベントの日付とタイムスタンプ：*YYYY-MM-DDTHH:MM:SS*。 **Note** UTCからの時間帯または夏時間（DST）オフセットは、すでに適用済みです。Tは、ハードコードされた時刻の区切りです。	/mml/header/time - ch:EventTime

データ項目（プレーンテキストおよびXML）	説明（プレーンテキストと XML）	XML タグ（XMLのみ）
メッセージ名	メッセージの名前。特に、テストタイプメッセージのテストメッセージ。具体的なイベント名については、イベントトリガ, on page 60を参照してください。	/mml/header/name
メッセージ タイプ	具体的には「Test Call Home」。	/mml/header/type - ch:Type
メッセージ グループ	このフィールドは、受信側の Call Home プロセス アプリケーションによって無視されますが、「proactive」または「reactive」を入力できます。	/mml/header/group
重大度	メッセージ、テスト Call Home メッセージの重大度（Table 10: 重大度と syslog レベルのマッピング , on page 64 を参照）。	/mml/header/level - aml-block:Severity
送信元 ID	ルーティングのための製品タイプ	/mml/header/source - ch:Series
デバイス ID	メッセージを生成するエンド デバイスの Unique Device Identifier（UDI）。メッセージがファブリック スイッチに固有のものでない場合、このフィールドは空です。フォーマットは、 *type@Sid@serial* です。各項目の意味は次のとおりです。 • *type* は、バックプレーン SEEPROM から取得した製品モデル番号です。 • @ は区切り文字です。 • *Sid* は C で、シリアル ID をシャーシ シリアル番号として特定します。 • *serial* は、Sid フィールドによって識別される番号です。 例：DS-C9509@C@12345678	/mml/ header /deviceId
カスタマー ID	任意のサポート サービスによって、連絡先情報またはその他の ID に使用される、オプションのユーザ設定可能フィールド。	/mml/header/customerID - ch:CustomerId
連絡先 ID	任意のサポート サービスによって、連絡先情報またはその他の ID に使用される、オプションのユーザ設定可能フィールド。	/mml/header/contractId - ch:ContractId
サイト ID	シスコが提供したサイト ID または別のサポート サービスにとって意味のあるその他のデータに使用されるオプションのユーザ設定可能なフィールド	/mml/header/siterId - ch:SiteId

データ項目（プレーンテキストおよびXML）	説明（プレーンテキストと XML）	XML タグ（XMLのみ）
Server ID	メッセージがファブリック スイッチから生成される場合、そのスイッチの Unique Device Identifier（UDI）。 フォーマットは、 *type@Sid@serial* です。各項目の意味は次のとおりです。 • *type* は、バックプレーン SEEPROM から取得した製品モデル番号です。 • @ は区切り文字です。 • *Sid* は C で、シリアル ID をシャーシ シリアル番号として特定します。 • *serial* は、Sid フィールドによって識別される番号です。 例：DS-C9509@C@12345678	/mml/header/serverId - -blank-
メッセージの説明	エラーを説明する短い文章。	/mml/body/msgDesc - ch:MessageDescription
装置名	イベントが発生したスイッチ。	/mml/body/sysName - ch:SystemInfo/Name
担当者名	イベント発生中のノードに関する問題の問い合わせ先の担当者名。	/mml/body/sysContact - ch:SystemInfo/Contact
[連絡先電子メール（Contact email）]	このユニットの連絡先である人物の電子メール アドレス。	/mml/body/sysContacte-mail - ch:SystemInfo/Contact email
連絡先電話番号	このユニットの連絡先である人物の電話番号	/mml/body/sysContactPhoneNumber - ch:SystemInfo/ContactPhoneNumber
住所	このユニットに関連した RMA 部品の送付先住所を格納しているオプションのフィールド。	/mml/body/sysStreetAddress - ch:SystemInfo/StreetAddress
モデル名	スイッチのモデル名。製品シリーズ名の一部である固有モデルです。	/mml/body/chassis/name - rme:Chassis/Model
シリアル番号	ユニットのシャーシのシリアル番号	/mml/body/chassis/serialNo - rme:Chassis/SerialNumber
シャーシの部品番号	シャーシの最上アセンブリ番号例：800-xxx-xxxx	/mml/body/fru/partNo - rme:chassis/Card/PartNumber
コマンド出力テキスト	イベント カテゴリに従って自動的に実行されるコマンドの出力（Table 9: イベント カテゴリと実行されるコマンド, on page 63 を参照）。	/mml/attachments/attachment/atdata - aml-block:Attachment/Data

データ項目（プレーンテキストおよびXML）	説明（プレーンテキストと XML）	XML タグ（XMLのみ）
MIME タイプ	通常は、テキスト、プレーン、符号化タイプのいずれか。	/mml/attachments/attachment/mime - aml-block:Attachment/Data encoding
添付ファイルの種類	コマンド出力を指定します。	/mml/attachments/attachment/type - aml-block:Attachment type
Command output name	実行されたコマンドの正確な名前。	/mml/attachments/attachment/name - aml-block:Attachment/Name

注意事項と制約事項

Call Home データベースのマージに関する注意事項

2 つの Call Home データベースをマージする場合は、次の注意事項に従ってください。

- マージされたデータベースには次の情報が格納されることに注意してください。
  - マージプロトコルに参加する、上位スイッチと下位スイッチのすべての宛先プロファイルのスーパーセット。
  - 接続先プロファイルの電子メール アドレスとアラート グループ。
  - マージ前に上位スイッチ内に存在した、スイッチからのその他の設定情報（メッセージ スロットリング、定期的インベントリなど）。

概念の詳細については、CFS マージのサポート, on page 12を参照してください。

Call Home の設定に関する注意事項

Call Home を設定する場合は、次の注意事項に従ってください。

- 電子メール サーバーと少なくとも 1 つの接続先プロファイル（事前定義またはユーザ定義）が構成されている必要があります。使用する接続先プロファイルは、受信エンティティがポケットベル、電子メール、Cisco Smart Call Home のような自動サービスのいずれであるかによって異なります。
- スイッチは、イベント（SNMP トラップ/インフォーム）を、最大 10 件の宛先に転送できます。
- Call Home をイネーブルにする前に、連絡先名（SNMP サーバの連絡先）、電話、住所の情報を設定する必要があります。この設定は、受信したメッセージの送信元を特定するために必要です。

- Cisco MDS 9000 シリーズ スイッチと Cisco Nexus 5000 シリーズ スイッチは、電子メール サーバーへの IP 接続が確立されている必要があります。
- Cisco Smart Call Home を使用する場合、設定しようとしているデバイスが、アクティブ サービス契約の対象になっている必要があります。

デフォルト設定

Table 15: Call Home のデフォルト設定 , on page 76 に Call Home のデフォルト設定の一覧を示します。

***Table 15: Call Home* のデフォルト設定**

パラメータ	デフォルト
フル テキスト形式で送信されるメッセージの宛先メッセージ サイズ。	500,000
XML 形式で送信されるメッセージの宛先メッセージ サイズ。	500,000
ショートテキスト形式で送信されるメッセージの宛先メッセージ サイズ。	4000
ポートが指定されていない場合にサーバに到達するための、SMTP サーバの DNS または IP アドレス	25
プロファイルとのアラート グループの関連付け	すべて
形式タイプ	XML
Call Home メッセージ レベル。	0（ゼロ）
HTTP プロキシ サーバの使用。	ディセーブルであり、プロキシ サーバは設定されていません。
HTTP プロキシ サーバのフル テキストの宛先のメッセージ サイズ。	1 MB
HTTP プロキシ サーバの XML のメッセージ サイズ。	1 MB

Call Home の設定

Call Home を設定するためのタスク フロー

次の手順を実行して、Call Home を設定します。

手順

ステップ 1 連絡先情報を設定します。

ステップ 2 Call Home をイネーブルまたはディセーブルにします。

ステップ 3 宛先プロファイルを設定します。

ステップ 4 ネットワークの必要性に応じて、1 つ以上のアラート グループを各プロファイルに関連付けます。必要に応じてアラート グループをカスタマイズします。

ステップ 5 電子メール オプションを構成します。

ステップ 6 Call Home メッセージをテストします。

連絡先情報の設定

スイッチプライオリティは、ファブリック内の各スイッチ固有です。このプライオリティは、運用要員または TAC サポート要員によって、最初に対処すべき Call Home メッセージを決定するために使用されます。各スイッチから送信される重大度が同じ Call Home アラートに優先順位を設定できます。

連絡先情報を割り当てるには、次の手順を実行します。

始める前に

各スイッチには、電子メール、電話、住所の情報が含まれている必要があります。オプションで、コンタクト ID、カスタマー ID、スイッチ プライオリティ情報を含めることができます。

手順

ステップ 1 次の構成モードを入力します。

switch# **configure terminal**

ステップ 2 SNMP コンタクト名を構成します。

switch(config)# **snmp-server contact personname@companyname.com**

ステップ 3 Call Home 構成サブモードに入ります。

switch(config)# **callhome**

switch(config-callhome)#

ステップ 4 お客様の電子メール アドレスを割り当てます。最大 128 文字の英数字を電子メール アドレス フォーマットで指定できます。

switch(config-callhome)# **email-contact username@company.com**

（注）
任意の有効な電子メール アドレスを使用できます。スペースは使用できません。

ステップ 5 お客様の電話番号を割り当てます。最大20文字の英数字を国際フォーマットで指定できます。

switch(config-callhome)# **phone-contact +1-800-123-4567**

（注）
スペースは使用できません。数字の前に、必ず + プレフィックスを使用してください。

ステップ 6 機器が設置されているお客様の所在地住所を割り当てます。最大 256 文字の英数字をフリー フォーマットで指定できます。

switch(config-callhome)# **streetaddress 1234 Picaboo Street, Any city, Any state, 12345**

ステップ 7 スイッチの優先順位を割り当てます。0 が最高の優先順位、7 が最低です。

switch(config-callhome)# **switch-priority 0**

ヒント
このフィールドを使用して、階層型の管理構造を作成します。

ステップ 8 （任意） お客様 ID を特定します。

switch(config-callhome)# **customer-id Customer1234**

最大 256 文字の英数字をフリー フォーマットで指定できます。

ステップ 9 （任意） お客様サイト ID を特定します。

switch(config-callhome)# **site-id Site1ManhattanNY**

最大 256 文字の英数字をフリー フォーマットで指定できます。

ステップ 10 スイッチのお客様 ID を割り当てます。

switch(config-callhome)# **contract-id Company1234**

最大 64 文字の英数字をフリー フォーマットで指定できます。

DCNM-SAN を使用したコンタクト情報の構成

DCNM-SAN を使用してコンタクト情報を割り当てるには、次の手順を実行します。

手順

ステップ 1 [物理属性（Physical Attributes）] ペインで **[イベント（Events）]** を展開し、**[Call Home]** を選択します。

[Information] ペインに [Call Home] タブが表示されます。

ステップ 2 Device Manager で、**[管理（Admin）]** > **[イベント（Events）]** > **[Call Home]** の順にクリックします。

ステップ 3 **[全般（General）]** タブをクリックし、コンタクト情報を割り当てて Call Home 機能を有効にします。Call Home はデフォルトではイネーブルになっていません。Call Home 通知の送信元を識別する電子メール アドレスを入力する必要があります。

ステップ 4 **[接続先（Destination(s)）]** タブをクリックし、Call Home 通知の接続先電子メール アドレスを構成します。Call Home 通知を受信する電子メール アドレスを 1 つ以上設定できます。

（注）
スイッチは、イベント（SNMP トラップ/インフォーム）を、最大 10 件の宛先に転送できます。

1. **[作成（Create）]** タブをクリックして、新しい接続先を作成します。[create destination] ウィンドウが表示されます。
2. 宛先のプロファイル名、ID、およびタイプを入力します。[Type] フィールドでは、[email] または [http] を選択できます。

   [email] を選択した場合、[EmailAddress] フィールドに電子メール アドレスを入力します。[HttpUrl] フィールドはディセーブルになります。

   [http] を選択した場合、[HttpUrl] フィールドに HTTP URL を入力します。[EmailAddress] フィールドはディセーブルになります。
3. **[作成（Create）]** をクリックして、接続先プロファイルの作成を完了します。

ステップ 5 **[電子メールのセットアップ（e-mail Setup）]** タブをクリックし、SMTP サーバを設定します。スイッチがアクセスできるメッセージ サーバを設定します。このメッセージ サーバは、Call Home 通知を宛先に転送します。

ステップ 6 DCNM-SAN で、**[変更の適用（Apply Changes）]** アイコンをクリックします。Device Manager で、**[適用（Apply）]** をクリックします。

Call Home 機能のイネーブル化

連絡先情報を設定したら、Call Home 機能をイネーブルにする必要があります。

Call Home 機能をイネーブルにするには、次の手順を実行します。

手順

ステップ 1 次の構成モードを入力します。

switch# **configure terminal**

ステップ 2 Call Home 構成サブモードに入ります。

switch(config)# **callhome**

ステップ 3 Call Home 機能の有効化

switch(config-callhome)# **enable**

Call Home が正常に有効になりました

ステップ 4 （任意） Call Home 機能の無効化

switch(config-callhome)# **disable**

（注）
Call Home が無効になっている場合でも、各 Call Home イベントの基本情報が送信されます。

Call Home 機能を無効にすると、すべての入力イベントが無視されます。

DCNM-SAN を使用した Call Home 機能の有効化

DCNM-SAN を使用して Call Home 機能を有効化するには、次の手順を実行します。

手順

ステップ 1 [Fabric] ペインでスイッチを選択します。

ステップ 2 [物理属性（Physical Attributes）] ペインで **[イベント（Events）]** を展開し、**[Call Home]** を選択します。

[Information] ペインに、Call Home 情報が表示されます。

ステップ 3 **[制御（Control）]** タブをクリックします。

ステップ 4 [information] ペインでスイッチを選択します。

ステップ 5 **[重複メッセージ スロットル（Duplicate Message Throttle）]** チェックボックスをオンにします。

ステップ 6 **[変更の適用（Apply Changes）]** アイコンをクリックします。

宛先プロファイルの設定

宛先プロファイルには、アラート通知に必要な配信情報が入っています。宛先プロファイルは、一般にネットワーク管理者によって設定されます。次の属性を宛先プロファイルに設定できます。

- プロファイル名：各ユーザ定義宛先プロファイルを一意に識別する文字列で、最大 32 文字の英数字で指定します。ユーザ定義の宛先プロファイルのフォーマット オプションは、フル テキスト、ショート テキスト、XML（デフォルト）のいずれかです。
- 宛先アドレス：アラートの送信先となる実際のアドレス（トランスポート メカニズムに関係します）。
- メッセージ フォーマット：アラート送信に使用されるメッセージ フォーマット（フル テキスト、ショート テキスト、または XML）。

（注） Cisco Smart Call Home サービスを使用する場合、XML 接続先プロファイルは必須です。

定義済みの宛先プロファイルのメッセージング オプションを設定するには、次の手順を実行します。

（注） この手順のステップ 3、4、および 5 は、スキップするか、任意の順序で構成できます。

始める前に

少なくとも 1 つの宛先プロファイルが必要です。1 つまたは複数のタイプの複数の宛先プロファイルを設定できます。事前に定義された宛先プロファイルのいずれかを使用するか、目的のプロファイルを定義できます。新しいプロファイルを定義する場合、プロファイル名を割り当てる必要があります。

手順

ステップ 1 次の構成モードを入力します。

switch# **configure terminal**

ステップ 2 Call Home 構成サブモードに入ります。

switch(config)# **callhome**

switch(config-callhome)#

ステップ 3 事前定義されたフルテキストの接続先プロファイルの電子メール アドレス、または接続先メッセージの最大サイズを構成します。

switch(config-callhome)# **destination-profile full-txt-destination** {**email-addr** *email-address* | **message-size** *msg-size-in-bytes*}

この接続先プロファイルの電子メールアドレスはフルテキストのフォーマットでメッセージを受信します。フルテキストのフォーマットでは、障害についての完全で詳細な説明が提供されます。

ヒント
テキスト サイズの制限がない標準電子メール アドレスを使用します。

有効な範囲は 0 ～ 1,000,000 バイトです。デフォルトは 500,000 です。値 0 は、任意のサイズのメッセージを送信できることを意味します。

（注）
メッセージ内の個々の添付ファイルの最大サイズは 250,000 バイトです。この最大サイズを超える添付ファイルがある場合、添付ファイルでキャプチャされた出力は切り捨てられます。

ステップ 4 事前定義されたショートテキストの接続先プロファイルの電子メールアドレス、または接続先メッセージの最大サイズを構成します。

switch(config-callhome)# **destination-profile short-txt-destination** {**email-addr** *email-address* | **message-size** *msg-size-in-bytes*}

この接続先プロファイルの電子メールアドレスはショートテキストのフォーマットでメッセージを受信します。このフォーマットは、Call Home メッセージの障害について基本的な説明を提供します。

ヒント
このオプションには、ポケットベル関連の電子メール アドレスを使用します。

有効な範囲は 0 ～ 1,000,000 バイトです。デフォルトは 4000 です。値 0 は、任意のサイズのメッセージを送信できることを意味します。

（注）
メッセージ内の個々の添付ファイルの最大サイズは 250,000 バイトです。この最大サイズを超える添付ファイルがある場合、添付ファイルでキャプチャされた出力は切り捨てられます。

ステップ 5 事前定義された XML 接続先プロファイルの電子メールアドレス、または接続先メッセージの最大サイズを構成します。

switch(config-callhome)# **destination-profile XML-destination** {**email-addr** *email-address* | **message-size** *msg-size-in-bytes*}

この接続先プロファイルの電子メール アドレスは XML フォーマットでメッセージを受信します。このフォーマットは、シスコ SYSTEMS の TAC サポートと互換性のある情報を提供します。

ヒント
メッセージ サイズが大きいため、この接続先プロファイルにポケットベル関連の電子メール アドレスを追加しないでください。

有効な範囲は 0 ～ 1,000,000 バイトです。デフォルトは 500,000 です。値 0 は、任意のサイズのメッセージを送信できることを意味します。

（注）
メッセージ内の個々の添付ファイルの最大サイズは 250,000 バイトです。この最大サイズを超える添付ファイルがある場合、添付ファイルでキャプチャされた出力は切り捨てられます。

DCNM-SAN を使用した事前定義済み接続先プロファイルの構成

DCNM-SAN を使用して定義済みの接続先プロファイルのメッセージング オプションを構成するには、次の手順を実行します。

手順

ステップ 1 **Events** を展開して、物理属性ペインで **Call Home** を選択します。

Profiles タブがクリックされるまで、**Destination** タブは無効になります。[Destination] タブに内容を設定するには、プロファイルをロードしておく必要があります。

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

複数のスイッチに対する Call Home プロファイルが表示されます。

ステップ 3 プロファイル名、メッセージ フォーマット、メッセージ サイズ、重大度を設定します。

ステップ 4 [Alert Groups] 列をクリックし、アラート グループを選択または削除します。

ステップ 5 **Apply Changes** アイコンをクリックして、選択したスイッチ上でこのプロファイルを作成します。

新規接続先プロファイルの構成

新しい宛先プロファイル（および関連するパラメータ）を設定するには、次の手順を実行します。

（注） この手順のステップ 4、5、および 6 は、スキップするか、任意の順序で構成できます。

手順

ステップ 1 次の構成モードを入力します。

switch# **configure terminal**

ステップ 2 Call Home 構成サブモードに入ります。

switch(config)# **callhome**

ステップ 3 test という新しい接続先プロファイルを構成します。

switch(config-callhome)# **destination-profile test**

ステップ 4 デフォルトの XML フォーマットで送信されるユーザ定義の接続先プロファイル（test）の電子メール アドレスを設定します。

switch(config-callhome)# **destination-profile test e-mail-addr** *email-address*

ステップ 5 デフォルトの XML 形式で送信されるユーザ定義の接続先プロファイル（test）の接続先電子メール アドレスの最大メッセージ サイズを構成します。

switch(config-callhome)# **destination-profile test message-size** *msg-size*

有効な範囲は 0 ～ 1,000,000 バイトです。デフォルトは 500,000 です。値 0 は、任意のサイズのメッセージを送信できることを意味します。

ステップ 6 ユーザ定義の接続先プロファイル（test）のメッセージフォーマットをフル テキストまたはショート テキスト フォーマットで構成します。

switch(config-callhome)# **destination-profile test format** {**full-txt** | **short-txt**}

DCNM-SAN を使用した新規接続先プロファイルの構成

DCNM-SAN を使用して新しい接続先プロファイル（および関連するパラメータ）を構成するには、次の手順を実行します。

手順

ステップ 1 **Events** を展開して、物理属性ペインで **Call Home** を選択します。

（注）
Profiles タブがクリックされるまで、**Destination** タブは無効になります。[Destination] タブに内容を設定するには、プロファイルをロードしておく必要があります。

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

複数のスイッチに対する Call Home プロファイルが表示されます。

ステップ 3 **Create Row** アイコンをクリックして新しいプロファイルを追加します。

ステップ 4 プロファイル名、メッセージ フォーマット、サイズ、重大度を設定します。

ステップ 5 アラート グループをクリックし、このプロファイルで送信する各グループを選択します。

ステップ 6 転送方式をクリックします。**email**、**http** または **emailandhttp** を選択できます。

ステップ 7 **Create** をクリックして、選択したスイッチ上でこのプロファイルを作成します。

アラート グループと宛先プロファイルのアソシエート

Call Home アラートはタイプごとに別のアラート グループにグループ化されます。ネットワークの必要性に応じて、1 つ以上のアラート グループを各プロファイルに関連付けることができます。

アラート グループ機能を使用することで、宛先プロファイル（定義済みまたはユーザ定義）が受信する Call Home アラートのセットを選択できます。複数のアラート グループを 1 つの宛先プロファイルに関連付けることができます。

アラート グループを宛先プロファイルに関連付けるには、次の手順を実行します。

始める前に

Call Home アラートが、接続先プロファイル内の電子メールの宛先に送信されるのは、その Call Home アラートが、その接続先プロファイルに関連付けられているいずれかのアラート グループに属する場合だけです。

手順

ステップ 1 次の構成モードを入力します。

switch# **configure terminal**

ステップ 2 Call Home 構成サブモードに入ります。

switch(config)# **callhome**

switch(config-callhome)#

ステップ 3 （任意） ユーザが生成したすべての Call Home テスト通知を受信するように、ユーザ定義の接続先プロファイル（test1）または事前定義されたショートテキストの接続先プロファイルを構成します。

switch(config-callhome)# **destination-profile** {*test1* | **short-txt-destination**} **alert-group** *test*

ステップ 4 （任意） すべてのイベントの Call Home 通知を受信するようにユーザ定義の接続先プロファイル（test1）を構成するか、デフォルト イベントの Call Home 通知を受信するように事前定義されたショート テキストの接続先プロファイルを構成します。

switch(config-callhome)# **destination-profile** {*test1* | **short-txt-destination**} **alert-group all**

ステップ 5 （任意） Cisco TAC または自動通知サービスのみを対象とするイベントの Call Home 通知を受信するように、ユーザ定義の接続先プロファイル（test1）または事前定義されたショートテキストの接続先プロファイルを構成します。

switch(config-callhome)# **destination-profile** {*test1* | **xml-destination**} **alert-group Cisco-TAC**

ステップ 6 （任意） ソフトウェア クラッシュ イベントの Call Home 通知を受信するように、ユーザ定義の接続先プロファイル（test1）または事前定義されたショートテキストの接続先プロファイルを構成します。

switch(config-callhome)# **destination-profile** {*test1* | **xml-destination**} **alert-group Crash**

ステップ 7 （任意） ユーザ定義の接続先プロファイル（test1）または事前定義されたショート テキストの接続先プロファイルを構成して、電源、ファン、および温度関連のイベントに関する Call Home 通知を受信します。

switch(config-callhome)# **destination-profile** {*test1* | **short-txt-destination**} **alert-group environmental**

ステップ 8 （任意） インベントリ ステータス イベントの Call Home 通知を受信するように、ユーザ定義の接続先プロファイル（test1）または事前定義されたショートテキストの接続先プロファイルを構成します。

switch(config-callhome)# **destination-profile** {*test1* | **short-txt-destination**} **alert-group inventory**

ステップ 9 （任意） ライセンス イベントの Call Home 通知を受信するように、ユーザ定義の接続先プロファイル（test1）または事前定義されたショート テキストの接続先プロファイルを構成します。

switch(config-callhome)# **destination-profile** {*test1* | **short-txt-destination**} **alert-group License**

ステップ 10 （任意） モジュール関連イベントの Call Home 通知を受信するように、ユーザ定義の接続先プロファイル（test1）または事前定義されたショートテキストの接続先プロファイルを構成します。

switch(config-callhome)# **destination-profile** {*test1* | **short-txt-destination**} **alert-group linecard-hardware**

ステップ 11 （任意） スーパーバイザ関連イベントの Call Home 通知を受信するように、ユーザ定義の接続先プロファイル（test1）または事前定義されたショートテキストの接続先プロファイルを構成します。

switch(config-callhome)# **destination-profile** {*test1* | **short-txt-destination**} **alert-group supervisor-hardware**

ステップ 12 （任意） ソフトウェア関連イベントの Call Home 通知を受信するように、ユーザ定義の接続先プロファイル（test1）または事前定義されたショートテキストの接続先プロファイルを構成します。

switch(config-callhome)# **destination-profile** {*test1* | **short-txt-destination**} **alert-group system**

DCNM-SAN を使用したアラート グループの関連付け

DCNM-SAN を使用してアラート グループを接続先プロファイルに関連付けるには、次の手順を実行します。

手順

ステップ 1 **Events** を展開して、物理属性ペインで **Call Home** を選択します。

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

複数のスイッチに対する Call Home プロファイルが表示されます。

ステップ 3 関連付けるプロファイルの行の **Alert Groups** カラムをクリックします。

[alert groups] ドロップダウン メニューが表示されます。

ステップ 4 関連付けるアラート グループをクリックして選択します。

ステップ 5 そのアラート グループの横にチェックが表示されます。

選択を解除してチェックを外すには、再度クリックします。

ステップ 6 **Apply Changes**アイコンをクリックします。

アラート グループ メッセージのカスタマイズ

アラートを送信するときに実行する show コマンドを割り当てるには、コマンドをアラート グループに割り当てる必要があります。アラートを送信する際、Call Home はアラート グループをアラート タイプに関連付け、show コマンドの出力をアラート メッセージに添付します。

（注） show コマンドが定義されているシスコ以外の TAC アラート グループに対する宛先プロファイルと、シスコ TAC アラート グループに対する宛先プロファイルが、同じでないことを確認してください。

Call Home アラート グループ メッセージをカスタマイズするには、次の手順を実行します。

始める前に

- 1 つのアラート グループには、最大 5 個のユーザー定義 show コマンドを割り当てることができます。アラート グループには show コマンドだけを割り当てることができます。
- カスタマイズされた show コマンドは、フルテキストおよび XML アラートのグループだけでサポートされます。ショート テキスト アラート グループ（short-txt-destination）では、テキストが 128 バイトに制限されるため、カスタマイズされた show コマンドはサポートされません。

手順

ステップ 1 次の構成モードを入力します。

switch# **configure terminal**

ステップ 2 Call Home 構成サブモードに入ります。

switch(config)# **callhome**

switch(config-callhome)#

ステップ 3 アラート グループ ライセンスの user-defined **show** コマンドを構成します。

switch(config-callhome)# **alert-group license user-def-cmd show license usage**

（注）
有効な **show** コマンドだけが受け入れられます。

ステップ 4 （任意） アラート グループからuser-defined **show** コマンドを削除します。

switch(config-callhome)# **no alert-group license user-def-cmd show license usage**

DCNM-SAN を使用したアラート グループ メッセージのカスタマイズ

DCNM SAN を使用して Call Home アラート グループ メッセージをカスタマイズするには、次の手順を実行します。

手順

ステップ 1 **Events** を展開して、物理属性ペインで **Call Home** を選択します。

ステップ 2 [情報（Information）] ペインで **User Defined Command** タブをクリックします。

ユーザ定義コマンドの情報が表示されます。

ステップ 3 **Create Row**アイコンをクリックします。

ステップ 4 受信するアラートの送信元となるスイッチの前にあるチェックボックスをオンにします。

ステップ 5 [Alert Group Type] ドロップダウン リストからアラート グループ タイプを選択します。

ステップ 6 CLI コマンドの ID（1 ～ 5）を選択します。ID は、メッセージを追跡するために使用します。

ステップ 7 CLI **show** コマンドを **CLI Command** フィールドに入力します。

ステップ 8 **Create** をクリックします。

ステップ 9 プロファイルに関連付ける各コマンドに対し、ステップ 3 ～ 7 を繰り返します。

ステップ 10 **Close** をクリックして、ダイアログボックスを閉じます。

Call Home メッセージ レベルの設定

Call Home の各宛先プロファイルに対してメッセージ レベルを設定するには、次の手順を実行します。

始める前に

緊急度の範囲は 0（最も緊急度が低い）から 9（最も緊急度が高い）であり、デフォルトは 0 です（すべてのメッセージが送信されます）。

手順

ステップ 1 次の構成モードを入力します。

switch# **configure terminal**

ステップ 2 Call Home 構成サブモードに入ります。

switch(config)# **callhome**

ステップ 3 （任意）ユーザ定義プロファイル（test1）のメッセージ レベルの緊急度を 5（level）以上に構成します。

switch(config-callhome)# **destination-profile** *test* **message-level** *level*

ステップ 4 以前に構成した緊急度レベルを削除し、デフォルトの 0 に戻します（すべてのメッセージが送信されます）。

switch(config-callhome)# **no destination-profile** *oldtest* **message-level** *level*

Syslog ベースのアラートの設定

syslog-group-port アラート グループを設定するには、次の手順を実行します。

手順

ステップ 1 次の構成モードを入力します。

switch# **configure terminal**

ステップ 2 Call Home 構成サブモードに入ります。

switch(config)# **callhome**

switch(config-callhome)#

ステップ 3 ポート ファシリティの syslog メッセージに対応する Call Home 通知を受信するように、定義済みの接続先プロファイル（short-txt-destination）を構成します。

switch(config-callhome)# **destination-profile short-txt-destination alert-group syslog-group-port**

ステップ 4 （任意） 定義済みの接続先プロファイル（short-txt-destination）を構成して、シビラティ（重大度）レベルが 5 以上の Call Home シビラティ（重大度）レベルに対応する syslog メッセージの Call Home メッセージを送信します。

switch(config-callhome)# **destination-profile** *short-txt-destination* **message-level** *level*

デフォルトはメッセージ レベル 0（すべての syslog メッセージ）です。

DCNM-SAN を使用した Syslog ベースのアラートの構成

DCNM-SAN を使用して syslog-group-port アラート グループを構成するには、次の手順を実行します。

手順

ステップ 1 [Fabric] ペインでスイッチを選択します。

ステップ 2 **Events** を展開して、物理属性ペインで **Call Home** を選択します。

[Information] ペインに、Call Home 情報が表示されます。

ステップ 3 [**Profiles**] タブをクリックします。

Call Home プロファイルが表示されます。

ステップ 4 **Create Row**アイコンをクリックします。

[Create Call Home Profile] ダイアログボックスが表示されます。

ステップ 5 アラートを送信するスイッチを選択します。

ステップ 6 プロファイル名を [Name] フィールドに入力します。

ステップ 7 メッセージ フォーマット、メッセージ サイズ、メッセージの重大度を選択します。

ステップ 8 [AlertGroups] セクションの **syslogGroupPort** チェックボックスをオンにします。

ステップ 9 **Create** をクリックして、syslog ベースのアラートのプロファイルを作成します。

ステップ 10 ダイアログボックスを閉じます。

RMON アラートの設定

RMON アラート グループを設定するには、次の手順を実行します。

手順

ステップ 1 次の構成モードを入力します。

switch# **config t**

ステップ 2 Call Home 構成サブモードに入ります。

switch(config)# **callhome**

ステップ 3 （任意） 構成された RMON メッセージの Call Home 通知を送信するように、接続先メッセージ プロファイル（rmon_group）を構成します。

switch(config-callhome)# **destination-profile**

DCNM-SAN を使用した RMON アラートの構成

DCNM-SAN を使用して RMON アラート グループを構成するには、次の手順を実行します。

手順

ステップ 1 [Fabric] ペインでスイッチを選択します。

ステップ 2 **Events** を展開して、物理属性ペインで **Call Home** を選択します。

[情報（Information）] ペインに、Call Home 情報が表示されます。

ステップ 3 [**Profiles**] タブをクリックします。

Call Home プロファイルが表示されます。

ステップ 4 **Create Row** アイコンをクリックします。

[Call Home プロファイルの作成（Create Call Home Profile）] ダイアログボックスが表示されます。

ステップ 5 アラートを送信するスイッチを選択します。

ステップ 6 プロファイル名を入力します。

ステップ 7 メッセージ フォーマット、メッセージ サイズ、メッセージの重大度を選択します。

ステップ 8 [AlertGroups] セクションの **RMON** チェックボックスをオンにします。

ステップ 9 **Create** をクリックして、RMON ベースのアラートのプロファイルを作成します。

ステップ 10 ダイアログボックスを閉じます。

イベント トラップ通知の構成

Call Homeイベント通知トラップ（Call Home定期メッセージを除く）を構成するには、次の手順を実行します。

手順

ステップ 1 次の構成モードを入力します。

switch# **configure terminal**

ステップ 2 Call Home 構成サブモードに入ります。

switch(config)# **callhome**

ステップ 3 Call Home の SNMP 通知トラップを有効にします。

switch(config-callhome)# **snmp-server enable traps callhome**

一般的な EMail オプションの構成

送信元、返信先、および受信確認の電子メールアドレスを構成できます。ほとんどの電子メール アドレス構成はオプションですが、Call Home 機能を使用するには、SMTP サーバーのアドレスを構成する必要があります。

一般的な電子メール オプションを構成するには、次の手順を実行します。

手順

ステップ 1 次の構成モードを入力します。

switch# **configure terminal**

ステップ 2 Call Home 構成サブモードに入ります。

switch(config)# **callhome**

ステップ 3 電子メール アドレスから構成します。

switch(config-callhome)#**transport email from** *person@company.com*

ステップ 4 すべての応答の送信先となる返信先電子メール アドレスを構成します。

switch(config-callhome)# person@company.com transport email reply-to

ステップ 5 SMTP サーバーの DNS、IPv4 アドレス、または IPv6 アドレスがサーバーに到達するように構成します。

switch(config-callhome)# **transport email smtp-server 192.168.1.1**

switch(config-callhome)# **transport email smtp-server 192.168.1.1 port 30**

指定されているポートがなければ、ポートの使用率はデフォルトで 25です。

（注）
ポート番号はオプションであり、必要に応じてサーバーの場所に応じて変更できます。

DCNM-SAN を使用した一般的なEMail オプションの構成

DCNM SAN を使用して一般的な電子メール オプションを構成するには、次の手順を実行します。

手順

ステップ 1 [Fabric] ペインでスイッチを選択します。

ステップ 2 **Events** を展開して、物理属性ペインで **Call Home** を選択します。

[情報（Information）] ペインに、Call Home 情報が表示されます。

ステップ 3 [**e-mail Setup**] タブをクリックします。

ステップ 4 [Information] ペインでスイッチを選択します。

ステップ 5 一般的な電子メール情報を入力します。

ステップ 6 SMTP サーバの IP アドレス タイプ、IP アドレスまたは名前、ポートを入力します。

ステップ 7 **Apply Changes** アイコンをクリックして、電子メール オプションを更新します。

HTTPS サポートの設定

事前定義またはユーザ定義の接続先プロファイルは、HTTPS URL アドレスを使用して構成できます。

接続先プロファイルの HTTPS URL アドレスを構成するには、次の手順に従います。

手順

ステップ 1 次の構成モードを入力します。

switch# **configure terminal**

ステップ 2 Call Home 構成サブモードに入ります。

switch(config)# **callhome**

ステップ 3 （任意） HTTPS URL アドレスを使用して、事前定義された full-txt-destination プロファイルを構成します。

switch(config-callhome)# **destination-profile full-txt-destination http**

完全なテキスト フォーマットの Call Home メッセージは、構成された HTTPS URL アドレスにアップロードされます。

ステップ 4 （任意） HTTPS URL アドレスを使用して、事前定義された CiscoTAC-1 プロファイルを構成します。

switch(config-callhome)# **destination-profile CiscoTAC-1 http**

XML フォーマットの Call Home メッセージは、構成された HTTPS URL アドレスにアップロードされます。

ステップ 5 （任意） HTTPS URL アドレスを使用して、ユーザ定義の接続先プロファイルを構成します。

switch(config-callhome)# **destination-profile test1 http**

構成されたフォーマットの Call Home メッセージは、構成された HTTPS URL アドレスにアップロードされます。

トランスポート メソッドの有効化または無効化

特定の転送方式を有効化または無効化するように、定義済みまたはユーザ定義の接続先プロファイルを構成できます。転送方式は HTTP および E メールです。

宛先プロファイルの転送方式をイネーブルまたはディセーブルにする手順は、次のとおりです。

手順

ステップ 1 次の構成モードを入力します。

switch# **configure terminal**

ステップ 2 Call Home 構成サブモードに入ります。

switch(config)# **callhome**

ステップ 3 （任意） 定義済みの接続先プロファイル CiscoTAC-1 を HTTP 転送メソッドに対して有効にします。

switch(config-callhome)# **destination-profile CiscoTAC-1 transport-method http**

（注）

ユーザ定義接続先ロファイルでは、電子メールがデフォルトです。片方または両方の転送メカニズムをイネーブルにできます。両方の方法を無効にすると、電子メールが有効になります。

ステップ 4 （任意） 定義済みの接続先プロファイル CiscoTAC-1 を 電子メール メソッドに対して無効にします。

switch(config-callhome)# **no destination-profile CiscoTAC-1 transport-method email**

ステップ 5 （任意） 定義済みのフルテキスト接続先プロファイルを HTTP 転送メソッドに対して有効にします。

switch(config-callhome)# **destination-profile full-txt transport-method http**

HTTP プロキシ サーバの設定

Cisco NX-OS Release 5.2 以降では、HTTP プロキシサーバーからの HTTP メッセージを送信するように、Smart Call Home を構成できます。HTTP プロキシサーバーを設定しない場合、Smart Call Home は、Cisco Transport Gateway（TG）に HTTP メッセージを直接送信します。

HTTP プロキシサーバーを設定するには、次の手順を実行します。

手順

ステップ 1 次の構成モードを入力します。

switch# **configure terminal**

ステップ 2 Call Home 構成サブモードに入ります。

switch(config)# **callhome**

ステップ 3 HTTP プロキシサーバーのドメインネームサーバー（DNS）の名前、IPv4 アドレス、または IPv6 アドレスを構成します。

switch(config-callhome)# **transport http proxy server 192.0.2.1**

任意でポート番号を設定します。ポート範囲は 1 ～ 65535 です。デフォルトのポート番号は 8080 です。

ステップ 4 Smart Call Home で、HTTP プロキシサーバー経由ですべての HTTP メッセージを送信できるようにします。

switch(config-callhome)# **transport http proxy enable**

（注）
プロキシ サーバ アドレスが設定された後にだけ、このコマンドを実行できます。

ステップ 5 （任意） Smart Call Home に対する転送関係の構成を表示します。

switch(config-callhome)# **show callhome transport**

（注）
フルテキストの宛先と XML のデフォルト値は 1 MB です。

DCNM-SAN を使用した HTTP プロキシサーバーの構成

DCNM-SAN を使用した Call Home HTTP プロキシサーバーを構成するには、次の手順を実行します。

手順

ステップ 1 [Fabric] ペインでスイッチを選択します。

ステップ 2 **Events** を展開して、物理属性ペインで **Call Home**、および **HTTP Proxy Server** を選択します。[情報（Information）] ペインに Call Home HTTP プロキシサーバーの情報が表示されます。

ステップ 3 [**Address Type**] タブをクリックします。
アドレス タイプのオプションが表示されます。

ステップ 4 **Address** タブをクリックし、HTTP プロキシサーバーのアドレスを入力します。

ステップ 5 **Port** タブをクリックし、整数値を入力して、HTTP プロキシサーバーのポートを指定します。

ステップ 6 **Enable** チェックボックスをオンにして、Call Home 用に構成された HTTP プロキシを有効にします。

ステップ 7 （任意） 空の値を **Address** タブに設定して、MDS スイッチから HTTP プロキシサーバーを削除します。

ステップ 8 アドレス タイプを選択します。[ipv4]、[ipv6]、または [DNS] を選択できます。

（注）
アドレスが空の場合、プロキシ サーバは設定されません。

ステップ 9 **Apply** をクリックして、HTTP プロキシサーバーのオプションを更新します。

Call Home ウィザードの設定

Call Home ウィザードを設定するためのタスク フロー

次の手順を実行して、Call Home ウィザードを設定します。

手順

ステップ 1 連絡先情報を設定します。
ステップ 2 SMTP 情報を設定します。
ステップ 3 電子メールの送信元と宛先の情報を設定します。
ステップ 4 CFS を使用して、設定データを読み込みます。
ステップ 5 ステータスを表示します。

Call Home ウィザードの起動

Call Home ウィザードを設定するには、次の手順を実行します。

始める前に

- DCNM-SAN 設定テーブルからスイッチ上のグローバル CFS をイネーブルにします。
- スイッチ上の CFS ロックをクリアします。
- スイッチ上の CFS のマージステータスを確認します。マージの失敗が検出されると、ウィザードは、実行中にバックエンド プロセスでマージの失敗を解決します。

手順

ステップ 1 論理ドメイン ツリー内のファブリックを選択します。
ステップ 2 **ToolsEvents** および **Call Home** を選択します。
[master switch] ペインが表示されます。
ステップ 3 （任意） Call Home の **Control** タブで **CallHome Wizard** アイコンをクリックして Call Home ウィザードを起動することもできます。
ステップ 4 **Master Switch** を選択して、**Next** をクリックします。
[contact information] ペインが表示されます。
ステップ 5 **Contact**、**Phone Number**、**Email Address** および **Street Address** 情報を入力します。

（注）
[Next] をクリックする前に、4 つのパラメータをすべて指定する必要があります。

ステップ 6 **Next** をクリックします。
[Email Setup] ペインが表示されます。
ステップ 7 **Email SMTP Servers** タブで、**Primary SNTP Server** アドレスを入力します。

マスター スイッチがバージョン 5.0 以上ならば、SMTP サーバを 2 台まで指定できます。マスター スイッチのバージョンが 5.0 未満の場合は、セカンダリ SMTP サーバを指定することはできません。

ウィザードは、SMTP サーバ テーブルに新しい行を作成します。

ステップ 8 **Destination** タブで、**Add** をクリックして Call Home 接続先を入力します。

Call Home 宛先は 3 つまで入力できます。

ステップ 9 （任意） **Remove** をクリックして Call Home 接続先のエントリを削除します。

ステップ 10 ドロップダウンリストから、**Protocol** および **Profile** を選択します。
[Profile] ドロップダウンには、[xml]、[short_txt]、および [full_txt] の 3 つのデフォルト プロファイルがリスト表示されます。

ステップ 11 **Finish** をクリックしてウィザードを構成します。

すべての重要な設定手順およびエラーが [Status Dialog] ウィンドウに表示されます。

Status Dialog ウィンドウが表示されます。

ステップ 12 **Run Test** をクリックして Call Home テストを実行します。

ステップ 13 **Yes** をクリックして選択したファブリック内のすべてのスイッチ上でコマンドをテストするか、**No** をクリックしてウィンドウを閉じます。

SMTP サーバーおよびポートの構成

SMTP サーバーおよびポートを構成するには、次の手順を実行します。

手順

ステップ 1 次の構成モードを入力します。

switch# **configure terminal**

ステップ 2 Call Home 構成サブモードに入ります。

switch(config)# **callhome**

ステップ 3 SMTP サーバーの DNS、IPv4 アドレス、または IPv6 アドレスがサーバーに到達するように構成します。

switch(config-callhome)# **transport email smtp-server 192.168.1.1**

switch(config-callhome)# **transport email smtp-server 192.168.1.1 port 30**

指定されているポートがなければ、ポートの使用率はデフォルトで 25です。

（注）

ポート番号はオプションで、必要に応じてサーバーの場所に応じて変更できます。

セキュアな電子メール アラートの構成

SMTP 接続認証、電子メール暗号化、および電子メール ユーザー認証は、MDS NX-OS リリース 9.4(3) からサポートされています。

セキュアな電子メールベースのアラートを構成するには、次の手順を実行します：

始める前に

電子メール認証と暗号化を設定する前に、スイッチのルート CA 証明書を構成する必要があります。詳細については、認証局およびデジタル証明書の構成章を参照してください。

手順

ステップ 1 次の構成モードを入力します。

```
switch# configure terminal
switch(config)#
```

ステップ 2 Smart Call Home 構成モードを開始します：

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

ステップ 3 （オプション）暗黙的な TLS（SMTPS）を使用して SMTP サーバーの TCP ポート 465 に送信されるアラートを構成します。

このポートを SMTPS に使用することは、IETF によって廃止されているため、推奨されません。

```
switch(config-callhome)# transport email smtp-server 10.1.1.174 port 465
```

ステップ 4 （オプション）SMTP および STARTTLS を使用して SMTP サーバーの TCP ポート 587 に送信されるアラートを構成します。

```
switch(config-callhome)# transport email smtp-server 10.1.1.174 port 587
```

25 および 465 以外のポートを構成すると、スイッチは SMTP サーバーへの接続で STARTTLS を使用します。

ステップ 5 （オプション）SMTP サーバーでの認証に使用するユーザー名とパスワードを構成します。

```
switch(config-callhome)# transport email username user1 passwd Y2FsbGhvbWUK encrypted
```

ユーザー名は英数字で、255 文字未満にする必要があります。パスワードオプションは、クリア テキストまたは base64 暗号フォーマットで入力できます（ユーザーが既に暗号化されたパスワードを持っている場合）。パスワードの長さは、クリア テキストで入力する場合は 64 文字未満、暗号化形式で入力する場合は 255 文字未満にする必要があります。

SMTP ユーザー認証はオプションです。SMTP サーバーがユーザー認証を行うように構成されていない場合は、この手順をスキップできます。その場合、電子メールの暗号化のみが実行され、ユーザー認証は行われません。

マルチ SMTP サーバー サポートの構成

マルチ SMTP サーバー サポートを構成するには、次の手順を実行します。

手順

ステップ 1 次の構成モードを入力します。

switch# **configure terminal**

ステップ 2 Call Home 構成サブモードに入ります。

switch(config)# **callhome**

ステップ 3 複数の SMTP サーバー機能を配布するには、次のコマンドを使用します：

switch(config-callhome)# [**no**] **transport email mail-server** {**ipv4** | **IPV6** | **hostname**} [**port** *number*] [**priority** *number*]

例

（注） **transport email mail-server** コマンドは、Cisco NX-OS リリース 5.0(1a) 以降を実行しているデバイスにのみ配布されます。**transport email smtp-server** コマンドは、以前のソフトウェア リリースを実行しているデバイスにのみ配布されます。

次の例は、複数の SMTP サーバーを Call Home メッセージに構成する方法を示しています。

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# callhome
switch(config-callhome)# transport email mail-server 192.0.2.10 priority 4
switch(config-callhome)# transport email mail-server 172.21.34.193
switch(config-callhome)# transport email smtp-server 10.1.1.174
switch(config-callhome)# transport email mail-server 64.72.101.213 priority 60
switch(config-callhome)# transport email from person@company.com
switch(config-callhome)# transport email reply-to person@company.com
```

上記の構成に基づいて、SMTP サーバーはこの順序で接続されます。

10.1.1.174（プライオリティ 0）

192.0.2.10（プライオリティ 4）

172.21.34.193（優先順位 50、デフォルト）

64.72.101.213（プライオリティ 60）

定期的なインベントリ通知のイネーブル化

間隔の値を設定せずにこの機能をイネーブルにすると、Call Home メッセージは 7 日間おきに送信されます。この値の範囲は、1 ～ 30 日間です。デフォルトでは、Cisco MDS 9000 シリーズと Cisco Nexus 5000 シリーズのすべてのスイッチにおいてこの機能は無効になっています。

Cisco MDS 9000 シリーズ スイッチまたは Cisco Nexus 5000 シリーズ スイッチで定期的なインベントリ通知を有効にするには、次の手順を実行します。

手順

ステップ 1 次の構成モードを入力します。

switch# **configure terminal**

ステップ 2 Call Home 構成サブモードに入ります。

switch(config)# **callhome**

ステップ 3 定期的なインベントリ通知機能の有効化

switch(config-callhome)# **periodic-inventory notification**

定期的なインベントリ通知機能の無効化（デフォルト）

switch(config-callhome)# **no periodic-inventory notification**

デフォルトでは、Call Home メッセージは 7 日ごとに送信されます。

ステップ 4 15 日ごとに送信される定期的なインベントリ通知メッセージを構成します。

switch(config-callhome)# **periodic-inventory notification interval 15**

デフォルトでは、7 日ごとに Call Home メッセージを送信する出荷時のデフォルトを使用します。

switch(config-callhome)# **no periodic-inventory notification interval 15**

この値の範囲は、1 ～ 30 日間です。

DCNM-SAN を使用した定期的なインベントリ通知の有効化

DCNM-SAN を使用して Cisco MDS 9000 シリーズ スイッチまたは Cisco Nexus 5000 シリーズ スイッチで定期的なインベントリ通知を有効にするには、次の手順を実行します。

手順

ステップ 1 [Fabric] ペインでスイッチを選択します。

ステップ 2 **Events** を展開して、物理属性ペインで **Call Home** を選択します。
[情報（Information）] ペインに、Call Home 情報が表示されます。

ステップ 3 [**Periodic Inventory**] タブをクリックします。
Call Home の定期的なインベントリ情報が表示されます。

ステップ 4 [Information] ペインでスイッチを選択します。

ステップ 5 [**Enable**] チェックボックスをオンにします。

ステップ 6 インベントリをチェックする間隔を日単位で入力します。

ステップ 7 **Apply Changes**アイコンをクリックします。

重複メッセージ スロットリングの構成

同じイベントに対して受信する Call Home メッセージの数を制限するために、スロットリング メカニズムを設定できます。短時間のうちにスイッチから何度も同じメッセージが送信される場合、重複する多数のメッセージであふれることがあります。

制約事項

- デフォルトでは、Cisco MDS 9000 シリーズと Cisco Nexus 5000 シリーズのすべてのスイッチにおいてこの機能は有効になっています。この機能をイネーブルにすると、送信されるメッセージの数が、2 時間あたりの最大値である 30 メッセージを超えると、そのアラートタイプの以降のメッセージは、その間廃棄されます。時間間隔やメッセージカウンタの上限は変更できません。
- 最初に該当するメッセージが送信されてから 2 時間が経過し、新しいメッセージを送信する必要がある場合、新しいメッセージが送信され、その時刻に時間間隔がリセットされ、カウントが 1 にリセットされます。

Cisco MDS 9000 シリーズ スイッチまたは Cisco Nexus 5000 シリーズ スイッチでメッセージ スロットリングを有効にするには、次の手順を実行します。

手順

ステップ 1 次の構成モードを入力します。

switch# **configure terminal**

ステップ 2 Call Home 構成サブモードに入ります。

switch(config)# **callhome**

ステップ 3 重複メッセージスロットリング機能を無効化します。

switch(config-callhome)# **no duplicate-message throttle**

ステップ 4 重複メッセージスロットリング機能（デフォルト）を有効にします。

switch(config-callhome)# **duplicate-message throttle**

DCNM-SAN を使用した重複メッセージ スロットリングの構成

DCNM-SAN を使用して Cisco MDS 9000 シリーズ スイッチでメッセージ スロットリングを有効にするには、次の手順を実行します：

手順

ステップ 1 [Fabric] ペインでスイッチを選択します。

ステップ 2 [物理属性（Physical Attributes）] ペインで **[イベント（Events）]** を展開し、**[Call Home]** を選択します。

[Information] ペインに、Call Home 情報が表示されます。

ステップ 3 **[制御（Control）]** タブをクリックします。

ステップ 4 [Information] ペインでスイッチを選択します。

ステップ 5 **[重複メッセージ スロットル（Duplicate Msg Throttle）]** チェックボックスをオンにします。

ステップ 6 **[変更の適用（Apply Changes）]** アイコンをクリックします。

Call Home ファブリック配信のイネーブル化

Call Home ファブリック配信をイネーブルにするには、次の手順を実行します。

手順

ステップ 1 次の構成モードを入力します。

switch# **configure terminal**

ステップ 2 Call Home 構成サブモードに入ります。

switch(config)# **callhome**

ステップ 3 ファブリック内のすべてのスイッチに対する Call Home 構成の配布を有効にします。

switch(config-callhome)# **distribute**

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 4 Call Home 構成の配信をファブリック内のすべてのスイッチで無効（デフォルト）にします。

switch(config-callhome)# **no distribute**

Call Home 構成変更のコミット

Call Home の構成変更をコミットする手順は、次のとおりです。

手順

ステップ 1 次の構成モードを入力します。

switch# **configure terminal**

ステップ 2 Call Home 構成サブモードに入ります。

switch(config)# **callhome**

ステップ 3 構成変更をファブリック内のすべてのスイッチに配信し、ロックを解除します。

switch(config-callhome)# **commit**

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。

Call Home 構成変更の破棄

Call Home 構成の変更を廃棄するには、次の手順を実行します。

手順

ステップ 1 次の構成モードを入力します。

switch# **configure terminal**

ステップ 2 Call Home 構成サブモードに入ります。

switch(config)# **callhome**

ステップ 3 保留中のデータベースの構成変更を廃棄し、ファブリック ロックを解除します。

switch(config-callhome)# **abort**

DCNM-SAN を使用した Call Home ファブリック配信の有効化

DCNM-SAN を使用した Call Home ファブリック配信を有効化するには、次の手順を実行します。

手順

ステップ 1 [Fabric] ペインでスイッチを選択します。

ステップ 2 [物理属性（Physical Attributes）] ペインで **[イベント（Events）]** を展開し、**[Call Home]** を選択します。

[Information] ペインに、Call Home 情報が表示されます。

ステップ 3 **[CFS]** タブをクリックします。

Call Home の CFS 情報が表示されます。

ステップ 4 [Information] ペインでスイッチを選択します。

ステップ 5 そのスイッチの行の [管理（Admin）] カラムのドロップダウンリストから、**[有効（Enable）]** を選択します。

ステップ 6 **[変更の適用（Apply Changes）]** アイコンをクリックして、変更を確定します。

ファブリックのロックの上書き

管理者権限を使用し、ロックされた Call Home セッションを解除する手順は、次のとおりです。

手順

管理者権限を使用して、ロックされた Call Home セッションを解除します。

switch# **clear callhome session**

Call Home 通信テスト

テスト メッセージを設定された宛先に送信するか、テスト インベントリ メッセージを設定された宛先に送信することで、Call Home の通信をテストできます。

test コマンドを使用して、メッセージ生成をシミュレートします。

Call Home 機能をテストするには、次の手順を実行します。

手順

ステップ 1 構成された接続先にテスト メッセージを送信します。

switch# **callhome test**

ステップ 2 構成された接続先にテスト インベントリ メッセージを送信します。

switch(config)# **callhome test inventory**

DCNM-SAN を使用した Call Home 通信テスト

DCNM-SAN を使用して Call Home の機能をテストし、メッセージ生成をシミュレートするには、次の手順を実行します。

手順

ステップ 1 [Fabric] ペインでスイッチを選択します。

ステップ 2 [物理属性（Physical Attributes）] ペインで **[イベント（Events）]** を展開し、**[Call Home]** を選択します。

[Information] ペインに、Call Home 情報が表示されます。

ステップ 3 **[Test]** タブをクリックします。

スイッチに対して設定されているテストと、最後のテストのステータスが表示されます。

ステップ 4 [Information] ペインでスイッチを選択します。

ステップ 5 そのスイッチの行の **[TestAction]** ドロップダウン リストから、**[test]** または **[testWithInventory]** を選択します。

ステップ 6 **[変更の適用（Apply Changes）]** アイコンをクリックして、テストを実行します。

表 16 : EMC Call Home のトラップ （106 ページ） に、EMC Call Home 用のトラップをすべて示します。

表 *16 : EMC Call Home* のトラップ

SNMP Trap	EMC Call Home の送信条件
connUnitStatusChange	operStatus == failed(5)
cefcModuleStatusChange	operStatus != {ok(2), boot(5), selfTest(6), poweredUp(16), syncInProgress(21)}

cefcPowerStatusChange	operStatus = {offDenied(4), offEnvPower(5),offEnvTemp(6),offEnvFan(7),failed(8)}
cefcFRURemoved	all
cefcFanTrayStatusChange	all
cieDelayedLinkUpDown	operStatusReason != {linkFailure, adminDown, portGracefulShutdown}
cefcFRUInserted	all
entSensorThresholdNotification	値 >= しきい値

遅延トラップの設定

server.callhome.delayedtrap.enable プロパティが、server.properties コンフィギュレーション ファイルのセクション 9 Call Home に追加されています。プロパティ ファイルでは、DCNM-SAN サーバーが、EMC E-mail Home メッセージに対し、通常の リンク ダウン トラップではなく遅延トラップを使用するように設定できます。

遅延トラップ機能の有効化

遅延トラップ機能を有効化するには、このタスクを実行します。

始める前に

この機能をイネーブルにするには、遅延トラップをスイッチ レベルで有効にし、server.properties コンフィギュレーション ファイルで server.callhome.delayedtrap.enable プロパティを true に設定する必要があります。デフォルトでは、server.callhome.delayedtrap.enable オプションはディセーブルになっており、通常の linkDown トラップが使用されます。

手順

ステップ 1 次の構成モードを入力します。

switch# **configure terminal**

ステップ 2 システム遅延トラップ機能を有効にします。

switch(config)# **system delayed-traps enable mode** *FX*

ステップ 3 システム遅延トラップのタイムアウト値を構成します。

switch(config)# **system delayed-traps timer** *<1-60>*

値が入力されない場合、デフォルト値の 4 分が使用されます。1 ～ 60 分の範囲内の値を選択できます。

DCNM-SAN を使用した遅延トラップ機能の有効化

DCNM-SAN を使用して NX-OS Release 4.1(3) 以降が動作するスイッチ上で遅延トラップを有効にするには、次の手順を実行します。

手順

ステップ 1 [物理属性（Physical Attributes）] ペインで **[イベント（Events）]** を展開し、**[SNMP トラップ（SNMP Traps）]** を選択します。

DCNM-SAN のマップ レイアウトの上にある表で、**[遅延トラップ（Delayed Traps）]** タブをクリックします。

ステップ 2 遅延トラップを有効にするスイッチの **[有効（Enable）]** チェックボックスをオンにします。

ステップ 3 [遅延（Delay）] カラムに **[タイマー（timer）]** 値を入力します。

ステップ 4 [適用（Apply）] をクリックして変更内容を保存します。

（注）
値を入力しないと、デフォルト値の 4 分が使用されます。

Cisco Device Manager を使用した遅延トラップのイネーブル化

デバイスマネージャを使用して遅延トラップ機能を有効にするには、次の手順を実行します。

手順

ステップ 1 デバイスマネージャで、**[管理（Admin）]** > **[イベント（Events）]** > **[フィルタ（Filters）]** > **[遅延トラップ（Delayed Traps）]** を選択します。

[Information] ペインにイベント フィルタの情報が表示されます。

ステップ 2 **[遅延トラップ（Delayed Traps）]** タブをクリックします。

ステップ 3 **[有効（Enable）]** チェックボックスをオンにし、遅延トラップを有効にします。

遅延時間は、この機能をイネーブルにしないと設定できません。

ステップ 4 遅延トラップを無効にするには、**[有効（Enable）]** チェックボックスをオフにして **[適用（Apply）]** をクリックします。

イベント フィルタ通知の表示

デバイスマネージャで、[管理（Admin）] > [イベント（Events）] > [フィルタ（Filters）] の順に選択して通知に関する説明を参照します。

[Information] ペインにイベント フィルタの情報が表示されます。

[Event Filters] 画面に、通知に関する説明が表示されます。

Call Home コンフィギュレーションの確認

Call Home 構成情報を表示するには、次のいずれかの作業を行います。

Call Home 情報の表示

show callhome コマンドを使用して、構成された Call Home 情報を表示します。

構成された Call Home 情報の表示

```
switch# show callhome

callhome enabled
Callhome Information:
contact person name:who@where
contact person's email:person@place.com
contact person's phone number:310-408-4000
street addr:1234 Picaboo Street, Any city, Any state, 12345
site id:Site1ManhattanNewYork
customer id:Customer1234
contract id:Cisco1234
switch priority:0
```

すべての接続先プロファイルの情報（定義済みおよびユーザ定義）の表示

```
switch# show callhome destination-profile

XML destination profile information
maximum message size:500000
message format:XML
message-level:0
email addresses configured:
alert groups configured:
cisco_tac
test destination profile information
maximum message size:100000
message format:full-txt
message-level:5
email addresses configured:
```

```
admin@yourcompany.com
alert groups configured:
test
full-txt destination profile information
maximum message size:500000
message format:full-txt
message-level:0
email addresses configured:
alert groups configured:
all
short-txt destination profile information
maximum message size:4000
message format:short-txt
message-level:0
email addresses configured:
alert groups configured:
all
```

ユーザ定義の接続先プロファイルの情報の表示

```
switch# show callhome destination-profile
 test
test destination profile information
maximum message size:100000
message format:full-txt
message-level:5
email addresses configured:
user
@
company
.com
alert groups configured:
test
```

フルテキスト プロファイルの表示

```
switch# show callhome destination-profile profile full-txt-destination

full-txt destination profile information
maximum message size:250000
email addresses configured:
person2@company2.com
```

ショートテキスト プロファイルの表示

```
switch# show callhome destination-profile profile short-txt-destination
Short-txt destination profile information
maximum message size:4000
email addresses configured:
person2@company2.com
```

XML 接続先プロファイルの表示

```
switch# show callhome destination-profile profile XML-destination
XML destination profile information
maximum message size:250000
email addresses configured:
```

```
findout@.cisco.com
```

EMail と SMTP 情報の表示

```
switch# show callhome transport-email
from email addr:user@company1.com
reply to email addr:pointer@company.com
return receipt email addr:user@company1.com
smtp server:server.company.com
smtp server port:25
```

実行構成 callhome 情報の表示

```
switch# show running-config callhome
!Command: show running-config callhome
!Time: Tue Sep  9 12:16:45 2014
version 6.2(9)
logging level callhome 5
callhome
  contract-id contact1
  customer-id cust1
  site-id Site1
  email-contact sakpuri@cisco.com
  phone-contact +1-800-000-0000
  streetaddress 12345 Cisco Way, San Jose, CA
  destination-profile Inventory
  destination-profile Inventory format full-txt
  destination-profile Inventory message-size 1000000
  destination-profile Service
  destination-profile Service format full-txt
  destination-profile Service message-size 1000000
  destination-profile dest1
  destination-profile dest1 format XML
  destination-profile dest1 message-size 500000
  destination-profile full_txt message-size 1000000
  destination-profile httpProf
  destination-profile httpProf format XML
  destination-profile httpProf message-size 0
  destination-profile short_txt message-size 4000
  destination-profile xml message-size 1000000
  destination-profile xml message-size 1000000
  destination-profile Inventory email-addr sakpuri@cisco.com
  destination-profile Service email-addr sakpuri@cisco.com
  destination-profile full_txt email-addr sakpuri@cisco.com
  destination-profile short_txt email-addr sakpuri@cisco.com
  destination-profile xml email-addr sakpuri@cisco.com
  destination-profile Service alert-group environmental
  destination-profile xml alert-group environmental
  destination-profile Inventory alert-group inventory
  destination-profile xml alert-group inventory
  destination-profile Service alert-group linecard-hardware
```

デフォルトの callhome の実行構成の表示

```
switch# show running-config callhome all
EG-9506-1-176# show running-config callhome all
!Command: show running-config callhome all
!Time: Tue Sep  9 12:18:22 2014
version 6.2(9)
```

```
logging level callhome 5
callhome
  contract-id contact1
  customer-id cust1
  switch-priority 7
  site-id Site1
  email-contact sakpuri@cisco.com
  phone-contact +1-800-000-0000
  streetaddress 12345 Cisco Way, San Jose, CA
  destination-profile Inventory
  destination-profile Inventory format full-txt
  destination-profile Inventory transport-method email
  no destination-profile Inventory transport-method http
  destination-profile Inventory message-size 1000000
  destination-profile Inventory message-level 0
  destination-profile Service
  destination-profile Service format full-txt
  destination-profile Service transport-method email
  no destination-profile Service transport-method http
  destination-profile Service message-size 1000000
  destination-profile Service message-level 0
  destination-profile dest1
  destination-profile dest1 format XML
  destination-profile dest1 transport-method email
  no destination-profile dest1 transport-method http
  destination-profile dest1 message-size 500000
  destination-profile dest1 message-level 0
  destination-profile full_txt
  destination-profile full_txt format full-txt
  destination-profile full_txt transport-method email
  no destination-profile full_txt transport-method http
  destination-profile full_txt message-size 1000000
  destination-profile full_txt message-level 0
  destination-profile httpProf
```

callhome のスタートアップ構成の表示

```
switch# show startup-config callhome

!Command: show startup-config callhome
!Time: Tue Sep  9 12:19:27 2014
!Startup config saved at: Fri Sep  5 12:13:53 2014
version 6.2(9)
logging level callhome 5
callhome
  contract-id contact1
  customer-id cust1
  site-id Site1
  email-contact sakpuri@cisco.com
  phone-contact +1-800-000-0000
  streetaddress 12345 Cisco Way, San Jose, CA
  destination-profile Inventory
  destination-profile Inventory format full-txt
  destination-profile Inventory message-size 1000000
  destination-profile Service
  destination-profile Service format full-txt
  destination-profile Service message-size 1000000
  destination-profile dest1
  destination-profile dest1 format XML
  destination-profile dest1 message-size 500000
  destination-profile full_txt message-size 1000000
  destination-profile httpProf
  destination-profile httpProf format XML
```

```
destination-profile httpProf message-size 0
destination-profile short_txt message-size 4000
destination-profile xml message-size 1000000
destination-profile xml message-size 1000000
destination-profile Inventory email-addr sakpuri@cisco.com
destination-profile Service email-addr sakpuri@cisco.com
destination-profile full_txt email-addr sakpuri@cisco.com
destination-profile short_txt email-addr sakpuri@cisco.com
destination-profile xml email-addr sakpuri@cisco.com
destination-profile Service alert-group environmental
destination-profile xml alert-group environmental
destination-profile Inventory alert-group inventory
destination-profile xml alert-group inventory
```

遅延トラップ情報の表示

システム遅延トラップの状態を表示するには、**show running-config | in delay** コマンドを使用します。タイマー値が指定されていない場合、またはタイマー値が 4 分に設定されている場合は、次のように表示されます。

タイマー値なしで遅延トラップ情報を表示する（デフォルトの 4 分に設定）

```
switch# show running-config | in delay
system delayed-traps enable mode FX
```

次の例は、タイマー値が 4 分以外の値に設定されている場合の出力を示しています。

タイマー値が 4 分以外の遅延トラップ情報を表示する

```
switch# show running-config | in delay
system delayed-traps enable mode FX
system delayed-traps timer 5
```

アラート グループのカスタマイズの確認

アラート グループのカスタマイズを確認するには、**show callhome user-def-cmds** コマンドを使用します。

```
switch# show callhome user-def-cmds
User configured commands for alert groups :
alert-group test user-def-cmd "show version"
```

イベント通知トラップの確認

SNMP イベント通知トラップを確認するには、show snmp trap | inc callhome コマンドを使用します。

```
switch# show snmp trap | inc callhome
callhome : event-notify Yes
callhome : smtp-send-fail No
```

Call Home トランスポートの確認

Call Home の転送に関するすべての構成を表示するには、show callhome transport コマンドを使用します。

```
switch# show callhome transport
http vrf:management
from email addr:xyz-1@cisco.com
reply to email addr:xyz-1@cisco.com
smtp server:72.163.62.211
smtp server port:25
smtp server vrf:management
smtp server priority:0
http proxy server:10.64.65.52
http proxy server port:8080
http proxy status:Enabled
```

次の例は、SMTP サーバー ポートを構成する方法を示しています。

```
switch# callhome
switch(config-callhome)# transport email mail-server 192.168.10.23 port 4
switch# config t
```

次の例は、SMTP サーバーの優先順位を構成する方法を示しています。

```
switch(config-callhome)# transport email mail-server 192.168.10.23 priority 60
switch# config t
```

Call Home のモニタリング

このセクションは、次のトピックで構成されています。

フルテキスト形式の Syslog アラート通知の例

```
source:MDS9000
Switch Priority:7
Device Id:DS-C9506@C@FG@07120011
Customer Id:basu
Contract Id:123
Site Id:San Jose
Server Id:DS-C9506@C@FG@07120011
Time of Event:2004-10-08T11:10:44
Message Name:SYSLOG_ALERT
Message Type:Syslog
Severity Level:2
System Name:10.76.100.177
Contact Name:Basavaraj B
Contact email:admin@yourcompany.com
Contact Phone:+91-80-310-1718
Street Address:#71 , Miller's Road
Event Description:2004 Oct  8 11:10:44 10.76.100.177 %PORT-5-IF_TRUNK_UP: %$VSAN 1%$
Interface fc2/5, vsan 1 is up
syslog_facility:PORT
start chassis information:
```

```
Affected Chassis:DS-C9506
Affected Chassis Serial Number:FG@07120011
Affected Chassis Hardware Version:0.104
Affected Chassis Software Version:3.1(1)
Affected Chassis Part No:73-8607-01
end chassis information:
```

XML 形式での syslog アラート通知の例

```
<?xml version="1.0" encoding="UTF-8" ?>
<soap-env:Envelope xmlns:soap-env="http://www.w3.org/2003/05/soap-envelope">
<soap-env:Header>
<aml-session:Session xmlns:aml-session="http://www.cisco.com/2004/01/aml-session"
soap-env:mustUnderstand="true"
soap-env:role="http://www.w3.org/2003/05/soap-envelope/role/next">
<aml-session:To>http://tools.cisco.com/neddce/services/DDCEService</aml-session:To>
<aml-session:Path>
<aml-session:Via>http://www.cisco.com/appliance/uri</aml-session:Via>
</aml-session:Path>
<aml-session:From>http://www.cisco.com/appliance/uri</aml-session:From>
<aml-session:MessageId>1004:FOX090306QT:3E55A81A</aml-session:MessageId>
</aml-session:Session>
</soap-env:Header>
<soap-env:Body>
<aml-block:Block xmlns:aml-block="http://www.cisco.com/2004/01/aml-block">
<aml-block:Header>
<aml-block:Type>http://www.cisco.com/2005/05/callhome/syslog</aml-block:Type>
<aml-block:CreationDate>2003-02-21 04:16:18 GMT+00:00</aml-block:CreationDate>
<aml-block:Builder>
<aml-block:Name>MDS</aml-block:Name>
<aml-block:Version>4.1</aml-block:Version>
</aml-block:Builder>
<aml-block:BlockGroup>
<aml-block:GroupId>1005:FOX090306QT:3E55A81A</aml-block:GroupId>
<aml-block:Number>0</aml-block:Number>
<aml-block:IsLast>true</aml-block:IsLast>
<aml-block:IsPrimary>true</aml-block:IsPrimary>
<aml-block:WaitForPrimary>false</aml-block:WaitForPrimary>
</aml-block:BlockGroup>
<aml-block:Severity>6</aml-block:Severity>
</aml-block:Header>
<aml-block:Content>
<ch:CallHome xmlns:ch="http://www.cisco.com/2005/05/callhome" version="1.0">
<ch:EventTime>2003-02-21 04:16:18 GMT+00:00</ch:EventTime>
<ch:MessageDescription>LICENSE_VIOLATION 2003 Feb 21 04:16:18 switch %$
%DAEMON-3-SYSTEM_MSG: <<%LICMGR-3-LOG_LICAPP_NO_LIC>> License file is missing for feature
 SAN_EXTN_OVER_IP</ch:MessageDescription>
<ch:Event>
<ch:Type>syslog</ch:Type>
<ch:SubType>LICENSE_VIOLATION</ch:SubType>
<ch:Brand>Cisco</ch:Brand>
<ch:Series>MDS9000</ch:Series>
</ch:Event>
<ch:CustomerData>
<ch:UserData>
<ch:email>esajjana@cisco.com</ch:email>
</ch:UserData>
<ch:ContractData>
<ch:CustomerId>eeranna</ch:CustomerId>
<ch:SiteId>Bangalore</ch:SiteId>
<ch:ContractId>123</ch:ContractId>
<ch:DeviceId>DS-C9216I-K9@C@FOX090306QT</ch:DeviceId>
```

```
</ch:ContractData>
<ch:SystemInfo>
<ch:Name>switch</ch:Name>
<ch:Contact>Eeranna</ch:Contact>
<ch:Contactemail>esajjana@cisco.com</ch:Contactemail>
<ch:ContactPhoneNumber>+91-80-310-1718</ch:ContactPhoneNumber>
<ch:StreetAddress>#71, Miller's Road</ch:StreetAddress> </ch:SystemInfo> </ch:CustomerData>
 <ch:Device> <rme:Chassis xmlns:rme="http://www.cisco.com/rme/4.0">
<rme:Model>DS-C9216I-K9</rme:Model>
<rme:HardwareVersion>1.0</rme:HardwareVersion>
<rme:SerialNumber>FOX090306QT</rme:SerialNumber>
</rme:Chassis>
</ch:Device>
</ch:CallHome>
</aml-block:Content>
<aml-block:Attachments>
<aml-block:Attachment type="inline">
<aml-block:Name>show logging logfile | tail -n 200</aml-block:Name> <aml-block:Data
encoding="plain">
<![CDATA[syslog_show:: command: 1055 param_count: 0
2003 Feb 21 04:11:48  %KERN-2-SYSTEM_MSG: Starting kernel... - kernel
2003 Feb 21 04:11:48  %KERN-3-SYSTEM_MSG: CMOS: Module initialized - kernel
2003 Feb 21 04:11:48  %KERN-2-SYSTEM_MSG: CARD TYPE: KING BB Index = 2344 - kernel
2003 Feb 21 04:12:04  %MODULE-5-ACTIVE_SUP_OK: Supervisor 1 is active (serial: JAB100700MC)
2003 Feb 21 04:12:04  %PLATFORM-5-MOD_STATUS: Module 1 current-status is
MOD_STATUS_ONLINE/OK
2003 Feb 21 04:12:06  %IMAGE_DNLD-SLOT1-5-ADDON_IMG_DNLD_COMPLETE:  Addon module image
download process completed. Addon Image download completed, installing image please
wait..
2003 Feb 21 04:12:07  %IMAGE_DNLD-SLOT1-5-ADDON_IMG_DNLD_SUCCESSFUL:  Addon module image
 download and install process successful. Addon image installed.
2003 Feb 21 04:12:08  %KERN-3-SYSTEM_MSG: klm_af_xipc: Unknown parameter `start' - kernel
2003 Feb 21 04:12:08  %KERN-3-SYSTEM_MSG: klm_ips_portcfg: Unknown parameter `start' -
kernel
2003 Feb 21 04:12:08  %KERN-3-SYSTEM_MSG: klm_flamingo: Unknown parameter `start' -
kernel
2003 Feb 21 04:12:10  %PORT-5-IF_UP: Interface mgmt0 is up
2003 Feb 21 04:12:21 switch %LICMGR-3-LOG_LIC_FILE_MISSING: License file(s) missing for
 feature ENTERPRISE_PKG.
2003 Feb 21 04:12:21 switch %LICMGR-3-LOG_LIC_FILE_MISSING: License file(s) missing for
 feature SAN_EXTN_OVER_IP.
2003 Feb 21 04:12:21 switch %LICMGR-3-LOG_LIC_FILE_MISSING: License file(s) missing for
 feature ENTERPRISE_PKG.
2003 Feb 21 04:12:21 switch %LICMGR-3-LOG_LIC_FILE_MISSING: License file(s) missing for
 feature SAN_EXTN_OVER_IP.
2003 Feb 21 04:12:23 switch %PLATFORM-5-MOD_STATUS: Module 1 current-status is
MOD_STATUS_ONLINE/OK
2003 Feb 21 04:12:23 switch %MODULE-5-MOD_OK: Module 1 is online (serial: JAB100700MC)
2003 Feb 21 04:12:25 switch %PORT-5-IF_DOWN_ADMIN_DOWN: %$VSAN 1%$ Interface fc1/1 is
down (Administratively down)
2003 Feb 21 04:12:25 switch %PORT-5-IF_DOWN_ADMIN_DOWN: %$VSAN 1%$ Interface fc1/2 is
down (Administratively down)
2003 Feb 21 04:12:25 switch %PORT-5-IF_DOWN_ADMIN_DOWN: %$VSAN 1%$ Interface fc1/3 is
down (Administratively down)
2003 Feb 21 04:12:25 switch %PORT-5-IF_DOWN_ADMIN_DOWN: %$VSAN 1%$ Interface fc1/4 is
down (Administratively down)
2003 Feb 21 04:12:26 switch %PLATFORM-5-PS_STATUS: PowerSupply 1 current-status is PS_FAIL
2003 Feb 21 04:12:26 switch %PLATFORM-2-PS_FAIL: Power supply 1 failed or shut down
(Serial number QCS1007109F)
2003 Feb 21 04:12:26 switch %PLATFORM-5-PS_FOUND: Power supply 2 found (Serial number
QCS1007109R)
2003 Feb 21 04:12:26 switch %PLATFORM-2-PS_OK: Power supply 2 ok (Serial number
QCS1007109R)
2003 Feb 21 04:12:26 switch %PLATFORM-5-PS_STATUS: PowerSupply 2 current-status is PS_OK
```

```
2003 Feb 21 04:12:26 switch %PLATFORM-2-PS_FANOK: Fan in Power supply 2 ok
2003 Feb 21 04:12:26 switch %PLATFORM-5-FAN_DETECT: Fan module 1 (Serial number
NWG0901031X) ChassisFan1 detected
2003 Feb 21 04:12:26 switch %PLATFORM-2-FAN_OK: Fan module ok
2003 Feb 21 04:12:26 switch %PLATFORM-2-CHASSIS_CLKMODOK: Chassis clock module A ok
2003 Feb 21 04:12:26 switch %PLATFORM-2-CHASSIS_CLKSRC: Current chassis clock source is
 clock-A
2003 Feb 21 04:12:26 switch %PORT-5-IF_DOWN_ADMIN_DOWN: %$VSAN 1%$ Interface fc1/5 is
down (Administratively down)
2003 Feb 21 04:12:26 switch %PORT-5-IF_DOWN_ADMIN_DOWN: %$VSAN 1%$ Interface fc1/6 is
down (Administratively down)
2003 Feb 21 04:12:26 switch %PORT-5-IF_DOWN_ADMIN_DOWN: %$VSAN 1%$ Interface fc1/7 is
down (Administratively down)
2003 Feb 21 04:12:26 switch %PORT-5-IF_DOWN_ADMIN_DOWN: %$VSAN 1%$ Interface fc1/8 is
down (Administratively down)
2003 Feb 21 04:12:26 switch %PORT-5-IF_DOWN_ADMIN_DOWN: %$VSAN 1%$ Interface fc1/9 is
down (Administratively down)
2003 Feb 21 04:12:26 switch %PORT-5-IF_DOWN_ADMIN_DOWN: %$VSAN 1%$ Interface fc1/10 is
down (Administratively down)
2003 Feb 21 04:12:27 switch %PORT-5-IF_DOWN_ADMIN_DOWN: %$VSAN 1%$ Interface fc1/11 is
down (Administratively down)
2003 Feb 21 04:12:27 switch %PORT-5-IF_DOWN_ADMIN_DOWN: %$VSAN 1%$ Interface fc1/12 is
down (Administratively down)
2003 Feb 21 04:12:27 switch %PORT-5-IF_DOWN_ADMIN_DOWN: %$VSAN 1%$ Interface fc1/13 is
down (Administratively down)
2003 Feb 21 04:12:27 switch %PORT-5-IF_DOWN_ADMIN_DOWN: %$VSAN 1%$ Interface fc1/14 is
down (Administratively down)
2003 Feb 21 04:12:30 switch %PLATFORM-2-MOD_DETECT: Module 2 detected (Serial number
JAB0923016X) Module-Type IP Storage Services Module Model DS-X9304-SMIP
2003 Feb 21 04:12:30 switch %MODULE-2-MOD_UNKNOWN: Module type [25] in slot 2 is not
supported
2003 Feb 21 04:12:45 switch %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configured from vty by root
on console0
2003 Feb 21 04:14:06 switch %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configured from vty by admin
on console0
2003 Feb 21 04:15:12 switch %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configured from vty by admin
on console0
2003 Feb 21 04:15:52 switch %SYSMGR-3-BASIC_TRACE: core_copy: PID 1643 with message Core
 not generated by system for licmgr(0). WCOREDUMP(9) returned zero .
2003 Feb 21 04:15:52 switch %SYSMGR-2-SERVICE_CRASHED: Service \"licmgr\" (PID 2272)
hasn't caught signal 9 (no core).
2003 Feb 21 04:16:18 switch %LICMGR-3-LOG_LIC_FILE_MISSING: License file(s) missing for
 feature ENTERPRISE_PKG.
2003 Feb 21 04:16:18 switch %LICMGR-3-LOG_LIC_FILE_MISSING: License file(s) missing for
 feature SAN_EXTN_OVER_IP.
2003 Feb 21 04:16:18 switch %LICMGR-3-LOG_LIC_FILE_MISSING: License file(s) missing for
 feature ENTERPRISE_PKG.
2003 Feb 21 04:16:18 switch %LICMGR-3-LOG_LIC_FILE_MISSING: License file(s) missing for
 feature SAN_EXTN_OVER_IP.
2003 Feb 21 04:16:18 switch %CALLHOME-2-EVENT: LICENSE_VIOLATION
2003 Feb 21 04:16:18 switch %CALLHOME-2-EVENT: LICENSE_VIOLATION
2003 Feb 21 04:16:18 switch %CALLHOME-2-EVENT: LICENSE_VIOLATION
2003 Feb 21 04:16:18 switch %CALLHOME-2-EVENT: LICENSE_VIOLATION ]]> </aml-block:Data>
</aml-block:Attachment> <aml-block:Attachment type="inline"> <aml-block:Name>show license
 usage</aml-block:Name> <aml-block:Data encoding="plain">
<![CDATA[Feature                        Ins  Lic   Status Expiry Date Comments
                                     Count
--------------------------------------------------------------------------------
DMM_184_PKG                    No    0   Unused             Grace expired
FM_SERVER_PKG                  No    -   Unused             Grace expired
MAINFRAME_PKG                  No    -   Unused             Grace expired
ENTERPRISE_PKG                 Yes   -   Unused never       license missing
DMM_FOR_SSM_PKG                No    0   Unused             Grace expired
SAN_EXTN_OVER_IP               Yes   8   Unused never       8 license(s) missing
```

```
PORT_ACTIVATION_PKG           No    0   Unused            -
SME_FOR_IPS_184_PKG           No    0   Unused            Grace expired
STORAGE_SERVICES_184          No    0   Unused            Grace expired
SAN_EXTN_OVER_IP_18_4         No    0   Unused            Grace expired
SAN_EXTN_OVER_IP_IPS2         No    0   Unused            Grace expired
SAN_EXTN_OVER_IP_IPS4         No    0   Unused            Grace expired
STORAGE_SERVICES_SSN16        No    0   Unused            Grace expired
10G_PORT_ACTIVATION_PKG       No    0   Unused            -
STORAGE_SERVICES_ENABLER_PKG  No    0   Unused            Grace expired
--------------------------------------------------------------------------------
**** WARNING: License file(s) missing. **** ]]> </aml-block:Data> </aml-block:Attachment>
 </aml-block:Attachments> </aml-block:Block> </soap-env:Body> </soap-env:Envelope>
```

XML 形式の RMON 通知の例

```
<?xml version="1.0" encoding="UTF-8" ?>
<soap-env:Envelope xmlns:soap-env="http://www.w3.org/2003/05/soap-envelope">
<soap-env:Header>
<aml-session:Session xmlns:aml-session="http://www.cisco.com/2004/01/aml-session"
soap-env:mustUnderstand="true"
soap-env:role="http://www.w3.org/2003/05/soap-envelope/role/next">
<aml-session:To>http://tools.cisco.com/neddce/services/DDCEService</aml-session:To>
<aml-session:Path>
<aml-session:Via>http://www.cisco.com/appliance/uri</aml-session:Via>
</aml-session:Path>
<aml-session:From>http://www.cisco.com/appliance/uri</aml-session:From>
<aml-session:MessageId>1086:FHH0927006V:48BA26BD</aml-session:MessageId>
</aml-session:Session>
</soap-env:Header>
<soap-env:Body>
<aml-block:Block xmlns:aml-block="http://www.cisco.com/2004/01/aml-block">
<aml-block:Header>
<aml-block:Type>http://www.cisco.com/2005/05/callhome/diagnostic</aml-block:Type>
<aml-block:CreationDate>2008-08-31 05:06:05 GMT+00:00</aml-block:CreationDate>
<aml-block:Builder>
<aml-block:Name>MDS</aml-block:Name>
<aml-block:Version>4.1</aml-block:Version>
</aml-block:Builder>
<aml-block:BlockGroup>
<aml-block:GroupId>1087:FHH0927006V:48BA26BD</aml-block:GroupId>
<aml-block:Number>0</aml-block:Number>
<aml-block:IsLast>true</aml-block:IsLast>
<aml-block:IsPrimary>true</aml-block:IsPrimary>
<aml-block:WaitForPrimary>false</aml-block:WaitForPrimary>
</aml-block:BlockGroup>
<aml-block:Severity>2</aml-block:Severity>
</aml-block:Header>
<aml-block:Content>
<ch:CallHome xmlns:ch="http://www.cisco.com/2005/05/callhome" version="1.0">
<ch:EventTime>2008-08-31 05:06:05 GMT+00:00</ch:EventTime>
<ch:MessageDescription>RMON_ALERT WARNING(4) Falling:iso.3.6.1.4.1.9.9.305.1.1.1.0=1 <=
 89:1, 4</ch:MessageDescription>
<ch:Event>
<ch:Type>environment</ch:Type>
<ch:SubType>minor</ch:SubType>
<ch:Brand>Cisco</ch:Brand>
<ch:Series>MDS9000</ch:Series>
</ch:Event>
<ch:CustomerData>
<ch:UserData>
<ch:email>mchinn@cisco.com</ch:email>
</ch:UserData>
```

```
<ch:ContractData>
<ch:CustomerId>12ss</ch:CustomerId>
<ch:SiteId>2233</ch:SiteId>
<ch:ContractId>rrr55</ch:ContractId>
<ch:DeviceId>DS-C9513@C@FHH0927006V</ch:DeviceId>
</ch:ContractData>
<ch:SystemInfo>
<ch:Name>sw172-22-46-174</ch:Name>
<ch:Contact>Mani</ch:Contact>
<ch:Contactemail>mchinn@cisco.com</ch:Contactemail>
<ch:ContactPhoneNumber>+1-800-304-1234</ch:ContactPhoneNumber>
<ch:StreetAddress>1234 wwee</ch:StreetAddress>
</ch:SystemInfo>
</ch:CustomerData>
<ch:Device>
<rme:Chassis xmlns:rme="http://www.cisco.com/rme/4.0">
<rme:Model>DS-C9513</rme:Model>
<rme:HardwareVersion>0.205</rme:HardwareVersion>
<rme:SerialNumber>FHH0927006V</rme:SerialNumber>
</rme:Chassis>
</ch:Device>
</ch:CallHome>
</aml-block:Content>
</aml-block:Block>
</soap-env:Body>
</soap-env:Envelope>
```

Call Home のフィールドの説明

このセクションでは、この機能のフィールドの説明を示します。

Call Home 一般

フィールド	説明
連絡先	このスイッチの連絡先担当者。この担当者への連絡方法に関する情報も含む。
PhoneNumber	連絡先担当者の電話番号。電話番号は、「+」で始まり、空白と「-」以外はすべて数字にする必要があります。+44 20 8332 9091、+45 44886556、+81-46-215-4678、+1-650-327-2600 などの電話番号が有効です。
EmailAddress	連絡先担当者の電子メールアドレス。raj@helpme.com、bob@service.com、mtom@abc.caview.ca.us などの電子メール アドレスが有効です。
StreetAddress	このスイッチの送付先住所です。
CustomerId	お客様を識別するための任意の適切な形式の文字列です。
ContractId	お客様とサポートパートナーの間のサポート契約を識別するための任意の適切な形式の文字列です。
SiteId	このデバイスのロケーション ID です。

フィールド	説明
DeviceServicePriority	デバイスのサービス プライオリティです。これにより、デバイスにサービスが提供される速さが決定されます。
有効	ローカル デバイス上で Call Home インフラストラクチャをイネーブルまたはディセーブルにします。

Related Topics

Call Home の概要, on page 51

Call Home 宛先

フィールド	説明
EmailAddress	この接続先プロファイルに関連付けられる電子メール アドレス。raj@helpme.com、bob@service.com、mtom@abc.caview.ca.us などになります。

Related Topics

Call Home 宛先プロファイル, on page 55

Call Home SMTP サーバ

フィールド	説明
Address Type、Address	SMTP サーバーの IP アドレス。
Port	SMTP サーバーの TCP ポート。
Priority	プライオリティ値。

Call Home 電子メール セットアップ

フィールド	説明
From	SMTP を使用して電子メールを送信する際に、From フィールドに使用される電子メール アドレス。raj@helpme.com、bob@service.com、mtom@abc.caview.ca.us などになります。
ReplyTo	SMTP を使用して電子メールを送信する際に、Reply-To フィールドに使用される電子メール アドレス。raj@helpme.com、bob@service.com、mtom@abc.caview.ca.us などになります。
IP アドレスタイプ	IP アドレス タイプ（IPv4、IPv6、または DNS）。

フィールド	説明
Name or IP Address	SMTP サーバの名前または IP アドレス。
Port	SMTP サーバーの TCP ポート。

Related Topics

HTTPS サポートを使用した一般的な EMail オプション, on page 57

Call Home アラート

フィールド	説明
操作	[Test]：Call Home メッセージを送信します。 [TestWithInventory]：インベントリの詳細付きメッセージを送信します。
ステータス	最後の Call Home アクション呼び出しのステータス。
FailureCause	最後の Call Home テスト呼び出しの失敗原因。
LastTimeSent	最後の Call Home アラートが送信された時刻。
NumberSent	Call Home アラートの送信数。
Interval	定期的なソフトウェア インベントリ Call Home メッセージを送信するためのタイム フレーム。
Throttling Enable	オンの場合、システムに実装されているメッセージ スロットリング メカニズムがイネーブルになり、一定のタイム フレーム内での特定のアラート タイプの Call Home メッセージの数が制限されます。最大は 2 時間のタイム フレーム内で 30 件であり、それ以上のそのアラート タイプのメッセージは廃棄されます。
Enable	オンの場合、システム上での定期的なソフトウェア インベントリ Call Home メッセージの送信がイネーブルになります。

Related Topics

Call Home アラート グループ, on page 55

Call Home のメッセージ レベル機能, on page 56

Call Home ユーザ定義コマンド

フィールド	説明
User Defined Command	Call Home アラート グループ タイプのユーザ定義コマンドを設定します。

遅延トラップ

フィールド	説明
Enable	遅延トラップをイネーブルまたはディセーブルにします。
遅延	分単位の遅延時間（有効な値の範囲は 1 ～ 60）。

Call Home プロファイル

フィールド	説明
MsgFormat	XML、フル テキスト、またはショート テキスト。
MaxMsgSize	この宛先プロファイルで示される宛先に送信可能な最大メッセージ サイズ。
MsgLevel	しきい値レベル。宛先に送信されるアラート メッセージのフィルタリングに使用されます。設定されたしきい値レベルよりも低い重大度の Callhome アラート メッセージは送信されなくなります。デフォルトのしきい値レベルはデバッグ（1）です。この場合、すべてのアラート メッセージが送信されます。
AlertGroups	この宛先プロファイルに設定されているアラート グループのリスト。

イベント宛先アドレス

フィールド	説明
Address/Port	イベントを送信する IP アドレスとポート。
Security Name	このアドレスに送信されるメッセージを生成する際に使用される SNMP パラメータ。
Security Model	このエントリを使用して SNMP メッセージを生成する際に使用されます。
Inform Type	• [Trap]：未確認応答イベント • [Inform]：確認応答イベント
Inform Timeout	このアドレスとの通信に求められる最大ラウンドトリップ時間。
RetryCount	生成したメッセージに対する応答が受信されない場合に行われる再試行の回数。

イベント宛先セキュリティ（詳細）

フィールド	説明
MPModel	このエントリを使用してSNMPメッセージを生成する際に使用されるメッセージ処理モデル。
SecurityModel	このエントリを使用してSNMPメッセージを生成する際に使用されるセキュリティ モデル。
SecurityName	このエントリを使用してSNMPメッセージが生成される対象者を識別します。
SecurityLevel	このエントリを使用してSNMPメッセージを生成する際に使用されるセキュリティ レベル。

イベント フィルター般

フィールド	説明
FSPF - Nbr State Changes	ローカル スイッチが VSAN 上のインターフェイスでネイバーの状態（FSPF ネイバー有限状態マシンの状態）の変化を検出したときに通知を発行するかどうかを指定します。
Domain Mgr - ReConfig Fabrics	ローカル スイッチが VSAN 上での ReConfigureFabric（RCF）の送受信時に通知を発行するかどうかを指定します。
Zone Server - Request Rejects	ゾーン サーバが拒否時に通知を発行するかどうかを指定します。
Zone Server - Merge Failures	Zone Server がマージ失敗時に通知を発行するかどうかを指定します。
Zone Server - Merge Successes	ゾーン サーバがマージ成功時に通知を発行するかどうかを指定します。
Zone Server - Default Zone Behavior Change	伝播ポリシーが変化した場合にゾーン サーバが通知を発行するかどうかを指定します。
Zone Server - Unsupp Mode	ゾーン サーバが unsupp モードの変化時に通知を発行するかどうかを指定します。
FabricConfigServer - Request Rejects	ファブリック コンフィギュレーション サーバが拒否時に通知を発行するかどうかを指定します。
RSCN - ILS Request Rejects	SW_RSCN要求が拒否されるときにRSCNモジュールが通知を生成するかどうかを指定します。

フィールド	説明
RSCN - ILS RxRequest Rejects	SW_RSCN 要求が拒否されるときに RSCN モジュールが通知を生成するかどうかを指定します。
RSCN - ELS Request Rejects	SCR または RSCN 要求が拒否されるときに RSCN モジュールが通知を生成するかどうかを指定します。
FRU Changes	false 値の場合、このシステムによって現場交換可能ユニット（FRU）通知は生成されません。
SNMP - Community Auth Failure	SNMP エンティティが authenticationFailure トラップの生成を許可されているかどうかを示します。
VRRP	VRRP 対応ルータがこの MIB に定義されているイベントに対して SNMP トラップを生成するかどうかを示します。
FDMI	登録要求が拒否されるときに FDMI が通知を生成するかどうかを指定します。
License Manager	システムが通知を生成するかどうかを示します。
Port/Fabric Security	ポート/ファブリック セキュリティの問題が発生したときにシステムが通知を生成するかどうかを指定します。
FCC	エージェントが通知を生成するかどうかを指定します。
Name Server	オンの場合、要求が拒否されるときにネーム サーバが通知を生成します。オフの場合、通知は生成されません。

イベント フィルタ インターフェイス

フィールド	説明
EnableLinkTrap	このインターフェイスに対して linkUp/linkDown トラップが生成されるかどうかを示します。

イベント フィルタ制御

フィールド	説明
Variable	制御される通知を表します。
Descr	通知に関する説明。
Enabled	オンにすると、コントロールの通知がイネーブルになります。コントロールのステータスを表示します。

Note [Descr] カラムは、Cisco NX-OS Release 5.0 以降が動作しているスイッチ上でのみ表示されます。

その他の参考資料

Call Home の実装に関連した情報については、次を参照してください。

MIB

MIB	MIB のリンク
• CISCO-CALLHOME-CAPABILITY-MIB • CISCO-CALLHOME-MIB	MIB を検索およびダウンロードするには、次の URL にアクセスください。 http://www.cisco.com/en/US/products/ps5989/prod_technical_referenc

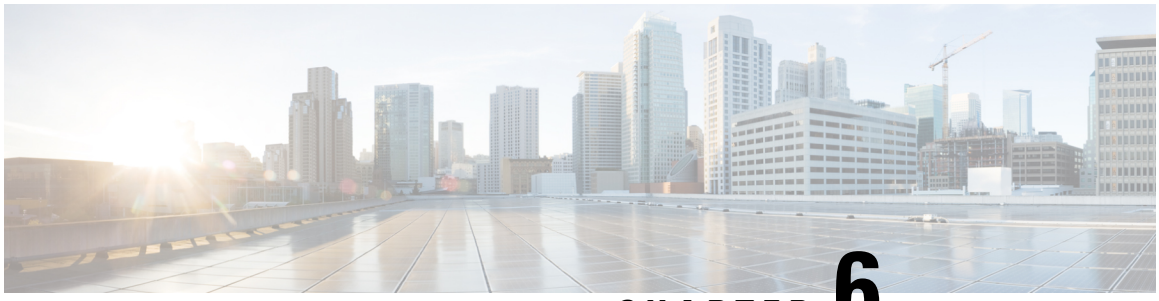
Call Home の機能履歴

Call Home の機能履歴, on page 125 に、この機能のリリース履歴を示します。リリース 3.x 以降のリリースで導入または変更された機能のみが表に記載されています。

***Table 17: Call Home* の機能履歴**

機能名	リリース	機能情報
Call Home HTTP プロキシ サーバ	5.2	Call Home HTTP プロキシ サーバ サポートの詳細が追加されました。
Call Home ウィザード	5.2	Call Home ウィザード設定の詳細が追加されました。
Call Home HTTP プロキシ サーバ	5.2	Call Home HTTP プロキシ サーバ サポートの詳細が追加されました。 Callhome 転送を確認するコマンドが追加されました。
複数 SMTP サーバ サポート	5.0(1a)	複数 SMTP サーバ サポートの詳細が追加されました。 Callhome 転送を確認するコマンドが追加されました。
通知の拡張	5.0(1a)	Device Manager を使用したイベント フィルタの通知の拡張が追加されました。
Call Home	4.1(1b)	Call Home の HTTPS サポートが追加されました。

機能名	リリース	機能情報
DCNM-SAN における [Call Home - Delayed Traps for EMC Call Home] 設定ウィンドウ	4.1(1a)	EMC Call Home の遅延トラップの拡張が追加されました。
[Call Home Destination] タブ	4.2(1)	[Destination] タブの拡張を追加。
Call Home HTTP のサポート	4.2(1)	Call Home HTTP 拡張を追加。
EMC Email Home	3.3(3)	この章に EMC Email Home 設定情報が追加されました。
EMC Call Home	3.0(1)	EMC 仕様に従い、電子メールを使用してトラップを XML データとして転送できるようになります。
Call Home の拡張	3.0(1)	アラートグループメッセージをカスタマイズできるようになります。



CHAPTER 6

メンテナンス ジョブのスケジューリング

Cisco MDS コマンド スケジューラ機能は、Cisco MDS 9000 ファミリの任意のスイッチで設定ジョブとメンテナンス ジョブをスケジュールするのに役立ちます。この機能を使用して、一度だけ実行するジョブや定期的に実行するジョブをスケジュールできます。

- コマンド スケジューラについて, on page 127
- コマンド スケジューラのライセンス要件, on page 128
- 注意事項と制約事項, on page 128
- デフォルト設定 , on page 129
- コマンド スケジューラの設定, on page 129
- スケジュールの指定, on page 133
- 一時的スケジュールの指定, on page 135
- スケジュールの削除, on page 136
- 割り当てられたジョブの削除, on page 136
- スケジュール時刻の削除, on page 137
- 実行ログの設定, on page 137
- 実行ログ ファイルの内容のクリア, on page 138
- スケジューラ設定の確認, on page 138
- スケジューラのコンフィギュレーション例, on page 140

コマンド スケジューラについて

Cisco NX-OS コマンド スケジューラは、将来の指定した時刻に 1 つ以上のジョブ（CLI コマンドのセット）をスケジュールするための機構を提供します。ジョブは、将来の指定した時刻に一度だけ実行することも、定期的に実行することもできます。

この機能を使用すると、ゾーンセットの変更、QoS ポリシーの変更、データのバックアップ、設定の保存などのジョブをスケジューリングできます。

スケジューラの用語

この章では次の用語を使用します。

- ジョブ：スケジュールの定義どおりに実行される NX-OS の CLI コマンド一式（EXEC および config モード）。
- スケジュール：スケジュールは割り当てたジョブを実行する時刻を決定します。スケジュールには複数のジョブを割り当てることができます。スケジュールは、一時モードまたは定期モードで実行されます。
- 定期モード：ユーザが指定した間隔でジョブを実行します。これは、管理者によって削除されるまで継続されます。サポートされている間隔は、次のとおりです。
  - 毎日：ジョブを 1 日に 1 回実行します。
  - 毎週：ジョブを 1 週間に 1 回実行します。
  - 毎月：ジョブを 1 か月に 1 回実行します。
  - 差分：ジョブをユーザ指定の開始時刻から一定間隔（日、時、分）ごとに実行します。
- 一時モード：ジョブをユーザ指定時刻に 1 回実行します。

コマンド スケジューラのライセンス要件

コマンド スケジューラを使用するために、ライセンスを取得する必要はありません。

注意事項と制約事項

Cisco MDS スイッチでジョブをスケジュールする前に、次の注意事項を確認してください。

- Cisco MDS SAN-OS Release 3.0(3) よりも前のリリースでは、スイッチに対してローカルなユーザだけがスケジューラを設定できました。Cisco MDS SAN-OS Release 3.0(3) から、リモート ユーザが AAA 認証を使用してジョブのスケジューリングを実行できるようになりました。
- ジョブの実行時に次のいずれかの状況になると、スケジュールされたジョブは実行されません。
  - ジョブの実行予定時刻に、スケジュールされたジョブに含まれるコマンドに関連する機能のライセンスが切れている場合。
  - ジョブの実行予定時刻に、スケジュールされたジョブに含まれるコマンドに関連する機能がディセーブルになっている場合。
  - スロットからモジュールを取り外したときに、そのモジュールまたはスロットに関連するコマンドがジョブに含まれている場合。
- 時刻が設定されていることを確認します。スケジューラにはデフォルトの設定時刻はありません。スケジュールを作成してジョブを割り当てても、時刻を設定しないと、スケジュールは開始されません。
- ジョブを定義する場合、ジョブの中に対話型コマンドや中断型コマンド（**copy bootflash:** *file* **ftp:** *URI*、 **write erase** など）が指定されていないことを確認します。これは、ジョブがスケジュールされた時刻に対話なしで実行されるためです。

デフォルト設定

Table 18: コマンド スケジューラのパラメータのデフォルト , on page 129 に、コマンド スケジューリング パラメータのデフォルト設定を示します。

Table 18: コマンド スケジューラのパラメータのデフォルト

パラメータ	デフォルト
コマンド スケジューラ	ディセーブル
ログ ファイル サイズ	16 KB。

コマンド スケジューラの設定

Cisco NX-OS コマンド スケジューラは、将来の指定した時刻に 1 つ以上のジョブ（CLI コマンドのセット）をスケジュールするための機構を提供します。

コマンド スケジューラを設定するためのタスク フロー

次の手順を実行して、コマンド スケジューラを設定します。

Procedure

ステップ 1 スケジューラをイネーブルにします。
ステップ 2 リモート ユーザ アクセスを許可します（オプション）。
ステップ 3 ジョブを定義します。
ステップ 4 スケジュールを定義して、スケジュールにジョブを割り当てます。
ステップ 5 スケジュールの時刻を指定します。
ステップ 6 スケジューリングされた設定を確認します。

コマンド スケジューラのイネーブル化

スケジューリング機能を使用するには、ファブリック内の目的のスイッチ上でこの機能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。

コマンド スケジューラ機能の設定および確認コマンドを使用できるのは、スイッチ上でコマンド スケジューラ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。

コマンド スケジューリング機能をイネーブルにするには次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

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

コマンド スケジューラをイネーブルにします。

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

スケジューラの設定を廃棄して、コマンド スケジューラをディセーブルにします（デフォルト）。

例

コマンド スケジュールのステータスを表示するには、 **show scheduler config** コマンドを使用します。

```
switch# show scheduler config
  config terminal
  feature scheduler
  scheduler logfile size 16
  end
```

リモート ユーザ認証の設定

Cisco MDS SAN-OS Release 3.0(3) よりも前のリリースでは、スイッチに対してローカルなユーザだけがスケジューラを設定できました。Cisco MDS SAN-OS Release 3.0(3) から、リモート ユーザが AAA 認証を使用してジョブのスケジューリングを実行できるようになりました。

リモート ユーザ認証を設定するには、次の手順を実行します。

Before you begin

AAA 認証では、コマンド スケジューラ ジョブを作成および設定する前に、リモート ユーザのクリア テキスト パスワードが必要になります。

Procedure

ステップ 1 switch# **configuration terminal**

構成モードに入ります。

ステップ 2 switch(config)# **scheduler aaa-authentication password X12y34Z56a**

リモート ユーザのクリア テキスト パスワードを設定します。

ステップ 3 switch(config)# **scheduler aaa-authentication password 0 X12y34Z56a**

リモート ユーザのクリア テキスト パスワードを設定します。

ステップ 4 switch(config)# **no scheduler aaa-authentication password**

リモート ユーザのクリア テキスト パスワードを削除します

ステップ 5 switch(config)#**scheduler aaa-authentication user newuser password Z98y76X54b**

リモート ユーザ newuser のクリア テキスト パスワードを設定します

ステップ 6 switch(config)#**scheduler aaa-authentication user newuser password 0 Z98y76X54b**

リモート ユーザ newuser のクリア テキスト パスワードを設定します

ステップ 7 switch(config)# **no scheduler aaa-authentication password user newuser**

リモート ユーザ newuser のクリア テキスト パスワードを削除します

ジョブの定義

ジョブを定義するには、ジョブ名を指定する必要があります。この操作を行うと、ジョブ定義（config-job）サブモードが開始されます。このサブモードでは、ジョブが実行する CLI コマンドのシーケンスを定義できます。ジョブの定義を完了するには、必ず config-job サブモードを終了してください。

- Cisco MDS NX-OS Release 4.1(1b) よりも前の MDS NX-OS または SAN-OS のリリースで作成されたジョブ設定ファイルはサポートされていません。ただし、ジョブ設定ファイルを編集し、ジョブの中のコマンドを、セミコロン（;）を使用して 1 行に結合することはできます。
- ジョブの定義を完了するには、config-job サブモードを終了する必要があります。
- config-job サブモードを終了した後では、コマンドの変更または削除はできません。変更するには、定義済みのジョブ名を明示的に削除し、新しいコマンドを使用してジョブを再設定する必要があります。

コマンド スケジューラのジョブを定義するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configuration terminal**

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)# **scheduler job name addMemVsan99**

switch(config-job)#

ジョブ名を定義して、ジョブ定義サブモードを開始します。

ステップ 3 switch(config-job)# *command1* ;[*command2* ;*command3* ;...]

switch(config-job-submode)# **end**

Example:

```
switch(config-job)# configure terminal;vsan database;vsan 99 interface fc1/1 4
switch(config-job-config-vsan-db)# end
switch#
```

指定されたジョブの処理シーケンスを指定します。定義済みのコマンドは有効性が確認されて、今後使用するために保管されます。

Note
config-job サブモードは必ず終了してください。

Example:

```
switch(config)# scheduler job name offpeakQOS
switch(config-job)# configuration terminal; qos class-map offpeakbackupcmap match-all ;
 match source-wwn 23:15:00:05:30:00:2a:1f ; match destination-wwn 20:01:00:05:30:00:28:df
 ;exit ; qos policy-map offpeakbackuppolicy ; class offpeakbackupcmap ; priority high ;
 exit ; exit ; qos service policy offpeakbackuppolicy vsan 1
switch(config-job)# end
switch#
```

一連のコンフィギュレーション コマンドをスケジューリングする例を示します。

ステップ 4 **exit**

Example:

```
switch(config-job)# exit
switch(config)#
```

ジョブ コンフィギュレーション モードを終了し、ジョブを保存します。

ステップ 5 **show scheduler job** [*name*]

Example:

```
switch(config)# show scheduler job
```

（任意）ジョブ情報を表示します。

ステップ 6 **copy running-config startup-config**

Example:

```
switch(config)# copy running-config startup-config
```

（任意）この設定の変更を保存します。

ジョブの削除

コマンド スケジューラのジョブを削除するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configuration terminal**

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)# **no scheduler job name addMemVsan99**

定義済みジョブおよびジョブ内で定義されたすべてのコマンドを削除します。

スケジュールの指定

ジョブを定義したら、スケジュールを作成してスケジュールにジョブを割り当てることができます。その後、実行時刻を設定できます。ジョブは、必要に応じて、1 回だけまたは定期的に実行できます。スケジュールの時刻が設定されていないと、ジョブは実行されません。

定期的なジョブの実行は、間隔（毎日、毎週、毎月、または差分）を指定できます。

コマンド スケジューラの定期ジョブを指定するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configuration terminal**

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)# **scheduler schedule name weekendbackupqos**

switch(config-schedule)#

ジョブ スケジュール（weekendbackup）を定義して、そのスケジュールのサブモードを開始します。

ステップ 3 switch(config)# **no scheduler schedule name weekendbackup**

定義したスケジュールを削除します。

ステップ 4 switch(config-schedule)# **job name offpeakZoning**

switch(config-schedule)# **job name offpeakQOS**

このスケジュールに 2 つのジョブ（offpeakZoning および offpeakQOS）を割り当てます。

ステップ 5 switch(config-schedule)# **no job name addMem99**

このスケジュールに割り当てられたジョブを削除します。

例

次に示す設定は参考例です。

コマンド	目的
switch(config-schedule)# **time daily 23:00**	指定されたジョブを、毎日午後 11 時に実行します。
switch(config-schedule)# **time weekly Sun:23:00**	毎週日曜日の午後 11 時に実行するように指定します。
switch(config-schedule)# **time monthly 28:23:00**	毎月 28 日の午後 11 時に実行するように指定します。日にちを 29、30、または 31 日に指定した場合、コマンドは各月の最終日に自動的に実行されます。
switch(config-schedule)# **time start now repeat 48:00**	*now* から 2 分後に 48 時間ごとに実行するジョブを指定します。今日が 2004 年 9 月 24 日で、現在の時刻が午後 2 時である場合、コマンドは 2004 年 9 月 24 日の午後 2 時 2 分に実行を開始します。その後も 48 時間ごとに実行され続けます。
switch(config-schedule)# **time start 14:00 repeat 14:00:00**	今日が 2004 年 9 月 24 日（金曜日）である場合、このコマンドは、隔週金曜日の午後 2 時（14 日ごと）に実行されるジョブを指定します。

time パラメータの主なフィールドは大半がオプションです。これらのフィールドを省略すると、現在時刻と同じ値が指定されたと見なされます。たとえば、現在時刻が 2004 年 9 月 24 日の 22:00 の場合、コマンドは次のように実行されます。

- **time start 23:00 repeat 4:00:00** コマンドの場合、開始時刻は 2004 年 9 月 24 日の 23 時 00 分です。
- **time daily 55** コマンドの場合、毎日 22 時 55 分に実行されます。
- **time weekly 23:00** コマンドの場合、 毎週金曜日の 23 時 00 分に実行されます。
- **time monthly 23:00** コマンドの場合、毎月 24 日の 23 時 00 分に実行されます。

Note スケジュールに対して設定された時間間隔が、割り当てられたジョブの実行に必要な時間よりも短い場合、直前のスケジュール実行完了時刻から設定された時間間隔が経過しないと後続のスケジュールは実行されません。たとえば、スケジュールが 1 分間隔で実行され、スケジュールに割り当てられたジョブが完了するのに 2 分かかる場合です。最初のスケジュールが 22:00 に実行され、ジョブが 22:02 に完了する場合、次の処理は 1 分間隔に従って 22:03 に実行されて 22:05 に完了します。

一時的スケジュールの指定

一時ジョブの実行を指定すると、そのジョブは一度だけ実行されます。

コマンド スケジューラの一時ジョブを指定するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configuration terminal**

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)# **scheduler schedule name configureVsan99**

switch(config-schedule)#

ジョブ スケジュール（configureVsan99）を定義して、そのスケジュールのサブモードを開始します。

ステップ 3 switch(config-schedule)# **job name addMemVsan99**

このスケジュールに定義済みジョブ名（addMemVsan99）を割り当てます。

ステップ 4 switch(config-schedule)# **time start 2004:12:14:23:00**

2004 年 12 月 14 日の午後 11 時に 1 回だけ実行するように指定します。

ステップ 5 switch(config-schedule)# **no time**

このスケジュールに割り当てられた時刻を削除します。

スケジュールの削除

スケジュールを削除するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configuration terminal**

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)# **no scheduler schedule name weekendbackup**

定義したスケジュールを削除します。

割り当てられたジョブの削除

割り当てられたジョブを削除するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configuration terminal**

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)# **scheduler schedule name weekendbackupqos**

switch(config-schedule)#

ジョブ スケジュール（weekendbackupqos）を指定して、そのスケジュールのサブモードを開始します。

ステップ 3 switch(config-schedule)# **no job name addMem99**

このスケジュールに割り当てられたジョブ（addMem99）を削除します。

スケジュール時刻の削除

スケジュール時刻を削除するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configuration terminal**

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)# **scheduler schedule name weekendbackupqos**

switch(config-schedule)#

ジョブ スケジュール（weekendbackup）を定義して、そのスケジュールのサブモードを開始します。

ステップ 3 switch(config-schedule)# **no time**

スケジュール時刻の設定を削除します。このスケジュールは時刻を再度設定するまで実行されません。

実行ログの設定

コマンド スケジューラはログ ファイルを管理しています。このファイルの内容は変更できませんが、ファイルサイズは変更できます。このログファイルは循環ログで、実行されたジョブの出力が格納されます。ジョブの出力がログ ファイルよりも大きい場合、このファイルに格納される出力は一部が切り捨てられます。

設定できるログ ファイルの最大サイズは 1024 KB です実行ログ ファイルのデフォルト サイズは 16 KB です。

実行ログ ファイルのサイズを設定するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configuration terminal**

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)# **scheduler logfile size 1024**

ログファイルを最大 1024 KB に設定します。

ステップ 3 switch(config)# **no scheduler logfile size**

ログのサイズをデフォルトの 16 KB に設定します。

実行ログ ファイルの内容のクリア

スケジューラ実行ログ ファイルの内容をクリアするには、EXEC モードで clear scheduler logfile コマンドを実行します。

```
switch# clear scheduler logfile
```

スケジューラ設定の確認

スケジューラの構成情報を表示するには、次のタスクのいずれかを行います。

コマンド	目的
show scheduler config	スケジューラ構成を表示します。
show scheduler schedule	コマンド スケジューラの実行ステータスの確認
show scheduler job	ジョブ定義の確認
show scheduler logfile	システムで実行されたすべてのジョブの実行ログを表示します
clear scheduler logfile	スケジューラ実行ログファイルの内容をクリアする

これらのコマンドの出力に表示される各フィールドの詳細については、『*Cisco MDS 9000 Family Command Reference*』を参照してください。

コマンド スケジューラの構成の確認

スケジューラ構成を表示するには、**show scheduler config** コマンドを使用します。

```
switch# show scheduler config
config terminal
  feature scheduler
  scheduler logfile size 512
end
config terminal
   scheduler job name addMemVsan99
     config terminal
       vsan database
       vsan 99 interface fc1/1
       vsan 99 interface fc1/2
       vsan 99 interface fc1/3
       vsan 99 interface fc1/4
```

```
end
config terminal
  scheduler schedule name configureVsan99
    time start 2004:8:10:9:52
    job name addMemVsan99
end
```

コマンド スケジューラの実行ステータスの確認

コマンド スケジューラの実行ステータスを確認するには、**show scheduler schedule** コマンドを使用します。

```
switch# show scheduler schedule configureVsan99
Schedule Name      : configureVsan99
-----------------------------------
User Name          : admin
Schedule Type      : Run once on Tue Aug 10 09:48:00 2004
Last Execution Time: Tue Aug 10 09:48:00 2004
-----------------------------------------------
          Job Name                  Status
```

ジョブ定義の確認

ジョブ定義を確認するには、**show scheduler job** コマンドを使用します。

```
switch# show scheduler job addMemVsan99
Job Name: addMemVsan99
----------------------
  config terminal
   vsan database
    vsan 99 interface fc1/1
    vsan 99 interface fc1/2
    vsan 99 interface fc1/3
    vsan 99 interface fc1/4
```

実行ログ ファイルの内容の表示

システムで実行されるすべてのジョブの実行ログを表示するには、**show scheduler logfile** コマンドを使用します。

```
switch# show scheduler logfile
Job Name       : addMemVsan99              Job Status: Success (0)
Schedule Name  : configureVsan99           User Name : admin
Completion time: Tue Aug 10 09:48:00 2004
-------------------------- Job Output --------------------------
`config terminal`
`vsan database`
`vsan 99 interface fc1/1`
`vsan 99 interface fc1/2`
`vsan 99 interface fc1/3`
`vsan 99 interface fc1/4`
```

リモート ユーザのスケジューラ パスワード構成を表示するには、**show running-config** コマンドを使用します。

```
switch# show running-config | include "scheduler aaa-authentication"
scheduler aaa-authentication username newuser password 7 "C98d76S54e"
```

Note スケジューラ リモート ユーザ パスワードは、**show running-config** コマンドの出力中で、常に暗号化された形式で表示されます。コマンド中の暗号化オプション（**7**）は、ASCII 構成のスイッチへの適用をサポートするためにあります。

実行ログ ファイルの構成を表示するには、 **show scheduler config** コマンドを使用します。

```
switch# show scheduler config
config terminal
  feature scheduler
  scheduler logfile size 1024
end
```

実行ログ ファイルの内容のクリア

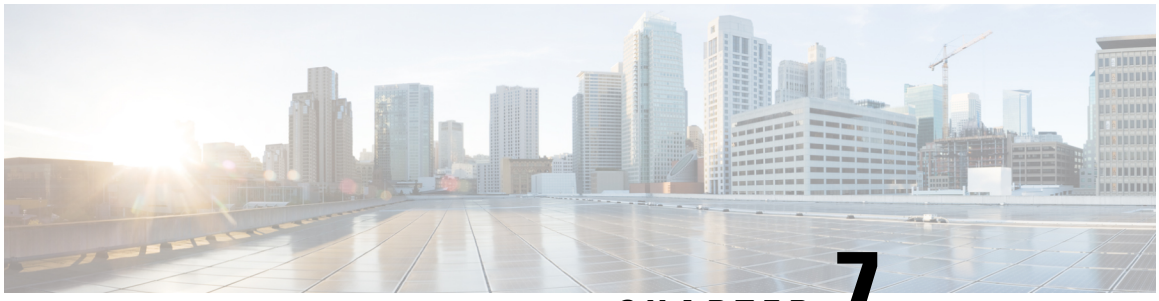
スケジューラ実行ログ ファイルの内容をクリアするには、EXEC モードで **clear scheduler logfile** コマンドを実行します。

```
switch# clear scheduler logfile
----------------------------------------------
addMemVsan99                        Success (0)
```

スケジューラのコンフィギュレーション例

```
configure terminal

scheduler job name start
 configure
 no cli var name time
 exit
 echo $(TIMESTAMP) | sed 's/^/cli var name time /' | vsh
 show switchname > debug-$(time)-1
 show switchname > debug-$(time)-2
 exit

scheduler job name part1
 show clock >> debug-$(time)-1
 show interface mgmt 0 >> debug-$(time)-1
 sleep 60
 show clock >> debug-$(time)-1
 show interface mgmt 0 >> debug-$(time)-1
 sleep 200
 gzip debug-$(time)-1
 exit
```

```
scheduler job name part2
 show clock >> debug-$(time)-2
 show processes cpu history >> debug-$(time)-2
 sleep 60
 show clock >> debug-$(time)-2
 show processes cpu history >> debug-$(time)-2
 show clock >> debug-$(time)-2
 gzip debug-$(time)-2
 exit

scheduler schedule name cpu-stats
  job name start
  job name part1
  job name part2
  time start 2001:12:31:01:00
  exit

end
```



CHAPTER 7

システム ステータス モニタリング

この章では、スイッチ状態のモニタリングについて詳細に説明します。

- システム ステータス モニタリングの機能履歴, on page 143
- システム ステータス モニタリングについての情報 （144 ページ）
- デフォルト設定, on page 149
- システム ヘルスの設定, on page 149
- オンボード障害ロギングの構成, on page 156
- モジュール カウンタのクリア, on page 159
- アラート、通知、およびカウンタのモニタリングの構成, on page 160
- コアの構成 （163 ページ）
- システム ステータスのモニタリング構成の確認, on page 166
- その他の参考資料, on page 177

システム ステータス モニタリングの機能履歴

Table 19: システム ステータス モニタリングの機能履歴 , on page 143 に、この機能のリリース履歴を示します。リリース 3.x 以降のリリースで導入または変更された機能のみが表に記載されています。

Table 19: システム ステータス モニタリングの機能履歴

機能名	リリース	機能情報
共通情報モデル（CIM）	3.3(1a)	共通情報モデルを表示するためのコマンドが追加されました。

機能名	リリース	機能情報
オンライン システム正常性メンテナンス（OHMS）の機能拡張	3.0(1)	次の OHMS 機能拡張が含まれています。 • スイッチ上のすべてのモジュールのループバック テストのグローバル フレーム長を構成します。 • 特定のモジュールでのループバック テストのフレーム カウントとフレーム長を指定します。 • 外部ループバック テスト用の送信元ポートと宛て先ポートの構成。 • ハードウェアをチェックするための serdes ループバック テストを提供します。
オンボード障害ロギング（OBFL）	3.0(1)	OBFL、第 2 世代モジュール用に OBFL を構成する方法、およびログ情報を表示する方法について説明します。

システム ステータス モニタリングについての情報

オンライン ヘルス管理システム

Online Health Management System（OHMS、システム ヘルス）は、ハードウェア障害検出および復旧機能です。OHMS は、Cisco MDS 9000 シリーズのすべてのスイッチのスイッチング モジュール、サービス モジュール、スーパーバイザ モジュールの全般的な状態を確認します。

OHMS は、システム ハードウェアを次のようにモニタリングします。

- アクティブ スーパーバイザ稼働する OHMS コンポーネントは、スイッチ内の他のモジュール上で稼働する他のすべての OHMS コンポーネントを制御します。
- スタンバイ スーパーバイザ モジュール上で稼働するシステム ヘルス アプリケーションは、そのモジュールが HA スタンバイ モードで使用できる場合でも、スタンバイ スーパーバイザ モジュールだけを監視します。

OHMS アプリケーションはすべてのモジュールでデーモン プロセスを起動して、各モジュール上で複数のテストを実行し、モジュールの個々のコンポーネントをテストします。これらのテストは、事前に設定されたインターバルで実行され、すべての主要な障害ポイントを対象として、障害が発生している MDS スイッチのコンポーネントを隔離します。アクティブ スーパーバイザ上で稼働する OHMS は、スイッチ内の他のすべてのモジュール上で稼働する他のすべての OHMS コンポーネントを制御します。

障害を検出すると、システム ヘルス アプリケーションは次のリカバリ アクションを試行します。

- 障害のあるコンポーネントを隔離するため、追加のテストを実行します。

- 永続的ストレージから設定情報を取得し、コンポーネントの再設定を試みます。
- 復旧できない場合、Call Home 通知、システム メッセージ、および例外ログを送信します。障害の発生しているモジュールまたはコンポーネント（インターフェイスなど）をシャットダウンし、テストを中止します。
- 障害を検出すると、ただちにCall Homeメッセージ、システム メッセージ、および例外ログを送信します。
- 障害の発生しているモジュールまたはコンポーネント（インターフェイスなど）をシャットダウンします。
- 詳細なテストが実行されないように、障害が発生したポートを隔離します。
- その障害を適切なソフトウェア コンポーネントに報告します。
- スタンバイ スーパーバイザ モジュールに切り替えます（障害がアクティブ スーパーバイザ モジュールで検出され、Cisco MDS スイッチにスタンバイ スーパーバイザ モジュールが搭載されている場合）。スイッチオーバーが完了すると、新しいアクティブ スーパーバイザ モジュールはアクティブ スーパーバイザ テストを再開します。
- スイッチをリロードします（スイッチにスタンバイ スーパーバイザ モジュールが搭載されていない場合）。
- テストの実行統計情報を表示、テスト、および取得したり、スイッチのシステム ヘルス テスト設定を変更したりするための CLI サポートを提供します。
- 問題領域に焦点を当てるためのテストを実行します。

各モジュールはそれぞれに対応するテストを実行するように設定されています。必要に応じて、各モジュールのデフォルト パラメータを変更できます。

ループバック テストの設定頻度

ループバック テストは、モジュール内のデータ パスおよびスーパーバイザ内の制御パスにおいてハードウェア エラーを特定するように設計されています。事前に設定された頻度でループバック フレームが各モジュールに1つずつ送信されます。このフレームは、それぞれに設定されたインターフェイスを通過した後、スーパーバイザ モジュールに戻ります。

ループバック テストは5（デフォルト）～255秒の範囲の頻度で実行できます。ループバック頻度の値を設定しなければ、デフォルトの頻度である5秒がスイッチ内のすべてのモジュールに対して使用されます。ループバック テストの頻度は、モジュールごとに変更できます。

ループバック テストのフレーム長の設定

ループバック テストは、モジュール内のデータ パスおよびスーパーバイザ内の制御パスにおいてハードウェア エラーを特定するように設計されています。事前に設定されたサイズでループバック フレームが各モジュールに1つずつ送信されます。このフレームは、それぞれに設定されたインターフェイスを通過した後、スーパーバイザ モジュールに戻ります。

ループバック テストは、0 ～ 128 バイトの範囲のフレーム サイズで実行できます。ループバック フレーム長の値を設定しなければ、スイッチ内のすべてのモジュールに対してランダムなフレーム長がスイッチによって生成されます（自動モード）。ループバック テストのフレーム長は、モジュールごとに変更できます。

ハードウェア障害時の処理

failure-action コマンドは、テストの実行中にハードウェア障害が発見された場合に、Cisco NX-OS ソフトウェアによる処理の実行を抑制します。

デフォルトでは、Cisco MDS 9000 ファミリのすべてのスイッチでこの機能はイネーブルになります。障害が発見されると処理が実行され、障害が発生したコンポーネントはそれ以降のテストから隔離されます。

障害処理は、個々のテスト レベル（モジュール単位）、モジュール レベル（すべてのテスト）、またはスイッチ全体で制御されます。

テストの実行要件

テストをイネーブルにしても、テストの実行が保障されるわけではありません。

特定のインターフェイスまたはモジュールのテストが実行されるのは、次のすべての項目に対してシステム ヘルスをイネーブルにしている場合だけです。

- スイッチ全体
- 必要なモジュール
- 必要なインターフェイス

Tip 上記のいずれかによってシステム ヘルスがディセーブルになっている場合、テストは実行されません。システム ヘルスでテストの実行がディセーブルになっている場合、テスト ステータスはディセーブル（Disabled）と表示されます。

Tip 特定のモジュールまたはインターフェイスでテストの実行がイネーブルになっているが、システム ヘルスがディセーブルであるためにテストが実行されない場合、テストはイネーブル（Enabled）と表示されます（実行中（Running）にはなりません）。

特定モジュールのテスト

NX-OS ソフトウェアのシステム ヘルス機能は、次の領域のテストを実行します。

- アクティブなスーパーバイザのファブリックへのインバンド接続。
- スタンバイ スーパーバイザのアービターの可用性。
- すべてのモジュール上でのブートフラッシュの接続性とアクセシビリティ。
- すべてのモジュール上での EOBC の接続性とアクセシビリティ。
- すべてのモジュール上の各インターフェイスのデータ パスの完全性。

- 管理ポートの接続。
- 外部接続性検証のためのユーザによるテスト。テスト中はポートがシャットダウンされます（ファイバ チャネル ポートのみ）。
- 内部接続性検証のためのユーザによるテスト（ファイバ チャネル ポートと iSCSI ポート）。

Note Cisco MDS 9700 シリーズ スイッチでは、iSCSI ポートは適用されません。

前回のエラー レポートのクリア

ファイバ チャネル インターフェイス、iSCSI インターフェイス、モジュール全体、またはモジュール全体の特定の 1 つのテストについて、エラー履歴をクリアできます。履歴をクリアすると、障害が発生してテストから除外されていたコンポーネントはすべて再度テストされます。

障害発生時に OHMS が一定期間（たとえば、1 週間）の間処理を実行しないようにオプション failure-action オプションをイネーブルにしていて、指定期間が経過した後でエラー受信を再開する準備が整った場合には、それぞれのテストのシステム ヘルス エラー ステータスをクリアする必要があります。

Tip 管理ポートテストは、スタンバイ スーパーバイザ モジュール上で実行することはできません。

現在のステータスの説明

各モジュールまたはテストのステータスは、その特定のモジュールでの OHMS テストの現在の設定状態によって異なります（Table 20: テストおよびモジュールに関する OHMS の設定ステータス , on page 147 を参照）。

Table 20: テストおよびモジュールに関する ***OHMS*** の設定ステータス

ステータス	説明
Enabled	このモジュールのテストは有効化されていますが、現在は実行されていません。
無効	現在このモジュールのテストは無効化されています。
Running	このモジュールのテストは有効化されていて、現在実行中です。
Failing	このステートは、このモジュールで実行中のテストで障害が発生しそうな場合に表示されます。このステートは、テストで回復できる可能性があります。

ステータス	説明
失敗しました	このモジュールのテストで障害が発生しました。ステートは回復できません。
停止（Stopped）	テストは、Cisco NX-OS ソフトウェアによってこのモジュールのテストが内部的に停止されました。
Internal failure	このモジュールのテストで、内部障害が発生しました。たとえば、システム ヘルス アプリケーションがテスト手順の一部でソケットをオープンできません。
Diags failed	このモジュールまたはインターフェイスの起動時の診断で障害が発生しました。
オン デマンド	現在、このモジュールで、システム正常性の外部ループバックまたはシステム正常性の内部ループバック テストが実行中です。オンデマンドで発行できるのは、これらの 2 つのコマンドだけです。
一時停止	1 つのオーバーサブスクライブ ポートが E または TE ポート モードに移行することにより、MDS 9100 シリーズでのみ発生します。1 つのオーバーサブスクライブ ポートがこのモードに移行すると、グループ内の他の 3 つのオーバーサブスクライブ ポートは中断されます。

各モジュールの各テストのステータスは、**show system health** コマンドで表示できます。「システム ヘルスの表示 , on page 166」を参照してください。

オンボード障害ロギング

第 2 世代ファイバ チャネル スイッチング モジュールでは、障害データを永続的ストレージに記録する機能が提供されます。この記録は、分析用に取得したり、表示したりできます。この On-Board Failure Logging（OBFL: オンボード障害ロギング）機能は、障害および環境情報をモジュールの不揮発性メモリに保管します。この情報は、障害が発生したカードの事後分析に役立ちます。

OBFL データは、モジュール上の既存の CompactFlash に保存されます。OBFL では、モジュールのファームウェアで使用できる永続的ロギング（PLOG）機能を使用して CompactFlash にデータを保存します。保存されたデータを取得するためのメカニズムも提供されます。

OBFL 機能によって保存されるデータは、次のとおりです。

- 最初の電源投入時刻
- カードのシャーシ スロット番号
- カードの初期温度
- ファームウェア、BIOS、FPGA、および ASIC のバージョン
- カードのシリアル番号
- クラッシュのスタック トレース

- CPU hog 情報
- メモリ リーク情報
- ソフトウェア エラー メッセージ
- ハードウェア例外ログ
- 環境履歴
- OBFL 固有の履歴情報
- ASIC 割り込みおよびエラー統計の履歴
- ASIC レジスタ ダンプ

デフォルト設定

Table 21: デフォルトのシステム ステータス モニタリング, on page 149 に、デフォルト設定を示します。

Table 21: デフォルトのシステム ステータス モニタリング

パラメータ	デフォルト
カーネル コア収集	無効
システム ヘルス	有効
ループバック頻度	5 秒
障害処理	有効（Enabled）

システム ヘルスの設定

Online Health Management System（OHMS、システム ヘルス）は、ハードウェア障害検出および復旧機能です。OHMS は、Cisco MDS 9000 ファミリのすべてのスイッチのスイッチング モジュール、サービス モジュール、スーパーバイザ モジュールの全般的な状態を確認します。

システムの正常性を構成するためのタスク フロー

システムの正常性を構成するには、次の手順を実行します。

Procedure

ステップ 1 システム正常性の開始を有効化します。
ステップ 2 ループバック テストの構成頻度を構成します。
ステップ 3 ループバック テスト構成のフレーム長を構成します。

ステップ 4 ハードウェア障害アクションを構成します。
ステップ 5 テストの実行要件を実施します。
ステップ 6 前回のエラー レポートをクリアします。
ステップ 7 内部ループバック テストを実施します。
ステップ 8 外部ループバック テストを実施します。
ステップ 9 Serdes ループバックを実施します。

システムの正常性開始の構成

デフォルトでは、システムの正常性機能はCisco MDS 9000 ファミリの各スイッチで有効です。

Cisco MDS 9000 ファミリの任意のスイッチでこの機能を無効化または有効化するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **no system health**

システム正常性が無効になっています。

このスイッチでテストを実行できないようにシステム ヘルスを設定します。

ステップ 3 switch(config)# **system health**

システム正常性が有効になっています。

このスイッチでテストを実行できるようにシステム ヘルスを設定します（デフォルト）。

ステップ 4 switch(config)# **no system health interface fc8/1**

インターフェイス fc8/13 のシステム正常性が無効になっています。

指定されたインターフェイスのテストを実行できないようにシステム正常性を設定します。

ステップ 5 switch(config)# **system health interface fc8/1**

インターフェイス fc8/13 のシステム正常性が有効になっています。

システム正常性を有効（デフォルト）にして、指定されたインターフェイスをテストします。

ループバック テストの構成頻度の構成

スイッチのすべてのモジュールにループバック テストの頻度を構成するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **system health loopback frequency 50**

```
The new frequency is set at 50 Seconds.
```

ループバック頻度を 50 秒に設定します。デフォルトのループバック頻度は 5 秒です。指定できる範囲は 5 ～ 255 秒です。

ループバック テスト構成のフレーム長の構成

スイッチのすべてのモジュールにループバック テストのフレーム長を構成するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **system health loopback frame-length 128**

ループバック フレーム長を 128 バイトに構成します。有効な範囲は 0 ～ 128 バイトです。

ステップ 3 switch(config)# **system health loopback frame-length auto**

ループバック フレーム長を自動的にランダム長（デフォルト）を生成するように構成します。

ハードウェア障害アクションの構成

スイッチの障害アクションを構成するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **system health failure-action**

```
System health global failure action is now enabled.
```

障害処理を実行できるようにスイッチを設定します（デフォルト）。

ステップ 3 switch(config)# **no system health failure-action**

```
System health global failure action now disabled.
```

障害処理が実行されないようにスイッチの設定を取り消します。

ステップ 4 switch(config)# **system health module 1 failure-action**

```
System health failure action for module 1 is now enabled.
```

モジュール 1 の障害処理を実行できるようにスイッチを設定します。

ステップ 5 switch(config)# **no system health module 1 loopback failure-action**

```
System health failure action for module 1 loopback test is now disabled.
```

モジュール 1 のループバック テストによって発見された障害に対する障害処理を実行しないようにスイッチを設定します。

テストの実行要件

特定のモジュールで必要なテストを実行するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

Note
次のステップは、任意の順序で実行できます。

Note
それぞれのテストの各種オプションについては、次のステップで説明します。各コマンドは任意の順序で設定できます。説明のため、各種オプションを同じステップに記述しています。

ステップ 2 switch(config)# **system health module 8 bootflash**

スロット 8 のモジュールでブートフラッシュ テストを有効にします。

ステップ 3 switch(config)# **system health module 8 bootflash frequency 200**

モジュール 8 のブートフラッシュ テストの新しい頻度を 200 秒に設定します。

ステップ 4 switch(config)# **system health module 8 eobc**

スロット 8 のモジュールで EOBC テストを有効にします。

ステップ 5 switch(config)# **system health module 8 loopback**

スロット 8 のモジュールでループバック テストを有効にします。

ステップ 6 switch(config)# **system health module 5 management**

スロット 5 のモジュールで管理テストを有効にします。

前回のエラー レポートのクリア

インターフェイスまたはモジュール レベルで EXEC レベルの **system health clear-errors** コマンドを使用すると、システム正常性アプリケーションで記録された古いエラー状態はすべて消去されます。**bootflash**、**eobc**、**inband**、**loopback**、および **mgmt** テスト オプションは所定のモジュールに対して個別に指定することができます。

次の例では、指定されたファイバチャネルインターフェイスのエラー履歴がクリアされます。

```
switch# system health clear-errors interface fc 3/1
```

次の例では、指定されたモジュールのエラー履歴がクリアされます。

```
switch# system health clear-errors module 3
```

次の例では、指定されたモジュールの管理テストのエラー履歴がクリアされます。

```
switch# system health clear-errors module 1 mgmt
```

内部ループバック テストの実行

手動ループバック テストを実行すると、スイッチング モジュールまたはサービス モジュールのデータ パスや、スーパーバイザ モジュールの制御パスにおけるハードウェア エラーを特定

できます。内部ループバック テストは同一のポートに対して FC2 フレームを送受信し、ラウンドトリップ時間をマイクロ秒単位で示します。このテストは、ファイバ チャネル インターフェイス、IPS インターフェイス、iSCSI インターフェイスで使用できます。

モジュール全体のポート内でこのテストを（ユーザが要求したときに）オンデマンドで明示的に実行するには、EXEC レベルで **system health internal-loopback** コマンドを使用します。

```
switch# system health internal-loopback interface iscsi 8/1
Internal loopback test on interface iscsi8/1 was  successful.
Sent 1 received 1 frames
Round trip time taken is 79 useconds
```

モジュール全体のポート内でこのテストを（ユーザが要求したときに）オンデマンドで明示的に実行し、スイッチに構成されているフレーム数を上書きするには、EXEC レベルで **system health internal-loopback** コマンドを使用します。

```
switch# system health internal-loopback interface iscsi 8/1 frame-count 20
Internal loopback test on interface iscsi8/1 was  successful.
Sent 1 received 1 frames
Round trip time taken is 79 useconds
```

モジュール全体のポート内でこのテストを（ユーザが要求したときに）オンデマンドで明示的に実行し、スイッチに構成されているフレーム長を上書きするには、EXEC レベルで **system health internal-loopback** コマンドを使用します。

```
switch# system health internal-loopback interface iscsi 8/1 frame-count 32
Internal loopback test on interface iscsi8/1 was  successful.
Sent 1 received 1 frames
Round trip time taken is 79 useconds
```

Note テストが正常に完了しなかった場合、ソフトウェアは失敗を分析し、次のエラーを出力します。「インターフェイス fc 7/2 の外部ループバック テストが失敗しました。」失敗の理由：ループバックが失敗しました。モジュール 1 での失敗したデバイス ID 3 の分析を完了します

外部ループバック テストの実行

手動ループバック テストを実行すると、スイッチング モジュールまたはサービス モジュールのデータ パスや、スーパーバイザ モジュールの制御パスにおけるハードウェア エラーを特定できます。外部ループバック テストは、同一のポートの間または2つのポート間でFC2フレームを送受信します。

テストを実行する前に、Rx ポートから Tx ポートへループさせるためにケーブル（またはプラグ）を接続する必要があります。同じポートの間でテストする場合は、特殊なループ ケーブルが必要です。異なるポートとの間でテストする場合は、通常のケーブルを使用できます。このテストを使用できるのは、ファイバ チャネル インターフェイスだけです。

長距離ネットワークに属するスイッチに接続されている外部デバイスに対してこのテストをオンデマンドで実行するには、EXEC レベルで **system health external-loopback interface** *interface* コマンドを使用します。

```
switch# system health external-loopback interface fc 3/1
This will shut the requested interfaces Do you want to continue (y/n)?  [n] y
External loopback test on interface fc3/1 was  successful.
Sent 1 received 1 frames
```

スイッチの2つのポート間でこのテストをオンデマンドで実行するには、EXEC レベルの **system health external-loopback source** *interface* **destination interface** *interface* コマンドを使用します。

```
switch# system health external-loopback source interface fc 3/1 destination interface
fc 3/2
This will shut the requested interfaces Do you want to continue (y/n)?  [n] y
External loopback test on interface fc3/1 and interface fc3/2 was  successful.
Sent 1 received 1 frames
```

長距離ネットワークに属するスイッチに接続されている外部デバイスに対してこのテストをオンデマンドで実行し、スイッチ上で構成されたフレーム カウントを上書きするには、EXEC レベルで **system health external-loopback** *interface* **frame-count** コマンドを使用します。

```
switch# system health external-loopback interface fc 3/1 frame-count 10
This will shut the requested interfaces Do you want to continue (y/n)?  [n] y
External loopback test on interface fc3/1 was  successful.
Sent 1 received 1 frames
```

長距離ネットワークに属するスイッチに接続されている外部デバイスに対してこのテストをオンデマンドで実行し、スイッチ上で構成されたフレーム長を上書きするには、EXEC レベルで **system health external-loopback** *interface* **frame-length** コマンドを使用します。

```
switch# system health external-loopback interface fc 3/1 frame-length 64
This will shut the requested interfaces Do you want to continue (y/n)?  [n] y
External loopback test on interface fc3/1 was  successful.
Sent 1 received 1 frames
```

system health external-loopback *interface* **force** コマンドを使用して、バック アウトの確認なしで必要なインターフェイスを直接シャットダウンします。

```
switch# system health external-loopback interface fc 3/1 force
External loopback test on interface fc3/1 was  successful.
Sent 1 received 1 frames
```

Note テストが正常に完了しなかった場合、ソフトウェアは失敗を分析し、次のエラーを出力します。「インターフェイス fc 7/2 の外部ループバック テストが失敗しました。」失敗の理由：ループバックが失敗しました。モジュール 1 での失敗したデバイス ID 3 の分析を完了します

Serdes ループバックの実行

シリアライザ/デシリアライザ（serdes）ループバックでは、ポートのハードウェアがテストされます。このテストは、ファイバチャネル インターフェイスで使用できます。

モジュール全体のポート内でこのテストを（ユーザが要求したときに）オンデマンドで明示的に実行するには、EXEC レベルで **system health serdes-loopback** コマンドを使用します。

```
switch# system health serdes-loopback interface fc 3/1
This will shut the requested interfaces Do you want to continue (y/n)?  [n] y
Serdes loopback test passed for module 3 port 1
```

モジュール全体のポート内でこのテストを（ユーザが要求したときに）オンデマンドで明示的に実行し、スイッチに構成されているフレーム数を上書きするには、EXEC レベルで **system health serdes-loopback** コマンドを使用します。

```
switch# system health serdes-loopback interface fc 3/1 frame-count 10
This will shut the requested interfaces Do you want to continue (y/n)?  [n] y
Serdes loopback test passed for module 3 port 1
```

モジュール全体のポート内でこのテストを（ユーザが要求したときに）オンデマンドで明示的に実行し、スイッチに構成されているフレーム長を上書きするには、EXEC レベルで **system health serdes-loopback** コマンドを使用します。

```
switch# system health serdes-loopback interface fc 3/1 frame-length 32
This will shut the requested interfaces Do you want to continue (y/n)?  [n] y
Serdes loopback test passed for module 3 port 1
```

Note テストが正常に完了しなかった場合、ソフトウェアは失敗を分析し、次のエラーを出力します。「インターフェイス fc 3/1 の外部ループバック テストが失敗しました。」失敗の理由：ループバックが失敗しました。モジュール 3 での失敗したデバイス ID 3 の分析を完了します。

オンボード障害ロギングの構成

各ハードウェア モジュールは障害データをオンモジュールの永続的ストレージに記録し、この記録は、分析用に取得したり、表示したりできます。この On-Board Failure Logging（OBFL: オンボード障害ロギング）機能は、障害および環境情報をモジュールの不揮発性メモリに保管します。この情報は、障害が発生したカードの事後分析に役立ちます。

Note インサービス ソフトウェア アップグレード（ISSU）を開始する前に、すべてのモジュールとスイッチの統計情報をクリアすることをお勧めします。ISSU を開始する前にハードウェア統計情報をクリアしなかった場合、システム ログに重複する OBFL エントリが表示されることがあります。

スイッチの OBFL の構成

スイッチのすべてのモジュールに OBFL を構成するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **hw-module logging onboard**

すべての OBFL 機能をイネーブルにします。

Note
この CLI は、no hw-module logging onboard コマンドによって無効にされた OBFL 機能のみを有効にします。個別に無効にされていた OBFL 機能については、hw-module logging onboard obfl-feature コマンドを使用して有効にしてください。

ステップ 3 switch(config)# **hw-module logging onboard cpu-hog**

OBFL CPU hog イベントを有効にします。

ステップ 4 switch(config)# **hw-module logging onboard environmental-history**

OBFL 環境履歴をイネーブルにします。

ステップ 5 switch(config)# **hw-module logging onboard error-stats**

OBFL エラー統計をイネーブルにします。

ステップ 6 switch(config)# **hw-module logging onboard interrupt-stats**

OBFL 割り込み統計をイネーブルにします。

ステップ 7 switch(config)# **hw-module logging onboard mem-leak**

OBFL メモリ リーク イベントを有効にします。

ステップ 8 switch(config)# **hw-module logging onboard miscellaneous-error**

OBFL のその他の情報を有効にします。

ステップ 9 switch(config)# **hw-module logging onboard obfl-log**

ブート動作時間、デバイス バージョン、および OBFL 履歴をイネーブルにします。

ステップ 10 switch(config)# **no hw-module logging onboard**

すべての OBFL 機能をディセーブルにします。

モジュールの OBFL の構成

スイッチの特定のモジュールに OBFL を構成するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **hw-module logging onboard module 1**

モジュールのすべての OBFL 機能を有効にします。

ステップ 3 switch(config)# **hw-module logging onboard module 1 cpu-hog**

モジュールの OBFL CPU hog イベントを無効にします。

ステップ 4 switch(config)# **hw-module logging onboard module 1 environmental-history**

モジュールの OBFL 環境履歴を有効にします。

ステップ 5 switch(config)# **hw-module logging onboard module 1 error-stats**

モジュールの OBFL エラー統計を有効にします。

ステップ 6 switch(config)# **hw-module logging onboard module 1 interrupt-stats**

モジュールの OBFL 割り込み統計を有効にします。

ステップ 7 switch(config)# **hw-module logging onboard module 1 mem-leak**

モジュールの OBFL メモリ リーク イベントを有効にします。

ステップ 8 switch(config)# **hw-module logging onboard module 1 miscellaneous-error**

モジュールの OBFL のその他の情報を有効にします。

ステップ 9 switch(config)# **hw-module logging onboard module 1 obfl-log**

モジュールのブート稼働時間、デバイス バージョン、および OBFL 履歴を有効にします。

ステップ 10 switch(config)# **no hw-module logging onboard module 1**

モジュールのすべての OBFL 機能を無効にします。

モジュール カウンタのクリア

Note モジュール カウンタは、Device Manager または DCNM-SAN を使用してクリアできません。

モジュール カウンタをリセットする手順は、次のとおりです。

Procedure

ステップ 1 switch# **attach module 1**

ModuleX#

モジュール 1 をシャーシに取り付けます。

ステップ 2 ModuleX# **clear asic-cnt all**

モジュール内のすべてのデバイスのカウンタをクリアします。

ステップ 3 ModuleX# **clear asic-cnt list-all-devices**

ModuleX# **clear asic-cnt device-id** *device-id*

指定されたデバイス ID のみのカウンタをクリアします。デバイス ID は、1 ～ 255 の範囲で指定できます。

すべてのモジュールのカウンタのリセット

すべてのモジュールのカウンタをリセットするには、次の手順に従います。

Procedure

switch# **debug system internal clear-counters all**

スイッチ内のすべてのモジュールのカウンタをクリアします。

アラート、通知、およびカウンタのモニタリングの構成

このセクションでは、アラート、通知、およびモニタのカウンタを構成する方法について説明します。

CPU 使用率のモニタリング

システム CPU の使用状況を表示するには、 **show processes cpu** コマンドを使用します。

次の例は、現在の VDC のプロセスと CPU 使用率を表示する方法を示しています。

```
switch# show processes cpu
PID    Runtime(ms)  Invoked   uSecs  1Sec    Process
-----  -----------  --------  -----  ------  -----------
    4       386829  67421866      5    0.9%  ksoftirqd/0
3667       270567    396229    682    9.8%  syslogd
3942          262       161   1632    7.8%  netstack
4006    106999945  354495641    301   28.2%  snmpd
4026      4454796    461564   9651    0.9%  sac_usd
4424        84187    726180    115    0.9%  vpc
4426       146378    919073    159    0.9%  tunnel
CPU util  :   25.0% user,   30.5% kernel,   44.5% idle
```

RAM 使用量情報の取得

プロセッサの RAM 使用量は、次の SNMP 変数を使用して取得できます。ceExtProcessorRam。

```
ceExtProcessorRam OBJECT-TYPE
    SYNTAX  Unsigned32
    UNITS   "bytes"
        MAX-ACCESS  read-only
        STATUS  current
        DESCRIPTION
        "Total number of bytes of RAM available on the
         Processor."
        ::= { ceExtPhysicalProcessorEntry 1 }
```

Rx および Tx トラフィック カウンタのモニタリング

Rx および Tx トラフィック カウンタをモニタするときは、Rx カウンタ OID を含める必要があります。

```
ifHCInOctets
```

インターフェイスのステータスのモニタリング

インターフェイスのステータスをモニタするには、ifAlias（このトラップはインターフェイスの説明を設定できます）と ifDescr を持つ IETF 拡張リンクダウン トラップを使用し、次に示すように ASCII 形式でポート名を表示します。

```
switch (config)# snmp-server enable traps link
  cieLinkDown                 Cisco extended link state down notification
  cieLinkUp                   Cisco extended link state up notification
  cisco-xcvr-mon-status-chg   Cisco interface transceiver monitor status change
                             notification
  delayed-link-state-change  Delayed link state change
  extended-linkDown           IETF extended link state down notification
  extended-linkUp             IETF extended link state up notification
  linkDown                   IETF Link state down notification
  linkUp                      IETF Link state up notification
switch (config)#
```

次に、トラップの例を示します。

```
[+]          10           16:41:39.79         IF-MIB:linkDown trap:SNMPv2c  from
[172.25.234.200  Port: 162 Community: public]
SNMPv2-MIB:sysUpTime.0 :  (35519336)      Syntax: TimeTicks
SNMPv2-MIB:snmpTrapOID.0 :  (IF-MIB:linkDown)      Syntax: ObjectID
IF-MIB:ifIndex.440414208 :   (440414208)  Syntax: INTEGER,  Instance IDs: (440414208)
IF-MIB:ifAdminStatus.440414208 :   (down)  Syntax: INTEGER,  Instance IDs: (440414208)
IF-MIB:ifOperStatus.440414208 :   (down)  Syntax: INTEGER,  Instance IDs: (440414208)
IF-MIB:ifDescr.440414208 :   (Ethernet9/4)  Syntax: RFC1213-MIB:DisplayString,  Instance
 IDs: (440414208)
IF-MIB:ifAlias.440414208 :   (eth9/4)  Syntax: SNMPv2-TC:DisplayString,  Instance IDs:
(440414208)
SNMPv2-MIB:snmpTrapEnterprise.0 :  (IF-MIB:linkDown)      Syntax: ObjectID
```

トランシーバしきい値のモニタリング

cisco-xcvr-mon-status-chg トラップ方法を使用して、次に示すように、しきい値のデジタル診断統計をモニタします。

```
switch (config)# snmp-server enable traps link cisco-xcvr-mon-status-chg
switch (config)#
```

トラップ MIB は次のとおりです。

```
cIfXcvrMonStatusChangeNotif NOTIFICATION-TYPE
    OBJECTS         {
                        ifName,
                        cIfXcvrMonDigitalDiagTempAlarm,
                        cIfXcvrMonDigitalDiagTempWarning,
                        cIfXcvrMonDigitalDiagVoltAlarm,
                        cIfXcvrMonDigitalDiagVoltWarning,
                        cIfXcvrMonDigitalDiagCurrAlarm,
                        cIfXcvrMonDigitalDiagCurrWarning,
                        cIfXcvrMonDigitalDiagRxPwrAlarm,
                        cIfXcvrMonDigitalDiagRxPwrWarning,
                        cIfXcvrMonDigitalDiagTxPwrAlarm,
                        cIfXcvrMonDigitalDiagTxPwrWarning,
                        cIfXcvrMonDigitalDiagTxFaultAlarm
                    }
    STATUS          current
```

次の例は、トランシーバの詳細情報を表示する方法を示します。

```
switch(config)# show interface ethernet 1/17 transceiver details
Ethernet1/17
    transceiver is present
    type is 10Gbase-SR
    name is CISCO-AVAGO
    part number is SFBR-7702SDZ
    revision is G2.3
    serial number is AGA1427618P
    nominal bitrate is 10300 MBit/sec
    Link length supported for 50/125um OM2 fiber is 82 m
    Link length supported for 62.5/125um fiber is 26 m
    Link length supported for 50/125um OM3 fiber is 300 m
    cisco id is --
    cisco extended id number is 4
           SFP Detail Diagnostics Information (internal calibration)
  ----------------------------------------------------------------------------
                Current              Alarms                  Warnings
                Measurement     High        Low         High          Low
  ----------------------------------------------------------------------------
  Temperature   27.65 C        75.00 C     -5.00 C     70.00 C        0.00 C
  Voltage        3.29 V         3.63 V      2.97 V      3.46 V        3.13 V
  Current        5.42 mA       10.50 mA     2.50 mA    10.50 mA       2.50 mA
  Tx Power      -2.51 dBm       1.69 dBm  -11.30 dBm   -1.30 dBm     -7.30 dBm
  Rx Power      -2.64 dBm       1.99 dBm  -13.97 dBm   -1.00 dBm     -9.91 dBm
  Transmit Fault Count = 0
  ----------------------------------------------------------------------------
  Note: ++  high-alarm; +  high-warning; --  low-alarm; -  low-warning
switch(config)#
```

スーパバイザ スイッチオーバー通知の構成

スーパーバイザ スイッチオーバー通知は、ciscoRFSwactNotif トラップをリッスンすることでモニタできます。

```
ciscoRFSwactNotif NOTIFICATION-TYPE
OBJECTS {
cRFStatusUnitId,
sysUpTime,
cRFStatusLastSwactReasonCode
}
```

CRC および FCS エラーを含むカウンタの構成

次の例に示すように、dot3StatsFCSErrors カウンタをポーリングすることにより、インターフェイスの CRC および FCS エラーを含めることができます。

dot3StatsFCSErrors Counter32

```
      Dot3StatsEntry ::= SEQUENCE {
dot3StatsIndex                    InterfaceIndex,
dot3StatsAlignmentErrors          Counter32,
dot3StatsFCSErrors                Counter32,
dot3StatsSingleCollisionFrames    Counter32,
dot3StatsMultipleCollisionFrames  Counter32,
dot3StatsSQETestErrors            Counter32,
dot3StatsDeferredTransmissions    Counter32,
dot3StatsLateCollisions           Counter32,
```

```
        dot3StatsExcessiveCollisions       Counter32,
        dot3StatsInternalMacTransmitErrors Counter32,
        dot3StatsCarrierSenseErrors        Counter32,
        dot3StatsFrameTooLongs             Counter32,
        dot3StatsInternalMacReceiveErrors  Counter32,
        dot3StatsEtherChipSet              OBJECT IDENTIFIER,
        dot3StatsSymbolErrors              Counter32,
        dot3StatsDuplexStatus              INTEGER,
        dot3StatsRateControlAbility        TruthValue,
        dot3StatsRateControlStatus         INTEGER
    }
```

アラートの Call Home の構成

Call Home 機能を使用すると、システムで例外が発生したときに Call Home 電子メールを受信できます。次の CLI または SNMP を使用して、Call Home 構成をセットアップし、すべてのアラート グループを有効にします。

```
switch (config)# callhome
switch-FC-VDC(config-callhome)# destination-profile full-txt-destination alert-group
All                     This alert group consists of all of the callhome
                        messages
  Cisco-TAC             Events which are meant for Cisco TAC only
  Configuration         Events related to Configuration
  Diagnostic            Events related to Diagnostic
  EEM                   EEM events
  Environmental         Power,fan,temperature related events
  Inventory             Inventory status events
  License               Events related to licensing
  Linecard-Hardware     Linecard related events
  Supervisor-Hardware   Supervisor related events
  Syslog-group-port     Events related to syslog messages filed by port manager
  System                Software related events
  Test                  User generated test events
switch-FC-VDC(config-callhome)#
```

ユーザ認証失敗のモニタリング

authenticationFailure トラップをリッスンすることで、ユーザ認証の失敗をモニタできます。

```
SNMPv2-MIB: authenticationFailure trap
```

コアの構成

コア ファイルは、ユーザが手動で保存することも、障害発生時に自動的に保存することもできます。コア ファイルが作成された場合は、それを不揮発性ファイル スペース（ホストなど）にコピーして保存し、診断のためにシスコに報告します。

コアは複数回コピーできます。コアをリモートホスト上のファイル スペースにコピーするために、IPv4、IPv6、および多くのプロトコルの両方がサポートされています。これには、安全な環境での自動コピーに便利なパスワードなしの SSH が含まれます。リモート ホストへのパスワードレス アクセスの構成の詳細については、『Cisco MDS 9000 シリーズ セキュリティの設

定ガイド、リリース 8.x』の「SSH サービスおよび Telnet の構成」の章の「パスワードレス ファイル コピーおよび SSH」セクションを参照してください。

アクティブ スーパーバイザ モジュールのコア ファイルの総数に上限はありません。

ヒント コアをコピーする前に、ユーザの書き込み権限を持つ接続先ディレクトリを作成していることを確認してください。

カーネル コア収集の構成

カーネル コア収集を構成する手順は、次のとおりです。

手順

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **system kernel core**

カーネル クラッシュが発生した場合に、カーネル コアの収集を有効にします。

ステップ 3 switch(config)# **no system kernel core**

（オプション）カーネル コアの収集を無効にします。

コアの手動コピー

サポート対象のスイッチ上の接続先は、slot0 です。コアをリモートの接続先に転送するサポート対象プロトコルは、TFTP、SFTP、および SCP です。

コアの手動保存を構成するには、次の手順を実行します。

Procedure

switch# **copy** *core://module/process-id[/instance] destination://[[user@]host/][directory]*

プロセスのコアを指定された場所にコピーします。

コアの自動コピー

サポートされているスイッチ上の接続先は、bootflash、slot0、およびusb1です。コアをリモートの接続先に転送するサポート対象プロトコルは、HTTP、HTTPS、TFTP、FTP、SFTP、およびSCPです。

コアの自動保存を構成するには、次の手順を実行します。

Procedure

ステップ1 switch# **configure**

構成モードに入ります。

ステップ2 switch(config)# **system cores** *destination://[[user@]host/][directory]*

コア ファイルが作成されるとすぐに、指定された接続先にコア ファイルを保存します。

ステップ3 switch(config)# **no system cores**

（オプション）コア ファイルの自動保存を無効にします。

コアの削除

コア ファイルはコピー後に自動的に削除されません。コアがコピーされたら、スイッチ コア リポジトリから削除してスペースを再利用し、分析のためにシスコ サポートに報告します。

clear core_file コマンドを使用して、スイッチ コア リポジトリから1つのコアを削除します。

switch# **clear core_file module** *module* **pid** *pid*

clear cores コマンドを使用して、スイッチ コア リポジトリ内のすべてのコアをクリアします。

switch# **clear cores**

例：コアの構成

次の例では、スロット5で生成されたPID 1524のプロセスのコアを、ユーザ *mdsadmin* としてHTTPSを持つホストの *cores* ディレクトリにコピーします。

```
switch# copy core://5/1524 https://mdsadmin@192.168.1.2/cores
```

次の例では、コア ファイルが作成された直後に、SCPがユーザmdsadminとしてホスト上の/tftpboot/coresディレクトリに自動的にコピーされます。これを機能させるには、最初にパスワードなしのSSHを構成します。

```
switch# configure
```

```
switch(config)# system cores scp://mdsadmin@192.168.1.2/tftpboot/cores
```

次の例では、PID 1234 のプロセスのモジュール 1 から生成されたコアを削除します。

```
switch# clear core_file module 1 pid 1234
```

システム ステータスのモニタリング構成の確認

システム ステータスのモニタリング構成情報を表示するには、次の作業のいずれかを行います。

システム ヘルスの表示

システム関連のステータス情報を表示するには、**show system health** コマンドを使用します（スイッチ内のすべてのモジュールの現在の正常性, on page 166～指定されたモジュールのループバック テスト時間ログ, on page 168 を参照）。

スイッチ内のすべてのモジュールの現在の正常性

次の例は、スイッチ内のすべてのモジュールの現在の正常性を表示しています。

```
switch# show system health

Current health information for module 2.
Test                      Frequency    Status          Action
------------------------------------------------------------------
Bootflash                 5 Sec        Running         Enabled
EOBC                      5 Sec        Running         Enabled
Loopback                  5 Sec        Running         Enabled
------------------------------------------------------------------
Current health information for module 6.
Test                      Frequency    Status          Action
------------------------------------------------------------------
InBand                    5 Sec        Running         Enabled
Bootflash                 5 Sec        Running         Enabled
EOBC                      5 Sec        Running         Enabled
Management Port           5 Sec        Running         Enabled
------------------------------------------------------------------
```

指定されたモジュールの現在の正常性

次の例は、指定されたモジュールの現在の正常性を表示しています。

```
switch# show system health module 8
Current health information for module 8.
Test                      Frequency    Status          Action
------------------------------------------------------------------
Bootflash                 5 Sec        Running         Enabled
EOBC                      5 Sec        Running         Enabled
```

```
Loopback                  5 Sec         Running         Enabled
----------------------------------------------------------------
```

すべてのモジュールの正常性統計

次の例は、すべてのモジュールの正常性統計を表示しています。

```
switch# show system health statistics
Test statistics for module # 1
-------------------------------------------------------------------------------
Test Name           State            Frequency Run    Pass    Fail CFail Errs
-------------------------------------------------------------------------------
Bootflash           Running             5s    12900   12900       0     0    0
EOBC                Running             5s    12900   12900       0     0    0
Loopback            Running             5s    12900   12900       0     0    0
-------------------------------------------------------------------------------
Test statistics for module # 3
-------------------------------------------------------------------------------
Test Name           State            Frequency Run    Pass    Fail CFail Errs
-------------------------------------------------------------------------------
Bootflash           Running             5s    12890   12890       0     0    0
EOBC                Running             5s    12890   12890       0     0    0
Loopback            Running             5s    12892   12892       0     0    0
-------------------------------------------------------------------------------
Test statistics for module # 5
-------------------------------------------------------------------------------
Test Name           State            Frequency Run    Pass    Fail CFail Errs
-------------------------------------------------------------------------------
InBand              Running             5s    12911   12911       0     0    0
Bootflash           Running             5s    12911   12911       0     0    0
EOBC                Running             5s    12911   12911       0     0    0
Management Port     Running             5s    12911   12911       0     0    0
-------------------------------------------------------------------------------
Test statistics for module # 6
-------------------------------------------------------------------------------
Test Name           State            Frequency Run    Pass    Fail CFail Errs
-------------------------------------------------------------------------------
InBand              Running             5s    12907   12907       0     0    0
Bootflash           Running             5s    12907   12907       0     0    0
EOBC                Running             5s    12907   12907       0     0    0
-------------------------------------------------------------------------------
Test statistics for module # 8
-------------------------------------------------------------------------------
Test Name           State            Frequency Run    Pass    Fail CFail Errs
-------------------------------------------------------------------------------
Bootflash           Running             5s    12895   12895       0     0    0
EOBC                Running             5s    12895   12895       0     0    0
Loopback            Running             5s    12896   12896       0     0    0
-------------------------------------------------------------------------------
```

指定されたモジュールの統計情報の表示

次の例は、指定されたモジュールの統計を表示しています。

```
switch# show system health statistics module 3
Test statistics for module # 3
-------------------------------------------------------------------------------
Test Name           State            Frequency Run    Pass    Fail CFail Errs
```

```
--------------------------------------------------------------------------------
Bootflash           Running             5s    12932   12932       0     0    0
EOBC                Running             5s    12932   12932       0     0    0
Loopback            Running             5s    12934   12934       0     0    0
--------------------------------------------------------------------------------
```

スイッチ全体のループバック テストの統計

次の例は、スイッチ全体のループバック テストの統計を表示しています。

```
switch# show system health statistics loopback
-----------------------------------------------------------------
Mod Port Status                Run     Pass     Fail   CFail Errs
  1   16 Running             12953    12953        0       0    0
  3   32 Running             12945    12945        0       0    0
  8    8 Running             12949    12949        0       0    0
-----------------------------------------------------------------
```

指定されたインターフェイスのループバック テスト統計

次の例は、指定されたインターフェイスのループバック テスト統計を表示しています。

```
switch# show system health statistics loopback interface fc 3/1
-----------------------------------------------------------------
Mod Port Status                Run     Pass     Fail   CFail Errs
  3    1 Running                 0        0        0       0    0
-----------------------------------------------------------------
```

Note モジュール固有のループバック テストでエラーまたは障害が報告されない限り、インターフェイス固有のカウンタはゼロのままです。

すべてのモジュールのループバック テスト時間ログ

次の例では、すべてのモジュールのループバック テスト時間ログを表示しています。

```
switch# show system health statistics loopback timelog
-----------------------------------------------------------------
Mod        Samples     Min(usecs)     Max(usecs)     Ave(usecs)
  1           1872            149            364            222
  3           1862            415            743            549
  8           1865            134            455            349
-----------------------------------------------------------------
```

指定されたモジュールのループバック テスト時間ログ

次の例では、指定されたモジュールのループバック テスト時間ログを表示しています。

```
switch# show system health statistics loopback module 8 timelog
-------------------------------------------------------------------
Mod        Samples     Min(usecs)     Max(usecs)     Ave(usecs)
  8           1867            134            455            349
-------------------------------------------------------------------
```

ループバック テスト構成のフレーム長の確認

ループバック周波数の構成を確認するには、**show system health loopback frame-length** コマンドを使用します。

```
switch# show system health loopback frame-length
Loopback frame length is set to auto-size between 0-128 bytes
```

スイッチの OBFL の確認

OBFL の構成ステータスを表示するには、**show logging onboard status** コマンドを使用します。

```
switch# show logging onboard status
    Switch OBFL Log:                                        Enabled
    Module:  6 OBFL Log:                                    Enabled
    error-stats                                             Enabled
    exception-log                                           Enabled
    miscellaneous-error                                     Enabled
    obfl-log (boot-uptime/device-version/obfl-history)  Enabled
    system-health                                           Enabled
    stack-trace                                             Enabled
```

モジュールの OBFL の確認

OBFL の構成ステータスを表示するには、**show logging onboard status** コマンドを使用します。

```
switch# show logging onboard status
    Switch OBFL Log:                                        Enabled
    Module:  6 OBFL Log:                                    Enabled
    error-stats                                             Enabled
    exception-log                                           Enabled
    miscellaneous-error                                     Enabled
    obfl-log (boot-uptime/device-version/obfl-history)  Enabled
    system-health                                           Enabled
    stack-trace                                             Enabled
```

カーネル コア収集の確認

カーネル コア 収集の構成は、実行構成をチェックすることで確認できます。

```
switch# show running-config | include 'kernel core'
system kernel core
```

自動コア コピーの確認

show system cores コマンドを使用して、自動コア コピー機能の構成を表示します。

```
switch# show system cores
Cores are transferred to scp://mdsadmin@192.168.1.2/tftpboot/cores
```

OBFL ログの表示

モジュールに保存されている OBFL 情報を表示するには、次のコマンドを使用します。

コマンド	目的
show logging onboard boot-uptime	ブートおよび動作時間の情報を表示します。
show logging onboard cpu-hog	CPU hog イベントの情報を表示します。
show logging onboard device-version	デバイス バージョン情報を表示します。
show logging onboard endtime	終了時刻までの OBFL ログを表示します。
show logging onboard environmental-history	環境履歴を表示します。
show logging onboard error-stats	エラー統計情報を表示します。
show logging onboard exception-log	例外ログ情報を表示します。
show logging onboard interrupt-stats	割り込み統計情報を表示します。
show logging onboard mem-leak	メモリ リーク情報を表示します。
show logging onboard miscellaneous-error	各種エラー情報を表示します。
show logging onboard module *slot*	指定したモジュールの OBFL 情報を表示します。
show logging onboard obfl-history	履歴情報を表示します。
show logging onboard register-log	登録ログ情報を表示します。
show logging onboard stack-trace	カーネル スタック トレース情報を表示します。
show logging onboard starttime	指定した開始時刻からの OBFL ログを表示します。
show logging onboard system-health	システム ヘルス情報を表示します。

モジュール カウンタ情報の表示

この例では、モジュール内のすべてのデバイスのデバイス ID を表示しています。

```
switch# attach  module 4
Attaching to module 4 ...
To exit type 'exit', to abort type '$.'
Linux lc04 2.6.10_mvl401-pc_target #1 Tue Dec 16 22:58:32 PST 2008 ppc GNU/Linux

module-4# clear asic-cnt list-all-devices
           Asic Name  |        Device ID
        Stratosphere  |               63
         transceiver  |               46
        Skyline-asic  |               57
          Skyline-ni  |               60
        Skyline-xbar  |               59
         Skyline-fwd  |               58
        Tuscany-asic  |               52
        Tuscany-xbar  |               54
         Tuscany-que  |               55
         Tuscany-fwd  |               53
       Fwd-spi-group  |               73
          Fwd-parser  |               74
                eobc  |               10
           X-Bus IO   |                1
   Power Mngmnt Epld  |               25
```

システム プロセスの表示

すべてのプロセスに関する一般的な情報を表示するには、**show processes** コマンドを使用します（CPU 使用率情報, on page 172 ～ プロセスに関するメモリ情報 , on page 174 を参照）。

システム プロセスの表示

次の例では、システム プロセスを表示します。

```
switch# show processes

PID    State  PC        Start_cnt    TTY   Process
-----  -----  --------  -----------  ----  -------------
  868      S  2ae4f33e            1     -  snmpd
  869      S  2acee33e            1     -  rscn
  870      S  2ac36c24            1     -  qos
  871      S  2ac44c24            1     -  port-channel
  872      S  2ac7a33e            1     -  ntp
    -     ER         -            1     -  mdog
    -     NR         -            0     -  vbuilder
```

それぞれの説明は次のとおりです。

- ProcessId = プロセス ID
- State = プロセスの状態
  - D = 中断なしで休止（通常 I/O）
  - R = 実行可能（実行キュー上）

- S = 休止中
- T = トレースまたは停止
- Z = defunct（「ゾンビ」）プロセス

- NR = 実行されていない
- ER = 実行されているべきだが、現在は実行されていない
- PC = 現在のプログラム カウンタ（16 進形式）
- Start_cnt = プロセスがこれまでに開始（または再開）された回数
- TTY = プロセスを制御している端末通常、ハイフンは、特定の TTY 上で実行されていないデーモンを表します。
- Process Name = プロセスの名前

CPU 使用率情報

次の例は、CPU 使用率情報を表示しています。

```
switch# show processes cpu
PID    Runtime(ms)  Invoked   uSecs  1Sec   Process
-----  -----------  --------  -----  -----  -----------
  842         3807    137001     27    0.0  sysmgr
 1112         1220     67974     17    0.0  syslogd
 1269          220     13568     16    0.0  fcfwd
 1276         2901     15419    188    0.0  zone
 1277          738     21010     35    0.0  xbar_client
 1278         1159      6789    170    0.0  wwn
 1279          515     67617      7    0.0  vsan
```

それぞれの説明は次のとおりです。

- MemAllocated = このプロセスがシステムから動的に割り当てられているすべてのメモリの合計。すでにシステムに返されたメモリが含まれている場合があります。
- Runtime CPU Time（ms）= プロセスが使用した CPU 時間（ミリ秒単位）
- Invoked = プロセスがこれまでに開始された回数
- uSecs = プロセスの呼び出しごとの平均 CPU 時間（ミリ秒単位）
- 1Sec = 最近の 1 秒間における CPU 使用率（パーセント単位）

プロセス ログ情報

次の例では、プロセス ログ情報を表示しています。

```
switch# show processes log
Process           PID     Normal-exit  Stack-trace  Core     Log-create-time
----------------  ------  -----------  -----------  -------  ---------------
fspf              1339              N            Y        N  Jan  5 04:25
lcm               1559              N            Y        N  Jan  2 04:49
rib               1741              N            Y        N  Jan  1 06:05
```

それぞれの説明は次のとおりです。

- Normal-exit = プロセスが正常に終了したかどうか。

- Stack-trace = ログにスタック トレースがあるかどうか。
- Core = コア ファイルが存在するかどうか。
- Log-create-time = ログ ファイルが生成された時刻。

プロセスに関する詳細ログ情報

次の例では、プロセスに関する詳細なログ情報を表示しています。

```
switch# show processes log pid 1339

Service: fspf
Description: FSPF Routing Protocol Application
Started at Sat Jan  5 03:23:44 1980 (545631 us)
Stopped at Sat Jan  5 04:25:57 1980 (819598 us)
Uptime: 1 hours 2 minutes 2 seconds
Start type: SRV_OPTION_RESTART_STATELESS (23)
Death reason: SYSMGR_DEATH_REASON_FAILURE_SIGNAL (2)
Exit code: signal 9 (no core)
CWD: /var/sysmgr/work
Virtual Memory:
    CODE      08048000 - 0809A100
    DATA      0809B100 - 0809B65C
    BRK       0809D988 - 080CD000
    STACK     7FFFFD20
    TOTAL     23764 KB
Register Set:
    EBX 00000005         ECX 7FFFF8CC         EDX 00000000
    ESI 00000000         EDI 7FFFF6CC         EBP 7FFFF95C
    EAX FFFFFDFE         XDS 8010002B         XES 0000002B
    EAX 0000008E (orig)  EIP 2ACE133E         XCS 00000023
    EFL 00000207         ESP 7FFFF654         XSS 0000002B
Stack: 1740 bytes. ESP 7FFFF654, TOP 7FFFFD20
0x7FFFF654: 00000000 00000008 00000003 08051E95 ................
0x7FFFF664: 00000005 7FFFF8CC 00000000 00000000 ................
0x7FFFF674: 7FFFF6CC 00000001 7FFFF95C 080522CD ........\....".."
0x7FFFF684: 7FFFF9A4 00000008 7FFFFC34 2AC1F18C ........4......*
```

すべてのプロセス ログの詳細

次の例では、すべてのプロセス ログの詳細を表示しています。

```
switch# show processes log details
============================================================
Service: snmpd
Description: SNMP Agent
Started at Wed Jan  9 00:14:55 1980 (597263 us)
Stopped at Fri Jan 11 10:08:36 1980 (649860 us)
Uptime: 2 days 9 hours 53 minutes 53 seconds
Start type: SRV_OPTION_RESTART_STATEFUL (24)
Death reason: SYSMGR_DEATH_REASON_FAILURE_SIGNAL (2)
Exit code: signal 6 (core dumped)
CWD: /var/sysmgr/work
Virtual Memory:
    CODE      08048000 - 0804C4A0
    DATA      0804D4A0 - 0804D770
    BRK       0804DFC4 - 0818F000
    STACK     7FFFFCE0
```

```
    TOTAL     26656 KB
...
```

プロセスに関するメモリ情報

次の例では、プロセスに関するメモリ情報を表示しています。

```
switch# show processes memory
PID    MemAlloc  MemLimit    MemUsed     StackBase/Ptr      Process
-----  --------  ----------  ----------  -----------------  ----------------
    1    147456  0      1667072     7ffffe50/7ffff950      init
    2         0  0            0                 0/0         ksoftirqd/0
    3         0  0            0                 0/0         desched/0
    4         0  0            0                 0/0         events/0
    5         0  0            0                 0/0         khelper
```

それぞれの説明は次のとおりです。

- MemAlloc = プロセスで割り当てられたメモリの総容量。
- StackBase/Ptr = プロセス スタック ベースと現在のスタック ポインタ（16 進形式）

システム ステータスの表示

システム関連のステータス情報を表示するには、**show system** コマンドを使用します（デフォルトのスイッチポートの状態, on page 174 ～ システム関連の CPU およびメモリ情報, on page 176を参照）。

デフォルトのスイッチポートの状態

次の例は、デフォルトのスイッチポートの状態を示しています。

```
switch# show system default switchport
System default port state is down
System default trunk mode is on
```

指定 ID のエラー情報

次の例では、指定された ID のエラー情報を表示します。

```
switch# show system error-id 0x401D0019
Error Facility: module
Error Description: Failed to stop Linecard Async Notification.
```

システム リセット情報

次の例は、システム リセット情報を表示します。

```
switch# Show system reset-reason module 5
```

```
----- reset reason for module 5 -----
1) At 224801 usecs after Fri Nov 21 16:36:40 2003
    Reason: Reset Requested by CLI command reload
    Service:
    Version: 1.3(1)
2) At 922828 usecs after Fri Nov 21 16:02:48 2003
    Reason: Reset Requested by CLI command reload
    Service:
    Version: 1.3(1)
3) At 318034 usecs after Fri Nov 21 14:03:36 2003
    Reason: Reset Requested by CLI command reload
    Service:
    Version: 1.3(1)
4) At 255842 usecs after Wed Nov 19 00:07:49 2003
    Reason: Reset Requested by CLI command reload
    Service:
    Version: 1.3(1)
```

- Cisco MDS 9513 ディレクタでは、スロット 7 およびスロット 8 にあるスーパーバイザ モジュールの最後の 4 つのリセット理由コードが表示されます。どのスーパーバイザ モジュールも存在しない場合には、そのスーパーバイザ モジュールのリセット理由コードは表示されません。
- Cisco MDS 9506 または Cisco MDS 9509 スイッチでは、スロット 5 およびスロット 6 にあるスーパーバイザ モジュールの最後の 4 つのリセット理由コードが表示されます。どのスーパーバイザ モジュールも存在しない場合には、そのスーパーバイザ モジュールのリセット理由コードは表示されません。
- Cisco MDS 9200 シリーズ スイッチでは、スロット 1 にあるスーパーバイザ モジュールの最後の 4 つのリセット理由コードが表示されます。
- **show system reset-reason module** *number* コマンドは、特定のスロットの特定のモジュールでの、最後の 4 つのリセット理由コードを表示します。モジュールが存在しない場合には、そのモジュールのリセット理由コードは表示されません。

NVRAM および揮発性永続ストレージに保存されているリセット理由情報をクリアするには、**clear system reset-reason** コマンドを使用します。

- Cisco MDS 9500 シリーズ スイッチでは、このコマンドで、アクティブおよびスタンバイ スーパーバイザ モジュールの NVRAM に保存されているリセット理由情報をクリアします。
- Cisco MDS 9200 シリーズ スイッチでは、このコマンドで、アクティブ スーパーバイザ モジュールの NVRAM に保存されているリセット理由情報をクリアします。

システム稼動時間

次の例は、システムの稼働時間を表示します。

```
switch# show system uptime
Start Time: Sun Oct 13 18:09:23 2030
Up Time:    0 days, 9 hours, 46 minutes, 26 seconds
```

システム関連の CPU およびメモリ統計を表示するには、**show system resources** コマンドを使用します（システム関連の CPU およびメモリ情報, on page 176 を参照）。

システム関連の CPU およびメモリ情報

次の例は、システム関連の CPU およびメモリ情報を表示します。

```
switch# show system resources
Load average:   1 minute: 0.43   5 minutes: 0.17   15 minutes: 0.11
Processes   :   100 total, 2 running
CPU states  :   0.0% user,   0.0% kernel,   100.0% idle
Memory usage:   1027628K total,    313424K used,    714204K free
                   3620K buffers,   22278K cache
```

それぞれの説明は次のとおりです。

- Load average：実行中のプロセス数が表示されます。Load average には、過去 1 分間、5 分間、および 15 分間のシステム負荷が表示されます。
- Processes：システム内のプロセス数、およびコマンド発行時に実際に実行されていたプロセス数が表示されます。
- CPU states：直前の 1 秒間における CPU のユーザ モードとカーネル モードでの使用率およびアイドル時間がパーセントで表示されます。
- Memory usage：合計メモリ、使用中メモリ、空きメモリ、バッファに使用されているメモリ、およびキャッシュに使用されているメモリが KB 単位で表示されます。また、バッファおよびキャッシュの値には、*used* メモリの統計も含まれます。

プロセス障害ログの表示

プロセス障害ログの概要の表示

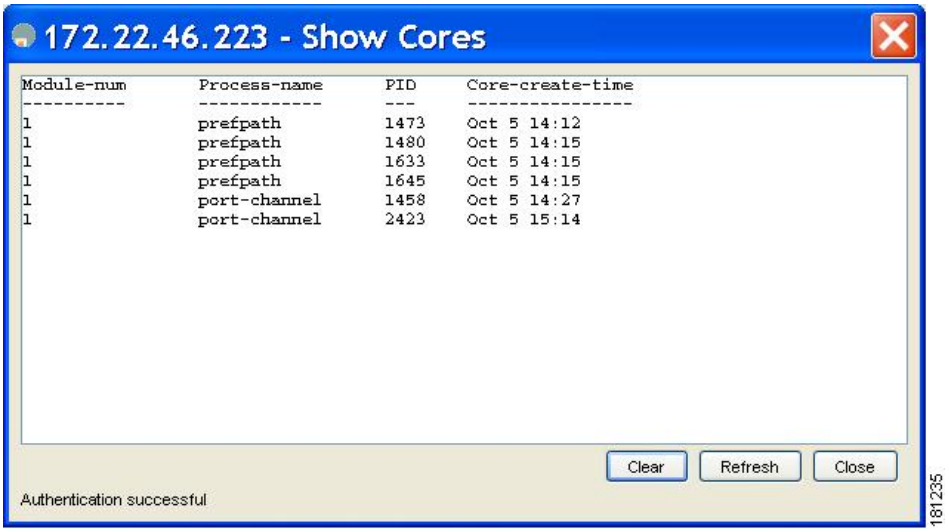
致命的なプロセス障害の履歴や、イベントごとに収集されたログをモジュール単位で表示できます。**slot** コマンドを使用して、特定のモジュールで **show processes log** コマンドを実行します。

次の例は、モジュール 2 のプロセス障害ログの概要を表示します。

```
switch# slot 2 show processes log
Process           PID     Normal-exit  Stack  Core   Log-create-time
----------------  ------  -----------  -----  -----  ---------------
ExceptionLog      2862             N      Y      N  Wed Aug  6 15:08:34 2003
acl               2299             N      Y      N  Tue Oct 28 02:50:01 2003
bios_daemon       2227             N      Y      N  Mon Sep 29 15:30:51 2003
```

次の例では、デバイスマネージャでシステムのプロセス コアを表示します。

Figure 4: [Show Cores] ダイアログボックス



プロセス コアの表示

次の例では、アクティブ スーパーバイザ モジュールに保存されているすべてのコアを表示します。

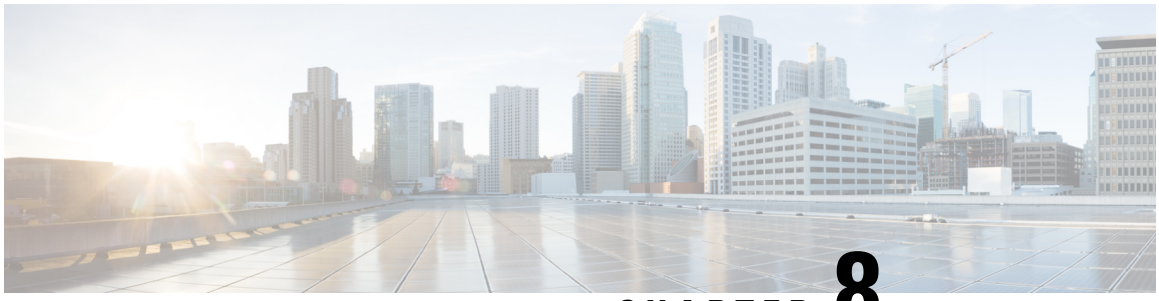
```
switch# show cores
Module-num  Process-name     PID     Core-create-time
----------  ------------     ---     ----------------
5           fspf             1524    Nov 9 03:11
6           fcc              919     Nov 9 03:09
8           acltcam          285     Nov 9 03:09
8           fib              283     Nov 9 03:08
```

その他の参考資料

システムプロセスとログの実装に関する詳細情報については、次のセクションを参照してください。

MIB

MIB	MIB のリンク
• CISCO-SYSTEM-EXT-MIB • CISCO-SYSTEM-MIB	MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 http://www.cisco.com/en/US/products/ps5989/prod_technical_reference_list.html



CHAPTER 8

組み込みイベント マネージャについて

ここでは、デバイス上の重要なイベントを検出し、処理するように、EEM を設定する方法について説明します。

- EEM の機能の履歴, on page 179
- EEM について, on page 180
- EEM のライセンス要件, on page 185
- EEM の前提条件, on page 185
- 注意事項と制約事項, on page 185
- デフォルト設定, on page 186
- Embedded Event Manager の設定, on page 186
- EEM の設定確認, on page 199
- EEM の設定例 , on page 200
- その他の参考資料, on page 201

EEM の機能の履歴

Table 22: EEM の機能の履歴 , on page 179 に、この機能のリリース履歴を示します。リリース 3.x 以降のリリースで導入または変更された機能のみが表に記載されています。

***Table 22: EEM* の機能の履歴**

機能名	リリース	機能情報
組み込みイベントマネージャ（EEM）	8.1(1)	**cli**キーワードが **action***number* コマンドに追加されました。
ゾーン、FCNS、および FLOGI	6,211	この機能により、ユーザはデフォルトのゾーン、FCNS、および FLOGI システム ポリシーのカスタム制限を構成できます。
組み込みイベントマネージャ（EEM）	4.1(3)	Embedded Event Manager（EEM）の設定方法に関する新しい章が追加されました。

EEM について

Embedded Event Manager はデバイス上で発生するイベントをモニタし、設定に基づいて各イベントの回復またはトラブルシューティングのためのアクションを実行します。

EEM の概要

EEM は次の 3 種類の主要コンポーネントからなります。

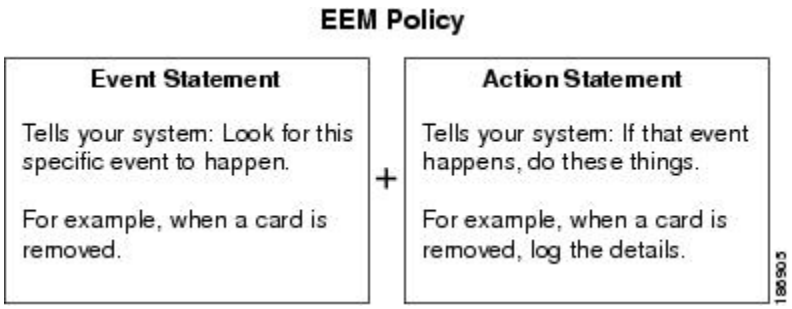
- イベント文：別の Cisco NX-OS コンポーネントからモニタし、アクション、回避策、または通知が必要になる可能性のあるイベント。
- アクションステートメント：電子メールの送信やインターフェイスの無効化などの、イベントから回復するために EEM が実行できるアクション。
- ポリシー：イベント文とアクションステートメントの組み合わせ。指定されたイベントが発生すると、構成されたアクションが実行されます。

ポリシー

EEM ポリシーは、イベント文および 1 つまたは複数のアクション文からなります。イベント文では、探すイベントとともに、イベントのフィルタリング特性を定義します。アクション文では、イベントの発生時に EEM が実行するアクションを定義します。

Figure 5: EEM ポリシー文, on page 180 に、EEM ポリシーの基本的な 2 種類の文を示します。

***Figure 5: EEM* ポリシー文**



EEM ポリシーを設定するには、CLI または VSH スクリプトを使用します。

Note EEM ポリシー照合は、MDS スイッチ上ではサポートされません。

EEM はスーパーバイザ上でイベント ログを維持します。

Cisco NX-OS には、設定済みのさまざまなシステム ポリシーがあります。これらのシステム ポリシーでは、デバイスに関連する多数の一般的なイベントおよびアクションが定義されています。システム ポリシー名は、2 個の下線記号（__）から始まります。

次に、Cisco MDS 9000 シリーズ スイッチで使用できる事前構成済みのシステム ポリシーの一部を示します。

- ゾーン
  - __zone_dbsize_max_per_vsan：ゾーン データベースのサイズが VSAN の最大制限である 4000000 バイトを超えた場合の Syslog 警告。
  - __zone_members_max_per_sw：ゾーン メンバー数がスイッチの最大制限である 32000 を超えた場合の Syslog 警告。
  - __zone_zones_max_per_sw：ゾーン数がスイッチの最大制限である 16000 を超えた場合の Syslog 警告。
  - __zone_zonesets_max_per_sw：ゾーンセット数がスイッチの最大制限である 1000 を超えた場合の Syslog 警告。
- ファブリック ログイン（FLOGI）
  - __flogi_fcids_max_per_switch：スイッチ内の flogis の数が 2000 を超えた場合の Syslog 警告。
  - __flogi_fcids_max_per_module：モジュール内の flogis の数が 400 を超えた場合の Syslog 警告。
  - __flogi_fcids_max_per_intf：インターフェイスの flogis の数が 256 を超えた場合の Syslog 警告。

Note 上記の 3 つの FLOGI ポリシーはすべて上書き可能です。

- ファイバ チャネル ネーム サーバー（FCNS）
  - __fcns_entries_max_per_switch：スイッチごとのすべての VSAN で検証されるネーム サーバー エントリの最大制限を構成します。

アクション：Syslog を表示します

Note ユーザは、別のコンポーネントのポリシーのイベントを構成しないでください。

使用するネットワークに合わせてユーザ ポリシーを作成できます。ユーザ ポリシーで定義されたアクションは、システム ポリシーで定義されたアクションと共に実行されます。ユーザ ポリシーを設定する場合には、CLI によるユーザ ポリシーの定義, on page 186を参照してください。

一部のシステム ポリシーは上書きすることもできます。オーバーライド ポリシーは、システム ポリシーを置き換えます。イベントまたはアクションの上書きが可能です。

show event manager system-policy コマンドを使用して、構成済みのシステム ポリシーを表示して、上書き可能なポリシーを判断します。

上書きポリシーを設定する場合は、ポリシーの上書き, on page 198を参照してください。

Note **show running-config eem** コマンドを使用して、各ポリシーの構成を確認してください。イベント文が指定されていて、アクション文が指定されていない上書きポリシーを設定した場合、アクションは開始されません。また、障害も通知されません。

Note 上書きポリシーには、必ずイベント文を指定します。上書きポリシーにイベント文が含まれていないと、システム ポリシーで可能性のあるイベントがすべて上書きされます。

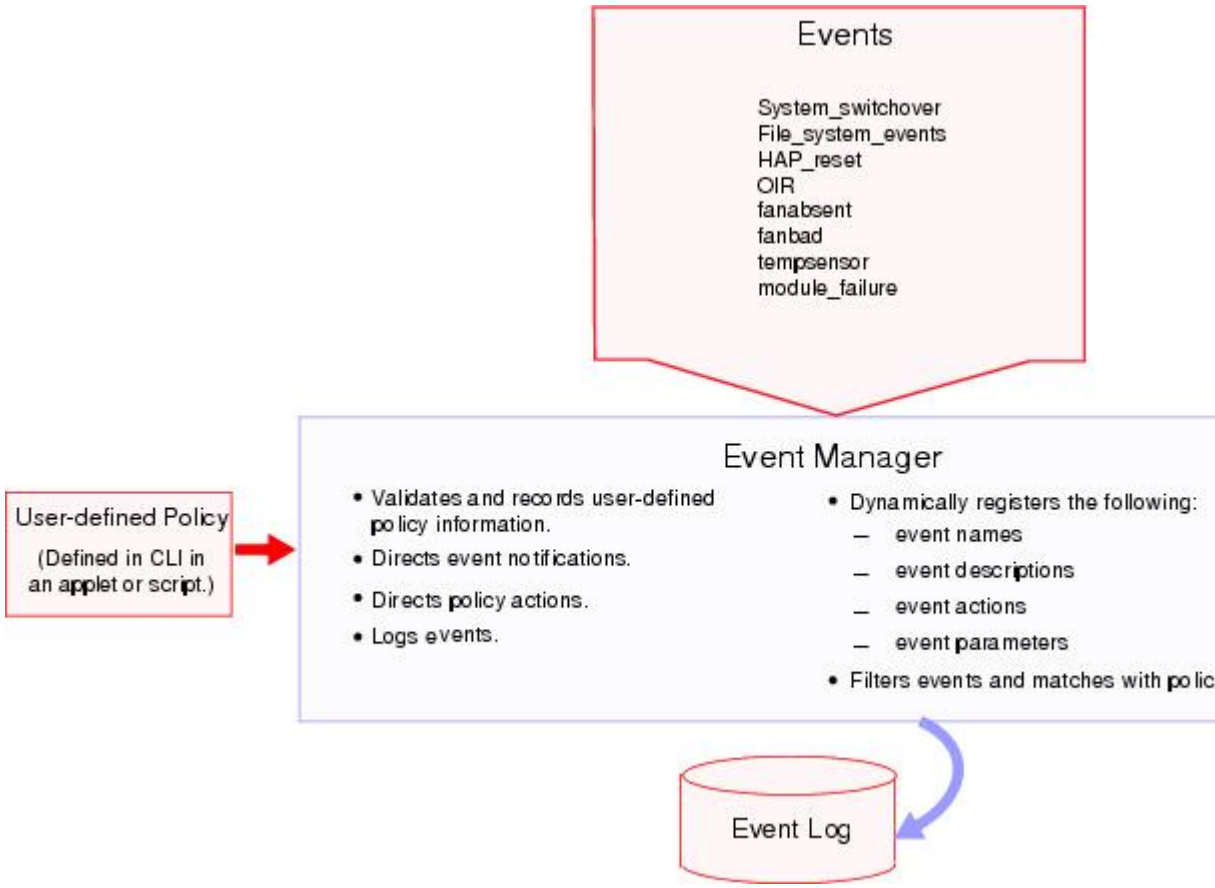
イベント文

イベントは、回避、通知など、何らかのアクションが必要なデバイス アクティビティです。これらのイベントは通常、インターフェイスやファンの誤動作といったデバイスの障害に関連します。

Figure 6: EEM の概要, on page 183 EEM ではイベント フィルタを定義して、クリティカル イベントまたは指定された時間内で繰り返し発生したイベントだけが関連付けられたアクションのトリガーになるようにします。

EEM が処理するイベントを示します。

Figure 6: EEM の概要



イベント文では、ポリシー実行のトリガーになるイベントを指定します。設定できるイベント文は、1 つのポリシーに 1 つだけです。

EEM はイベント文に基づいてポリシーをスケジューリングし、実行します。EEM はイベントおよびアクション コマンドを検証し、定義に従ってコマンドを実行します。

アクション文

アクション文では、ポリシーによって実行されるアクションを記述します。各ポリシーに複数のアクション文を設定できます。ポリシーにアクションを関連付けなかった場合、EEM はイベント観察を続けますが、アクションは実行されません。

EEM がアクション文でサポートするアクションは、次のとおりです。

- CLI コマンドの実行。
- カウンタのアップデート。
- 例外の記録。
- モジュールの強制的シャットダウン。
- デバイスをリロードします。

- 電力のバジェット超過による特定モジュールのシャットダウン。
- Syslog メッセージの生成。
- Call Home イベントの生成。
- SNMP 通知の生成。
- システム ポリシー用デフォルト アクションの使用。

Note トリガーされたイベントでデフォルト アクションも処理されるようにする場合は、EEM アクションをポリシーのタイプに応じて event-default または policy-default で明示的に設定する必要があります。たとえば、一致文で CLI コマンドを照合する場合、EEM ポリシーに event-default アクション文を追加する必要があります。event-default アクション文が追加されないと、EEM では CLI コマンドを実行できません。

Note ユーザ ポリシーまたは上書きポリシーの中に、相互に否定したり、関連付けられたシステム ポリシーに悪影響を与えたりするようなアクション文がないかどうかを確認してください。

VSH スクリプト ポリシー

テキスト エディタを使用し、VSH スクリプトでポリシーを作成することもできます。このようなポリシーにも、他のポリシーと同様、イベント文およびアクション文（複数可）を使用します。また、これらのポリシーでシステム ポリシーを補うことも上書きすることもできます。スクリプト ポリシーの作成後、そのポリシーをデバイスにコピーしてアクティブにします。スクリプト ポリシーを設定する場合は、VSH スクリプトによるポリシーの定義, on page 197を参照してください。

環境変数

すべてのポリシーに使用できる、EEM の環境変数を定義できます。環境変数は、複数のポリシーで使用できる共通の値を設定する場合に便利です。たとえば、外部電子メール サーバの IP アドレスに対応する環境変数を作成できます。

パラメータ置換フォーマットを使用することによって、アクション文で環境変数を使用できます。

アクション

次の例では、「EEM action」というリセット理由を指定し、モジュール 1 を強制的にシャットダウンするアクション文の例を示します。

```
switch (config-eem-policy)# action 1.0 forceshut module 1 reset-reason "EEM action"
```

環境変数を使用するアクション文

シャットダウンの理由に default-reason という環境変数を定義すると、次の例のように、リセット理由を環境変数に置き換えることができます。

```
switch (config-eem-policy)# action 1.0 forceshut module 1 reset-reason $default-reason
```

この環境変数は、任意のポリシーで再利用できます。環境変数の詳細については、環境変数の定義, on page 199を参照してください

EEM イベント相関

Cisco NX-OS Release 5.2 以降では、イベントの組み合わせに基づいて EEM ポリシーをトリガーできます。まず、**tag** キーワードを使用して EEM ポリシーに複数のイベントを作成し区別します。次に、一連のブール演算子（**and**、**or**、および **not**）を使用して、回数および時間をもとに、カスタム処理をトリガーするこれらのイベントの組み合わせを定義できます。

高可用性

Cisco NX-OS は、EEM のステートレス リスタートをサポートします。リブートまたはスーパーバイザ スイッチオーバーの後、Cisco NX-OS は実行コンフィギュレーションを適用します。

EEM のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
NX-OS	EEM にはライセンスは不要です。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。

EEM の前提条件

EEM の前提条件は、次のとおりです。

- EEM を設定するには、network-admin のユーザ権限が必要です。

注意事項と制約事項

EEM 設定時の注意事項と制約事項は次のとおりです。

- ユーザ ポリシーまたは上書きポリシー内のアクション文が、相互に否定したり、関連付けられたシステム ポリシーに悪影響を与えたりするようなことがないようにする必要があります。
- トリガーされたイベントでデフォルト アクションも処理されるようにする場合は、EEM アクションをポリシーのタイプに応じて event-default または policy-default で明示的に設定する必要があります。たとえば、match 文で CLI コマンドを照合する場合、EEM ポリシーに event-default アクション文を追加する必要があります。この文がないと、EEM では CLI コマンドを実行できません。
- イベント文が指定されていて、アクション文が指定されていない上書きポリシーを設定した場合、アクションは開始されません。また、障害も通知されません。
- 上書きポリシーにイベント文が含まれていないと、システム ポリシーで可能性のあるイベントがすべて上書きされます。
- 複数のイベント文が EEM ポリシーに存在する場合は、各イベント文に **tag** キーワードと一意な tag 引数が必要です。

デフォルト設定

Table 23: デフォルトの EEM パラメータ , on page 186 に、EEM パラメータのデフォルト設定を示します。

Table 23: **デフォルトの *EEM* パラメータ**

パラメータ	デフォルト
システム ポリシー	アクティブ

Embedded Event Manager の設定

CLI によるユーザ ポリシーの定義

CLI を使用したユーザ ポリシーを定義できます。

CLI を使用したユーザ ポリシーを定義するには、次の手順に従います。

Procedure

ステップ 1 **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 **event manager applet** *applet-name*

EEM にアプレットを登録し、アプレット コンフィギュレーション モードを開始します。*applet-name* は大文字と小文字を区別し、最大 29 文字の英数字を使用できます。

ステップ 3 **description** *policy-description*

（任意）ポリシーの説明になるストリングを設定します。string には最大 80 文字の英数字を使用できます。ストリングは引用符で囲みます。

ステップ 4 **event** *event-statement*

ポリシーのイベント文を設定します。イベント文の設定, on page 187 を参照してください。

ステップ 5 **maxrun**最大ランタイム

Embedded Event Manager（EEM）でのアプレットの最大ランタイムを構成します。範囲は 0 ～ 2147483647 秒です。

ステップ 6 次のいずれかを実行します。

- **tag** *tagname1* {**and** | **andnot**} *tagname2* [{**and** | **andnot**} *tagname3* [{**and** | **andnot**} *tagname4*]] **happens** *occurs* **in** *seconds*

（オプション）ポリシー内の複数のイベントを相互に関連付けます。

occurs の範囲は 1 ～ 4294967295 です。*seconds* の範囲は 0 ～ 4294967295 秒です。

ステップ 7 **action** *action-statement*

ポリシーのアクション文を設定します。アクション文の設定, on page 192 を参照してください。

アクション文が複数の場合は、ステップ 5 を繰り返します。

ステップ 8 **show event manager policy internal** *name*

（任意）設定したポリシーに関する情報を表示します。

ステップ 9 **copy running-config startup-config**

（任意）この設定の変更を保存します。

イベント文の設定

イベント文を構成するには、EEM 構成モードでつぎのいずれかのコマンドを使用します。

コマンド	目的
event cli [**tag** *tag_name* **match** *expression*] [**count** *repeats* |**time** *seconds*]	正規表現と一致する CLI コマンドが入力された場合に、イベントがトリガーします。 **tag** *tag_name* キーワードと引数のペアは、複数のイベントがポリシーに含まれている場合、この特定のイベントを識別します。 *repeats* の範囲は 1 ～ 65000 です。time の範囲は 0 ～ 4294967295 秒です。0 は無制限を示します。
event counter name *counter* **entry-val** *entry* **entry-op** {**eq**|**ge**|**gt**|**le**|**lt**|**ne** }[**exit-val** *exit* **exit-op** *exit* {**eq**|**ge**|**gt**|**le**|**lt**|**ne** }]	カウンタが、開始演算子に基づいて開始のしきい値を超えた場合（値より大きい、小さいなど）にイベントを発生させます。イベントはただちにリセットされます。任意で、カウンタが終了のしきい値を超えたあとでリセットされるように、イベントを設定できます。*counter* name は大文字と小文字を区別し、最大 28 の英数字を使用できます。*entry* および *exit* の値の範囲は 0 ～ 2147483647 です。
event fanabsent [**fan** *number*] **time** *seconds*	秒数で設定された時間を超えて、ファンがデバイスから取り外されている場合に、イベントを発生させます。ファン番号の範囲は、さまざまなスイッチに依存します (たとえば、9513 スイッチの場合、範囲は 1 から 2 です。9506/9509 スイッチの場合、範囲は 1 です)。seconds の範囲は 10 ～ 64000 です。
event fanbad [**fan** *number*] **time** *seconds*	秒数で設定された時間を超えて、ファンが故障状態の場合に、イベントを発生させます。ファン番号の範囲は、さまざまなスイッチに依存します (たとえば、9513 スイッチの場合、範囲は 1 から 2 です。9506/9509 スイッチの場合、範囲は 1 です)。seconds の範囲は 10 ～ 64000 です。
event memory {**critical** | **minor** |**severe**}	メモリのしきい値を超えた場合にイベントを発生させます。

コマンド	目的
event module-failure type *failure-type* **module** { *slot* | **all** { *slot* | **count** *repeats* [**time** *seconds*]	モジュールが設定された障害タイプになった場合に、イベントを発生させます。 スロット の範囲は、さまざまなスイッチに依存します（たとえば、9513 スイッチの場合、範囲は 1 ～ 13 です。9509 スイッチの場合、範囲は 1 ～ 9 です）。*repeats* 範囲は 0 ～ 4294967295 です。秒 の範囲は 0 ～ 4294967295 秒です。
event oir {**fan** | **module** | **powersupply**} {**anyoir** | **insert** | **remove** [*number*]}	設定されたデバイス構成要素（ファン、モジュール、または電源モジュール）がデバイスに取り付けられた場合、またはデバイスから取り外された場合に、イベントを発生させます。任意で、ファン、モジュール、または電源モジュールの具体的な番号を設定できます。*number* の範囲は次のとおりです。 • ファン番号は、さまざまなスイッチに依存しています。 • モジュール番号は、さまざまなスイッチに依存しています。 • 電源モジュール番号の範囲は 1 ～ 2 です。
event policy-default count *repeats* [**time** *seconds*]	システム ポリシーで設定されているイベントを使用します。このオプションは、ポリシーを上書きする場合に使用します。 *repeats* の範囲は 1 ～ 65000 です。秒 の範囲は 0 ～ 4294967295 秒です。
event poweroverbudget	電力バジェットが設定された電源モジュールの容量を超えた場合に、イベントを発生させます。

コマンド	目的
event snmp oid *oid* **get-type**{**exact** | **next**} **entry-op** {**eq** | **ge** | **gt** | **le** | **lt** |**ne**} **entry-val** *entry* [**exit-comb** {**and** | **or**}] **exit-op** {**eq** | **ge** | **gt** | **le** | **lt** |**ne**} **exit-val** *exit***exit-time** *time***polling-interval** *interval*	SNMP OID が、開始演算子に基づいて開始のしきい値を超えた場合（値より大きい、小さいなど）にイベントを発生させます。イベントはただちにリセットされます。または任意で、カウンタが終了のしきい値を超えたあとでリセットされるように、イベントを設定できます。OID はドット付き10進表記です。*entry* および *exit* の値の範囲は 0 ～ 18446744073709551615 です。時間の範囲は 0 ～ 2147483647 です。間隔の範囲は 1 ～ 2147483647 です。

コマンド	目的
event syslog {**occurs occurs number** | **pattern syslog** *pattern* | **period** *time intervals* | **priority syslog** *priority* | **tag** *tag_name* }	syslog ログファイルに記録されたメッセージに基づいてイベントをトリガーします。 occurs occurs number：発生回数を指定します。指定できる範囲は 1 ～ 65000 です。 pattern syslog pattern：syslog パターンを指定します。通常の正規表現パターンの一致が使用されます。最長で英数字 256 文字です。 period time interval：メッセージ間の最大時間間隔を指定します。値の範囲は 0 ～ 4294967295 秒です。 priority syslog priority：syslog の優先順位を指定します。 • alerts：アラート ログ メッセージを指定します。 • critical：重大なログ メッセージを指定します。 • debugging：デバッグ メッセージを指定します。 • emergencies：Emergency（致命的）ログ メッセージを指定します。 • errors：エラー ログ メッセージを指定します。 • informational：情報ログ メッセージを指定します。 • notification：Notification（通告）ログ メッセージを指定します。 • pattern：パターン一致を指定します。 • warnings：警告メッセージを指定します。 tag tag_name：タグ名を指定します。最長で英数字 29 文字です。 tag tag_name キーワード引数のペアは、複数のイベントがポリシーに含まれている場合、この特定のイベントを識別します。

コマンド	目的
event temperature [**module** *slot*] [**sensor** *sensor number*]**threshold** {**any** | **major** | **minor**}	温度センサーが設定されたしきい値を超えた場合に、イベントを発生させます。スロット 番号は、さまざまなスイッチに依存しています。センサー範囲はMDSモジュールの 1 ～ 8 ですが、現在の MDS モジュールは 1 ～ 3 の範囲のみを使用し、一部のモジュールは 1 ～ 2 の範囲を使用します。

アクション文の設定

アクション文を設定するには、EEM コンフィギュレーション モードで次のいずれかのコマンドを使用します。

コマンド	目的
action *number* **add** *variable-name*	EEM アプレットがトリガーされたときに変数の値を **action** コマンドに追加します。追加のアクションを取り消すには、このコマンドの **no** フォームを使用します。
action *number* **append** *variable-name*	EEM アプレットがトリガーされたときに、変数値を既存の変数文字列に追加します。追加のアクションを取り消すには、このコマンドの **no** 形式を使用します。
action *number* **break**	EEM アプレットがトリガーされたときに、アクションのループを終了します。ブレーク アクションを無効にするには、このコマンドの **no** フォームを使用します。
action *number* **cli command** *command-name*	EEM アプレットがトリガーされたときに、構成された VSH CLI コマンドを実行します。CLI コマンドのアクションを無効にするには、このコマンドの **no** フォームを使用します。VSH コマンド名の有効な値は 256 文字です。 Cisco MDS NX-OS リリース 8.1(1) から、**command** キーワードが追加されました。**command** キーワードは、Cisco NX-OS CLI に送信されるメッセージを指定します。コマンド名はダブルクォーテーションで囲んで追加してください。

コマンド	目的
action *number* **cli local command** *command-name*	イベントがトリガーされたのと同じカードでアクション コマンドを実行します。**action cli local command** を無効にするには、このコマンドの **no** フォームを使用します。VSH コマンド名の有効な値は 256 文字です。 Cisco MDS NX-OS リリース 8.1(1) から、**command** キーワードが追加されました。**command** キーワードは、Cisco NX-OS CLI に送信されるメッセージを指定します。コマンド名はダブル クォーテーションで囲んで追加してください。
action *number* **comment** *string*	EEM アプレットがトリガーされたときに、アプレットに追加するコメントのアクションを指定します。コメント アクションを無効にするには、このコマンドの **no** フォームを使用します。文字列シーケンスの有効な値は 256 文字です。
action *number* **continue**	EEM アプレットがトリガーされたときに、アクションのループを継続するアクションを指定します。コメント アクションを無効にするには、このコマンドの **no** フォームを使用します。
action *number* [**.** *number*] **counter name** *counter* **value** *val* **op** {**dec** | **inc** | **nop** | **set**}	設定された値および操作でカウンタを変更します。アクション ラベルのフォーマットは number1.number2 です。 *number* は 16 桁までの任意の数値にできます。*number2* の範囲は 0 ～ 9 です。 counter name は大文字と小文字を区別し、最大 29 の英数字を使用できます。*val* には 0 ～ 2147483647 の整数または置換パラメータを指定できます。
action *number* **decrement** *decrement-name*	EEM アプレットがトリガーされたときに、変数の値をデクリメントするアクションを指定します。アプレットからアクションを削除するには、このコマンドの **no** フォームを使用します。
action *number* **divide** *divide-name*	EEM アプレットがトリガーされたときに、与えられた序数の値で非除数を割ります。計算プロセスを削除するには、このコマンドの **no** フォーマットを使用します。
action *number* **eem**	EEM アプレットがトリガーされたときに、EEM アクション コマンドを指定します。EEM アクション コマンドを削除するには、このコマンドの **no** フォームを使用します。
action *number* **else**	EEM アプレットがトリガーされたときに、if / else 条件付きアクション ブロックの else 条件付きアクション ブロックの開始を指定します。else 条件付きアクションブロックを削除するには、このコマンドの **no** フォームを使用します。

コマンド	目的
action *number* **elseif**	EEM アプレットがトリガーされたときに、if / else 条件付きアクション ブロックの elseif 条件付きアクション ブロックの開始を指定します。else 条件付きアクションブロックを削除するには、このコマンドの **no** フォームを使用します。
action *number* **end**	EEM アプレットがトリガーされたときに、if / else および while 条件付きアクション ブロックの条件付きアクション ブロックの終了を指定します。end 条件付きアクションブロックを削除するには、このコマンドの **no** フォームを使用します。
action *number* [**.** *number*] **event-default**	関連付けられたイベントのデフォルト アクションを実行します。アクション ラベルのフォーマットは number1.number2 です。 *number* は 16 桁までの任意の数値にできます。*number2* の範囲は 0 ～ 9 です。
action *number* **exit**	EEM アプレットがトリガーされたときに、実行中のアプレット構成を終了します。実行中のアプレットからの即時終了のプロセスをキャンセルするには、このコマンドの **no** フォームを使用します。
action *number* **file** {**close** | **delete** | **gets** | **open** | **puts** | **read** | **write**}	EEM アプレット ファイルの動作を構成するには、アプレット構成モードで action file コマンドを使用します。この設定を無効にするには、このコマンドの **no** 形式を使用します。
action *number* **foreach** *foreach-name*	デリミタをトークン化されたパターンとして使用した入力文字列の繰り返しを指定します。入力文字列の繰り返しを削除するには、このコマンドの **no** フォームを使用します。
action *number* **if** *if-name*	EEM アプレットがトリガーされたときに、if 条件付きブロック開始を特定します。アプレットの構成モードで action if コマンドを使用してください。**if** 条件付きアクション ブロックを削除するには、このコマンドの **no** フォームを使用します。
action *number* **increment** *increment-name*	EEM アプレットがトリガーされたときに、変数の値を増分するアクションを指定します。アプレットからアクションを削除するには、このコマンドの **no** フォームを使用します。
action *number* **multiply** *multiply-name*	EEM アプレットがトリガーされたときに、変数値に指定された整数値を掛けるアクションを指定します。計算プロセスを削除するには、このコマンドの **no** フォーマットを使用します。
action *number* **overbudgetshut** [**module** *module-name*]	電力バジェット超過の問題により、1つまたは複数のモジュールまたはシステム全体を強制的にシャットダウンします。

コマンド	目的
action *number* **policy-default**	上書きしているポリシーのデフォルト アクションを実行します。構成から action policy コマンドを削除するには、このコマンドの **no** フォームを使用します。
action *number* **publish-event**	EEM アプレットに指定されたイベントがトリガーされたときに、アプリケーション固有のイベントを発行するアクションを指定します。アプリケーション固有のイベントを発行するアクションを削除するには、このコマンドの **no** フォームを使用します。
action *number* **puts**	EEM アプレットがトリガーされたときにデータを直接ローカル TTY に出力するアクションを有効にします。この機能を無効にするには、このコマンドの **no** 形式を使用します。
action *number* **regexp***regexp-name*	EEM アプレットがトリガーされたときに入力文字列の正規表現パターンと比較します。この機能を無効にするには、このコマンドの **no** 形式を使用します。
action *number* **reload**	1 つまたは複数のモジュールまたはシステム全体を強制的にリロードします。
action *number* **set***set-name*	EEM アプレットがトリガーされたときに、変数の値を設定します。EEM アプレット変数の値を削除するには、このコマンドの **no** フォームを使用します。
action *number* [**.** *number2*] **snmp-trap** {[**intdata1** *data* [**intdata2** *data* [**strdata** **string**]]]}	設定されたデータとともにSNMPトラップを送信します。numberには、最大16桁の任意の数値を指定できます。*number2* の範囲は 0 ～ 9 です。 *data* 引数には、最大 80 桁の任意の数を指定できます。*string* には最大 80 文字の英数字を使用できます。
action *number* **string**	EEM アプレットの string action コマンドを指定します。文字列の操作アクションを削除するには、このコマンドの **no** フォームを使用します。
action *number* **wait** *wait-value*	EEM アプレットのアクションの待機時間を指定します。この機能を無効にするには、このコマンドの**no**形式を使用します。
action *number* **while** *while-number*	EEM アプレットがトリガーされたときに条件付きブロックのループの開始を特定します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

コマンド	目的
action *number* [**.** *number2*] **exceptionlog module** *module* **syserr** *error* **devid** *id* **errtype** *type* **errcode** *code* **phylayer** *layer* **ports** *list* **harderror** *error* [**desc** *string*]	EEM アプレットがトリガーされたときに特定の条件が発生した場合、例外をログに記録します。
action *number* [**.** *number number2*] **forceshut** [**module** *slot* | **xbar** *xbar number*] **reset-reason** *seconds*	モジュール、クロスバー、またはシステム全体を強制的にシャットダウンします。アクション ラベルのフォーマットは number1.number2 です。 *number* は 16 桁までの任意の数値にできます。*number2* の範囲は 0 ～ 9 です。 *slot* 範囲は、さまざまなスイッチに依存しています。*xbar-number* の範囲は 1 ～ 2 で、MDS 9513 モジュールでのみ使用できます。 リセット理由は、引用符で囲んだ最大 80 文字の英数字ストリングです。
action *number* [**.** *number*] **overbudgetshut** [**module** *slot* [**-** *slot*]]	電力バジェット超過の問題により、1つまたは複数のモジュールまたはシステム全体を強制的にシャットダウンします。 *number* は 16 桁までの任意の数値にできます。*number2* の範囲は 0 ～ 9 です。 *slot* 範囲は、さまざまなスイッチに依存しています。
action *number* [**.** *number*] **policy-default**	上書きしているポリシーのデフォルト アクションを実行します。アクション ラベルのフォーマットは number1.number2 です。 *number* は 16 桁までの任意の数値にできます。*number2* の範囲は 0 ～ 9 です。
action *number* [**.** *number*] **reload** [**module** *slot* [**-** *slot*]]	1つまたは複数のモジュールまたはシステム全体を強制的にリロードします。 *number* は 16 桁までの任意の数値にできます。*number2* の範囲は 0 ～ 9 です。 *slot* 範囲は、さまざまなスイッチに依存しています。
action *number* [**.** *number2*] **syslog** [**priority** *prio-val*] **msg** *error message*	構成されている優先順位で、カスタマイズされた Syslog メッセージが送信されます。*number* は16桁までの任意の数値にできます。*number2* の範囲は 0 ～ 9 です。 *error-message* には最大256文字の英数字を引用符で囲んで使用できます。

Note トリガーされたイベントでデフォルト アクションも処理されるようにする場合は、EEM アクションをポリシーのタイプに応じて event-default または policy-default で明示的に設定する必要があります。たとえば、match 文で CLI コマンドを照合する場合、EEM ポリシーに event-default アクション文を追加する必要があります。この文がないと、EEM では CLI コマンドを実行できません。**terminal event-manager bypass** コマンドを使用して、すべての CLI ベースの EEM ポリシーをバイパスできます。元に戻すには、**terminal no event-manager bypass** コマンドを使用します。

VSH スクリプトによるポリシーの定義

VSH スクリプトを使用してポリシーを定義するには、次の手順に従います。

Procedure

ステップ 1 テキスト エディタで、ポリシーを定義する CLI コマンド リストを指定します。

ステップ 2 テキスト ファイルに名前をつけて保存します。

ステップ 3 ファイルを次のシステム ディレクトリにコピーします。

bootflash://eem/user_script_policies

VSH スクリプト ポリシーの登録およびアクティブ化

VSH スクリプトで定義したポリシーを登録してアクティブにするには、次の手順に従います。

Procedure

ステップ 1 **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 **event manager policy** *policy-script*

EEM スクリプト ポリシーを登録してアクティブにします。*policy-script* は大文字と小文字を区別し、最大 29 の英数字を使用できます。

ステップ 3 **show event manager internal policy** *name*

（任意）設定したポリシーに関する情報を表示します。

ステップ 4 **copy running-config startup-config**

（任意）この設定の変更を保存します。

ポリシーの上書き

システム ポリシーを上書きするには、次の手順に従います。

Procedure

ステップ 1 **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 **show event manager policy-state** *system-policy*

（任意）上書きするシステム ポリシーの情報をしきい値を含めて表示します。**show event manager system-policy** コマンドを使用して、システム ポリシーの名前を探します。

ステップ 3 [**no**] **event manager applet** *applet-name* **override** *system-policy*

システム ポリシーを上書きし、アプレット コンフィギュレーション モードを開始します。*applet-name* は大文字と小文字を区別し、最大 29 文字の英数字を使用できます。*system-policy* は、システム ポリシーの 1 つにする必要があります。

ステップ 4 **description** *policy-description*

（任意）ポリシーの説明になるストリングを設定します。string には最大 80 文字の英数字を使用できます。ストリングは引用符で囲みます。

ステップ 5 [**no**] **event** *event-statement*

ポリシーのイベント文を設定します。イベント文の設定, on page 187 を参照してください。**no** キーワードを使用すると、上書きされたイベントがあればそれを削除します。

- 上書きされたポリシーを削除しても、デフォルトのシステム ポリシーは削除されません。
- それぞれのゾーン、FCNS、または FLOGI 制限値を変更することにより、上書きされたポリシーを変更できます。

ステップ 6 **action** *action-statement*

ポリシーのアクション文を設定します。アクション文の設定, on page 192 を参照してください。

アクション文が複数の場合は、ステップ 6 を繰り返します。

- ゾーン、FLOGI、および FCNS は、アクションとして syslog メッセージの生成のみをサポートします。
- アクションが構成されていない場合、デフォルトのシステム ポリシーに関連付けられたデフォルトのアクションが実行されます。アクションが構成されている場合、構成されたア

クションとデフォルトのアクションの両方が実行されます。この機能は、ゾーン、FLOGI、および FCNS システム ポリシーにのみ適用されます。

ステップ 7 **show event manager policy-state** *name*

（任意）設定したポリシーに関する情報を表示します。

ステップ 8 **copy running-config startup-config**

（任意）この設定の変更を保存します。

Note
ゾーン、FLOGI、および FCNS EEM ポリシーの複数の上書きは許可されていません。

環境変数の定義

EEMポリシーでパラメータとして機能する変数を定義するには、次の手順に従ってください。

Procedure

ステップ 1 **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 **event manager environment** *variable-name variable-value*

EEM 用の環境変数を作成します。*variable-name* は大文字と小文字を区別し、最大 29 文字の英数字を使用できます。*variable-value* には最大 39 文字の英数字を引用符で囲んで使用できます。

ステップ 3 **show event manager environment**

（任意）設定した環境変数に関する情報を表示します。

ステップ 4 **copy running-config startup-config**

（任意）この設定の変更を保存します。

EEM の設定確認

EEM 設定情報を表示するには、次のいずれかの作業を実行します。

コマンド	目的
show event manager environment [**variable-name** | **all**]	イベントマネージャの環境変数に関する情報を表示します。

コマンド	目的
show event manager event-types [*event* | **all** | **module** *slot*]	イベント マネージャのイベント タイプに関する情報を表示します。
show event manager history events [detail] [maximum *num-events***] [severity {catastrophic | minor | moderate | severe}]**	すべてのポリシーについて、イベント履歴を表示します。
show event manager policy internal [*policy-name*] [**inactive**]	設定したポリシーに関する情報を表示します。
show event manager policy-state *policy-name*	しきい値を含め、ポリシーの状態に関する情報を表示します。
show event manager script system [*policy-name*}**all**]	スクリプトポリシーに関する情報を表示します。
show event manager system-policy [**all**]	定義済みシステム ポリシーに関する情報を表示します。
show running-config eem	EEM の実行コンフィギュレーションに関する情報を表示します。
show startup-config eem	EEM のスタートアップ コンフィギュレーションに関する情報を表示します。

EEM の設定例

モジュール 3 の中断のないアップグレード エラーのしきい値だけを変更することによって、__lcm_module_failure システム ポリシーを上書きする例を示します。次の例では、syslog メッセージも送信されます。その他のすべての場合、システム ポリシー __lcm_module_failure の設定値が適用されます。

```
event manager applet example2 override __lcm_module_failure
 event module-failure type hitless-upgrade-failure module 3 count 2
 action 1 syslog priority errors msg module 3 “upgrade is not a hitless upgrade!”
 action 2 policy-default
```

次の例では、FCNS データベース エントリの数を 1500 に変更して、上書きされたポリシーを変更します。また、デフォルトのシステム ポリシーの構成済みおよびデフォルトの syslog メッセージの両方を生成します。

```
event manager applet fcns_policy override __fcns_entries_max_per_switch
event fcns entries max-per-switch 1500
      action 1.0 syslog priority warnings msg  FCNS DB entries have reached the EEM limit
```

次の例では、上書きされたポリシーのイベントを削除します。

```
no event manager applet zone_policy
```

次に、CLI コマンドの実行を許可し、ユーザがデバイスで構成モードを開始すると SNMP 通知を送る EEM ポリシーを作成する例を示します。

```
event manager applet TEST
event cli match "conf t"
action 1.0 snmp-trap strdata "Configuration change"
action 2.0 event-default
```

Note EEM ポリシーに event-default アクション文を追加する必要があります。この文がないと、EEM では CLI コマンドを実行できません。

次に、EEM アプレットが起動されたときに実行される VSH コマンド文字列を構成する例を示します。

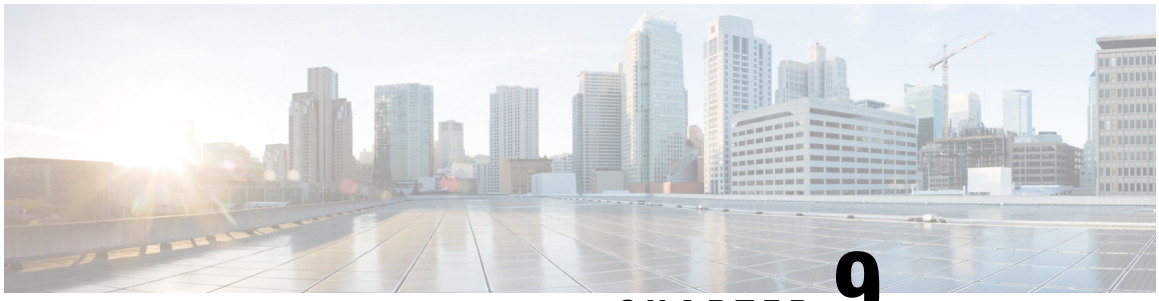
```
switch# configure terminal
switch(config)# event manager applet cli-applet
switch(config-applet)# action 1.0 cli command "show interface e 3/1"
```

その他の参考資料

EEM の実装に関する詳細情報については、次の項を参照してください。

MIB

MIB	MIB のリンク
• CISCO-EMBEDDED-EVENT-MGR-MIB	MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 http://www.cisco.com/en/US/products/ps5989/prod_technical_reference_list.html



CHAPTER 9

RMON の設定

RMON は、各種のネットワーク エージェントおよびコンソール システムがネットワーク モニタリング データを交換できるようにするための、Internet Engineering Task Force（IETF）標準モニタリング仕様です。RMON のアラームとイベントを使用し、Cisco SAN-OS Release 2.0(1b) 以降または Cisco NX-OS Release 4.1(3) 以降のソフトウェアが動作する Cisco MDS 9000 ファミリ スイッチを監視できます。

- RMON について, on page 203
- デフォルト設定, on page 205
- RMON の設定, on page 206
- RMON 設定の確認, on page 208
- その他の参考資料, on page 209
- RMON の機能履歴, on page 209

RMON について

スイッチでは RMON はデフォルトでディセーブルに設定されており、イベントまたはアラームは設定されていません。

Cisco MDS 9000 ファミリのすべてのスイッチは、次の RMON 機能（RFC 2819 で定義）をサポートしています。

- アラーム：指定された期間、特定の管理情報ベース（MIB）オブジェクトを監視します。MIB オブジェクトの値が指定された値（上昇しきい値）を超えた場合、アラーム状態がセットされ、条件がどれだけ長い時間存在したかにかかわらず 1 つのイベントだけをトリガーします。MIB オブジェクトの値が特定の値（下限しきい値）を下回った場合、アラーム状態がクリアされます。これにより、上昇しきい値を再度超えた場合に、再度アラームがトリガーされます。
- イベント：アラームによってイベントが発生したときのアクションを決定します。アクションは、ログ エントリ、SNMP トラップ、またはその両方を生成できます。

エージェントおよび管理については、『*Cisco MDS 9000 Family MIB Quick Reference*』を参照してください。

SNMP 互換ネットワーク管理ステーションの詳細については、『System Management Configuration Guide, Cisco DCNM for SAN』を参照してください。

SNMP セキュリティに関連する CLI の構成については、を参照してください。

RMON 設定情報

スイッチでは RMON はデフォルトでディセーブルに設定されており、イベントまたはアラームは設定されていません。RMON アラームおよびイベントを設定するには、CLI または SNMP 互換ネットワーク管理ステーションを使用します。

Tip RMON のネットワーク管理機能を活用するために、ネットワーク管理ステーション（NMS）で追加の汎用 RMON コンソール アプリケーションを使用することを推奨します。『System Management Configuration Guide, Cisco DCNM for SAN』を参照してください。

Threshold Manager を使用した RMON 設定

スイッチでは RMON はデフォルトでディセーブルに設定されており、イベントまたはアラームは設定されていません。RMON のアラームおよびイベントを設定するには、CLI を使用するか、Device Manager の Threshold Manager を使用します。

Threshold Monitor では、選択した統計情報が設定されたしきい値を超えた場合に、SNMP イベントをトリガーするか、メッセージをログに取得できます。RMON では、これを上昇しきい値と呼びます。設定可能な内容は次のとおりです。

- 変数：しきい値を設定する統計情報。
- 値：アラームをトリガーする変数の値。この値は、Device Manager が変数を連続して 2 度ポーリングしたときの差分です。
- サンプル：変数の連続する 2 度のポーリングの間のサンプル周期（秒単位）。サンプル周期は、変数が通常の動作状態でしきい値を超えないように選択してください。
- 警告：Device Manager によって使用される、トリガーされたアラームの重大度を示す警告レベル。これは、RMON に対する DCNM-SAN と Device Manager の拡張です。

Note 任意の種類の RMON アラーム（absolute または delta、rising threshold または falling threshold）を設定するには、[Threshold Manager] ダイアログボックスで [More] をクリックします。これらの高度なアラーム タイプを設定する前に、RMON がこれらの概念を定義する方法について理解しておく必要があります。RMON アラームの設定方法については、RMON-MIB（RFC 2819）を参照してください。

Note RMON MIB オブジェクトにアクセスするために、スイッチ上で SNMP を設定することも必要です。

RMON アラーム設定情報

Threshold Manager では、RMON しきい値とアラームを設定する、一般的な MIB オブジェクトのリストが提供されています。アラーム機能は、特定の MIB オブジェクトを指定された間隔でモニタし、指定された値（上昇しきい値）でアラームをトリガーし、別の値（下限しきい値）でアラームをリセットします。

また、任意の MIB オブジェクトにアラームを設定できます。指定する MIB は、標準のドット付き表記（ifInOctets.167772161616777216 の場合、1.3.6.1.2.1.2.2.1.14.16777216 16 16777216）の既存の SNMP MIB でなければなりません。

次のいずれかのオプションを使用して、MIB 変数を監視する間隔（1 ～ 4294967295 秒）を指定します。

- **delta** オプションを使用して、MIB 変数サンプル間の変化をテストします。
- **absolute** オプションを使用して、各 MIB 変数を直接テストします。
- **delta** オプションを使用して、カウンタである任意の MIB オブジェクトをテストします。

rising threshold および **falling threshold** の値の範囲は -2147483647 ～ 2147483647 です。

Caution **falling threshold** は **rising threshold** 未満である必要があります。

次のパラメータを任意で指定することもできます。

- 上限および下限しきい値が指定値を超えた場合に発生させるイベント番号。
- アラームのオーナー

デフォルト設定

Table 24: RMON のデフォルト設定値 , on page 205 に、スイッチのすべての RMON 機能のデフォルト設定値を示します。

***Table 24: RMON* のデフォルト設定値**

パラメータ	デフォルト
RMON アラーム	無効
RMON イベント	無効化

RMON の設定

スイッチでは RMON はデフォルトでディセーブルに設定されており、イベントまたはアラームは設定されていません。

SNMP での RMON トラップの構成

SNMP 構成で RMON トラップを有効にするには、次の手順を実行します。

Before you begin

RMON 構成が正しく機能するには、SNMP 構成で RMON トラップを有効にする必要があります。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **snmp-server enable traps rmon**

RMON トラップ タイプを有効にします。

Note
RMON MIB オブジェクトにアクセスするために、スイッチ上で SNMP を設定することも必要です。

RMON アラームの構成

RMON アラームを有効にするには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **rmon alarm 20 1.3.6.1.2.1.2.2.1.14.16777216 2900 delta rising-threshold 15 1 falling-threshold 0 owner test**

RMON アラーム番号 20 を構成します。このアラームは、無効化されない限り、900 秒に 1 回 1.3.6.1.2.1.2.2.1.14.16777216 をモニタし、変数の上下変動をチェックします。値が 15 以上の

MIB カウンタの増加を示した場合、アラームが発生します。そのアラームによってさらにイベント番号 1 が発生します。イベント番号 1 は、RMON event コマンドで構成されています。使用できるイベントは、ログ エントリまたは SNMP トラップです。MIB 値の変化が 0 の場合、アラームはリセットされ、再び発生が可能になります。

Note
次の rmon イベントの構成もできます。

- イベント 1：重大
- イベント 3：エラー
- イベント 4：Warning（注意）
- イベント 5：情報

ステップ 3 switch(config)# **no rmon alarm 2**

アラーム テーブルから指定されたエントリを削除します。

RMON イベントの構成

RMON イベントを有効にするには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **rmon event 2 log trap eventtrap description CriticalErrors owner Test2**

CriticalErrors を定義する RMON イベント番号 2 を作成し、アラームによるイベントのトリガー時にログ エントリを生成します。ユーザ Test2 が、このコマンドによってイベント テーブルに作成される行を所有します。次の例の場合も、イベント発生時に SNMP トラップが生成されます。

Note
次の rmon イベントの構成もできます。

- イベント 1：重大
- イベント 3：エラー
- イベント 4：Warning（注意）
- イベント 5：情報

ステップ 3 switch(config)# **no rmon event 5**

RMON イベント テーブルからエントリを削除します。

RMON 設定の確認

RMON 構成情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show rmon alarms	構成済みの RMON アラームの表示
show rmon hcalarms	構成済みの RMON 高キャパシティ アラームの表示
show rmon events	構成済みの RMON イベントの表示

これらのコマンドの出力に表示される各フィールドの詳細については、『Cisco MDS 9000 NX-OS Command Reference』を参照してください。

show rmon および **show snmp** コマンドを使用して、構成済みの RMON および SNMP 情報を表示します（RMON アラームの構成, on page 208 および RMON イベントの構成, on page 209 を参照）。

RMON アラームの構成

次に、構成済みの RMON アラームを表示する例を示します。

```
switch# show rmon alarms
Alarm 1 is active, owned by admin
 Monitors 1.3.6.1.2.1.2.2.1.16.16777216 every 1 second(s)
 Taking delta samples, last value was 0
 Rising threshold is 1, assigned to event 0
 Falling threshold is 0, assigned to event 0
 On startup enable rising or falling alarm
```

RMON 高キャパシティ アラームの確認

次の例は、確認された RMON 高キャパシティ アラームを表示します。

```
switch# show rmon hcalarms
High Capacity Alarm 10 is active, owned by Testuser
 Monitors 1.3.6.1.2.1.31.1.1.1.6.16785408 every 300 second(s)
 Taking absolute samples, last value was 0 (valuePositive)
 Rising threshold low is 4294967295 & high is 15 (valuePositive)
 Rising threshold assigned to event 1
 Falling threshold low is 0 & high is 0 (valueNotAvailable)
 Falling threshold assigned to event 0
 On startup enable rising alarm
 Number of Failed Attempts is 0
```

Note 高キャパシティ RMON アラームは、CISCO-HC-ALARM-MIB を使用して構成できます。『*Cisco MDS 9000 Series MIB Quick Reference*』を参照してください。

RMON イベントの構成

次に、構成済みの RMON イベントを表示する例を示します。

```
switch# show rmon events
Event 2 is active, owned by Test2
 Description is CriticalErrors
 Event firing causes log and trap to community eventtrap, last fired 0
Event 500 is active, owned by admin
 Description is
 Event firing causes log, last fired 138807208
```

その他の参考資料

RMON の実装に関する詳細情報については、次の項を参照してください。

MIB

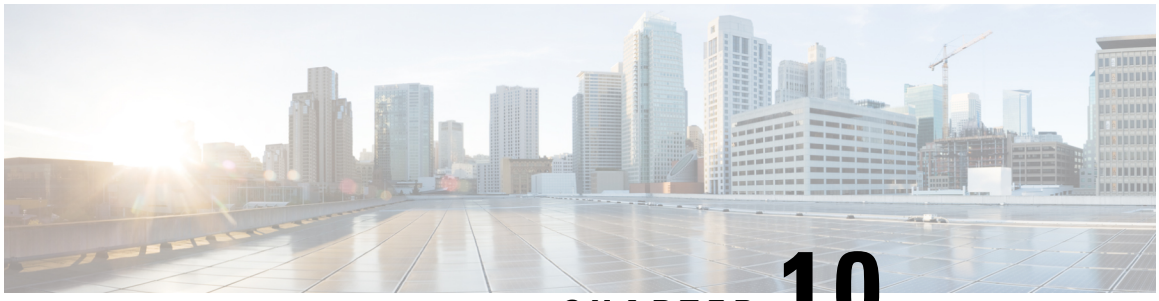
MIB	MIB のリンク
• CISCO-RMON-CAPABILITY.my • CISCO-RMON-CONFIG-CAPABILITY.my • CISCO-RMON-CONFIG-MIB	MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 http://www.cisco.com/en/US/products/ps5989/prod_technical_reference_list.html

RMON の機能履歴

次の表に、この機能のリリース履歴を示します。リリース 3.x 以降のリリースで導入または変更された機能のみが表に記載されています。

***Table 25: RMON* の機能履歴**

機能名	リリース	機能情報
RMON 高キャパシティ アラーム	3.0(1)	RMON 高キャパシティ アラーム値を表示する、show rmon high capacity alarms コマンドを提供します。



CHAPTER 10

オンライン診断の設定

Cisco MDS NX-OS リリース 6.2 以降、Cisco MDS 9700 シリーズは GOLD（総合オンライン診断）機能をサポートしています。GOLD は、Cisco Nexus 7000 および 7700 シリーズ スイッチでもサポートされる診断サービスです。この章では、Cisco MDS 9700 シリーズ スイッチで GOLD 機能を構成する方法について説明します。

- オンライン診断について, on page 211
- オンライン診断機能のライセンス要件 , on page 218
- デフォルト設定, on page 218
- オンライン診断の設定, on page 218
- オンライン診断の確認, on page 226
- オンライン診断のコンフィギュレーション例, on page 227
- その他の参考資料, on page 227

オンライン診断について

オンライン診断では、ハードウェアとデータ パスを検証し、障害のあるデバイスを特定します。

オンライン診断機能の概要

GOLD（総合オンライン診断）フレームワークは、ライブ システムのハードウェア デバイスとデータ パスをテストおよび検証します。

GOLD テストは、次の 3 つのモードで実行できます。

- ブートアップ
- ヘルスモニタリング（ランタイムとも呼ばれる）
- オンデマンド

次に、診断テスト スイートの属性について説明します。

- B/C/*：バイパス ブートアップ レベル テスト / 完全なブートアップ レベル テスト / NA

- P/*：ポートごとのテスト / NA
- S/*：アクティブへの適用のみ / スタンバイ ユニット / NA
- D/N/* - Disruptive test / Non-disruptive test / NA
- H/O/*：常に有効なモニタリング テスト / 条件付きで有効なテスト / NA
- F/* - Fixed monitoring interval test / NA
- X/* - Not a health monitoring test / NA
- E/*：ラインカード テストまで / NA
- L/*：このテストを排他的に実行する / NA
- T/*：オンデマンド テストではない / NA
- A/I/*：モニタリングがアクティブ / モニタリングが / NA

ブートアップ診断

ブートアップ診断は起動中に実行され、Cisco MDS 9700 シリーズ スイッチがモジュールをオンラインにする前に、障害ハードウェアが検出されます。たとえば、デバイスに障害のあるモジュールがある場合、適切なブートアップ診断テストで障害が示されません。

Note ブートアップ診断テストは、起動中にトリガーされます。

Table 26: ブートアップ診断 , on page 212 で、モジュールおよびスーパーバイザのブートアップ診断テストについて説明します。

Table 26: **ブートアップ診断**

診断	属性	説明
ラインカード		
EOBCPortLoopback	C**D**X**T*	EOBC（イーサネット アウトオブバンド接続）インターフェイスの正常性を確認します。
OBFL	C**N**X**T*	OBFL（オンボード障害ロギング）フラッシュの完全性を確認します。
BootupPortLoopback	CP*N**XE*T*	PortLoopback テストはモジュールのブートアップ時にだけ実行されます。
Supervisor（スーパバイザ）		
USB	C**N**X**T*	モジュールにおけるUSBコントローラの初期化を確認します。
ManagementPortLoopback	C**D**X**T*	モジュールの管理インターフェイスの正常性を確認します。

診断	属性	説明
EOBCPortLoopback	C**D**X**T*	EOBC（イーサネット アウトオブバンド接続）インターフェイスの正常性を確認します。
OBFL	C**N**X**T*	OBFL（オンボード障害ロギング）フラッシュの完全性を確認します。

show module コマンドを実行すると、ブートアップ診断の結果が Online Diag Status として表示されます。個別のテストの結果は、該当するモジュールとテスト ID またはテスト名に対して **show diagnostic result** コマンドを実行すると表示されます。

ブートアップ診断テストをバイパスするように Cisco MDS 9700 ファミリ スイッチを構成することも、またはすべてのブートアップ診断テストを実行するように設定することもできます。「起動診断レベルの設定, on page 218」を参照してください。

ヘルス モニタリング診断

稼働中のシステムの正常性を定期的に検証するために、ヘルスモニタリング（HM）診断はデフォルトで有効になっています。モニタリング間隔（許可された範囲内）は、テストごとに異なるユーザが構成できます。詳細については、ヘルスモニタリング診断テストのアクティブ化, on page 220を参照してください。診断テストは、ハードウェア エラーとデータ パスの問題を検出します。

ヘルスモニタリング診断は中断を伴いません（データや制御トラフィックは中断させません）。ヘルスモニタリングテストは、ユーザが無効にすることができます。詳細については、ヘルスモニタリング診断テストの非アクティブ化, on page 221を参照してください。

次の表に、スーパーバイザのヘルスモニタリング診断を示します。

診断	デフォルトのテスト実施の間隔	属性	説明
Supervisor（スーパバイザ）			
ASICRegisterCheck	20 秒	***N******A	スーパーバイザ上の ASIC のスクラッチ レジスタへの読み取りまたは書き込みアクセスを確認します。
NVRAM	5 分	***N******A	スーパーバイザの NVRAM ブロックの健全性を確認します。
RealTimeClock	5 分	***N******A	スーパーバイザ上のリアルタイム クロックが時を刻んでいるかどうかを確認します。

診断	デフォルトのテスト実施の間隔	属性	説明
PrimaryBootROM	30 分	***N******A	スーパーバイザ上のプライマリ ブートデバイスの完全性を確認します。
SecondaryBootROM	30 分	***N******A	スーパーバイザ上のセカンダリ ブートデバイスの完全性を確認します。
CompactFlash	30 分	***N******A	Compact Flash デバイスにアクセスできるかどうかを確認します。
ExternalCompactFlash	30 分	***N******A	外部コンパクト フラッシュ デバイスにアクセスできるかどうかを確認します。
PwrMgmtBus	30 秒	**MN******A	スタンバイの電源管理制御バスを確認します。
SystemMgmtBus	30 秒	**MN******A	スタンバイ システム管理バスの使用可能性を確認します。
StatusBus	30 秒	**MN******A	スーパーバイザ、モジュール、およびファブリック カードに対するステータス バイパスによって送信されるステータスを確認します。
StandbyFabricLoopback	30 秒	**SN******A	ファブリック モジュールへのスタンバイ スーパーバイザの接続を確認します。

Table 27: ヘルス モニタリング診断, on page 214 では、 のヘルスモニタリング診断について説明します。

Table 27: ヘルス モニタリング診断

診断	デフォルトのテスト実施の間隔	属性	説明
ラインカード			
ASICRegisterCheck	1分	***N******A	モジュール上の ASIC のスクラッチ レジスタへの読み取りまたは書き込みアクセスを確認します。
PrimaryBootROM	30 分	***N******A	モジュール上のプライマリ ブート デバイスの完全性を確認します。

診断	デフォルトのテスト実施の間隔	属性	説明
SecondaryBootROM	30 分	***N******A	モジュール上のセカンダリ ブート デバイスの完全性を確認します。
SnakeLoopback	20 分	*P*N***E**	SUP からラインカードのすべてのポートへの接続を確認します。これは、MAC コンポーネントまでのデータ パスの整合性をプログレッシブな方法でチェックします（1 回のテスト実行ですべてのポートが対象になります）。状態に関係なく、すべてのポートで実行されます。 これは無停止テストです。
IntPortLoopback	5 分	*P*N***E***	SUP からラインカードのすべてのポートへの接続を確認します（一度に 1 つのポート）。これは、MAC コンポーネントまでのデータ パスの完全性をチェックします。このテストは、ヘルスモニタリング（HM）モードで実行されるだけでなく、「オンデマンドモード」でトリガーすることもできます。 このテストは無停止です。 **Note** IntPortLoopback テストは、Cisco MDS NX-OS リリース 6.2(7) からサポートされています。
RewriteEngine ループバック	1分	*P*N***E**A	sup から linecard へのファブリック モジュール上の各リンクの完全性を確認します。

オンデマンド診断

すべてのヘルスモニタリングテストをオンデマンドでも実行できます。オンデマンド診断は、ユーザによって呼び出された場合にのみ実行されます。

Note 他のヘルスモニタリング テストでは検証されないデータ パス（PHY および SFP）は、PortLoopback および ExtPortLoopback テストで検証できます。

必要なときにいつでもオンデマンド診断を実行できます。詳細については、オンデマンド診断テストの開始または中止, on page 221を参照してください。

では、PortLoopback テストと ExtPortLoopback テストの両方がオンデマンド モードでのみ使用可能です。これらは中断を伴うためです。

Table 28: オンデマンド診断, on page 216 に、のオンデマンド診断（モジュールのみ）について説明します。

Table 28: オンデマンド診断

診断	属性	説明
ラインカード		
PortLoopback	*P*D**XE***	sup からモジュールのすべてのポートへの接続を確認します。PHY までのデータ パスの完全性をチェックします。このテストは、「オンデマンド モード」でのみ利用できます。テストは、ポートの状態に関係なく、すべてのポートで実行されます。 **Note** Portloopback テストは、OHMS の Serdes ループバック テストに相当します。
ExtPortLoopback	*P*D**XE***	SFP を含む PHY までのデータ パス全体のハードウェア エラーを識別します。 **Note** テストを実行する前に、ループバック プラグを接続して、ポートの Tx をポートの Rx にループさせます。ループバック プラグが接続されていない場合、このテストは失敗します。 **Note** ExtPortLoopback テストは、Cisco MDS NX-OS リリース 6.2(11c) からサポートされています。

Caution PortLoopback および ExtPortLoopback テストは、診断操作のためにポートをダウンさせるため、中断を伴います。

指定されたヘルスモニタリング診断でのリカバリ アクション

ヘルスモニタリング診断テストが最大 10 回のしきい値で連続して失敗すると、EEM を介してデフォルト アクションが実行されます。これには、アラートの生成（callhome、syslog）およびロギング（OBFL、例外ログ）が含まれます。また、診断テストは失敗したインスタンス（ポート、ファブリック、またはデバイス）で無効化されます。

これらのアクションは有益ですが、ネットワーク中断、トラフィック ブラックホールなどの結果が生じるデバイス障害をライブ システムから除くものではありません。

Note テスト結果をクリアし、非アクティブ化してから、同じモジュールでテストをアクティブ化することにより、失敗したインスタンスのヘルスモニタリングテストを再開します。詳細については、診断結果の消去, on page 224、ヘルスモニタリング診断テストの非アクティブ化, on page 221、およびヘルスモニタリング診断テストのアクティブ化, on page 220 を参照してください。

Cisco MDS NX-OS リリース 6.2(11) 以降では、次のヘルスモニタリング テストのいずれかで、連続して失敗するしきい値の数に達した後に、デフォルト アクションに加えて修正（リカバリ）アクションを実行するようにシステムを構成できます。

- PortLoopback テスト（Cisco MDS 48 ポート 10 Gbps FCoE モジュールでのみサポート）
- RewriteEngineLoopback テスト
- StandbyFabricLoopback テスト
- 内部 PortLoopback テスト

Note 修正（リカバリ）アクションは、デフォルトで無効になっています。

スーパーバイザの修正（リカバリ）アクション

sup の修正アクションは次のとおりです。

StandbyFabricLoopback テスト：システムはスタンバイ スーパーバイザをリロードし、3 回再試行した後、スタンバイ スーパーバイザの電源をオフにします。

Note リロード後、スタンバイ スーパーバイザがオンラインになると、ヘルスモニタリング診断がデフォルトで開始されます。

Note 1 回の再試行は、スタンバイ スーパーバイザをリロードする完全なサイクルと、それに続く StandbyFabricLoopback テストの連続失敗のしきい値数を意味します。

高可用性

高可用性の重要な機能は、稼働しているシステムでハードウェア障害を検出して、修正アクションを行うことです。GOLD は、ハードウェア障害を検出し、スイッチオーバーの決定を行うためにソフトウェア コンポーネントにフィードバックを提供することにより、システムの高可用性に貢献します。

Cisco MDS 9700 ファミリ スイッチは、再起動後に実行構成を適用することにより、GOLD のステートレスな再起動をサポートします。スーパーバイザのスイッチオーバーの後、GOLD は新しいアクティブ スーパーバイザから診断を再開します。

オンライン診断機能のライセンス要件

製品	ライセンス要件
Cisco NX-OS	オンライン診断機能にライセンスは不要です。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。Cisco NX-OS ライセンス スキームの詳細については、『*Cisco NX-OS* ライセンス ガイド』を参照してください。

デフォルト設定

Table 29: デフォルトのオンライン診断パラメータ , on page 218 に、オンライン診断パラメータのデフォルト設定を示します。

Table 29: デフォルトのオンライン診断パラメータ

パラメータ	デフォルト
起動時診断レベル	complete
ヘルスモニタリング テスト	アクティブ
修正（リカバリ）アクション	無効

オンライン診断の設定

起動診断レベルの設定

一連のテストを実行するようにブートアップ診断を構成し、またはモジュールがより高速に起動してすべてのブートアップ診断テストをバイパスするように構成するには、これらのタスクを行います。。

Note ブートアップ オンライン診断レベルを **complete** に設定することが推奨されています。

Procedure

ステップ 1 **configure terminal**

Example:

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

グローバル構成モードにします。

ステップ 2 **diagnostic bootup level** {**complete** | **bypass** }

Example:

```
switch(config)# diagnostic bootup level complete
```

デバイスの起動時に診断テストがトリガーされるように、ブートアップ診断レベルを構成します。

- **complete**：すべてのブートアップ診断を実行します。complete がデフォルトです。
- **bypass**：ブートアップ診断を実行しません。

ステップ 3 **show diagnostic bootup level**

Example:

```
switch(config)# show diagnostic bootup level
```

（任意）デバイスに現在設定されている起動診断レベル（bypass または complete）を表示します。

ステップ 4 **copy running-config startup-config**

Example:

```
switch(config)# copy running-config startup-config
```

（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

利用可能なテストの一覧の表示

Procedure

show diagnostic content module *slot*

Example:

```
switch# show diagnostic content module 1
```

（オプション）診断テストの情報のリストおよび所定のモジュールの対応する属性を表示します。

slot：テストがアクティブ化するモジュールの数です。

ヘルスモニタリング診断テストのアクティブ化

Procedure

ステップ 1 **configure terminal**

Example:

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

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 2 **diagnostic monitor interval module** *slot* **test** [*test-id* | *name* | **all**] **hour** *hour* **min** *minutes* **second** *sec*

Example:

```
switch(config)# diagnostic monitor interval module 6 test 3 hour 1 min 0 sec 0
```

（任意）指定されたテストを実行するインターバルを設定します。インターバルを設定しなかった場合は、過去に設定されたインターバルまたはデフォルトのインターバルでテストが実行されます。

引数は次のとおりです。

- slot：テストがアクティブ化するモジュールの数です。
- test-id：テストの一意の識別番号。
- name：テストの定義済みの名前。
- hour：範囲は 0 ～ 23 時間
- minute：範囲は 0 ～ 59 分
- second：範囲は 0 ～ 59 秒

ステップ 3 **diagnostic monitor module** *slot* **test** [*test-id* | *name* | **all**]

Example:

```
switch(config)# diagnostic monitor module 6 test 3
switch(config)# diagnostic monitor module 6 test SecondaryBootROM
```

指定されたテストをアクティブにします。

引数は次のとおりです。

- slot：テストがアクティブ化するモジュールの数です。
- test-id：テストの一意の識別番号。
- name：テストの定義済みの名前。

ステップ 4 **show diagnostic content module** {*slot* | **all**}

Example:

```
switch(config)# show diagnostic content module 6
```

（任意）診断テストおよび対応する属性の情報を表示します。

引数は以下のようになります。

- slot：テストがアクティブ化するモジュールの数です。

ヘルスモニタリング診断テストの非アクティブ化

Note 非アクティブにしたテストでは、現在の設定が維持されますが、スケジュール上の間隔ではテストは実行されません。

テストを非アクティブ化するには、次のタスクを実行します。

コマンド	目的

no diagnostic monitor module *slot* **test** [*test-id* | *name* | **all**]
Examples:
`switch(config)# no diagnostic monitor interval module 8 test 3`
`switch(config)# no diagnostic monitor interval module 8 test SecondaryBootROM`
	指定されたテストを非アクティブ化します。
	引数は次のとおりです。
	• slot：テストがアクティブ化するモジュールの数です。
	• test-id：テストの一意の識別番号。
	• name：テストの定義済みの名前。

オンデマンド診断テストの開始または中止

オンデマンド診断テストは、アクション（オプション）を使用して開始または停止でき、反復回数を変更してテストを繰り返し、テストの失敗時に実行するアクションを決定します。

Note スケジューリングされたネットワーク メンテナンス期間内に、中断モードの診断テストを開始する場合は、手動による開始が推奨されています。

オンデマンド診断テストを開始または停止するには、次の作業を行います。

Procedure

ステップ 1 **diagnostic ondemand iteration** *number*

Example:

```
switch# diagnostic ondemand iteration 5
```

（任意）オンデマンド テストの実行回数を設定します。範囲は 1 ～ 999 です。デフォルトは 1 です。

ステップ 2 **diagnostic ondemand action-on-failure** {**continue failure-count** *num-fails* | **stop**}

Example:

```
switch# diagnostic ondemand action-on-failure stop
```

（任意）オンデマンド テストが失敗した場合のアクションを設定します。

ステップ 3 **show diagnostic ondemand setting**

Example:

```
switch# show diagnostic ondemand setting
Test iterations = 1
Action on test failure = continue until test failure limit reaches 1
```

（オプション）オンデマンド診断に関する情報を表示します。

ステップ 4 **diagnostic start module** *slot* **test** [*test-id* | *name* | **all** | **non-disruptive**][**port** *port-number* | **all**]

Example:

```
switch# diagnostic start module 6 test all
```

モジュール上で 1 つまたは複数の診断テストを開始します。

引数は次のとおりです。

- all：すべてのテストがトリガーされます。

Note
複数のテスト ID または名前は、コンマで区切って指定できます。

- non-disruptive：すべての non-disruptive テストがトリガーされます。

- port：テストは、単一のポート、ポートの範囲、またはすべてのポートで呼び出すことができます。

ステップ 5 **diagnostic run module** *slot* **test** {**PortLoopback** | **RewriteEngineLoopback** | **SnakeLoopback** | **IntPortLoopback** | **ExtPortLoopback**} {**port** *port-id* }

Example:

```
switch# diagnostic run module 3 test PortLoopback port 1
```

モジュールで選択したテストを開始し、テストの完了時に結果を表示します。

Note
このコマンドは、Cisco MDS NX-OS リリース 6.2(11c) から導入されました。

詳細については、オンデマンド モードでのオンデマンド診断テストの開始, on page 223を参照してください。

ステップ 6 **diagnostic stop module** *slot* **test** [*test-id* | *name* | **all**]

Example:

```
switch# diagnostic stop module 6 test all
```

（オプション）モジュール上で 1 つまたは複数の診断テストを中止します。

ステップ 7 **show diagnostic status module** *slot*

Example:

```
switch# show diagnostic status module 6
```

（オプション）実行中でキューに入れられているすべてのテストを、そのモジュールのテストモードに関する情報とともに表示します。

特定のモジュールでテストが実行またはエンキューされていない場合、ステータスはNA と表示されます。

ステップ 8 **show diagnostic result module** *slot* **test** [*test-id* | *name*]

Example:

```
switch# show diagnostic result module 1 test 3 SecondaryBootROM
```

（オプション）指定されたテストの結果を表示します。

オンデマンド モードでのオンデマンド診断テストの開始

OHMS（オンライン正常性管理システム）は、テストの実行直後に結果を表示する「オンデマンド モード」でのテストの呼び出しをサポートしています。

Cisco MDS NX-OS リリース 6.2(11c) 以降、GOLD は「オンデマンド モード」での一連のテストからの特定のテストの呼び出しと、テストの実行直後にテスト結果を表示することをサポートします。

GOLD テストは、**diagnostic start module** コマンドを使用して「オンデマンド」モードで呼び出すことができます。**diagnostic run module** コマンドも同じアクションをサポートしていますが、この2つにはいくつかの重要な違いがあります。2つのコマンドの違いは次のとおりです。

- **diagnostic start module** コマンドとは対照的に、**diagnostic run module** コマンドはテストが完了するまで現在の CLI セッションをブロックします。テストが完了すると、CLI セッションのブロックが解除され、結果が同じコンソールに表示されます。

Note CLI セッションは、テストが完了するまで、または最大 15 秒間ブロックされます。テストが 15 秒以内に完了しない場合、GOLD は CLI セッションのブロックを解除し、完了するまでテストをバックグラウンドで実行できるようにします。

Note **diagnostic run module** コマンドを使用して特定のモジュールで呼び出すことができるテストは 1 つだけです。ユーザが同じモジュールで別のテストを呼び出そうとすると、エラーが表示され、テストは呼び出されません。

- **diagnostic start module** コマンドでは、テスト結果を表示するために、ユーザ が **show diagnostic result** コマンドを実行する必要があります。テストはバックグラウンドで実行されるため（現在の CLI セッションはブロックされていません）、ユーザは結果を表示するために **show diagnostic result** コマンドを発行する必要がありますが、**diagnostic run module** コマンドが実行されると、テスト結果が同じコンソールに暗黙的に表示されます。
- diagnostic run コマンドで表示される結果は、show diagnostic results コマンドで表示される結果よりも直感的です。

Note **diagnostic run module** コマンドで推奨されるポートの最大数は 5 です。

診断結果の消去

診断テストの結果を消去するには、次のコマンドを使用します。

コマンド	目的

diagnostic clear result module [*slot* |**all**] **test** {*test-id* | **all** }
Example:
`switch# diagnostic clear result module 2 test all`
`switch# diagnostic clear result module 2 test 3`
	指定されたテストのテスト結果を消去します。

診断結果のシミュレーション

診断テストが失敗した場合のGOLDの動作をテストするために、GOLDは、ポート、SUP、またはファブリックでテストの失敗をシミュレートするメカニズムを提供します。

Note 修正措置を有効にした後に障害をシミュレートすると、障害がシミュレートされたコンポーネントでアクション（修正措置を参照）がトリガーされます。

診断テストの結果をシミュレーションするには、次のコマンドを使用します。

コマンド	目的
diagnostic test simulation module *slot* **test** *test-id* {**fail** | **random-fail** | **success** } [**port** *number* | **all**] **Example:** `switch# diagnostic test simulation module 2 test 2 fail`	テスト結果のシミュレーションを行います。

診断テストの結果をシミュレーションするには、次のコマンドを使用します。

コマンド	目的
diagnostic test simulation module *slot* **test** *test-id* **clear** **Example:** `switch# diagnostic test simulation module 2 test 2 clear`	シミュレーションしたテスト結果を消去します。

修正（リカバリ）アクションの有効化

修正（リカバリ）アクションを有効にするには、次のコマンドを使用します。

Procedure

ステップ 1 **configure terminal**

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 2 **diagnostic eem action conservative**

Example:

```
switch(config)# diagnostic eem action conservative
```

修正またはリカバリ アクションを有効にします。

Note
このコマンドはシステム全体に適用でき、特定のモジュールまたはテストに特別に構成することはできません。

ステップ 3 **no diagnostic eem action conservative**

修正（リカバリ）アクションを無効にします。

オンライン診断の確認

GOLDテストの結果、ステータス、および構成情報を表示するには、次のコマンドのいずれかを使用します。

コマンド	目的
show diagnostic bootup level	起動診断に関する情報を表示します。
show diagnostic content module {*slot* | **all**}	モジュールの診断テスト内容に関する情報を表示します。
show diagnostic description module *slot* **test** [*test-name* | **all**]	診断テストの説明を表示します。
show diagnostic events [**error** | **info**]	診断イベントをエラーおよび情報イベント タイプ別に表示します。
show diagnostic ondemand setting	オンデマンド診断に関する情報を表示します。
show diagnostic result module *slot* [**test** [*test-name* | **all**]] [**detail**]	診断結果に関する情報を表示します。
show diagnostic simulation module *slot*	シミュレーションした診断テストに関する情報を表示します。

コマンド	目的
show diagnostic status module *slot*	モジュールのすべてのテストについて、テスト状況を表示します。
show module	オンライン診断テストの状況を含むモジュール情報を表示します。
show diagnostic eem action	修正（リカバリ）アクションのステータスを表示します。

オンライン診断のコンフィギュレーション例

この例は、1つのモジュールですべてのオンデマンドテストを開始する方法を示しています。

diagnostic start module 6 test all

この例は、1つのモジュールでテストをアクティブにして、テストインターバルを設定する方法を示しています。

configure terminal

diagnostic monitor module 6 test 2

diagnostic monitor interval module 6 test 2 hour 3 min 30 sec 0

その他の参考資料

オンライン診断の実装に関する詳細情報については、次の項を参照してください。

関連資料

関連項目	マニュアル タイトル
オンライン診断 CLI コマンド	Cisco MDS 9000 シリーズ コマンド資料

オンライン診断機能の履歴

Table 30: オンライン診断機能の履歴, on page 227 に、この機能のリリース履歴を示します。

Table 30: オンライン診断機能の履歴

機能名	リリース	機能情報
Generic Online Diagnostics（GOLD）	6.2	この機能が導入されました。

CHAPTER 11

スイッチ間リンク診断の構成

この章では、Cisco MDS スイッチで ISL 診断を構成する方法について説明します。

- ISL 診断に関する情報, on page 229
- ISL 診断の構成, on page 233
- ISL 診断のデバッグ, on page 245
- その他の参考資料, on page 245

ISL 診断に関する情報

ISL 診断機能は、ネットワーク内の Cisco MDS スイッチ間のスイッチ間リンクの正常性を検証するのに役立ちます。

ISL 診断を使用して、次のテストを実行できます。

- 遅延テスト
- シングル ホップ トラフィック テスト
- マルチホップ エンドツーエンド トラフィック テスト

サポートされるプラットフォーム

ISL 診断は、次のプラットフォームでサポートされています。

ISL 診断は、Cisco MDS 9700 スイッチの次の FC モジュールでサポートされています。

- Cisco MDS 9500 シリーズ スイッチの高度な 8 Gbps モジュール
  - DS-X9232-256K9
  - DS-X9248-256K9
- Cisco MDS 9700 シリーズ スイッチの 16 Gbps モジュール
  - DS-X9448-768K9
  - DS-X9334-K9

ISL 診断は、Cisco MDS 9500 スイッチの次の FC モジュールではサポートされていません。

- DS-X9224-96K9
- DS-X9248-96K9
- DS-X9248-48K9
- DS-X9304-18K9

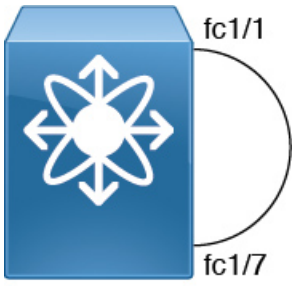
注意事項と制約事項

- 診断テストは、両側の異なるスイッチファミリの2つのサポートされているモジュール間で実行できます。
- モジュールの ISL 診断サポートは、ジェネレータ ポートとリフレクタ ポートのみに制限されています。
- ISL 診断は、Nexus 2000、Nexus 5000 などの他の非 MDS スイッチではサポートされていません。
- ISL 診断は、Cisco MDS スイッチの FCoE および IPS ポートではサポートされていません。
- ISL 診断は、16 Gbps FEC 対応リンクではサポートされていませんが、FEC のない 16 Gbps リンクではサポートされています。
- ISL 診断は、高密度波長分割多重化（DWDM）リンクではサポートされていません。

遅延テスト

遅延テストは、2 つの Cisco MDS スイッチ間の ISL の遅延を測定します。同じスイッチ上にあるポートで遅延テストを実行できます。テストを実行するには **diagnostic isl reflector** および **diagnostic isl generator** コマンドを使用します。詳細については、スイッチ間リンク診断の構成, on page 229を参照してください。

Figure 7: 同じスイッチのポートで実行される遅延テスト



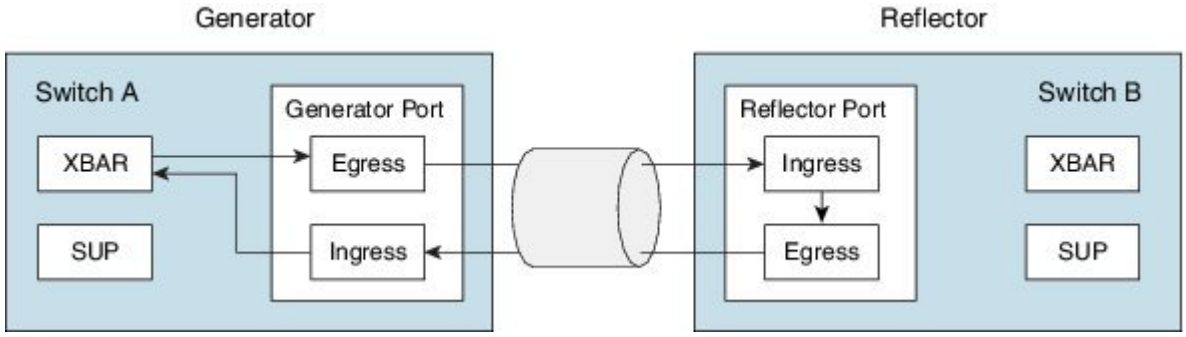
フレームは、リフレクタ スイッチポートによって、タイムスタンプがキャプチャされるジェネレータ スイッチにループバックされます。

タイムスタンプを使用すると、リフレクタ ポートの遅延だけでなく、リンクの遅延も両方向で測定できます。ケーブル長は、リンク遅延のみを使用して計算されます。報告されたケーブル長の精度は +/- 2 メートルです。Cisco MDS スイッチでは、ケーブル長（遅延テスト用）は、ケーブル長の 50 メートルまで検証されています。

Note 遅延テストを実行するときは、ジェネレータ ポートとリフレクタ ポートの両方が管理ダウン（「シャットダウン」）状態であり、ポートチャネルの一部ではない必要があります。

Figure 8: 遅延テスト, on page 231 に、遅延テストの詳細を示します。

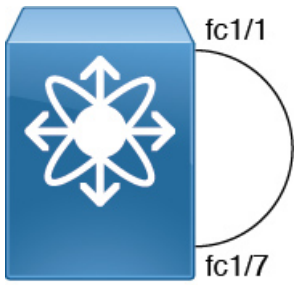
Figure 8: 遅延テスト



シングル ホップ トラフィック テスト

シングル ホップ トラフィック テストでは、さまざまなフレーム レートでトラフィックを処理する ISL の効率をチェックすることにより、ISL の状態を検証します。同じスイッチ上にあるポートでシングルホップ トラフィック テストを実行できます。テストを実行するには**diagnostic isl reflector** および **diagnostic isl generator** コマンドを使用します。詳細については、スイッチ間リンク診断の構成, on page 229を参照してください。

Figure 9: 同じスイッチのポートで実行されるシングル ホップ トラフィック テスト



ファイバチャネル（FC）フレームは、MACハードウェアで使用可能な内部トラフィック ジェネレータ機能を使用してジェネレータ スイッチで生成されます。これらのフレームは、テスト対象の ISL を介してジェネレータ スイッチポートから送信されます。リフレクタ スイッチは

フレームを受信し、通常のファブリック スイッチング パスを介してそれらを切り替え、受信したポートを介してフレームをテスト中の ISL に送信します。

ISL トラフィックの効率は、ジェネレータ スイッチポートで受信したパケット数に基づいて計算されます。

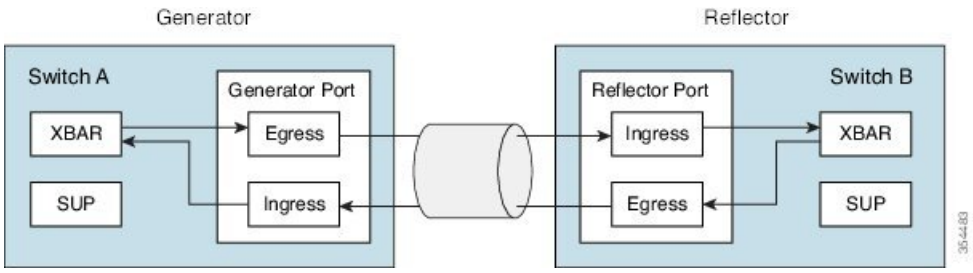
Note シングル ホップ テストを実行する場合、ジェネレータ ポートとリフレクタ ポートの両方が管理ダウン（「シャットダウン」）状態であり、ポートチャネルの一部ではない必要があります。

次のシナリオでは、トラフィック テストがエラーを返します。

- ISL が起動していない場合。
- ジェネレータ ポートに内部トラフィック ジェネレータ機能がない場合。
- リフレクタがループバック モードになっていない場合。

Figure 10: シングル ホップ トラフィック テスト, on page 232 は、シングル ホップ トラフィック テストの詳細を示しています。

Figure 10: シングル ホップ トラフィック テスト



トラフィックはすべてのクロスバー リンクを横切ります。

マルチホップ エンドツーエンド トラフィック テスト

マルチホップ テストでは、ファブリック内のホスト スイッチとターゲット スイッチ間の ISL の状態を評価します。

ホストをファブリック内のターゲットに接続する前に、マルチホップテストを使用して、ホスト ポートとターゲット ポート間のファブリック パスをテストします。

ホスト スイッチとターゲット スイッチの間に複数のホップが存在できます。中間スイッチに特定の構成は必要ありません。

Note ファブリック内の中間スイッチには、ジェネレータとリフレクタ ポートの間にルートが存在する限り、それらの間に任意のインターフェイスまたはリンク（FC、FCoE、IPS など）を含めることができます。

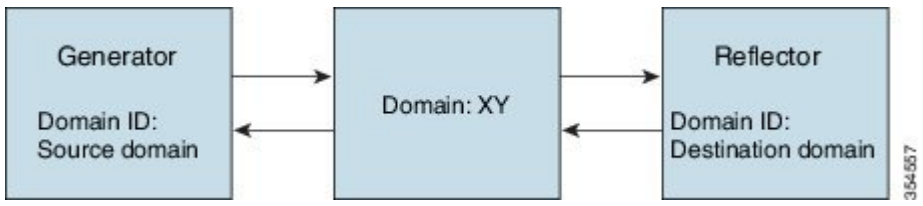
ファイバーチャネル（FC）フレームは、ジェネレータ スイッチポートで生成され、最初のホップ リンクに送信されます。これらのフレームは、リフレクタ スイッチに到達するまで中間スイッチを通過します。次に、リフレクタ スイッチがフレームを切り替え、ジェネレータ スイッチに戻します。ジェネレータ スイッチで受信したパケット数に基づいて、ISL の効率が表示されます。

マルチホップ トラフィック テストは、ジェネレータおよびリフレクタ スイッチのドメイン ID に基づいています。

Note マルチホップ トラフィック テストを実行する場合、ジェネレータ ポートとリフレクタ ポートの両方が管理ダウン（「シャットダウン」）状態であり、ポートチャネルの一部ではない必要がありますが、マルチホップ トラフィック テストによって使用される ISL 上でトラフィックが実行される可能性があります。

Figure 11: マルチホップ エンドツーエンド トラフィック テスト , on page 233 は、マルチホップ エンドツーエンド トラフィック テストの詳細を示しています。

Figure 11: マルチホップ エンドツーエンド トラフィック テスト



トラフィックはすべてのクロスバー リンクを横切ります。

ISL 診断の構成

Cisco MDS 9700 シリーズ スイッチでの遅延テストの構成

ジェネレータとリフレクタ スイッチ間の遅延テストを構成するには、次のタスクを実行します。

Note このタスクは、Cisco MDS 9700 シリーズ スイッチの次のモジュールでサポートされています。

- DS-X9448-768K9
- DS-X9334-K9
- DS-X9648-1536K9

Procedure

ステップ 1 次のコマンドを使用してループバック モードに設定することにより、遅延をテストするためにリフレクタ スイッチのテスト インターフェイスを有効にします。

switch B# **diagnostic isl reflector latency_test loop-back interface** *interface id* **enable**

ステップ 2 テストを実行して結果を表示するようにジェネレータ スイッチを構成します。

switch A# **diagnostic isl latency-test interface** *interface id*

ステップ 3 遅延テストのためにリフレクタ ポートを無効にするには、リフレクタ スイッチで次のコマンドを構成します。

switch B# **diagnostic isl reflector latency_test loop-back interface** *interface id* **disable**

遅延テスト

遅延テストを開始する前に、両方のスイッチのテストインターフェイスポートをシャットダウンします。

```
switch A# shutdown interface fc4/1
switch B# shutdown interface fc1/13
```

次の例は、遅延テストのためにリフレクタ スイッチのポートを有効にする方法を示しています。

```
switch B# diagnostic isl reflector latency_test loop-back interface fc1/13 enable
Reflector Configuration Successful.
```

次の例は、遅延テストを実行する方法を示しています。

```
switch A# diagnostic isl latency-test interface fc4/1
Waiting for sync to be achieved on the link ....
Sync is achieved, Link has been initialized.
Starting the test ....
-----------------------------------------------------------
Latency test Result for port:                   fc4/1
Latency in the switch (in ns):                  399
Latency in the cable (in ns):                   39
```

```
Length of the cable (accuracy +/- 2m):           4 m
-------------------------------------------------------------
```

次の例は、遅延テストのためにリフレクタ スイッチのポートを無効にする方法を示しています。

```
switch B# diagnostic isl reflector latency_test loop-back interface fc1/13 disable
Reflector Configuration Successful.
```

無効化されたインターフェイス ポートを再起動します。

```
switch A# no shutdown interface fc4/1
switch B# no shutdown interface fc1/13
```

他のサポートされているプラットフォームでの遅延テストの構成

ジェネレータとリフレクタ スイッチ間の遅延テストを構成するには、次のタスクを実行します。

Note このタスクは、次の Cisco MDS スイッチでサポートされています。

- Cisco MDS 9500 シリーズ スイッチ
- Cisco MDS 9396S スイッチ
- Cisco MDS 9396T スイッチ
- Cisco MDS 9148T スイッチ
- Cisco MDS 9132T スイッチ

Procedure

ステップ 1 次のコマンドを使用してループバック モードに設定することにより、遅延をテストするためにリフレクタ スイッチのテスト インターフェイスを有効にします。

switch B# **system health isl reflector latency_test loop-back interface** *interface id* **enable**

ステップ 2 テストを実行して結果を表示するようにジェネレータ スイッチを構成します。

switch A# **system health isl latency-test interface** *interface id*

ステップ 3 遅延テストのためにリフレクタ ポートを無効にするには、リフレクタ スイッチで次のコマンドを構成します。

switch B# **system health isl reflector latency_test loop-back interface** *interface id* **disable**

遅延テスト

遅延テストを開始する前に、両方のスイッチのテストインターフェイスポートをシャットダウンします。

```
switch A# shutdown interface fc1/13
switch B# shutdown interface fc4/25
```

次の例は、遅延テストのためにリフレクタ スイッチのポートを有効にする方法を示しています。

```
switch B# system health isl reflector latency_test loop-back interface fc4/25 enable
Reflector Configuration Successful.
```

次の例は、遅延テストを実行する方法を示しています。

```
switch A# system health isl latency-test interface fc1/13
Waiting for sync to be achieved on the link ....
Sync is achieved, Link has been initialized.
Starting the test ....


------------------------------------------------------------
Latency test Result for port: fc1/13
Latency in the switch (in ns): 5504
Latency in the cable (in ns): 664
Length of the cable (accuracy +/- 2m): 4.816514 m
------------------------------------------------------------
```

次の例は、遅延テストのためにリフレクタ スイッチのポートを無効にする方法を示しています。

```
switch B# system health isl reflector latency_test loop-back interface fc4/25 disable
Reflector Configuration Successful.
```

無効化されたインターフェイス ポートを再起動します。

```
switch A# no shutdown interface fc1/13
switch B# no shutdown interface fc4/25
```

Cisco MDS 9700 シリーズ スイッチでのシングル ホップ トラフィック テストの構成

ジェネレータ スイッチとリフレクタ スイッチ間のシングル ホップ トラフィック テストを構成するには、次のタスクを実行します。

Procedure

ステップ 1 次のコマンドを使用してループバック モードに設定することにより、シングル ホップ トラフィック テスト用のリフレクタ スイッチのテスト インターフェイスを有効にします。

switch B# **diagnostic isl reflector traffic_test loop-back interface** *interface id* **enable**

ステップ 2 次のオプションの 1 つを使用してインターフェイスを構成します。

- 所定のフレーム カウント、フレーム サイズ、およびレート（リンク スピード）パラメータ向けのトラフィック テストを実行するように、ジェネレータ スイッチのインターフェイスを構成します。

  switch A# **diagnostic isl generator interface** *interface id* **start frame-count** *number* **rate** *value* **frame_size min** *minimum size* **max** *maximum size* **step** *num*

- 所定の期間、フレーム サイズ、およびレート（リンク スピード）パラメータ向けのトラフィック テストを実行するように、ジェネレータ スイッチのインターフェイスを構成します。

  switch A# **diagnostic isl generator interface** *interface id* **start duration** *seconds* **rate** *value* **frame_size min** *minimum size* **max** *maximum size* **step** *num*

ステップ 3 シングル ホップ トラフィック テストのリフレクタ ポートを無効にします。

switch B# **diagnostic isl reflector traffic_test loop-back interface** *interface id* **disable**

ステップ 4 シングル ホップ トラフィック テストの結果を表示します。

switch B# **show diagnostic isl result interface** *interface id*

ステップ 5 シングル ホップ トラフィック テストを停止するには、次のコマンドを使用します。

switch A# **diagnostic isl generator interface** *interface id* **stop**

シングル ホップ トラフィック テスト

シングル ホップ トラフィック テストを開始する前に、両方のスイッチのテスト インターフェイス ポートをシャットダウンします。

```
switch A# shutdown interface fc4/5
switch B# shutdown interface fc9/37
```

次の例は、ループバック モードに設定して、シングル ホップ トラフィック テスト向けにリフレクタ スイッチのテスト インターフェイスを有効にする方法を示しています。

```
switch B# diagnostic isl reflector traffic_test loop-back interface fc9/37 enable
Reflector Configuration Successful.
```

次の例は、特定の期間、速度、およびフレーム サイズのパラメータでジェネレータ スイッチ上でトラフィック テストを実行する方法を示しています。

```
switch A# diagnostic isl generator interface fc4/5 start duration 100 rate 25% frame_size
 min 16 max 517 step 1
```

次の例は、シングル ホップ トラフィック テストの結果を示しています。

```
switch A# show  diagnostic isl result interface fc4/5
------------------------------------------------------------
Single hop  Traffic test Result for port: fc4/5
Packets Transmitted:                              30621868
Packets Recieved:                                 30621868
ISL traffic Efficiency (percent):                 100.0000
------------------------------------------------------------
```

無効化されたインターフェイス ポートを再起動します。

```
switch A# no shutdown interface fc4/5
switch B# no shutdown interface fc9/37
```

他のサポートされているプラットフォームでのシングル ホップ トラフィック テストの構成

ジェネレータ スイッチとリフレクタ スイッチ間のシングル ホップ トラフィック テストを構成するには、次のタスクを実行します。

Procedure

ステップ 1 ループバック モードに設定して、シングル ホップ トラフィック テスト向けにリフレクタ スイッチのテスト インターフェイスを有効にします。

switch B# **system health isl reflector traffic_test loop-back interface** *interface id* **enable**

ステップ 2 次のオプションの 1 つを使用してインターフェイスを構成します。

- 所定のフレーム カウント、フレーム サイズ、およびレート（リンク スピード）パラメータ向けのトラフィック テストを実行するように、ジェネレータ スイッチのインターフェイスを構成します。

  switch A# **system health isl generator interface** *interface id* **start frame-count** *number* **rate** *value* **frame_size min** *minimum size* **max** *maximum size* **step** *num*

- 所定の期間、フレーム サイズ、およびレート（リンク スピード）パラメータ向けのトラフィック テストを実行するように、ジェネレータ スイッチのインターフェイスを構成します。

  switch A# **system health isl generator interface** *interface id* **start duration** *seconds* **rate** *value* **frame_size min** *minimum size* **max** *maximum size* **step** *num*

ステップ 3 シングル ホップ トラフィック テストのためにリフレクタ ポートを無効にするには、リフレクタ スイッチで次のコマンドを構成します。

switch B# **system health isl reflector traffic_test loop-back interface** *interface id* **disable**

ステップ 4 シングル ホップ トラフィック テストの結果を表示します。

switch B# **show system health isl result interface** *interface id*

ステップ 5 シングル ホップ トラフィック テストを停止するには

switch A# **system health isl generator interface** *interface id* **stop**

シングル ホップ トラフィック テスト

シングル ホップ トラフィック テストを開始する前に、両方のスイッチのテスト インターフェイス ポートをシャットダウンします。

```
switch A# shutdown interface fc12/16
switch B# shutdown interface fc9/37
```

次の例は、ループバック モードに設定して、シングル ホップ トラフィック テスト向けにリフレクタ スイッチのテスト インターフェイスを有効にする方法を示しています。

```
switch B# system health isl reflector traffic_test loop-back interface fc9/37 enable
Reflector Configuration Successful.
```

次の例は、ジェネレータ スイッチで期間パラメータのトラフィック テストを実行する方法を示しています。

```
switch A# system health isl generator interface fc12/16 start duration 100
Waiting for sync to be achieved on the link .....
Link initialized successfully. Starting the test.

switch A# system health isl generator interface fc12/16 stop
-------------------------------------------------------
Traffic test Result for port:                    fc12/16
Packets Transmitted:                             5293153
Packets Recieved:                                5293153
ISL traffic Efficiency (percent):                100.0000
-------------------------------------------------------

switch B# system health isl reflector traffic_test loop-back interface fc9/37 disable
Reflector Configuration Successful.
```

次の例は、シングル ホップ トラフィック テストの結果を示しています。

```
switch A# show system health isl result interface fc12/16
-------------------------------------------------------
Single hop  Traffic test Result for port:      fc12/16
Packets Transmitted:                           1019885186
Packets Recieved:                              1019885186
ISL traffic Efficiency (percent):              100.0000
-------------------------------------------------------
```

無効化されたインターフェイス ポートを再起動します。

```
switch A# no shutdown interface fc12/16
switch B# no shutdown interface fc9/37
```

Cisco MDS 9700 シリーズ スイッチでのマルチホップ トラフィック テストの構成

ジェネレータ スイッチとリフレクタ スイッチ間のマルチホップ トラフィック テストを構成するには、次のタスクを実行します。

Procedure

ステップ 1 マルチホップ トラフィック テスト用に、ジェネレータ スイッチの特定の VSAN およびドメイン ID に対してループバック モードに設定して、リフレクタ スイッチのテスト インターフェイスを有効にします。

Cisco MDS NX-OS リリース 8.4(1) 以降では、次のコマンドを使用してください。

switch B# **diagnostic isl multi_hop reflector loop-back interface** *interface id* **enable vsan** *vsan id* **source-domain** *source id*

Note
送信元ドメインを取得するには、リフレクタ スイッチで次のコマンドを使用してください。

switch B# **show fcdomain domain-list vsan** *vsan id*

Cisco MDS NX-OS リリース 8.3(2) 以前のリリースでは、次のコマンドを使用してください。

switch B# **diagnostic isl multi_hop reflector loop-back interface** *interface id* **vsan** *vsan id* **source-domain** *source id* **enable**

ステップ 2 特定の VSAN、接続先ドメイン（リフレクタ スイッチのドメイン ID）、フレーム カウント、リンク速度、およびフレーム サイズ パラメータのマルチホップ トラフィック テストを実行するようにジェネレータ スイッチのインターフェイスを構成します。

Cisco MDS NX-OS リリース 8.4(1) 以降では、次のコマンドを使用してください。

switch A# **diagnostic isl multi_hop generator interface** *interface id* **start vsan** *vsan id* **dest-domain** *dest id* **frame-count** *number* **rate** *value* **frame_size min** *minimum size* **max** *maximum size* **step** *num*

Cisco MDS NX-OS リリース 8.3(2) 以前のリリースでは、次のコマンドを使用してください。

switch A# **diagnostic isl multi_hop generator interface** *interface id* **vsan** *vsan id* **dest-domain** *dest id* **startframe-count** *number* **rate** *value* **frame_size min** *minimum size* **max** *maximum size* **step** *num*

ステップ 3 特定の VSAN、接続先ドメイン（リフレクタ スイッチのドメイン ID）、期間レート、リンク速度、およびフレーム サイズ パラメータのマルチホップ トラフィック テストを実行するようにジェネレータ スイッチのインターフェイスを構成します。

Cisco MDS NX-OS リリース 8.4(1) 以降では、次のコマンドを使用してください。

switch A# **diagnostic isl multi_hop generator interface** *interface id* **start vsan** *vsan id* **dest-domain** *dest id* **duration** *seconds* **rate** *value* **frame_size min** *minimum size* **max** *maximum size* **step** *num*

Note
接続先ドメインを取得するには、ジェネレータ スイッチで次のコマンドを使用してください。

switch A# **show fcdomain domain-list vsan** *vsan id*

Cisco MDS NX-OS リリース 8.3(2) 以前のリリースでは、次のコマンドを使用してください。

switch A# **diagnostic isl multi_hop generator interface** *interface id* **vsan** *vsan id* **dest-domain** *dest id***start duration** *seconds* **rate** *value* **frame_size min** *minimum size* **max** *maximum size* **step** *num*

ステップ 4 マルチホップ トラフィック テスト向けにリフレクタ ポートを無効にするには、リフレクタ スイッチで次のコマンドを構成します。

Cisco MDS NX-OS リリース 8.4(1) 以降では、次のコマンドを使用してください。

switch B# **diagnostic isl multi_hop reflector loop-back interface** *interface id* **disable**

Cisco MDS NX-OS リリース 8.3(2) 以前のリリースでは、次のコマンドを使用してください。

switch B# **diagnostic isl multi_hop reflector loop-back interface** *interface id* **vsan** *vsan id***source-domain** *source id* **disable**

ステップ 5 マルチホップ トラフィック テストの結果を表示します。

switch A# **show diagnostic isl result interface** *interface id*

ステップ 6 マルチホップ トラフィック テストを停止するには

Cisco MDS NX-OS リリース 8.4(1) 以降では、次のコマンドを使用してください。

switch A# **diagnostic isl multi_hop generator interface** *interface id* **stop**

Cisco MDS NX-OS リリース 8.3(2) 以前のリリースでは、次のコマンドを使用してください。

switch A# **diagnostic isl multi_hop generator interface** *interface id* **vsan** *vsan id* **dest-domain** *dest id* **stop**

マルチホップ トラフィック テスト

マルチホップ トラフィック テストを開始する前に、両方のスイッチのテスト インターフェイス ポートをシャットダウンします。

```
switch A# shutdown interface fc4/10
switch B# shutdown interface fc9/36
```

次の例は、ジェネレータ スイッチおよびリフレクタ スイッチの両方でドメイン リストを表示する方法を示しています。

```
switch# show fcdomain domain-list vsan 1
Number of domains: 3
Domain ID              WWN
---------    -----------------------
0x85(133)    20:01:00:0d:ec:b7:20:01 [Principal]
```

```
0xef(239)    20:01:40:55:39:0c:70:81 [Local]
0x02(2)      20:01:00:0d:ec:b7:28:c1
```

次の例は、マルチホップ トラフィック テスト用に、特定の VSAN およびジェネレータ スイッチのドメイン ID に対してループバック モードに設定することにより、リフレクタ スイッチのテスト インターフェイスを有効にする方法を示しています。

```
switch B# diagnostic isl multi_hop reflector loop-back interface fc9/36 enable vsan 1
source_domain 239
```

次の例は、特定の期間、速度、およびフレーム サイズのパラメータでジェネレータ スイッチ上でトラフィック テストを実行する方法を示しています。

```
switch A# diagnostic isl multi_hop generator interface fc4/10 start vsan 1 dest_domain
133 duration 100 rate 16G frame_size min 16 max 517 step 1
```

次の例は、マルチホップ トラフィック テストの結果を示しています。

```
switchA #show diagnostic isl result interface fc 4/10

------------------------------------------------------------
Multi hop Traffic test Result for port:    fc4/10
Packets Transmitted:                            6131424
Packets Recieved:                               6131424
ISL traffic Efficiency (percent):               100.0000
------------------------------------------------------------
```

無効化されたインターフェイス ポートを再起動します。

```
switch A# no shutdown interface fc4/10
switch B# no shutdown interface fc9/36
```

サポートされている他のプラットフォームでのマルチホップ トラフィック テストの構成

ジェネレータ スイッチとリフレクタ スイッチ間のマルチホップ トラフィック テストを構成するには、次のタスクを実行します。

Procedure

ステップ 1 ジェネレータ スイッチの特定の VSAN およびドメイン ID に対してループバック モードに設定して、リフレクタ スイッチのテスト インターフェイスを有効にします。

Cisco MDS NX-OS リリース 8.4(1) 以降では、次のコマンドを使用してください。

switch B# **system health isl multi_hop reflector loop-back interface** *interface id***enable vsan** *vsan id* **source-domain** *source id*

Cisco MDS NX-OS リリース 8.3(2) 以前のリリースでは、次のコマンドを使用してください。

switch B# **system health isl multi_hop reflector loop-back interface** *interface id* **vsan** *vsan id* **source-domain** *source id* **enable**

送信元ドメインを取得するには、リフレクタ スイッチで次のコマンドを使用してください。

switch B# **show fcdomain domain-list vsan** *vsan id*

ステップ 2 特定の VSAN、接続先ドメイン（リフレクタ スイッチのドメイン ID）、フレーム カウント、リンク速度、およびフレーム サイズ パラメータのマルチホップ トラフィック テストを実行するようにジェネレータ スイッチのインターフェイスを構成します。

Cisco MDS NX-OS リリース 8.4(1) 以降では、次のコマンドを使用してください。

switch A# **system health isl multi_hop generator interface** *interface id* **start vsan** *vsan id* **dest-domain** *dest id* **frame-count** *number* **rate** *value* **frame_size min** *minimum size* **max** *maximum size* **step** *num*

Cisco MDS NX-OS リリース 8.3(2) 以前のリリースでは、次のコマンドを使用してください。

switch A# **system health isl multi_hop generator interface** *interface id* **vsan** *vsan id* **dest-domain** *dest id* **start frame-count** *number* **rate** *value* **frame_size min** *minimum size* **max** *maximum size* **step** *num*

ステップ 3 特定の VSAN、接続先ドメイン（リフレクタ スイッチのドメイン ID）、期間レート、リンク速度、およびフレーム サイズ パラメータのマルチホップ トラフィック テストを実行するようにジェネレータ スイッチのインターフェイスを構成します。

Cisco MDS NX-OS リリース 8.4(1) 以降では、次のコマンドを使用してください。

switch A# **system health isl multi_hop generator interface** *interface id* **start vsan** *vsan id* **dest-domain** *dest id* **duration** *seconds* **rate** *value* **frame_size min** *minimum size* **max** *maximum size* **step** *num*

Cisco MDS NX-OS リリース 8.3(2) 以前のリリースでは、次のコマンドを使用してください。

switch A# **system health isl multi_hop generator interface** *interface id* **vsan** *vsan id* **dest-domain** *dest id* **start duration** *seconds* **rate** *value* **frame_size min** *minimum size* **max** *maximum size* **step** *num*

接続先ドメインを取得するには、ジェネレータ スイッチで次のコマンドを使用してください。

switch A# **show fcdomain domain-list vsan** *vsan id*

ステップ 4 マルチホップ トラフィック テスト向けにリフレクタ ポートを無効にし、リフレクタ スイッチで次のコマンドを構成します。

Cisco MDS NX-OS リリース 8.4(1) 以降では、次のコマンドを使用してください。

switch B# **system health isl multi_hop reflector loop-back interface** *interface id* **disable**

Cisco MDS NX-OS リリース 8.3(2) 以前のリリースでは、次のコマンドを使用してください。

switch B# **system health isl multi_hop reflector loop-back interface** *interface id* **vsan** *vsan id* **source-domain** *source id* **disable**

ステップ 5 マルチホップ トラフィック テストの結果を表示します。

switch A# **show system health isl result interface** *interface id*

ステップ 6 ジェネレータ スイッチでマルチホップ トラフィック テストを停止するには、次のコマンドを使用します。

Cisco MDS NX-OS リリース 8.4(1) 以降では、次のコマンドを使用してください。

switch A# **system health isl multi_hop generator interface** *interface id* **stop**

Cisco MDS NX-OS リリース 8.3(2) 以前のリリースでは、次のコマンドを使用してください。

switch A# **system health isl multi_hop generator interface** *interface id* **vsan** *vsan id* **dest-domain** *dest id* **stop**

マルチホップ トラフィック テスト

マルチホップ トラフィック テストを開始する前に、両方のスイッチのテストインターフェイス ポートをシャットダウンします。

```
switch A# shutdown interface fc3/18
switch B# shutdown interface fc9/36
```

次の例は、ジェネレータ スイッチおよびリフレクタ スイッチの両方でドメイン リストを表示する方法を示しています。

```
switch# show fcdomain domain-list vsan 1
Number of domains: 3
Domain ID              WWN
---------    -----------------------
0x85(133)    20:01:00:0d:ec:b7:20:01 [Principal]
0xef(239)    20:01:40:55:39:0c:70:81 [Local]
0x02(2)      20:01:00:0d:ec:b7:28:c1
```

次の例は、マルチホップ トラフィック テスト向けに、リフレクタ スイッチからVSANに存在するジェネレータ スイッチ インターフェイスへのループバックを有効にする方法を示しています。

```
switch B# system health isl multi_hop reflector loop-back interface fc9/36 enable vsan
1 source_domain 239
```

次の例は、特定の期間、速度、およびフレーム サイズのパラメータでジェネレータ スイッチ上でトラフィック テストを実行する方法を示しています。

```
switch A# system health isl multi_hop generator interface fc3/18 start vsan 1 dest_domain
 133 duration 100 rate 16G frame_size min 16 max 517 step 1
```

次の例は、マルチホップ トラフィック テストの結果を示しています。

```
switch A# show system health isl result interface fc3/18
------------------------------------------------------------
Multi hop Traffic test Result for port:    fc3/18
Packets Transmitted:                            3065550
Packets Recieved:                               3065550
ISL traffic Efficiency (percent):               100.0000
------------------------------------------------------------
```

無効化されたインターフェイス ポートを再起動します。

```
switch A# no shutdown interface fc3/18
switch B# no shutdown interface fc9/36
```

ISL 診断のデバッグ

次の表に、この機能のデバッグ コマンドを示します。ISL 診断テストのステータスを表示するには、次のコマンドのいずれかを使用します。

***Table 31: Debug* コマンド**

コマンド	リファレンス（**Reference**）
Cisco MDS 9700 スイッチ [Cisco MDS NX-OS リリース 8.2(1) 以前]	
	ポートごとに構成された ISL 診断テストのステータスを表示します。
Cisco MDS 9700 スイッチ [Cisco MDS NX-OS リリース 8.3(1) 以降]	

その他の参考資料

オンライン診断の実装に関する詳細情報については、次の項を参照してください。

関連資料

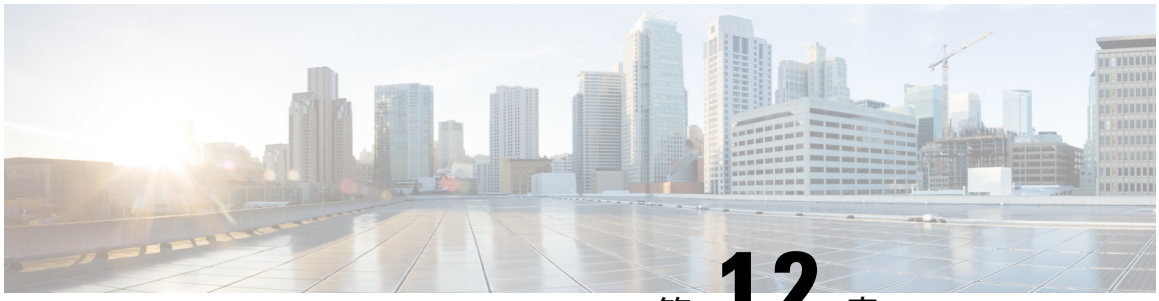
関連項目	マニュアル タイトル
InterSwitch リンク診断 CLI コマンド	『Cisco MDS 9000 Family Command Reference』

オンライン診断機能の履歴

Table 32: オンライン診断機能の履歴, on page 245 に、この機能のリリース履歴を示します。

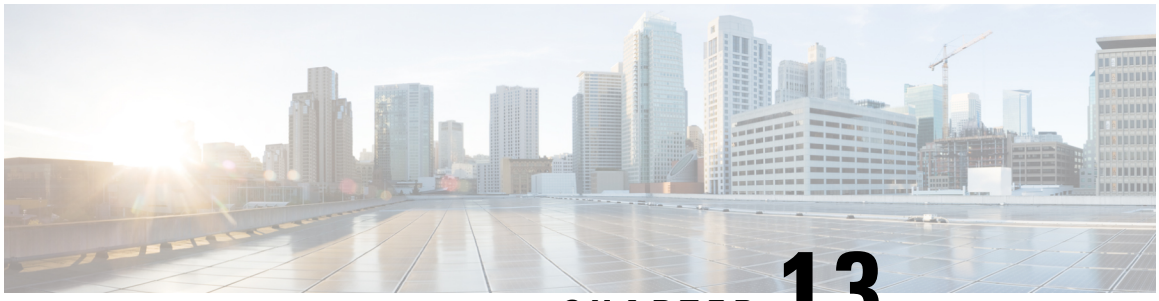
***Table 32:* オンライン診断機能の履歴**

機能名	リリース	機能情報
ISL 診断	7.3(0)D1(1)	この機能が導入されました。



第 12 章

Pathtrace の使用



CHAPTER 13

SNMP の設定

CLI と SNMP は、Cisco MDS 9000 ファミリのすべてのスイッチで共通のロールを使用します。SNMP を使用して CLI で作成したロールを変更したり、その逆を行うことができます。

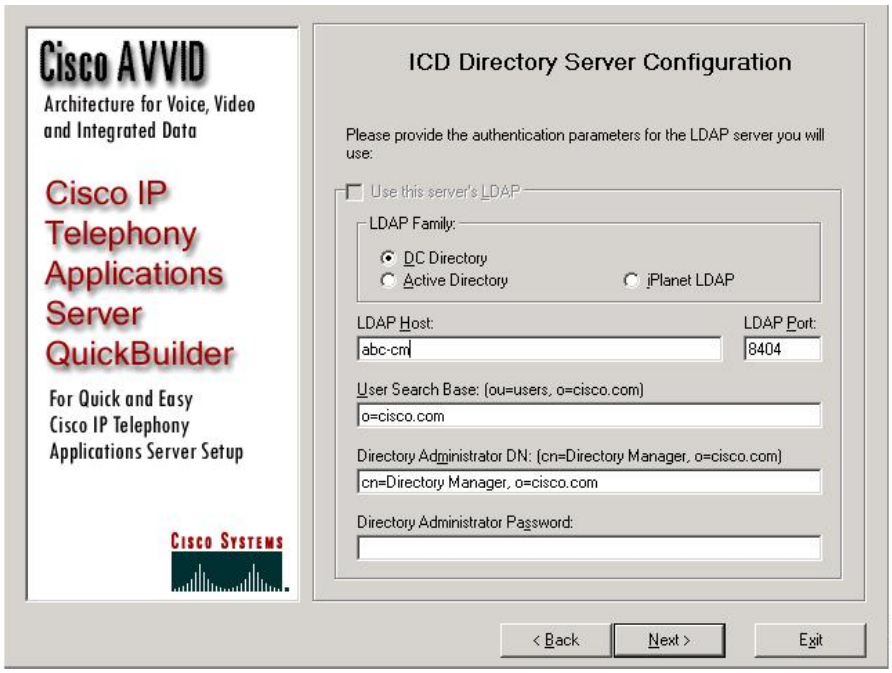
CLI ユーザーと SNMP ユーザーのユーザー、パスワード、ロールは、すべて同じです。CLI を通じて構成されたユーザは SNMP（たとえば、Cisco DCNM-SAN や Device Manager）を使用してスイッチにアクセスでき、その逆も可能です。

- SNMP セキュリティについて, on page 249
- デフォルト設定, on page 256
- SNMP の設定, on page 257
- SNMP の設定の確認, on page 274
- その他の参考資料, on page 279

SNMP セキュリティについて

SNMPは、ネットワーク デバイス間での管理情報の交換を容易にするアプリケーション層プロトコルです。すべての Cisco MDS 9000 ファミリ スイッチで、SNMPv1、SNMPv2c、および SNMPv3 の 3 つの SNMP バージョンが使用できます（Figure 12: SNMPセキュリティ, on page 250 を参照）。

*Figure 12: SNMP*セキュリティ



SNMP バージョン 1 およびバージョン 2c

SNMP バージョン 1（SNMPv1）および SNMP バージョン 2c（SNMPv2c）は、コミュニティ ストリングを使用してユーザ認証を行います。コミュニティ ストリングは、SNMP の初期のバージョンで使用されていた弱いアクセス コントロール方式です。SNMPv3 は、強力な認証を使用することによってアクセス コントロールを大幅に改善しています。したがって、SNMPv3 がサポートされている場合は、SNMPv1 および SNMPv2c に優先して使用してください。

SNMP バージョン 3

SNMP バージョン 3（SNMPv3）は、ネットワーク管理のための相互運用可能な標準ベースのプロトコルです。SNMPv3 は、ネットワーク経由のフレームの認証と暗号化を組み合わせることによって、デバイスへのセキュア アクセスを実現します。SNMPv3 で提供されるセキュリティ機能は、次のとおりです。

- メッセージの完全性：パケットが伝送中に改ざんされていないことを保証します。
- 認証：メッセージのソースが有効かどうかを判別します。
- 暗号化：許可されていないソースにより判読されないように、パケットの内容のスクランブルを行います。

SNMPv3 では、セキュリティ モデルとセキュリティ レベルの両方が提供されています。セキュリティ モデルは、ユーザおよびユーザが属するロールを設定する認証方式です。セキュリティ レベルとは、セキュリティ モデル内で許可されるセキュリティのレベルです。セキュリティ

モデルとセキュリティ レベルの組み合わせにより、SNMPパケット処理中に採用されるセキュリティ メカニズムが決まります。

SNMPv3 CLI のユーザ管理および AAA の統合

Cisco NX-OS ソフトウェアは RFC 3414 と RFC 3415 を実装しています。これには、ユーザベース セキュリティ モデル（USM）とロール ベースのアクセス コントロールが含まれています。SNMP と CLI のロール管理は共通化されており、同じ証明書とアクセス権限を共有しますが、以前のリリースではローカル ユーザ データベースは同期化されませんでした。

SNMPv3 のユーザ管理を AAA サーバ レベルで一元化できます。ユーザ管理を一元化すると、Cisco MDS スイッチ上で稼働する SNMP エージェントが AAA サーバのユーザ認証サービスを利用できます。ユーザ認証が検証されると、SNMP PDU の処理が進行します。また、AAA サーバにはユーザ グループ名も格納されます。SNMP はグループ名を使用して、スイッチでローカルに使用できるアクセス ポリシーまたはロール ポリシーを適用します。

CLI および SNMP ユーザの同期

ユーザ グループ、ロール、またはパスワードの設定が変更されると、SNMP と AAA の両方のデータベースが同期化されます。

SNMP または CLI ユーザを作成するには、**username** コマンドまたは **snmp-server user** コマンドを使用します。

- **snmp-server user** コマンドで指定された パスフレーズは、CLI ユーザのパスワードと同期します。
- **username** コマンドで指定したパスワードは、SNMP ユーザ用の auth および priv パスフレーズとして同期されます。

ユーザの同期化は、次のように処理されます。

- いずれかのコマンドを使用してユーザを削除すると、SNMP と CLI の両方の該当ユーザが削除されます。
- ユーザとロールの対応関係の変更は、SNMP と CLI で同期化されます。

Note パスフレーズ/パスワードをローカライズド キー/暗号化形式で指定すると、パスワードは同期化されません。

- 既存の SNMP ユーザは、特に変更しなくても、引き続き auth および priv のパスフレーズを維持できます。
- 管理ステーションが usmUserTable 内に SNMP ユーザを作成する場合、対応する CLI ユーザはパスワードなし（ログインは無効）で作成され、network-operator のロールが付与されます。

SNMPv3 サーバーの AAA 排他動作

AAA の排他的な動作機能を使用して、ロケーションに基づいてユーザを認証できます。

ユーザがローカルユーザまたはリモート AAA ユーザでない場合、一意の SNMPv3 ユーザは認証されません。ユーザがローカルおよびリモートデータベースの両方に存在する場合、ユーザは AAA の排他的な動作が有効かそうでないかに基づいて許可または拒否されます。

表 *33 : AAA* の排他的な動作のシナリオ

ユーザの場所	AAA サーバー	AAA の排他的な動作	ユーザー認証
ローカルユーザデータベース	無効	有効	ユーザが認証されました。
ローカルユーザデータベース	有効	有効	ユーザは認証されません。
ローカルユーザデータベース	有効	無効	ユーザが認証されました。
ローカルユーザデータベース	無効	無効	ユーザが認証されました。
リモートおよびローカルユーザーデータベース（同一ユーザ名）	有効	有効	リモート ユーザは認証されますが、ローカル ユーザは認証されません。
リモートおよびローカルユーザーデータベース（同一ユーザ名）	無効	有効	ローカル ユーザは認証されますが、リモート ユーザは認証されません。
リモートおよびローカルユーザーデータベース（同一ユーザ名）	無効	無効	ローカル ユーザは認証されますが、リモート ユーザは認証されません。
リモートおよびローカルユーザーデータベース（同一ユーザ名）	有効	無効	ローカル ユーザは認証されますが、リモート ユーザは認証されません。

（注） AAA サーバが到達不能な場合、ユーザがローカル ユーザーデータベースに対して検証されるようにフォールバック オプションをサーバーで構成することができます。ユーザがローカル データベースまたはリモート ユーザーデータベースで使用できない場合、SNMPv3 サーバーはエラーを返します。SNMPv3 サーバはー、リモート ユーザーデータベースにユーザが存在しない場合、AAA サーバの可用性をチェックせずに「Unknown user」メッセージを返します。

スイッチ アクセスの制限

IP アクセス コントロール リスト（IP-ACL）を使用して、Cisco MDS 9000 ファミリ スイッチへのアクセスを制限できます。

グループベースの SNMP アクセス

Note *group* が業界全体で使用されている標準規格 SNMP 用語なので、この SNMP のセクションでは、ロールのことをグループと言います。

SNMP アクセス権は、グループ別に編成されます。SNMP 内の各グループは、CLI を使用する場合のロールに似ています。各グループは3つのアクセス権により定義されます。つまり、読み取りアクセス、書き込みアクセス、および通知アクセスです。それぞれのアクセスを、各グループでイネーブルまたはディセーブルに設定できます。

ユーザ名が作成され、ユーザのロールが管理者によって設定され、ユーザがそのロールに追加されていれば、そのユーザはエージェントとの通信を開始できます。

ユーザの作成および変更

SNMP、DCNM-SAN、またはCLIを使用して、ユーザの作成、または既存のユーザの変更を実行できます。

- SNMP：スイッチ上の usmUserTable に存在するユーザのクローンとして、新規のユーザを作成します。ユーザを作成した後、クローンの秘密キーを変更してから、そのユーザをアクティブにします。RFC 2574 を参照してください。
- DCNM-SAN。
- CLI：**snmp-server user** コマンドを使用して、ユーザの作成または既存のユーザの変更を実行します。

Cisco MDS 9000 ファミリ スイッチ上で使用できるロールは、network-operator および network-admin です。GUI（DCNM-SAN および Device Manager）を使用する場合は、default-role もあります。また、Common Roles データベースに設定されている任意のロールも使用できます。

Tip CLI セキュリティ データベースおよび SNMP ユーザ データベースに対する更新はすべて同期化されます。SNMP パスワードを使用して、DCNM-SAN または Device Manager のいずれかにログインできます。ただし、CLI パスワードを使用して DCNM-SAN または Device Manager にログインした場合、その後のログインには必ず CLI パスワードを使用する必要があります。Cisco MDS SAN-OS Release 2.0(1b) にアップグレードする前から SNMP データベースと CLI データベースの両方に存在しているユーザの場合、アップグレードすると、そのユーザに割り当てられるロールは両方のロールを結合したものになります。

AES 暗号ベースの機密保全

Advanced Encryption Standard（AES）は対称暗号アルゴリズムです。Cisco NX-OS ソフトウェアは、SNMP メッセージ暗号化用のプライバシー プロトコルの 1 つとして AES を使用し、RFC 3826 に準拠しています。

priv オプションで、SNMP セキュリティ暗号化方式として、DES または 128 ビット AES 暗号化を選択できます。Cisco MDS NX-OS リリース 8.5(1) 以前では、**aes-128** トークンと連動する **priv** オプションは、128 ビットの AES キーを生成するためのプライバシ パスワードであることを示します。AES-128 は、Cisco MDS NX-OS リリース 8.5(1) からデフォルトのプライバシー オプションになりました。これは、Cisco MDS NX-OS リリース 8.5(1) から構成または変更されたすべてのユーザが **aes-128** をプライバシー オプションとして使用することを示しています。AES のプライバシー パスワードは最小で 8 文字です。パスフレーズをクリア テキストで指定する場合、最大 64 文字を指定できます。ローカライズド キーを使用する場合は、最大 130 文字を指定できます。

Note 外部の AAA サーバを使用して SNMPv3 を使う場合、外部 AAA サーバのユーザ設定でプライバシー プロトコルに AES を指定して、SNMP PDU を暗号化する必要があります。

トラップ、通知、およびインフォーム

トラップは、SNMP エージェントから SNMPv1 の SNMP マネージャに送信される未確認のメッセージです。SNMPv2 および SNMPv3 では通知と呼ばれます。インフォームは、SNMP エージェントから SNMP マネージャに送信される確認応答メッセージです。エージェントが応答を受信しない場合は、インフォーム要求を再度送信します。

ただし、インフォームは、エージェントやネットワークでより多くのリソースを消費します。送信と同時にエージェントによって廃棄されるトラップまたは通知とは異なり、インフォーム要求は応答を受信するまで、または要求がタイムアウトになるまで、メモリ内に保持する必要があります。トラップと通知は 1 回だけ送信できますが、インフォームは複数回送信できます。インフォームの再送信によりトラフィックが増加し、ネットワークのオーバーヘッドが高くなる原因になります。同じトラップ、通知、およびインフォームを複数のホスト受信者に送信できます。

Note SNMPv3 インフォームを機能させるには、**snmp-server user***name* **engineID** コマンドを使用して、SNMP ユーザでネットワーク管理サーバー（NMS）engineID を構成する必要があります。

NMS から Linux engineID を取得するには、**snmptarpd** を起動し、出力で **lcd_set_enginetime** 文字列を探します。

```
#snmptrapd -f -D -Le 3162
lcd_set_enginetime: engineID 80 00 1F 88 80 14 D4 89 07 46 D5 74 5A 00 00 00
00 : boots=96, time=0
```

EngineID

SNMP engineID は、送信元アドレスに関係なくエンティティを識別するために使用されます。エンティティは、SNMP エンジンと SNMP アプリケーションで構成されます。プロトコルデータユニット（PDU）がプロキシまたはネットワーク アドレス変換（NAT）を通過する必要がある場合、または送信元エンティティ自体に動的に割り当てられたトランスポートアドレスまたは複数の送信元アドレスがある場合、engineID は重要です。

SNMPv3 では、安全な PDU のエンコードとデコードにも engineID が使用されます。これは、SNMPv3 ユーザーベース セキュリティ モデル（USM）の要件です。

engineID には、ローカルとリモートの 2 種類があります。Cisco MDS 9000 シリーズ スイッチでは、リモート engineID のみを構成できます。ローカル engineID は、MAC アドレスに基づいてスイッチによって自動的に生成され、変更されません。

スイッチの LinkUp/LinkDown 通知

スイッチに対して、イネーブルにする LinkUp/LinkDown 通知を設定できます。次のタイプの LinkUp/LinkDown 通知をイネーブルにできます。

- Cisco：インターフェイスに対して ifLinkUpDownTrapEnable（IF-MIB で定義）がイネーブルになっている場合、そのインターフェイスについて CISCO-IF-EXTENSION-MIB.my で定義された通知（cieLinkUp、cieLinkDown）のみが送信されます。
- IETF：インターフェイスに対して ifLinkUpDownTrapEnable（IF-MIB で定義）がイネーブルになっている場合、そのインターフェイスについて IF-MIB で定義された通知（LinkUp、LinkDown）のみが送信されます。通知定義で定義された変数バインドのみが、それらの通知とともに送信されます。
- IEFT extended：インターフェイスに対して ifLinkUpDownTrapEnable（IF-MIB で定義）がイネーブルになっている場合、そのインターフェイスについて IF-MIB で定義された通知（LinkUp、LinkDown）のみが送信されます。通知定義で定義された変数バインドに加え、シスコの実装に固有の IF-MIB で定義された変数バインドも送信されます。これがデフォルト設定です。
- IEFT Cisco：インターフェイスに対して ifLinkUpDownTrapEnable（IF-MIB で定義）がイネーブルになっている場合、そのインターフェイスについて IF-MIB で定義された通知（LinkUp、LinkDown）および CISCO-IF-EXTENSION-MIB.my で定義された通知

（cieLinkUp、cieLinkDown）のみが送信されます。通知定義で定義された変数バインドのみが、linkUp 通知や linkDown 通知とともに送信されます。

- IEFT extended Cisco：インターフェイスに対して ifLinkUpDownTrapEnable（IF-MIB で定義）がイネーブルになっている場合、そのインターフェイスについて IF-MIB で定義された通知（LinkUp、LinkDown）および CISCO-IF-EXTENSION-MIB.my で定義された通知（cieLinkUp、cieLinkDown）のみが送信されます。linkUp と linkDown の通知定義で定義された変数バインドに加え、シスコの実装に固有の IF-MIB で定義された変数バインドも LinkUp 通知や LinkDown 通知とともに送信されます。

Note シスコの実装に固有の IF-MIB で定義される変数バインドの詳細については、『*Cisco MDS 9000 Family MIB Quick Reference*』を参照してください。

LinkUp および LinkDown トラップ設定の範囲

インターフェイスに対する LinkUp および LinkDown トラップ設定は、次の範囲に基づいてトラップを生成します。

スイッチレベルのトラップ設定	インターフェイスレベルのトラップ設定	インターフェイス リンクについて生成されるトラップか?
有効（デフォルト）	有効（デフォルト）	はい
有効	無効	×
無効	有効	いいえ
無効	無効	×

デフォルト設定

Table 34: SNMP のデフォルト設定 , on page 256 に、すべてのスイッチの SNMP 機能のデフォルト設定を示します。

***Table 34: SNMP* のデフォルト設定**

パラメータ	デフォルト
ユーザー アカウント	有効期限なし（設定されていない場合）
パスワード	なし

SNMP の設定

SNMPは、ネットワーク デバイス間での管理情報の交換を容易にするアプリケーション層プロトコルです。

SNMP スイッチの連絡先および場所の情報の割り当て

スイッチの連絡先情報（スペースを含めず、最大 32 文字まで）およびスイッチの場所を割り当てることができます。

連絡先および場所の情報を設定するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **snmp-server contact NewUser**

スイッチの担当者名を割り当てます。

ステップ 3 switch(config)# **no snmp-server contact NewUser**

スイッチの担当者名を削除します。

ステップ 4 switch(config)# **snmp-server location SanJose**

スイッチのロケーションを割り当てます。

ステップ 5 switch(config)# **no snmp-server location SanJose**

スイッチのロケーションを削除します。

CLI から SNMP ユーザの構成

snmp-server userコマンドで指定したパスフレーズと、**username** コマンドが同期します。

Note パスフレーズまたはパスワードが **localizedkey** または暗号化フォーマットで指定されている場合、パスワードは同期されません。あるデバイスに別のデバイスで生成した構成ファイルをコピーした場合、パスワードが正しく設定されない可能性があります。構成ファイルをデバイスにコピーした場合は、望ましいパスワードを明示的に構成してください。

CLI から SNMP ユーザを作成または変更するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **snmp-server user joe network-admin auth sha abcd1234**

HMAC-SHA-96 認証パスワード（abcd1234）を使用して、ネットワーク管理者ロールのユーザ（joe）の設定を作成または変更します。

ステップ 3 switch(config)# **snmp-server user sam network-admin auth md5 abcdefgh**

HMAC-MD5-96 認証パスワード（abcdefgh）を使用して、ネットワーク管理者ロールのユーザ（sam）の設定を作成または変更します。

ステップ 4 switch(config)# **snmp-server user Bill network-admin auth sha abcd1234 priv abcdefgh**

HMAC-SHA-96 認証レベルを使用して、network-admin ロールのユーザ（Bill）の設定を作成または変更します。AES-128 は、Cisco MDS NX-OS リリース 8.5(1) のプライバシー暗号化パラメータとして使用されます。Cisco MDS NX-OS リリース 8.5(1) より前は、DES がプライバシープロトコルとして使用されていました。

ステップ 5 switch(config)# **no snmp-server user usernameA**

ユーザ（usernameA）および関連するすべてのパラメータを削除します。

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

vsan-admin ロールから指定のユーザー（usam）を削除します。

ステップ 7 switch(config)# **snmp-server user user1 network-admin auth md5 0xab0211gh priv 0x45abf342 localizedkey**

ローカライズされたキー フォーマット（RFC 2574）でパスワードを指定します。ローカライズされたキーは、16 進数フォーマット（0xacbdef など）で提供されます。

ステップ 8 switch(config)# **snmp-server user user2 auth md5 asdgfsadf priv aes-128 asgfsgkhkj**

MD5 認証プロトコルと AES-128 プライバシー プロトコルを使用して user2 を構成します。このコマンドは、Cisco NX-OS リリース 8.5(1) より前のリリースではサポートされています。AES-128 は、Cisco MDS NX-OS リリース 8.5(1) 以降、デフォルトのプライバシー オプションです。

ステップ 9 switch(config)# **snmp-server user joe sangroup**

指定したユーザ（joe）を sangroup ロールに追加します。

ステップ 10 switch(config)# **snmp-server user joe techdocs**

指定したユーザ（joe）を techdocs ロールに追加します。

パスワードの作成または変更

CLI から SNMP ユーザのパスワードを作成または変更するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **snmp-server user user1 role1 auth md5 0xab0211gh priv 0x45abf342 localizedkey**

セキュリティ暗号化に DES オプションを使用して、ローカライズされたキー フォーマットでパスワードを指定します。

ステップ 3 switch(config)# **snmp-server user user1 role2 auth sha 0xab0211gh priv aes-128 0x45abf342 localizedkey**

セキュリティ暗号化に 128 ビット AES オプションを使用して、ローカライズされたキーフォーマットでパスワードを指定します

Note
このコマンドは、Cisco NX-OS リリース 8.5(1) より前のリリースではサポートされています。AES-128 は、Cisco MDS NX-OS リリース 8.5(1) 以降、デフォルトのプライバシー オプションです。

snmp-server user コマンドは、追加のパラメータとして engineID を受け取ります。engineID により、Notification（通告）対象ユーザが作成されます（通知ターゲット ユーザの設定 , on page 269 を参照）。engineID が指定されていない場合、ローカル ユーザが作成されます。

SNMPv3 メッセージ暗号化の適用

デフォルトでは、SNMP エージェントは、auth キーと priv キーを使用したユーザ設定の SNMPv3 メッセージ暗号化を使用する。SNMPv3 メッセージの authNoPriv および authPriv の securityLevel パラメータを許可します。

ユーザのメッセージ暗号化を適用するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **snmp-server user testUser enforcePriv**

このユーザに対して SNMPv3 メッセージのメッセージ暗号化を適用します。

Note
auth および priv の両方のキーが構成された既存のユーザに対してだけ、このコマンドを使用できます。ユーザがプライバシーを適用するように構成されている場合、noAuthNoPriv または authNoPriv の securityLevel パラメータを使用している SNMPv3 PDU 要求に対して、SNMP エージェントは authorizationError で応答します。

ステップ 3 switch(config)# **no snmp-server user testUser enforcePriv**

SNMPv3 メッセージ暗号化の適用を無効にします。

SNMPv3 メッセージ暗号化のグローバルでの適用

または、次のコマンドを使用して、SNMPv3 メッセージ暗号化をすべてのユーザに対してグローバルに適用することもできます。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **snmp-server globalEnforcePriv**

スイッチのすべてのユーザに SNMPv3 メッセージの暗号化を適用します。

ステップ 3 switch(config)# **no snmp-server globalEnforcePriv**

グローバル SNMPv3 メッセージ暗号化の適用を無効にします。

SNMPv3 ユーザに対する複数のロールの割り当て

SNMP サーバのユーザ設定が強化され、SNMPv3 ユーザに複数のロール（グループ）を割り当てることが可能になっています。最初に SNMPv3 ユーザを作成した後で、そのユーザにロールを追加できます。

Note 他のユーザにロールを割り当てることができるのは、network-admin ロールに属するユーザだけです。

CLI から SNMPv3 ユーザに複数のロールを構成するには、次の手順に従います。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **snmp-server user NewUser role1**

role1 ロールの SNMPv3 ユーザ（NewUser）の設定を作成または変更します。

ステップ 3 switch(config)# **snmp-server user NewUser role2**

role2 ロールの SNMPv3 ユーザ（NewUser）の設定を作成または変更します。

ステップ 4 switch(config)# **no snmp-server user User5 role2**

指定されたユーザー (User5) の role2 を削除します。

コミュニティの追加

SNMPv1 および SNMPv2 のユーザの場合は、読み取り専用または読み取り/書き込みアクセスを設定できます。RFC 2576 を参照してください。

SNMPv1 または SNMPv2c のコミュニティを作成するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **snmp-server community snmp_Community ro**

指定された SNMP コミュニティに読み取り専用アクセスを追加します。

ステップ 3 switch(config)# **snmp-server community snmp_Community rw**

指定された SNMP コミュニティの読み取り/書き込みアクセスを追加します。

ステップ 4 switch(config)# **no snmp-server community snmp_Community**

指定された SNMP コミュニティのアクセスを削除します（デフォルト）。

SNMP トラップとインフォーム通知の設定

特定のイベントが発生したときにSNMPマネージャに通知を送信するようにCisco MDSスイッチを設定できます。

Note スイッチは、イベント（SNMP トラップおよびインフォーム）を、最大 10 件の宛先に転送できます。SNMP 用に 11 番目のターゲット ホストを構成しようとすると、次のメッセージが表示されます。

```
switch(config)# snmp-server host 10.4.200.173 traps version 2c noauth
reached maximum allowed targets limit
```

- SNMP 設定で RMON トラップをイネーブルにする必要があります。詳細については、RMON の設定, on page 203 を参照してください。
- 通知をトラップまたはインフォームとして送信する宛先の詳細情報を入手するには、SNMP-TARGET-MIB を使用します。詳細については、『Cisco MDS 9000 Family MIB Quick Reference』を参照してください。

Tip SNMPv1 オプションは、**snmp-server host** *ip-address* **informs** コマンドでは使用できません。

Note 0. または 127. で始まる DSN サーバー名を使用した SNMP ホスト名はサポートされていません。

SNMPv2c 通知の設定

IPv4 を使用した SNMPv2c 通知の構成

IPv4 を使用して SNMPv2c 通知を構成するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **snmp-server host 171.71.187.101 traps version 2c private udp-port 1163**

SNMPv2c コミュニティ文字列（プライベート）を使用して SNMPv2c トラップを受信するように指定されたホストを構成します。

ステップ 3 switch(config)# **no snmp-server host 171.71.187.101 traps version 2c private udp-port 2162**

指定されたホストが SNMPv2c コミュニティ文字列（プライベート）を使用して、構成された UDP ポートで SNMPv2c トラップを受信しないようにします。

ステップ 4 switch(config)# **snmp-server host 171.71.187.101 informs version 2c private udp-port 1163**

SNMPv2c コミュニティ文字列（プライベート）を使用して SNMPv2c インフォームを受信するように指定されたホストを構成します。

ステップ 5 switch(config)# **no snmp-server host 171.71.187.101 informs version 2c private udp-port 2162**

指定されたホストが SNMPv2c コミュニティ文字列（プライベート）を使用して、構成された UDP ポートで SNMPv2c インフォームを受信しないようにします。

IPv6 を使用した SNMPv2c 通知の構成

IPv6 を使用して SNMPv2c 通知を構成するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **snmp-server host 2001:0DB8:800:200C::417A traps version 2c private udp-port 1163**

SNMPv2c コミュニティ文字列（プライベート）を使用して SNMPv2c トラップを受信するように指定されたホストを構成します。

ステップ 3 switch(config)# **no snmp-server host 2001:0DB8:800:200C::417A traps version 2c private udp-port 2162**

指定されたホストが SNMPv2c コミュニティ文字列（プライベート）を使用して、構成された UDP ポートで SNMPv2c トラップを受信しないようにします。

ステップ 4 switch(config)# **snmp-server host 2001:0DB8:800:200C::417A informs version 2c private udp-port 1163**

SNMPv2c コミュニティ文字列（プライベート）を使用して SNMPv2c インフォームを受信するように指定されたホストを構成します。

ステップ 5 switch(config)# **no snmp-server host 2001:0DB8:800:200C::417A informs version 2c private udp-port 2162**

指定されたホストが SNMPv2c コミュニティ文字列（プライベート）を使用して、構成された UDP ポートで SNMPv2c インフォームを受信しないようにします。

DNS ネームを使用した SNMPv2c 通知の構成

SNMP 通知ホスト myhost.cisco.com の DNS 名を使用して SNMPv2c 通知を構成するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **snmp-server host myhost.cisco.com traps version 2c private udp-port 1163**

SNMPv2c コミュニティ文字列（プライベート）を使用して SNMPv2c トラップを受信するように指定されたホストを構成します。

ステップ 3 switch(config)# **no snmp-server host myhost.cisco.com traps version 2c private udp-port 2162**

指定されたホストが SNMPv2c コミュニティ文字列（プライベート）を使用して、構成された UDP ポートで SNMPv2c トラップを受信しないようにします。

ステップ 4 switch(config)# **snmp-server host myhost.cisco.com informs version 2c private udp-port 1163**

SNMPv2c コミュニティ文字列（プライベート）を使用して SNMPv2c インフォームを受信するように指定されたホストを構成します。

ステップ 5 switch(config)# **no snmp-server host myhost.cisco.com informs version 2c private udp-port 2162**

指定されたホストが SNMPv2c コミュニティ文字列（プライベート）を使用して、構成された UDP ポートで SNMPv2c インフォームを受信しないようにします。

Note
スイッチは、イベント（SNMP トラップおよびインフォーム）を、最大 10 件の宛先に転送できます。

SNMPv3 通知の設定

IPv4 を使用した SNMPv3 通知の構成

IPv4 を使用して SNMPv3 通知を構成するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **snmp-server host 16.20.11.14 traps version 3 noauth testuser udp-port 1163**

SNMPv3 ユーザ（testuser）を使用して指定済みホストが SNMPv3 トラップを受信できるように構成し、noAuthNoPriv の securityLevel を構成します。

ステップ 3 switch(config)# **snmp-server host 16.20.11.14 informs version 3 auth testuser udp-port 1163**

SNMPv3 ユーザ（testuser）を使用して指定済みホストが SNMPv3 情報を受信できるように構成し、AuthNoPriv の securityLevel を構成します。

ステップ 4 switch(config)# **snmp-server host 16.20.11.14 informs version 3 priv testuser udp-port 1163**

SNMPv3 ユーザ（testuser）を使用して指定済みホストが SNMPv3 情報を受信できるように構成し、AuthPriv の securityLevel を構成します。

ステップ 5 switch(config)# **no snmp-server host 172.18.2.247 informs version 3 testuser noauth udp-port 2162**

指定済みホストが SNMPv3 情報を受信できないようにします。

IPv6 を使用した SNMPv3 通知の構成

IPv6 を使用して SNMPv3 通知を構成するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **snmp-server host 2001:0DB8:800:200C::417A traps version 3 noauth testuser udp-port 1163**

SNMPv3 ユーザ（testuser）を使用して指定済みホストが SNMPv3 トラップを受信できるように構成し、noAuthNoPriv の securityLevel を構成します。

ステップ 3 switch(config)# **snmp-server host 2001:0DB8:800:200C::417A informs version 3 auth testuser udp-port 1163**

SNMPv3 ユーザ（testuser）を使用して指定済みホストが SNMPv3 情報を受信できるように構成し、AuthNoPriv の securityLevel を構成します。

ステップ 4 switch(config)# **snmp-server host 2001:0DB8:800:200C::417A informs version 3 priv testuser udp-port 1163**

SNMPv3 ユーザ（testuser）を使用して指定済みホストが SNMPv3 情報を受信できるように構成し、AuthPriv の securityLevel を構成します。

ステップ 5 switch(config)# **no snmp-server host 2001:0DB8:800:200C::417A informs version 3 testuser noauth udp-port 2162**

指定済みホストが SNMPv3 情報を受信できないようにします。

DNS ネームを使用した SNMPv3 通知の構成

SNMP 通知ホスト myhost.cisco.com の DNS 名を使用して SNMPv3 通知を構成するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **snmp-server host myhost.cisco.com traps version 3 noauth testuser udp-port 1163**

SNMPv3 ユーザ（testuser）を使用して指定済みホストが SNMPv3 トラップを受信できるように構成し、noAuthNoPriv の securityLevel を構成します。

ステップ 3 switch(config)# **snmp-server host myhost.cisco.com informs version 3 auth testuser udp-port 1163**

SNMPv3 ユーザ（testuser）を使用して指定済みホストが SNMPv3 情報を受信できるように構成し、AuthNoPriv の securityLevel を構成します。

ステップ 4 switch(config)# **snmp-server host myhost.cisco.com informs version 3 priv testuser udp-port 1163**

SNMPv3 ユーザ（testuser）を使用して指定済みホストが SNMPv3 情報を受信できるように構成し、AuthPriv の securityLevel を構成します。

ステップ 5 switch(config)# **no snmp-server host myhost.cisco.com informs version 3 testuser noauth udp-port 2162**

指定済みホストが SNMPv3 情報を受信できないようにします。

場所に基づく SNMPv3 ユーザの認証

場所に基づいて、ローカルまたはリモートの SNMPv3 ユーザを認証できます。

SNMPv3 サーバーの AAA 排他的動作を有効にするには、グローバル構成モードで次のコマンドを使用します。

コマンド	目的
snmp-server aaa exclusive-behavior enable	場所に基づいてユーザを認証するために SNMPv3 サーバーの AAA 排他的動作を有効にします。 ユーザの場所および AAA サーバーが有効かどうかによって、排他的動作は以下のようになります。 • ユーザがローカル ユーザであり、AAA サーバーが有効の場合、ユーザに対するクエリは失敗し、「Unknown user」というメッセージが表示されます。 • ユーザがリモート AAA ユーザであり、AAA サーバーが無効の場合、ユーザに対するクエリは失敗し、「Unknown user」というメッセージが表示されます。 • ユーザがローカル ユーザとリモート ユーザの両方である場合 AAA ユーザと AAA サーバーが有効の場合、リモート ログイン情報を持つクエリは成功し、ローカル ログイン情報を持つクエリは失敗し、「Incorrect password」というメッセージが表示されます。AAA サーバーが無効の場合、ローカル リモート ログイン情報を持つクエリは成功し、リモート ログイン情報を持つクエリは失敗し、「Incorrect password」というメッセージが表示されます。

SNMP 通知のイネーブル化

Table 35: SNMP 通知のイネーブル化 , on page 267 に、Cisco NX-OS MIB の通知を有効化する CLI コマンドを示します。

***Table 35: SNMP* 通知のイネーブル化**

MIB	DCNM-SAN チェックボックス
CISCO-ENTITY-FRU-CONTROL-MIB	**Click the Other tab and check FRU Changes.**
CISCO-FCC-MIB	**Click the Other tab and check FCC.**
CISCO-DM-MIB	**Click the FC tab and check Domain Mgr RCF.**

MIB	DCNM-SAN チェックボックス
CISCO-NS-MIB	**Click the FC tab and check Name Server.**
CISCO-FCS-MIB	**Click the Other tab and check FCS Rejects.**
CISCO-FDMI-MIB	**Click the Other tab and check FDMI.**
CISCO-FSPF-MIB	**Click the FC tab and check FSPF Neighbor Change.**
CISCO-LICENSE-MGR-MIB	**Click the Other tab and check License Manager.**
CISCO-IPSEC-SIGNALLING-MIB	**Click the Other tab and check IPSEC.**
CISCO-PSM-MIB	**Click the Other tab and check Port Security.**
CISCO-RSCN-MIB	**Click the FC tab and check RSCN ILS, and RCSN ELS.**
SNMPv2-MIB	**Click the Other tab and check SNMP AuthFailure.**
VRRP-MIB, CISCO-IETF-VRRP-MIB	**Click the Other tab and check VRRP.**
CISCO-ZS-MIB	**Click the FC tab and check Zone Rejects, Zone Merge Failures, Zone Merge Successes, Zone Default Policy Change, and Zone Unsuppd Mode.**

次の通知はデフォルトでイネーブルになっています。

- entity fru
- ライセンス
- link ietf-extended

他の通知はすべて、デフォルトではディセーブルです。

サポートされているトラップは、次のレベルで有効または無効にできます。

- スイッチ レベル：snmp-server enable traps コマンドを使用して、サポートされている MIB のすべてのトラップをスイッチ レベルで有効にできます。
- 機能レベル：機能名を指定して snmp-server enable traps コマンドを使用すると、機能レベルでトラップを有効にできます。

```
switch =>snmp-server enable traps callhome ?
event-notify    Callhome External Event Notification
smtp-send-fail  SMTP Message Send Fail notification
```

- 個々のトラップ：機能名を指定して snmp-server enable traps コマンドを使用して、個々のレベルでトラップを有効にできます。

```
switch =>snmp-server enable traps callhome event-notify ?
```

Note snmp-server enable traps CLI コマンドを使用すると、SNMP に行った構成に応じて、トラップとインフォームの両方を有効にできます。snmp-server host CLI コマンドによって表示される通知を参照してください。

個々の通知をイネーブルにするには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **snmp-server enable traps fcdomain**

指定された SNMP（fcdomain）通知を有効にします。

ステップ 3 switch(config)# **no snmp-server enable traps**

指定した SNMP 通知を無効にします。通知名を指定しないと、すべての通知が無効になります。

通知ターゲット ユーザの設定

SNMPv3 インフォーム通知を SNMP マネージャに送信するには、スイッチ上で通知対象ユーザを設定する必要があります。

SNMP マネージャは、受信した INFORM PDU を認証および復号化するために、同じユーザ資格情報をユーザのローカル設定データ ストアに持っている必要があります。

通知ターゲット ユーザを構成するには次のコマンドを使用します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **snmp-server user testusr auth md5 xyub20gh priv xyub20gh engineID 00:00:00:63:00:01:00:a1:ac:15:10:03**

指定されたエンジン ID を持つ SNMP マネージャの指定されたログイン情報を使用して、通知ターゲット ユーザを構成します。

ステップ 3 switch(config)# **no snmp-server user testusr auth md5 xyub20gh priv xyub20gh engineID 00:00:00:63:00:01:00:a1:ac:15:10:03**

通知ターゲット ユーザを削除します。

通知ターゲットユーザのログイン情報は、構成した SNMPmanager へ送る SNMPv3 インフォーム通知メッセージの暗号化に使用されます（**snmp-server host** コマンドに表記されているとおり）。

スイッチの LinkUp/LinkDown 通知の構成

NX-OS リリース 4.2(1) 以降を使用してスイッチの LinkUp/LinkDown 通知を構成するには、次の手順に従います。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **snmp-server enable traps link extended-link**

IETF 拡張 linkUp 通知のみを有効にします。

ステップ 3 switch(config)# **snmp-server enable traps link extended-linkDown**

IETF 拡張 linkDown 通知のみを有効にします。

ステップ 4 switch(config)# **snmp-server enable traps link cieLinkDown**

シスコ拡張リンク ステート ダウン通知を有効にします。

ステップ 5 switch(config)# **snmp-server enable traps link cieLinkUp**

シスコ拡張リンク ステート アップ通知を有効にします。

ステップ 6 switch(config)# **snmp-server enable traps link connUnitPortStatusChange**

FCMGMT を有効にします。接続ユニットの全体的なステータス 通知。

ステップ 7 switch(config)# **snmp-server enable traps link delayed-link-state-change**

遅延リンク ステートの変更を有効にします。

遅延リンク ステート トラップを無効にして、デバイスがポート ダウン SNMP アラートをすぐに生成できるようにします。

- NX-OS バージョン 6.2(5) 以前で、**no system delayed-traps enable mode FX** コマンドを使用します。

- NX-OS バージョン 6.2(7) 以降で、**no snmp-server enable traps link delayed-link-state-change** コマンドを使用します。

Note
特定の NX-OS リリース バージョン間のアップグレードについては、遅延リンク ステート トラップが無効になっていることを確認してください。5.(x)、6.1(x)、6.2(x) などの以前のリリースから 6.2(7) 以降のリリースに移行する場合は、**no snmp-server enable traps link delayed-link-state-change** コマンドを使用して遅延リンク ステート トラップを明示的に無効にしてください。

ステップ 8 switch(config)# **snmp-server enable traps link extended-linkDown**

IETF 拡張リンク ステート ダウン通知を有効にします。

ステップ 9 switch(config)# **snmp-server enable traps link extended-linkUp**

IETF 拡張リンク ステート ダウン通知を有効にします。

ステップ 10 switch(config)# **snmp-server enable traps link fcTrunkIfDownNotify**

FCFE リンク ステート ダウン通知を有効にします。

ステップ 11 switch(config)# **snmp-server enable traps link fcTrunkIfUpNotify**

FCFE リンク ステート アップ通知を有効にします。

ステップ 12 switch(config)# **snmp-server enable traps link fcot-inserted**

FCOT 情報トラップを有効にします。

ステップ 13 switch(config)# **snmp-server enable traps link fcot-removed**

FCOT 情報トラップを有効にします。

ステップ 14 switch(config)# **snmp-server enable traps link linkDown**

IETF リンク ステート ダウン通知を有効にします。

ステップ 15 switch(config)# **snmp-server enable traps link linkUp**

IETF リンク ステート アップ通知を有効にします。

ステップ 16 switch(config)# **no snmp-server enable traps link**

デフォルト設定に戻します（IETF 拡張済み）。

インターフェイスの Up/Down SNMP リンクステート トラップの設定

デフォルトでは、SNMP リンクステート トラップがすべてのインターフェイスに対してイネーブルになっています。リンクの状態が Up と Down の間で切り替わるたびに、SNMP トラップが生成されます。

何百ものインターフェイスを装備したスイッチが多数存在し、それらの多くでリンクの状態をモニタする必要がない場合があります。そのような場合には、リンクステート トラップをディセーブルにすることも選択できます。

特定のインターフェイスに対してSNMP リンクステートを無効にするには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **interface fc** *slot/port*

SNMP リンクステート トラップを無効にするインターフェイスを指定します。

ステップ 3 switch(config-if)# **no link-state-trap**

インターフェイスの SNMP リンクステート トラップをディセーブルにします。

ステップ 4 switch(config-if)# **link-state-trap**

インターフェイスの SNMP リンクステート トラップを有効にします。

エンティティ（FRU）トラップの構成

個々の SNMP トラップ制御を有効にするには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 **switch(config)# snmp-server enable traps entity**

個別の SNMP トラップ制御を有効にします。

ステップ 3 **switch(config)# snmp-server enable entity_fan_status_change**

エンティティ ファン ステータスの変更を有効にします。

ステップ 4 **switch(config)# snmp-server enable entity_mib_change**

エンティティ MIB の変更を有効にします。

ステップ 5 **switch(config)# snmp-server enable entity_module_inserted**

エンティティ モジュールを挿入できるようにします。

ステップ 6 **switch(config)# snmp-server enable entity_module_removed**

エンティティ モジュールを削除できるようにします。

ステップ 7 **switch(config)# snmp-server enable entity_module_status_change**

エンティティ モジュールのステータス変更を有効にします。

ステップ 8 **switch(config)# snmp-server enable entity_power_out_change**

エンティティの電源切断の変更を有効にします。

ステップ 9 **switch(config)# snmp-server enable entity_power_status_change**

エンティティの電源ステータスの変更を有効にします。

ステップ 10 **switch(config)# snmp-server enable entity_unrecognised_module**

エンティティが認識されないモジュールを有効にします。

Note
これらのトラップはすべて、従来の FRU トラップに関係しています。

AAA 同期時間の変更

同期したユーザ設定を Cisco NX-OS に維持させる時間の長さを変更できます。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		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 2	**snmp-server aaa-user cache-timeout** *seconds* 例： `switch(config)# snmp-server aaa-user cache-timeout 1200`	ローカル キャッシュで AAA 同期ユーザ設定を維持する時間を設定します。値の範囲は 1 ～ 86400 秒です。デフォルトは 60000 です。
ステップ 3	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

SNMP の設定の確認

SNMP のコンフィギュレーション情報を表示するには、次の作業のいずれかを行います。

コマンド	目的
show running-config	実行構成を表示します。 **Note** Cisco MDS NX-OS リリース 8.5(1) 以降、構成されたプライバシー プロトコル AES-128 または DES を持つ SNMP ユーザが実行構成に表示されます。これは、実行構成で AES-128 ユーザだけが **aes-128** オプションとして表示されていた Cisco MDS NX-OS リリース 8.5(1) より前のリリースとは異なります。Cisco MDS NX-OS リリース 8.5(1) 以降、ユーザはデフォルトで AES-128 プロトコルで構成されます。
show interface	特定のインターフェイスの SNMP リンク ステート トラップ構成を表示します。
show snmp trap	すべての通知とそのステータスを表示します
show snmp	構成された SNMP 情報、SNMP 連絡先のカウンタ情報、場所、およびパケット設定を表示します。

これらのコマンドの出力に表示される各フィールドの詳細については、『*Cisco MDS 9000 Family Command Reference*』を参照してください。

インターフェイスの SNMP リンクステート トラップの Up/Down の表示

インターフェイスの SNMP リンクステート トラップを無効にするたびに、コマンドがシステムの実行構成にも追加されます。

実行構成を表示するには、インターフェイスに **show running-config** コマンドを使用します。

```
switch# no link-state-trap
switch# show running-config interface fc2/25

!Command: show running-config interface fc2/25
!Running configuration last done at: Fri Sep 20 11:28:19 2019
!Time: Fri Sep 20 11:28:22 2019

version 8.4(1)

interface fc2/25
  no link-state-trap
  no shutdown
```

特定のインターフェイスの SNMP リンクステート トラップ構成を表示するには、**show interface** コマンドを入力します。

```
switch# show interface fc2/25

fc2/25 is trunking
    Hardware is Fibre Channel, SFP is long wave laser cost reduced
    Port WWN is 20:59:54:7f:ee:ea:c0:00
    Peer port WWN is 20:1d:00:de:fb:b1:7b:80
    Admin port mode is auto, trunk mode is on
    snmp link state traps are enabled
    Port mode is TE
    Port vsan is 1
    Admin Speed is auto max 32 Gbps
    Operating Speed is 32 Gbps
    Rate mode is dedicated
    Port flow-control is ER_RDY
.
.
.
```

SNMP トラップの表示

すべての通知とそのステータスを表示するには、**show snmp trap** コマンドを使用します。

```
switch# show snmp trap
--------------------------------------------------------------------------------
Trap type                                                              Enabled
--------------------------------------------------------------------------------
entity               : entity_mib_change                               Yes
entity               : entity_module_status_change                     Yes
entity               : entity_power_status_change                      Yes
entity               : entity_module_inserted                          Yes
entity               : entity_module_removed                           Yes
entity               : entity_unrecognised_module                      Yes
entity               : entity_fan_status_change                        Yes
entity               : entity_power_out_change                         Yes
link                 : linkDown                                        Yes
link                 : linkUp                                          Yes
link                 : extended-linkDown                               Yes
link                 : extended-linkUp                                 Yes
link                 : cieLinkDown                                     Yes
link                 : cieLinkUp                                       Yes
link                 : connUnitPortStatusChange                        Yes
link                 : fcTrunkIfUpNotify                               Yes
link                 : fcTrunkIfDownNotify                             Yes
link                 : delayed-link-state-change                       Yes
link                 : fcot-inserted                                   Yes
link                 : fcot-removed                                    Yes
callhome             : event-notify                                    No
callhome             : smtp-send-fail                                  No
cfs                  : state-change-notif                              No
cfs                  : merge-failure                                   No
fcdomain             : dmNewPrincipalSwitchNotify                      No
fcdomain             : dmDomainIdNotAssignedNotify                     No
fcdomain             : dmFabricChangeNotify                            No
rf                   : redundancy_framework                            Yes
aaa                  : server-state-change                             No
license              : notify-license-expiry                           Yes
license              : notify-no-license-for-feature                   Yes
```

```
license              : notify-licensefile-missing                 Yes
license              : notify-license-expiry-warning              Yes
scsi                 : scsi-disc-complete                         No
fcns                 : reject-reg-req                             No
fcns                 : local-entry-change                         No
fcns                 : db-full                                    No
fcns                 : remote-entry-change                        No
rscn                 : rscnElsRejectReqNotify                     No
rscn                 : rscnIlsRejectReqNotify                     No
rscn                 : rscnElsRxRejectReqNotify                   No
rscn                 : rscnIlsRxRejectReqNotify                   No
fcs                  : request-reject                             No
fcs                  : discovery-complete                         No
fctrace              : route                                      No
zone                 : request-reject1                            No
zone                 : merge-success                              No
zone                 : merge-failure                              No
zone                 : default-zone-behavior-change               No
zone                 : unsupp-mem                                 No
port-security        : fport-violation                            No
port-security        : eport-violation                            No
port-security        : fabric-binding-violation                   No
vni                  : virtual-interface-created                  No
vni                  : virtual-interface-removed                  No
vsan                 : vsanStatusChange                           No
vsan                 : vsanPortMembershipChange                   No
fspf                 : fspfNbrStateChangeNotify                   No
upgrade              : UpgradeOpNotifyOnCompletion                No
upgrade              : UpgradeJobStatusNotify                     No
feature-control      : FeatureOpStatusChange                      No
vrrp                 : cVrrpNotificationNewMaster                 No
fdmi                 : cfdmiRejectRegNotify                       No
snmp                 : authentication                             No
```

SNMP セキュリティ情報の表示

show snmp コマンドを使用して、構成済みの SNMP 情報を表示します（以下の例を参照）。

SNMPユーザの詳細

次の SNMP ユーザの詳細の例：

```
switch# show snmp user
_____________________________________________________________________
                    SNMP USERS
_____________________________________________________________________
User                            Auth  Priv(enforce) Groups
____                            ____  _____________ ______
admin                           md5   des(no)       network-admin
testusr                         md5   aes-128(no)   role111
                                                    role222
_____________________________________________________________________
 NOTIFICATION TARGET USERS (configured  for sending V3 Inform)
_____________________________________________________________________
User                            Auth  Priv
____                            ____  ____
testtargetusr                   md5   des
(EngineID 0:0:0:63:0:1:0:0:0:15:10:3)
```

SNMPコミュニティ情報

次の例では、SNMP コミュニティ情報を表示します。

```
switch# show snmp community

Community             Group / Access      context
_________             ______________      _______
dcnm_user             network-admin
admin                 network-admin
```

SNMP ホスト情報

次の例は、SNMP ホスト情報を表示します。

```
switch# show snmp host
Host                              Port Version  Level  Type   SecName
____                              ____ _______  ______ ____   _______
171.16.126.34                     2162 v2c      noauth trap   public
171.16.75.106                     2162 v2c      noauth trap   public
...
171.31.58.97                      2162 v2c      auth   trap   public
...
```

show snmp コマンドは、SNMP の連絡先、場所、およびパケット設定のカウンタ情報を表示します。このコマンドは、Cisco MDS 9000 ファミリ DCNM-SAN 全体で使用される情報を提供します（『System Management Configuration Guide、Cisco DCNM for SAN』を参照）。次の例を参照してください。

SNMP 情報

次の例では、SNMP 情報を表示します。

```
switch# show snmp
sys contact:
sys location:
1631 SNMP packets input
        0 Bad SNMP versions
        0 Unknown community name
        0 Illegal operation for community name supplied
        0 Encoding errors
        64294 Number of requested variables
        1 Number of altered variables
        1628 Get-request PDUs
        0 Get-next PDUs
        1 Set-request PDUs
152725 SNMP packets output
        0 Too big errors
        1 No such name errors
        0 Bad values errors
        0 General errors
Community                     Group / Access
---------                     ------
public                         rw
```

```
_____________________________________________________________________
                    SNMP USERS
_____________________________________________________________________
User                            Auth  Priv(enforce) Groups
____                            ____  _____________ ______
admin                           md5   des(no)       network-admin
testusr                         md5   aes-128(no)   role111
                                                    role222
_____________________________________________________________________
 NOTIFICATION TARGET USERS (configured  for sending V3 Inform)
_____________________________________________________________________
User                            Auth  Priv
____                            ____  ____
testtargetusr                   md5   des
(EngineID 0:0:0:63:0:1:0:0:0:15:10:3)
```

SNMP エンジン ID を表示します

次の例では、SNMP エンジン ID を表示します。

```
switch# show snmp engineID
Local SNMP engineID: [Hex] 8000000903000DEC2CF180
                     [Dec] 128:000:000:009:003:000:013:236:044:241:128
```

SNMP セキュリティ グループに関する情報

次の例では、SNMP セキュリティ グループに関する情報を表示します。

```
switch# show snmp group
groupname: network-admin
security model: any
security level: noAuthNoPriv
readview: network-admin-rd
writeview: network-admin-wr
notifyview: network-admin-rd
storage-type: permanent
row status: active
groupname: network-admin
security model: any
security level: authNoPriv
readview: network-admin-rd
writeview: network-admin-wr
notifyview: network-admin-rd
storage-type: permanent
row status: active
groupname: network-operator
security model: any
security level: noAuthNoPriv
readview: network-operator-rd
writeview: network-operator-wr
notifyview: network-operator-rd
storage-type: permanent
row status: active
groupname: network-operator
security model: any
security level: authNoPriv
readview: network-operator-rd
writeview: network-operator-wr
```

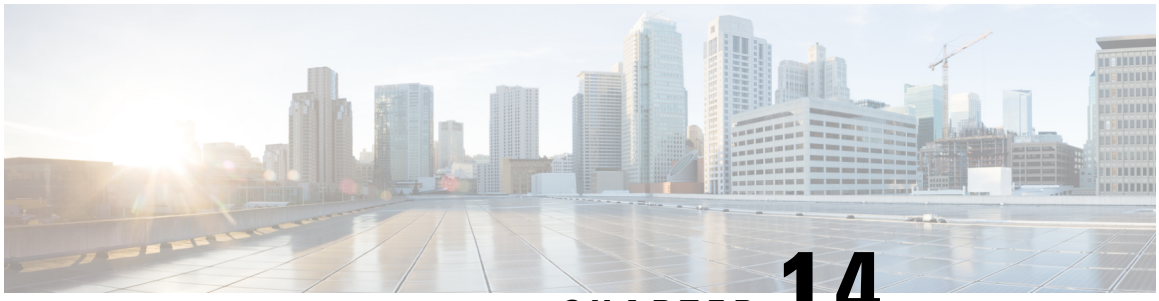
```
notifyview: network-operator-rd
storage-type: permanent
row status: active
```

その他の参考資料

SNMP の実装に関する詳細情報については、次の各項を参照してください。

MIB

MIB	MIB のリンク
• CISCO-SNMP-TARGET-EXT-MIB • CISCO-SNMP-VACM-EXT-MIB	MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 http://www.cisco.com/en/US/products/ps5989/prod_technical_reference_list.html



CHAPTER 14

ドメイン パラメータの構成

ファイバ チャネル ドメイン（fcdomain）機能では、FC-SW-2 標準で記述されているように、主要スイッチ選択、ドメイン ID 配信、FC ID 割り当て、ファブリック再設定機能が実行されます。

- ファイバ チャネル ドメインの概要, on page 281
- 注意事項と制約事項, on page 291
- デフォルト設定, on page 291
- ファイバ チャネル ドメインの設定, on page 292
- ドメイン ID の設定, on page 297
- FC ID の設定, on page 301
- FC ドメイン設定の確認, on page 306

ファイバ チャネル ドメインの概要

ファイバ チャネル ドメイン（fcdomain）機能では、FC-SW-2 標準で記述されているように、主要スイッチ選択、ドメイン ID 配信、FC ID 割り当て、ファブリック再設定機能が実行されます。ドメインは VSAN 単位で設定されます。ドメイン ID を設定しない場合、ローカル スイッチはランダムな ID を使用します。

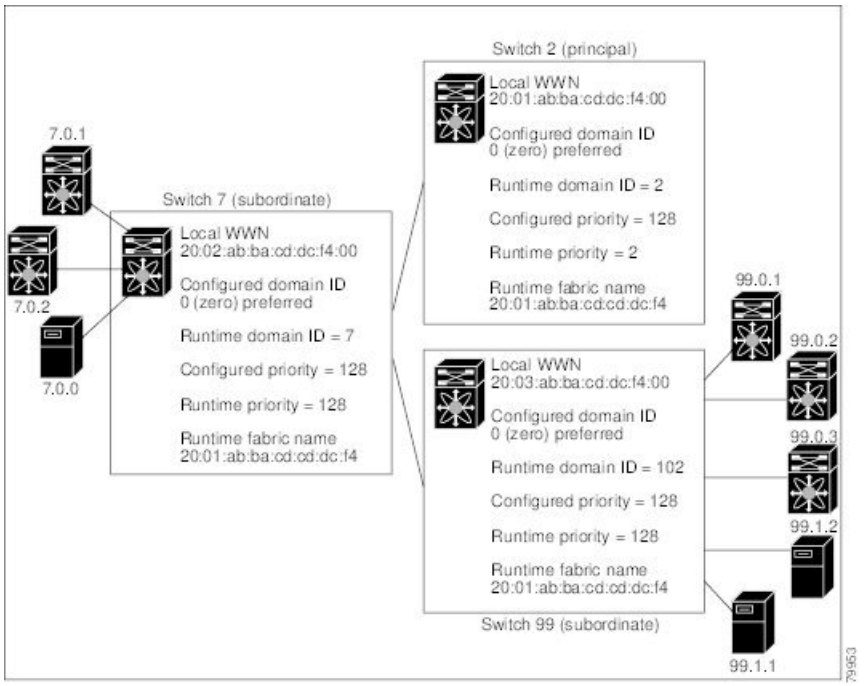
ここでは、fcdomain の各フェーズについて説明します。

- 主要スイッチの選択：このフェーズでは、ファブリック内で一意の主要スイッチを選択できます。
- ドメイン ID の配信：このフェーズでは、ファブリック内のスイッチごとに、一意のドメイン ID を取得できます。
- FC ID の割り当て：このフェーズでは、ファブリック内の対応するスイッチに接続された各デバイスに、一意の FC ID を割り当てることができます。
- ファブリックの再設定：このフェーズでは、ファブリック内のすべてのスイッチを再同期化して、新しい主要スイッチ選択フェーズを同時に再開できるようにします。

Caution fcdomain パラメータは、通常変更しないでください。これらの変更は、管理者が行うか、スイッチ操作を熟知している人が行ってください。

Figure 13: fcdomain の構成例, on page 282 に fcdomain の設定例を示します。

***Figure 13: fcdomain* の構成例**



ドメインの再起動

ファイバ チャネル ドメインは、中断を伴う方法または中断を伴わない方法で起動できます。中断再起動を実行した場合は、Reconfigure Fabric（RCF）フレームがファブリック内のその他のスイッチに送信され、VSAN（リモートでセグメント化された ISL を含む）内のすべてのスイッチでデータ トラフィックは中断されます。非中断再起動を実行した場合は、Build Fabric（BF）フレームがファブリック内のその他のスイッチに送信され、該当スイッチでだけデータ トラフィックは中断されます。

ドメイン ID の競合を解消するには、手動でドメイン ID を割り当てる必要があります。ドメイン ID を手動で割り当てるなど、ほとんどの設定変更では中断再起動が必要になります。ドメインの非中断再起動は、優先ドメイン ID をスタティック ドメイン ID（実ドメイン ID は変更なし）に変更する場合にかぎり実行できます。

Note 中断を伴う再起動に続いて VSAN の一時停止/一時停止なしを使用することは推奨されていません。これは、通常の再起動では問題が解決しない場合のリカバリ目的でのみ使用されるためです。

Note スタティック ドメインはユーザによって固有に設定されるため、実行時のドメインと異なることがあります。ドメイン ID が異なる場合は、次回の中断または非中断再起動後にスタティック ドメイン ID を使用するように、実行時のドメイン ID が変更されます。

Tip VSAN が INTEROP モードである場合は、その VSAN の fcdomain で中断を伴う再起動を実行できません。

ほとんどの設定は、対応する実行時の値に適用できます。ここでは、実行時の値に fcdomain パラメータを適用する方法について詳細に説明します。

fcdomain restart コマンドを使用すると、変更がランタイムの設定に適用されます。**disruptive** オプションを使用すると、優先ドメイン ID を含むほとんどの構成は、対応するランタイムの値に適用できます（ドメイン ID, on page 285を参照）。

ドメイン マネージャのすべての最適化

Domain Manager All Optimization 機能を使用して、すべての最適化モードを有効または無効にすることができます。

Note 相互運用モードが有効になっている（非ネイティブ モード）VSAN では、選択的再起動、高速再起動、スケール再起動などのすべての最適化を有効にすることはできません。また、最適化が有効になっている VSAN を相互運用モード 1 から 4 に移動することはできません。

ドメイン マネージャの高速再起動

Cisco MDS SAN-OS Release 3.0(2) からは、主要リンクに障害が発生したときに、ドメイン マネージャが新しい主要リンクを選択する必要があります。デフォルトでは、ドメイン マネージャは Build Fabric フェーズを開始し、その後主要スイッチ選択フェーズが続きます。これらのフェーズは両方とも VSAN 内のすべてのスイッチに影響を及ぼし、完了するまで合計 15 秒以上かかります。ドメインマネージャが新しい主要リンクの選択に必要な時間を短縮するために、ドメイン マネージャの高速再起動機能をイネーブルにできます。

高速再起動がイネーブルで、バックアップ リンクを利用できる場合、ドメイン マネージャはわずか数ミリ秒で新しい主要リンクを選択し、障害が発生したリンクを交換します。また、新

しい主要リンクの選択に必要な再設定は、VSAN 全体ではなく、障害が発生したリンクに直接接続した 2 つのスイッチにだけ影響します。バックアップ リンクが利用できない場合、ドメイン マネージャはデフォルトの動作に戻り、Build Fabric フェーズを開始します。その後、主要スイッチ選択フェーズが続きます。大部分のファブリックでは、特に多数の論理ポート（3200 以上）を使用する場合、高速再起動を使用することを推奨します。論理ポートは VSAN の物理ポートのインスタンスであるためです。

ドメイン マネージャのスケール再起動

ファブリックの再構成中に、主要なスイッチがドメイン ID をスイッチ（それ自体を含む）に割り当てると、Exchange ファブリック パラメータ（EFP）リクエストを送信します。このリクエストは、基本的にファブリックのドメイン リスト情報を運びます。したがって、ドメイン リストが大きくなるたびに、Exchange ファブリック パラメータがファブリックにフラッディングされます。この機能の最適化を有効にすると、ドメイン識別子の割り当てフェーズが完了すると、単一の統合された Exchange ファブリック パラメータ リクエストが主要スイッチによってフラッディングされます。この機能の最適化は、相互運用モードではサポートされていません。

Scale Restart は、すべてのネイティブ VSAN でデフォルトで有効になります。相互運用 VSAN では有効になりません。

ドメイン マネージャの選択的再起動

ファイバチャネル プロトコルでは、ファブリックの再構成はビルド ファブリック フレーム フラッディングから始まります。これは、ファブリックが変更中であることをファブリック内のすべてのスイッチに示します。このプロセスの後に、主要なスイッチの選択とドメイン ID の割り当てフェーズが続きます。ビルド ファブリック フラッディング フェーズ中に、ビルド ファブリック フレームがすべてのリンクでフラッディングされます。スイッチには、ピア スイッチへのリンクが複数ある場合があります。このような場合、ビルド ファブリック フレームは、ピア スイッチへのリンクの 1 つのみに送信できます。この状況により、ファブリック再構成のビルド ファブリック フェーズ中に交換されるビルド ファブリック フレームの数が減少します。この機能の最適化を有効にすると、ビルド フレームがピア スイッチ リンクの 1 つのみに送信されるため、スケーリングに役立ちます。

スイッチの優先度

新しいスイッチは、安定したファブリックに参加する場合、主要スイッチになることがあります。主要スイッチ選択フェーズ中に、最高のプライオリティを持つスイッチが主要スイッチになります。2 つのスイッチに同じプライオリティが設定されている場合は、WWN が小さいスイッチが主要スイッチになります。

プライオリティ設定は、fcdomain の再起動の実行時に適用されます（ドメインの再起動, on page 282を参照）。この設定は、中断再起動および非中断再起動のどちらにも適用できます。

fcdomain の開始

デフォルトでは、fcdomain 機能は各スイッチ上でイネーブルになっています。スイッチ内で fcdomain 機能をディセーブルにすると、そのスイッチはファブリック内のその他のスイッチと共存できなくなります。fcdomain 設定は中断再起動の実行時に適用されます。

着信 RCF

インターフェイス単位、VSAN 単位で RCF 要求フレームを拒否するように選択できます。RCF 拒否オプションはデフォルトでディセーブルになっています（つまり、RCF 要求フレームは自動的に拒否されません）。

RCF 拒否オプションは、中断を伴う再起動によって、実行時にすぐに有効になります（ドメインの再起動, on page 282を参照）。

rcf-reject オプションはインターフェイス単位、VSAN 単位で設定できます。デフォルトでは、rcf-reject オプションはディセーブルです（つまり、RCF 要求フレームは自動的に拒否されません）。

rcf-reject オプションは即座に有効になります。fcdomain の再起動は不要です。

マージされたファブリックの自動再構成

デフォルトでは、autoreconfigure オプションはディセーブルです。ドメインが重なる別々の安定ファブリックに属する 2 つのスイッチを結合する場合は、次のような状況になる可能性があります。

- 両方のスイッチで autoreconfigure オプションがイネーブルの場合、中断再設定フェーズが開始します。
- いずれかまたは両方のスイッチで autoreconfigure オプションがディセーブルの場合は、2 つのスイッチ間のリンクが隔離されます。
- RCF は、ファブリック全体で自動再構成が有効になっている場合にのみ想定されます。

autoreconfigure オプションは実行時に即座に有効になります。fcdomain を再起動する必要はありません。ドメインが重複によって現在隔離されており、後で両方のスイッチの autoreconfigure オプションをイネーブルにする場合は、ファブリックは隔離状態のままです。ファブリックを接続する前に両方のスイッチで autoreconfigure オプションをイネーブルにした場合、中断再設定（RCF）が発生します。中断再設定が発生すると、データ トラフィックが影響を受けることがあります。fcdomain に非中断再設定を行うには、重複リンク上の設定済みドメインを変更し、ドメインの重複を排除します。

ドメイン ID

ドメイン ID は VSAN 内のスイッチを一意に識別します。スイッチは異なる VSAN に異なるドメイン ID を持つことがあります。ドメイン ID は FC ID 全体の一部です。

設定済みドメイン ID のタイプは優先またはスタティックになります。デフォルトで、設定済みドメイン ID は 0（ゼロ）、設定タイプは優先です。

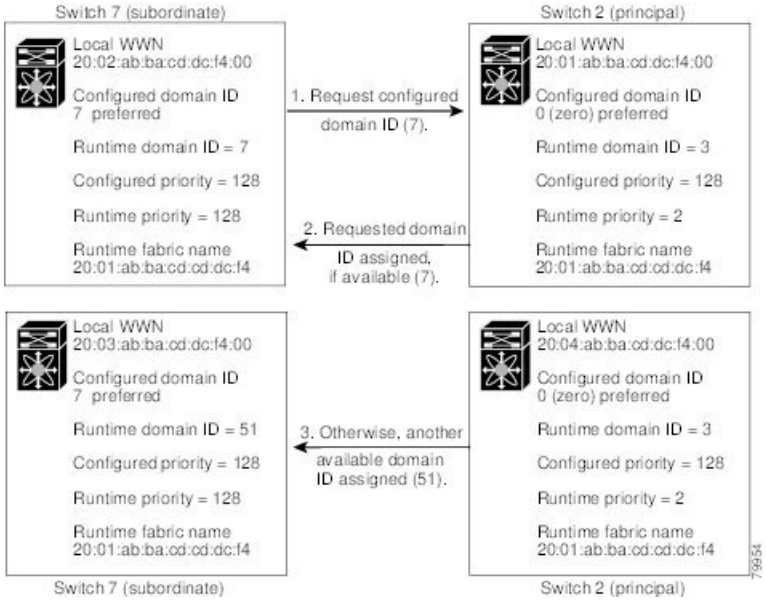
Note 値 0（ゼロ）を設定できるのは、優先オプションを使用した場合だけです。

ドメイン ID を設定しない場合、ローカル スイッチは要求内でランダムな ID を送信します。スタティック ドメイン ID を使用することを推奨します。

下位スイッチがドメインを要求する場合は、次のプロセスが実行されます（Figure 14: 優先オプションを使用した設定プロセス, on page 286を参照）。

1. ローカル スイッチは主要スイッチに設定済みドメイン ID 要求を送信します。
2. 要求されたドメイン ID が使用可能な場合、主要スイッチはこの ID を割り当てます。使用不可能な場合は、使用可能な別のドメイン ID を割り当てます。

Figure 14: 優先オプションを使用した設定プロセス



下位スイッチの動作は、次の要因によって変化します。

- 許可ドメイン ID リスト。
- 設定済みドメイン ID。
- 主要スイッチが要求元スイッチに割り当てたドメイン ID。

状況に応じて、次のように変更されます。

- 受信されたドメイン ID が許可リストに含まれない場合は、要求されたドメイン ID が実行時ドメイン ID になり、該当する VSAN のすべてのインターフェイスが隔離されます。

- 割り当てられたドメイン ID と要求されたドメイン ID が同じである場合は、優先およびスタティック オプションは関係せず、割り当てられたドメイン ID が実行時ドメイン ID になります。
- 割り当てられたドメイン ID と要求されたドメイン ID が異なる場合は、次のようになります。
  - 設定タイプがスタティックの場合は、割り当てられたドメイン ID が廃棄され、すべてのローカル インターフェイスは隔離され、ローカル スイッチには設定済みのドメイン ID が自動的に割り当てられます（この ID が実行時ドメイン ID になります）。
  - 設定タイプが preferred の場合、ローカル スイッチは主要スイッチによって割り当てられたドメイン ID を受け入れ、割り当てられた ID が実行時ドメイン ID になります。

設定済みドメイン ID を変更したときに、変更が受け入れられるのは、新しいドメイン ID が、VSAN 内に現在設定されているすべての許可ドメイン ID リストに含まれている場合だけです。または、ドメイン ID を 0 の優先に設定することもできます。

Tip 特定の VSAN で FICON 機能がイネーブルになっている場合、その VSAN のドメイン ID はスタティックな状態のままになります。スタティック ID 値は変更できますが、優先オプションには変更できません。

Note NAT 構成のない IVR では、IVR トポロジ内の 1 つの VSAN でスタティック ドメイン ID が設定されている場合、トポロジ内の他の VSAN（エッジまたは中継）にもスタティック ドメイン ID を設定する必要があります。IVR NAT 設定で、IVR トポロジ内の 1 つの VSAN に静的ドメイン ID が設定されている場合は、その VSAN にエクスポート可能な IVR ドメインにも静的ドメインを割り当てる必要があります。

Caution 設定済みドメインの変更を実行時ドメインに適用する場合は、fcdomain restart コマンドを入力する必要があります。

Caution 構成したドメインの変更をランタイム ドメインに適用する場合は、**fcdomain** を再起動する必要があります。

Note 許可ドメイン ID リストを設定した場合、追加するドメイン ID は VSAN でその範囲に収まっている必要があります。「許可ドメイン ID リストの構成, on page 299」を参照してください。

static または preferred ドメイン ID の指定

スタティック ドメイン ID タイプを割り当てる場合、特定のドメイン ID を要求します。スイッチは、要求したアドレスを取得できなかった場合、自分自身をファブリックから分離します。優先ドメイン ID を指定した場合も特定のドメイン ID を要求しますが、要求したドメイン ID を取得できない場合スイッチは、別のドメイン ID を受け入れます。

スタティック オプションは、中断再起動または非中断再起動後の実行時に適用できますが、優先オプションは中断再起動後の実行時にだけ適用できます（ドメインの再起動, on page 282を参照）。

許可ドメイン ID リスト

デフォルトでは、割り当て済みのドメイン ID リストの有効範囲は 1 ～ 239 です。許可ドメイン ID リストに複数の範囲を指定し、各範囲をカンマで区切れます。主要スイッチは、ローカルに設定された許可ドメイン リストで使用可能なドメイン ID を割り当てます。

重複しないドメイン ID で VSAN を設計するには、許可ドメイン ID リストを使用します。このリストは将来 NAT 機能を使用しない IVR を実装する必要がある場合に役立ちます。

許可ドメイン ID リストの CFS 配信

Cisco Fabric Service（CFS）インフラストラクチャを使用し、ファブリックのすべての Cisco MDS スイッチに許可ドメイン ID リストの設定情報を配信することをイネーブルにすることができます。この機能により、1 つの MDS スイッチのコンソールからファブリック全体の設定を同期できます。同じ設定が VSAN 全体に配信されるため、発生する可能性がある設定ミスや、同一 VSAN の 2 つのスイッチで互換性がない許可ドメインを設定する可能性を回避できます。

CFS を使用して許可ドメイン ID リストを配信し、VSAN 内のすべてのスイッチで許可ドメイン ID リストの整合性をとるようにします。

Note 許可ドメイン ID リストを設定し、主要スイッチで確定することを推奨します。

CFS の詳細については、CFS インフラストラクチャの使用, on page 7を参照してください。

連続ドメイン ID の割り当て

デフォルトでは、連続ドメイン割り当てはディセーブルです。下位スイッチが複数のドメインを主要スイッチに要求し、ドメインが連続していない場合は、次のような状況になる可能性があります。

- 主要スイッチで連続ドメイン割り当てがイネーブルの場合、主要スイッチは連続ドメインを特定し、それらを下位スイッチに割り当てます。連続ドメインが使用できない場合、NX-OS ソフトウェアはこの要求を却下します。
- 主要スイッチで連続ドメイン割り当てがディセーブルの場合、主要スイッチは使用可能なドメインを下位スイッチに割り当てます。

ファブリックのロック

既存の設定を変更するときの最初のアクションによって、保留中の設定が作成され、ファブリック内の機能がロックされます。ファブリックをロックすると、次の条件が適用されます。

- 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。
- アクティブな設定をコピーすると保留中の設定が作成されます。これ以後の変更は保留設定に対して行われ、アクティブな設定（およびファブリック内の他のスイッチ）に変更をコミットするか、または変更を廃棄するまで、保留設定にとどまります。

変更のコミット

保留されているドメイン設定の変更を VSAN のその他の MDS スイッチに適用するには、変更を確定する必要があります。保留中の設定変更が配信され、正常に確定された時点で、設定変更は VSAN 全体の MDS スイッチでアクティブな設定に適用されて、ファブリックのロックが解除されます。

ファブリックのロックのクリア

ドメイン設定作業を実行し、変更をコミットまたは廃棄してロックを解除していない場合、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。管理者がこのタスクを実行すると、保留中の変更は廃棄され、ファブリック ロックが解除されます。

保留中の変更は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。

FC ID

Cisco MDS 9000 ファミリ スイッチに N または NL ポートがログインする場合、FC ID が割り当てられます。デフォルトでは、固定的FC ID機能はイネーブルです。この機能をディセーブルにした場合、次の結果になります。

- N ポートまたは NL ポートが Cisco MDS 9000 ファミリ スイッチにログインします。要求側の N ポートまたは NL ポートの WWN、および割り当てられた FC ID は保持され、揮発性キャッシュに保存されます。この揮発性キャッシュの内容は、再起動時に保存されません。
- スイッチは、FC ID と WWN のバインディングをベストエフォート方式で保持するように設計されています。たとえば、スイッチから 1 つの N ポートを切断したあとに、別のデバイスから FC ID が要求されると、この要求が許可されて、WWN と初期 FC ID の関連付けが解除されます。
- 揮発性キャッシュには、WWN と FC ID のバインディングのエントリを 4000 まで格納できます。このキャッシュが満杯になると、新しい（より最近の）エントリによって、キャッシュ内の最も古いエントリが上書きされます。この場合、最も古いエントリの対応する WWN と FC ID の関連付けが失われます。
- スイッチ接続動作は、N ポートと NL ポートで異なります。

- N ポートを取り外し、同じスイッチの任意のポートに接続すると、（このポートが同じ VSAN に属するかぎり）この N ポートには同じ FC ID が割り当てられます。
- NL ポートが同じ FC ID になるのは、スイッチ上の以前接続されていたポートと同じポートに再度接続された場合だけです。

永続的 FC ID

固定的 FC ID がイネーブルである場合は、次のようになります。

- fcdomain 内の現在 *in use* の FC ID は、リブートしても保持されます。
- fcdomain は、デバイス（ホストまたはディスク）をポートインターフェイスに接続したあとに学習されたダイナミック エントリを、自動的にデータベースに入力します。

固定的 FC ID 設定

固定的 FC ID 機能をイネーブルにすると、固定的 FC ID サブモードを開始して、FC ID データベースにスタティックまたはダイナミック エントリを追加できるようになります。デフォルトでは、追加されたすべてのエントリはスタティックです。固定的 FC ID は VSAN 単位で設定します。固定的 FC ID を手動で設定するには、次の要件に従ってください。

- 必要な VSAN 内で固定的 FC ID 機能がイネーブルになっていることを確認します。
- 必要な VSAN がアクティブ VSAN であることを確認してください。固定的 FC ID は、アクティブな VSAN に対してだけ設定できます。
- FC ID のドメイン部分が必要な VSAN 内の実行時ドメイン ID と同じであることを確認します。ソフトウェアがドメインの不一致を検出した場合、コマンドは拒否されます。
- エリアを設定するときに、FC ID のポート フィールドが 0（ゼロ）であることを確認します。

Note FICON は、前面パネルのポート番号に基づき、異なる方式を使用して FC ID を割り当てます。この方式は、FICON VSAN における FC ID の固定化よりも優先されます。

HBA の固有エリア FC ID の概要

Note HBA ポートおよびストレージ ポートを同一スイッチに接続している場合に限り、この項を読んでください。

HBA ポートとストレージ ポートを両方とも同一スイッチに接続している場合、一部の HBA ポートにはストレージ ポートとは別のエリア ID が必要となります。たとえば、ストレージ ポート FC ID が 0x6f7704 の場合、このポートのエリアは 77 です。この場合、HBA ポートのエリアには 77 以外の値を構成できます。HBA ポートの FC ID は、ストレージ ポートの FC ID と異なる値に手動で構成する必要があります。

Cisco MDS 9000 ファミリのスイッチでは、FC ID の固定化機能により、この要件への準拠が容易になります。この機能を使用すると、ストレージ ポートまたは HBA ポートに異なるエリアを持つ FC ID を事前に割り当てることができます。

固定的 FC ID の選択消去

固定的 FC ID は、選択的に消去できます。現在使用中のスタティック エントリおよび FC ID は、削除できません。Table 36: 消去される FC ID , on page 291 に、固定的 FC ID の消去時に削除または保持される FC ID エントリを示します。

Table 36: 消去される ***FC ID***

固定的 FC ID の状態	固定的 FC ID の使用状態	アクション
スタティック	利用中	削除されません
スタティック	使用しない	削除されません
ダイナミック	利用中	削除されません
ダイナミック	使用しない	Deleted

注意事項と制約事項

- 設定を変更した場合は、必ず実行コンフィギュレーションを保存してください。次回にスイッチを再起動したときに、保存された設定が使用されます。設定を保存しない場合は、前回保存されたスタートアップ コンフィギュレーションが使用されます。
- すべての手順で使用されるドメイン ID および VSAN 値は、単なる例です。必ずご使用の設定に適用される ID および値を使用してください。

デフォルト設定

Table 37: デフォルトの FC ドメイン パラメータ, on page 291 に、すべての FC ドメイン パラメータのデフォルト設定を示します。

Table 37: デフォルトの ***FC*** ドメイン パラメータ

パラメータ	デフォルト
fcdomain 機能	イネーブル
構成された domain_ID	0（ゼロ）
設定済みドメイン	優先
auto-reconfigure オプション	ディセーブル

パラメータ	デフォルト
contiguous-allocation オプション	ディセーブル
プライオリティ	128
許可リスト	1 ～ 239。
ファブリック名	20:01:00:05:30:00:28:df
rcf-reject	ディセーブル
固定的 FC ID	イネーブル
許可 domain_ID リスト構成の配信	ディセーブル

ファイバ チャネル ドメインの設定

このセクションでは、fcdomain の機能について説明します。

ドメインの再起動

ドメイン構成のシナリオ

スイッチ構成

VSAN 6 のスイッチがどのように構成されているかに関係なく、fcdomain が中断を伴う vsan 6 を再起動すると、VSAN 6 のすべてのスイッチのすべてのデバイスがログアウトし、データトラフィックが中断します。

構成されたドメインとランタイム ドメインが同じである

構成されたドメインとランタイム ドメインがすべてのスイッチで同じであると仮定すると、fcdomain が vsan 6 を再起動しても、VSAN 6 内のデバイスがログアウトすることはありません。

構成されたドメインとランタイム ドメインが同じでない

VSAN 6 の一部のスイッチで、構成されたドメインとランタイム ドメインが同じではないと仮定すると、fcdomain が vsan 6 を再起動すると、静的に構成されたドメインとランタイム ドメインが異なるスイッチに接続されている VSAN 6 のデバイスがログアウトされ、データトラフィックが中断されます。

中断を伴うファブリックの再起動、または中断を伴わない再起動を行うには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **fcdomain restart vsan 1**

ネットワーク全体のデータトラフィックは中断されませんが、構成されたドメインが静的で、数値的にランタイムドメインと同じでない場合は、スイッチ上で中断される可能性があります（たとえば、構成されたドメインが 11 静的で、ランタイム ドメインが 99 である場合）。

ステップ 3 switch(config)# **fcdomain restart disruptive vsan1**

VSAN 内のすべてのスイッチでデータトラフィックを破棄します。

ドメイン マネージャのすべての最適化を有効にする

ドメイン マネージャのすべての最適化機能を有効にするには、次の手順に従ってください。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **fcdomain optimize all vsan 3**

VSAN 3 ですべてのドメイン マネージャの最適化（selective-restart、fast-restart、scale-restart）を有効にします。

ステップ 3 switch(config)# **fcdomain optimize all vsan 7 - 10**

VSAN 7 から VSAN 10 までの VSAN の範囲で、ドメイン マネージャのすべての最適化を有効にします。

ステップ 4 switch(config)# **no fcdomain optimize all vsan 8**

VSAN 8 でドメイン マネージャのすべての最適化を無効にします。

ドメイン マネージャの高速再起動の有効化

Cisco SAN-OS リリース 3.0(2) 以降、または MDS NX-OS リリース 4.1(1a) 以降でドメイン マネージャの高速再起動機能を有効にするには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **fcdomain optimize fast-restart vsan 3**

VSAN 3 でドメイン マネージャの高速再起動を有効にします。

ステップ 3 switch(config)# **fcdomain optimize fast-restart vsan 7 - 10**

VSAN 7 から VSAN 10 までの VSAN の範囲で、ドメイン マネージャの高速再起動を有効にします。

ステップ 4 switch(config)# **no fcdomain optimize fast-restart vsan 8**

VSAN 8 でドメイン マネージャの高速再起動を無効にします（デフォルト）。

ドメイン マネージャのスケール再起動の有効化

ドメイン マネージャのスケール再起動機能を有効にするには、次の手順に従ってください。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **fcdomain optimize scale-restart vsan 3**

VSAN 3 でドメイン マネージャ スケールの再起動を有効にします。

ステップ 3 switch(config)# **fcdomain optimize scale-restart vsan 7 - 10**

VSAN 7 から VSAN 10 までの VSAN の範囲で、ドメイン マネージャ スケールの再起動を有効（デフォルト）にします。

ステップ 4 switch(config)# **no fcdomain optimize scale-restart vsan 8**

VSAN 8 でドメイン マネージャ スケールの再起動を無効にします。

ドメイン マネージャの選択的再起動の有効化

Cisco SAN-OS リリース 3.0(2) 以降、または MDS NX-OS リリース 4.1(1a) 以降でドメイン マネージャの選択的再起動機能を有効にするには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **fcdomain optimize selective-restart vsan 3**

VSAN 3 でドメイン マネージャの選択的再起動を有効にします。

ステップ 3 switch(config)# **fcdomain optimize selective-restart vsan 7 - 10**

VSAN 7 から VSAN 10 までの VSAN の範囲で、ドメイン マネージャの選択的再起動を有効にします。

ステップ 4 switch(config)# **no fcdomain optimize selective-restart vsan 8**

VSAN 8 でドメイン マネージャの選択的再起動を無効にします（デフォルト）。

スイッチ優先順位の構成

Note デフォルトでは、プライオリティは 128 に設定されます。プライオリティの有効設定範囲は 1 ～ 254 です。プライオリティ 1 が最高のプライオリティです。値 255 は、他のスイッチからは受け入れられますが、ローカルには設定できません。

主要スイッチのプライオリティを設定するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **fcdomain priority 25 VSAN 99**

VSAN 99 のローカル スイッチの優先順位を 25 に構成します。

ステップ 3 switch(config)# **no fcdomain priority 25 VSAN 99**

VSAN 99 の優先順位を出荷時のデフォルト（128）に戻します。

ファブリック名の構成

ディセーブルになっている fcdomain のファブリック名の値を設定するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **fcdomain fabric-name 20:1:ac:16:5e:0:21:01 vsan 3**

VSAN に構成済みファブリック名の値を割り当てます。

ステップ 3 switch(config)# **no fcdomain fabric-name 20:1:ac:16:5e:0:21:01 vsan 3010**

VSAN 3010 のファブリック名の値を出荷時のデフォルト設定（20:01:00:05:30:00:28:df）に変更します。

着信 RCF の拒否

着信 RCF 要求フレームを拒否するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **interface fc1/1**

switch(config-if)#

指定されたインターフェイスを設定します。

ステップ 3 switch(config-if)# **fcdomain rcf-reject vsan 1**

VSAN 1 内の指定されたインターフェイス上で RCF フィルタを有効にします。

ステップ 4 switch(config-if)# **no fcdomain rcf-reject vsan 1**

VSAN 1 内の指定されたインターフェイス上で RCF フィルタを無効（デフォルト）にします。

自動再構成の有効化

特定の VSAN（または VSAN 範囲）で自動再構成をイネーブルにするには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **fcdomain auto-reconfigure vsan 10**

VSAN 10 で自動再構成オプションを有効にします。

ステップ 3 switch(config)# **no fcdomain auto-reconfigure 69**

VSAN 69 で自動再構成オプションを無効にし、出荷時のデフォルト設定に戻します。

ドメイン ID の設定

ドメイン ID は VSAN 内のスイッチを一意に識別します。スイッチは異なる VSAN に異なるドメイン ID を持つことがあります。ドメイン ID は FC ID 全体の一部です。

設定済みドメイン ID のタイプは優先またはスタティックになります。デフォルトで、設定済みドメイン ID は 0（ゼロ）、設定タイプは優先です。

static または preferred ドメイン ID の指定

Note 1 つの VSAN 内のスイッチは、すべて同じドメイン ID タイプ（スタティックまたは優先）を持っている必要があります。あるスイッチがスタティック ドメイン タイプで、別のスイッチが優先ドメインタイプであるというように、設定が混在している場合は、リンクが分離されることがあります。

新しいドメイン ID が構成されている場合、fcdomain restart コマンドを使用してドメインを手動で再起動することにより、新しい構成を適用する必要があります。以降のファブリック マージ中に、構成されたドメイン ID とランタイム ドメイン ID の間に不一致が検出された場合、リンクは分離されます。

スタティックまたは優先のドメイン ID を指定するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **fcdomain domain 3 preferred vsan 8**

preferred ドメイン ID 3 を要求するために VSAN 8 内のスイッチを構成し、主要スイッチによって割り当てられた値をすべて受け入れます。ドメインの範囲は 1 ～ 239 です。

ステップ 3 switch(config)# **no fcdomain domain 3 preferred vsan 8**

VSAN 8 内の構成済みドメイン ID を 0（デフォルト）にリセットします。設定済みドメイン ID は 0 preferred になります。

ステップ 4 switch(config)# **fcdomain domain 2 static vsan 237**

特定の値だけを受け入れるように VSAN 237 内のスイッチを設定し、要求されたドメイン ID が許可されない場合は、VSAN 237 内のローカル インターフェイスを隔離ステートに移行します。

ステップ 5 switch(config)# **no fcdomain domain 18 static vsan 237**

構成済みドメイン ID を、VSAN 237 内の出荷時のデフォルト構成にリセットします。設定済みドメイン ID は 0 preferred になります。

許可ドメイン ID リストの構成

ファブリック内の 1 つのスイッチに許可リストを設定する場合は、整合性を保つために、ファブリック内のその他のすべてのスイッチに同じリストを設定するか、CFS を使用して設定を配信することを推奨します。

許可ドメイン ID リストを構成するには、次の手順を実行します。

始める前に

許可ドメイン ID リストは、次の条件を満たす必要があります。

- スイッチが主要スイッチである場合は、現在割り当てられているすべてのドメイン ID が許可リストに含まれている必要があります。
- このスイッチが下位スイッチである場合は、ローカル実行時ドメイン ID が許可リストに含まれている必要があります。
- ローカルに設定されたスイッチのドメイン ID が許可リスト内に含まれている必要があります。
- 割り当てられたドメイン ID の一部が、その他の設定済みドメイン ID のリストのいずれかに含まれている必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	構成モードに入ります。
ステップ 2	switch# **fcdomain allowed 50-110 vsan 4**	VSAN 4 で ドメイン ID 50 ～ 110 のスイッチを許可するようにリストを構成します。 switch# **no fcdomain allowed 50-110 vsan 4** VSAN 5 でドメイン ID 1 ～ 239 のスイッチを許可する出荷時のデフォルト設定に戻します。

許可ドメイン ID 配信のイネーブル化

許可ドメイン ID リストの CFS 配信はデフォルトではディセーブルになっています。許可ドメイン ID リストを配信するすべてのスイッチで配信をイネーブルにする必要があります。

許可ドメイン ID リスト設定の配信をイネーブル（またはディセーブル）にするには、次の手順を実行します。

Before you begin

CFS を使用して許可ドメイン ID リストを配信するには、ファブリック内のすべてのスイッチは Cisco SAN-OS Release 3.0(1) 以降を実行している必要があります。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

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

ドメイン設定の配信をイネーブルにします。

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

ドメイン設定の配信をディセーブル（デフォルト）にします。

変更のコミット

保留中のドメイン設定変更をコミットし、ロックを解除するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **fcdomain commit vsan 10**

保留中のドメイン設定変更をコミットします。

変更の破棄

いつでもドメイン設定への保留変更を廃棄して、ファブリックのロックを解除できます。保留中の変更を廃棄（終了）する場合、構成には影響せずに、ロックが解除されます。

保留中のドメイン設定変更を廃棄し、ロックを解除するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **fcdomain abort vsan 10**

保留中のドメイン設定変更を廃棄します。

連続ドメイン ID 割り当ての有効化

特定のVSAN（またはVSAN範囲）で連続ドメインをイネーブルにするには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **fcdomain contiguous-allocation vsan 81-83**

VSAN 81 から 83 で連続割り当てオプションを有効にします。

Note
contiguous-allocation オプションは実行時に即座に有効になります。fcdomain を再起動する必要はありません。

ステップ 3 switch(config)# **no fcdomain contiguous-allocation vsan 1030**

VSAN 1030 で連続割り当てオプションを無効にし、出荷時のデフォルト設定に戻します。

FC ID の設定

Cisco MDS 9000 ファミリ スイッチに N または NL ポートがログインする場合、FC ID が割り当てられます。

永続的 FC ID 機能の有効化

AIX または HP-UX ホストからスイッチに接続する場合は、それらのホストに接続する VSAN で固定的 FC ID 機能をイネーブルにする必要があります。

F ポートに割り当てられた固定的 FC ID は、インターフェイス間を移動させることができ、同じ固定的 FC ID をそのまま維持することができます。

Note

- FC ID はデフォルトでイネーブルになっています。このデフォルト動作は、Cisco MDS SAN-OS Release 2.0(1b) よりも前のリリースから変更されており、リブートした後で FC ID が変更されなくなります。このオプションは、VSAN ごとにディセーブルにできます。
- ループ接続デバイス（FL ポート）を使用した固定的 FC ID は、構成されたポートと同じポートに接続され続ける必要があります。
- デバイス上の Arbitrated Loop Physical Address（ALPA）のサポートの違いにより、ループ接続デバイスの FC ID の固定化は保証されません。
- Cisco MDS 9124、9134、9148、9148S、および 9250i スイッチの場合、インターフェイスごとに完全な FCID エリアを割り当て、これらのプラットフォームでは FCID（port_id）の右側の最後のバイトが常にゼロであることを確認してください（NPV スイッチに接続された NPIV モードで動作する MDS 9148 を除きます）。したがって、ゼロ以外の port_id で静的 FCID を構成することはできません。たとえば、以下は MDS 9124、9134、9148、9148S、および 9250i では機能しません。

  vsan 1000 **wwn** 33:e8:00:05:30:00:16:df **fcid** 0x070128

  次のように変更する必要があります。**vsan** 1000 **wwn** 33:e8:00:05:30:00:16:df **fcid** 0x070100

固定的 FC ID 機能をイネーブルにするには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **fcdomain fcid persistent vsan** *1000*

```
FCID(s) persistent feature is enabled.
```

VSAN 1000 の FC ID 永続性をアクティブ（デフォルト）にします。

ステップ 3 switch(config)# **no fcdomain fcid persistent vsan** *20*

VSAN 20 の FC ID 永続性機能を無効化します。

永続的 FC ID の構成

固定的 FC ID を設定するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **fcdomain fcid database**

switch(config-fcid-db)#

FC ID 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-fcid-db)# **vsan 1000 wwn 33:e8:00:05:30:00:16:df fcid 0x070128**

VSAN 1000 のデバイス WWN（33:e8:00:05:30:00:16:df）に FC ID 0x070128 を構成します。

Note
重複 FC ID の割り当てを回避するには、**show fcdomain address-allocation vsan** コマンドを使用して、使用中の FC ID を表示します。

ステップ 4 switch(config-fcid-db)# **vsan 1000 wwn 11:22:11:22:33:44:33:44 fcid 0x070123 dynamic**

ダイナミック モードで、VSAN 1000 のデバイス WWN（11:22:11:22:33:44:33:44）に FC ID 0x070123 を構成します。

ステップ 5 switch(config-fcid-db)# **vsan 1000 wwn 11:22:11:22:33:44:33:44 fcid 0x070100 area**

VSAN 1000 のデバイス WWN（11:22:11:22:33:44:33:44）に FC ID 0x070100 ～ 0x701FF を構成します。

Note
この fcdomain のエリア全体を保護するには、FC ID の末尾 2 文字に 00 を割り当てます。

HBA に対する一意のエリア FC ID の設定

HBA ポートに別のエリア ID を設定するには、次の手順を実行します。

Note この例の手順では、スイッチ ドメイン 111（16 進法では 6f）を使用しています。HBA ポートはインターフェイス fc1/9 に、ストレージ ポートは同じスイッチのインターフェイス 1/10 に接続します。

Procedure

ステップ 1 **show flogi database** コマンドを使用して、HBA のポート WWN（Port Name フィールド）ID を取得します。

```
switch# show flogi database
--------------------------------------------------------------------------------
INTERFACE   VSAN    FCID        PORT NAME                 NODE NAME
--------------------------------------------------------------------------------

 fc1/9      3       0x6f7703    50:05:08:b2:00:71:c8:c2     50:05:08:b2:00:71:c8:c0
 fc1/10     3       0x6f7704    50:06:0e:80:03:29:61:0f     50:06:0e:80:03:29:61:0f
```

Note
この設定では、両方の FC ID に同じエリア 77 が割り当てられています。

ステップ 2 MDS スイッチの HBA インターフェイスをシャットダウンします。

```
switch# configure terminal
switch(config)# interface fc1/9
switch(config-if)# shutdown
switch(config-if)# end
switch#
```

Example:

ステップ 3 **show fcdomain vsan** コマンドを使用して、FC ID 機能が有効であることを確認します。

```
switch# show fcdomain vsan 1
Local switch run time information:
        State: Stable
        Local switch WWN:    20:01:54:7f:ee:de:b3:01
        Running fabric name: 20:01:00:05:9b:2c:1c:71
        Running priority: 128
        Current domain ID: 0xee(238)
Local switch configuration information:
        State: Enabled
        FCID persistence: Disabled
        Auto-reconfiguration: Disabled
        Contiguous-allocation: Disabled
        Configured fabric name: 20:01:00:05:30:00:28:df
        Optimize Mode: Disabled
        Configured priority: 128
        Configured domain ID: 0x00(0) (preferred)
Principal switch run time information:
        Running priority: 2
Interface               Role          RCF-reject
----------------    -------------    ------------
fc1/1               Non-principal    Disabled
fc1/2               Upstream         Disabled
fc1/11              Non-principal    Disabled
fc1/37              Non-principal    Disabled
port-channel 1      Downstream       Disabled
----------------    -------------    ------------
```

この機能がディセーブルの場合は、この手順を継続して、固定的 FC ID をイネーブルにします。

この機能がすでに有効の場合は、ステップ 7 に進みます。

ステップ 4 Cisco MDS スイッチで永続的 FC ID を有効にします。

```
switch# configure terminal
switch(config)# fcdomain fcid persistent vsan 1
switch(config)# end
switch#
```

ステップ 5 異なるエリアの新しい FC ID を割り当てます。この例では、*77* を *ee* に置き換えます。

```
switch# configure terminal
switch(config)# fcdomain fcid database
switch(config-fcid-db)# vsan 3 wwn 50:05:08:b2:00:71:c8:c2 fcid 0x6fee00 area
```

ステップ 6 Cisco MDS スイッチの HBA インターフェイスを有効にします。

```
switch# configure terminal
switch(config)# interface fc1/9
switch(config-if)# no shutdown
switch(config-if)# end
switch#
```

ステップ 7 **show flogi database** コマンドを使用して、HBA の pWWN ID を確認します。

```
switch# show flogi database
--------------------------------------------------------------------------------
INTERFACE   VSAN    FCID        PORT NAME                NODE NAME
--------------------------------------------------------------------------------
fc1/9       3       0x6fee00    50:05:08:b2:00:71:c8:c2  50:05:08:b2:00:71:c8:c0
fc1/10      3       0x6f7704    50:06:0e:80:03:29:61:0f  50:06:0e:80:03:29:61:0f
```

Note
これで、両方の FC ID にそれぞれ異なるエリアが割り当てられました。

永続的 FC ID の消去

固定的 FC ID を消去するには、次の手順を実行します。

Procedure

ステップ 1 switch# **purge fcdomain fcid vsan 4**

VSAN 4 の未使用のダイナミック FC ID をすべて消去します。

ステップ 2 switch# **purge fcdomain fcid vsan 3-5**

VSAN 3、4、および 5 の未使用のダイナミック FC ID を消去します。

ファブリックのロックのクリア

ファブリック ロックを解除するには、管理者権限を持つログイン ID を使用して EXEC モードで **clear fcdomain session vsan** コマンドを発行します。

```
switch# clear fcdomain session vsan 10
```

FC ドメイン設定の確認

ドメイン ID の設定情報を表示するには、次の作業を行います。

コマンド	目的
show fcdomain status	許可されたドメイン ID リストの CFS 配信のステータスを表示します。
show fcdomain pending	保留中の構成変更を表示します。
show fcdomain session-status vsan	配布セッションのステータスを表示します。
show fcdomain	fcdomain 構成のグローバル情報を表示します。
show fcdomain domain-list	すべてのスイッチのドメインIDのリストを表示します。
show fcdomain allowed vsan	このスイッチで構成されている許可されたドメイン ID のリストを表示します。
show fcdomain fcid persistent	指定の VSAN の既存の永続的 FC ID をすべて表示します。
show fcdomain statistics	指定の VSAN または PortChannel のフレームおよびその他の fcdomain 統計を表示します。
show fcdomain address-allocation	割り当てられた FC ID および空いている FC ID のリストを含めて、FC ID 割り当てに関する統計を表示します。
show fcdomain address-allocation cache	有効なアドレス割り当てキャッシュを表示します。

これらのコマンドの出力に表示される各フィールドの詳細については、『*Cisco MDS 9000 Family Command Reference*』を参照してください。

CFS 配信ステータスの表示

許可ドメイン ID リストの CFS 配信のステータスは **show fcdomain status** コマンドを使用して表示できます。

```
switch# show fcdomain status
CFS distribution is enabled
```

保留中の変更の表示

保留中の構成変更は show fcdomain pending コマンドを使用して表示できます。

```
switch# show fcdomain pending vsan 10
Pending Configured Allowed Domains
---------------------------------
VSAN 10
Assigned or unallowed domain IDs: 1-9,24,100,231-239.
[User] configured allowed domain IDs: 10-230.
```

保留中の設定と現在の設定の違いは、show fcdomain pending-diff コマンドを使用して表示できます。

```
switch#show fcdomain pending-diff vsan 10
Current Configured Allowed Domains
---------------------------------
VSAN 10
Assigned or unallowed domain IDs: 24,100.
[User] configured allowed domain IDs: 1-239.
Pending Configured Allowed Domains
---------------------------------
VSAN 10
Assigned or unallowed domain IDs: 1-9,24,100,231-239.
[User] configured allowed domain IDs: 10-230.
```

セッション ステータスの表示

配信セッションのステータスは **show fcdomain session-status vsan** コマンドを使用して表示できます。

```
switch# show fcdomain session-status vsan 1
Last Action: Distribution Enable
Result: Success
```

fcdomain 情報の表示

グローバル fcdoman 情報

showfcdomain コマンドを使用して、fcdomain 構成のグローバル情報を表示します。次の例を参照してください。

Note 次の例では、fcdomain 機能が無効になっています。その結果、ランタイム ファブリック名は構成済みファブリック名と同じです。

```
switch# show fcdomain vsan 2
The local switch is the Principal Switch.
Local switch run time information:
        State: Stable
        Local switch WWN:    20:01:00:0b:46:79:ef:41
        Running fabric name: 20:01:00:0b:46:79:ef:41
        Running priority: 128
        Current domain ID: 0xed(237)
Local switch configuration information:
        State: Enabled
        FCID persistence: Disabled
        Auto-reconfiguration: Disabled
        Contiguous-allocation: Disabled
        Configured fabric name: 20:01:00:05:30:00:28:df
        Optimize Mode: Disabled
        Configured priority: 128
        Configured domain ID: 0x00(0) (preferred)
Principal switch run time information:
        Running priority: 128
No interfaces available.
switch# show fcdomain vsan 1
The local switch is the Principal Switch.
Local switch run time information:
State: Stable
Local switch WWN: 20:01:54:7f:ee:46:5b:41
Running fabric name: 20:01:54:7f:ee:46:5b:41
Running priority: 128
Current domain ID: 0xe9(233)
Local switch configuration information:
State: Enabled
FCID persistence: Enabled
Auto-reconfiguration: Disabled
Contiguous-allocation: Disabled
Configured fabric name: 20:01:00:05:30:00:28:df
Optimize Mode: Enabled (Fast Restart, Selective Restart, Scale Restart)
Configured priority: 128
Configured domain ID: 0xe9(233) (static)
Principal switch run time information:
Running priority: 128
No interfaces available.
switch#
```

Note Cisco MDS 6.2(9) リリース以降から 6.2(7) 以前のリリースにダウングレードするときに、スケール再起動機能が有効になっていて、他の最適化モードが無効になっている場合、最適化モードは disabled ではなく blank になります。

fcdomain リスト

指定された VSAN に属するすべてのスイッチのドメイン ID リストを表示するには、**show fcdomain domain-list** コマンドを使用します。このリストには、各ドメイン ID を所有するスイッチの WWN が記載されています。次に例を示します。

- 20:01:00:05:30:00:47:df の WWN を持つスイッチが主要スイッチで、ドメインは 200 です。
- 20:01:00:0d:ec:08:60:c1 の WWN を持つスイッチはローカル スイッチ（CLI コマンドを入力してドメイン リストを表示したスイッチ）で、ドメインは 99 です。
- IVR マネージャは 20:01:00:05:30:00:47:df を仮想スイッチの WWN として使用して仮想ドメイン 97 を取得しました。

```
switch# show fcdomain domain-list vsan 76
Number of domains: 3
Domain ID              WWN
---------    -----------------------
0xc8(200)    20:01:00:05:30:00:47:df [Principal]
 0x63(99)    20:01:00:0d:ec:08:60:c1 [Local]
 0x61(97)    50:00:53:0f:ff:f0:10:06 [Virtual (IVR)]
```

許可ドメイン ID リスト

show fcdomain allowed vsan コマンドを使用して、このスイッチで構成されている許可されたドメイン ID のリストを表示します。次の例を参照してください。

```
switch# show fcdomain allowed vsan 1

Assigned or unallowed domain IDs: 1-96,100,111-239.
[Interoperability Mode 1] allowed domain IDs: 97-127.
[User] configured allowed domain IDs: 50-110.
```

Tip このスイッチに **interop 1** モードが必要な場合は、要求されたドメイン ID が Cisco NX-OS ソフトウェア チェックをパスすることを確認してください。

指定された VSAN の永続的 FC ID

show fcdomain fcid persistent コマンドを使用して、指定の VSAN の既存の永続的 FC ID をすべて表示します。**unused** オプションを指定しても、未使用の永続的 FC ID だけを表示できます。次の例を参照してください。

```
switch# show fcdomain fcid persistent vsan 1000
Total entries 2.
Persistent FCIDs table contents:
VSAN             WWN               FCID        Mask        Used    Assignment
----    -----------------------    --------    -----------    ----    ----------
```

```
1000    11:11:22:22:11:11:12:23    0x700101    SINGLE FCID      NO    STATIC
1000    44:44:33:33:22:22:11:11    0x701000    ENTIRE AREA      NO    DYNAMIC
```

fcdomain 内のすべての永続的 FC ID

次の例では、fcdomain 内のすべての永続的な FC ID を表示します。

```
switch# show fcdomain fcid persistent
Total entries 2.
Persistent FCIDs table contents:
VSAN             WWN                 FCID         Mask        Used    Assignment
----    ----------------------    --------    -----------    ----    ----------
1000    11:11:22:22:11:11:22:22    0x700501    SINGLE FCID      NO    STATIC
1003    44:44:33:33:22:22:11:11    0x781000    ENTIRE AREA     YES    DYNAMIC
```

指定された VSAN の fcdomain 統計

show fcdomain statistics コマンドを使用して、指定の VSAN または PortChannel のフレームおよびその他の fcdomain 統計を表示します。次の例および ドメインマネージャの選択的再起動, on page 284 を参照してください。

```
switch# show fcdomain statistics vsan1

VSAN Statistics
        Number of Principal Switch Selections: 5
        Number of times Local Switch was Principal: 0
        Number of 'Build Fabric's: 3
        Number of 'Fabric Reconfigurations': 0
```

指定された PortChannel の fcdomain 統計

次の例は、指定された PortChannel の fcdomain 統計を表示します。

```
switch# show fcdomain statistics interface port-channel 10 vsan 1

        Interface Statistics:
                Transmitted      Received
                -----------      --------
                EFPs      13       9
                DIAs      7        7
                RDIs      0        0
                ACCs      21       25
                RJTs      1        1
                BFs       2        2
                RCFs      4        4
                Error     0        0
                Total     48       48
        Total Retries: 0
        Total Frames: 96
                -----------      --------
```

FC ID 情報

show fcdomain address-allocation コマンドを使用して、割り当てられた FC ID および空いている FC ID のリストを含めて、FC ID 割り当てに関する統計を表示します。次の例を参照してください。

```
switch# show fcdomain address-allocation vsan 1
Free FCIDs: 0x020000 to 0x02fdff
            0x02ff00 to 0x02fffe

Assigned FCIDs: 0x02fe00 to 0x02feff
                0x02ffff

Reserved FCIDs: 0x020100 to 0x02f0ff
                0x02fe00 to 0x02feff
                0x02ffff


Number free FCIDs: 65279
Number assigned FCIDs: 257
Number reserved FCIDs: 61697
```

アドレスの割り当て情報

show fcdomain address-allocation cache コマンドを使用して、有効なアドレス割り当てキャッシュを表示します。ファブリックから取り除かれたデバイス（ディスクやホスト）を元のファブリックに戻す場合、主要スイッチはキャッシュを使用して FC ID を再度割り当てます。キャッシュ内では、VSAN はこのデバイスを含む VSAN を、WWN は FC ID を所有していたデバイスを、マスクは FC ID に対応する 1 つのエリアまたはエリア全体を表します。次の例を参照してください。

```
switch# show fcdomain address-allocation cache
Cache content:
line#    VSAN              WWN                FCID         mask
-----    ----    ----------------------    --------    -----------
   1.      12    21:00:00:e0:8b:08:a2:21    0xef0400    ENTIRE AREA
   2.       6    50:06:04:82:c3:a1:2f:5c    0xef0002    SINGLE FCID
   3.       8    20:4e:00:05:30:00:24:5e    0xef0300    ENTIRE AREA
   4.       8    50:06:04:82:c3:a1:2f:52    0xef0001    SINGLE FCID
```

CHAPTER 15

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

この章では、Cisco MDS 9000 ファミリ スイッチに提供されるスイッチド ポート アナライザ（SPAN）機能について説明します。

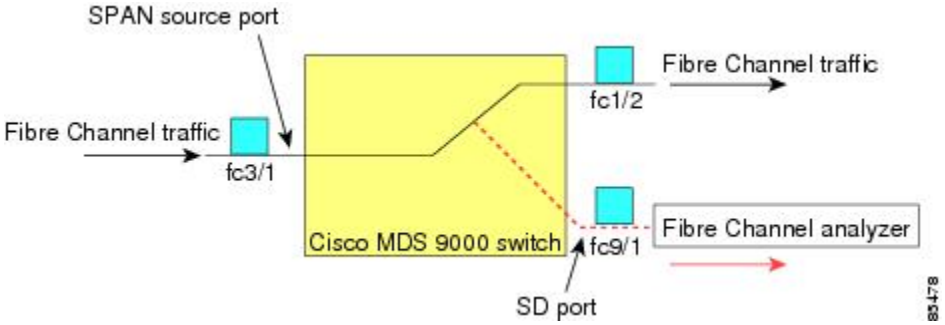
- SPAN について, on page 313
- 注意事項と制約事項, on page 327
- SPAN および RSPAN のデフォルト設定, on page 330
- SPAN の設定, on page 331
- 送信元スイッチの設定 , on page 339
- すべての中間スイッチの設定 , on page 342
- 宛先スイッチの設定 , on page 343
- SPAN 構成の確認, on page 347
- RSPAN の設定例, on page 352

SPAN について

SPAN 機能は、Cisco MDS 9000 ファミリ スイッチに特有の機能です。SPAN は、ファイバ チャネル インターフェイスを通じてネットワーク トラフィックをモニタします。任意のファイバ チャネル インターフェイスを通るトラフィックは、SPAN 宛先ポート（SD ポート）という専用ポートに複製することができます。スイッチの任意のファイバ チャネル ポートを SD ポートとして設定できます。SD ポート モードに設定したインターフェイスは、標準データ トラフィックには使用できません。ファイバ チャネル アナライザを SD ポートに接続して、SPAN トラフィックをモニタできます。

SD ポートはフレームを受信しませんが、SPAN 送信元トラフィックのコピーを送信します。SPAN 機能は他の機能に割り込むことなく、SPAN 送信元ポートのネットワーク トラフィックのスイッチングに影響しません（Figure 15: SPAN の送信, on page 314 を参照）。

Figure 15: SPAN の送信

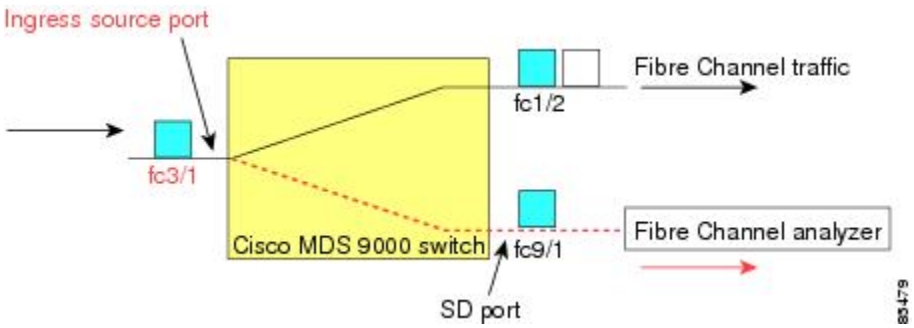


SPAN ソース

SPAN 送信元とは、トラフィックをモニタリングできるインターフェイスを表します。VSAN を SPAN 送信元として指定することもできます。この場合は、指定された VSAN でサポートされているすべてのインターフェイスが、SPAN 送信元に含まれます。送信元として VSAN が指定されている場合は、この VSAN 内のすべての物理ポートおよび PortChannel が SPAN 送信元として含まれます。任意の送信元インターフェイスで、入力方向、出力方向、または両方向の SPAN トラフィックを選択できます。

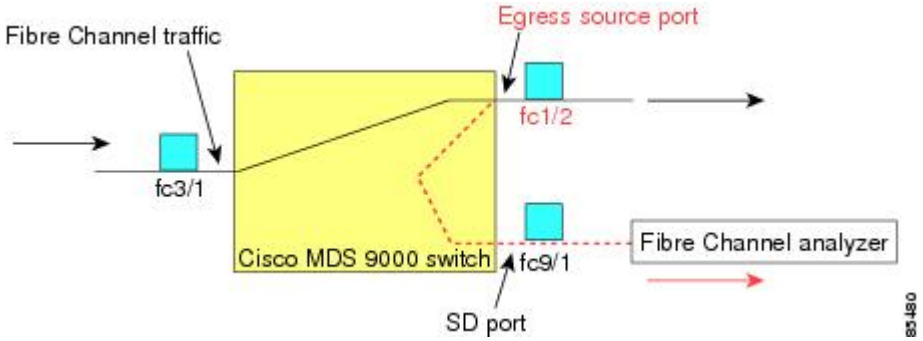
- 入力送信元（Rx）：この送信元インターフェイスを介してスイッチ ファブリックに入るトラフィックは、SD ポートに *spanned* またはコピーされます（Figure 16: 入力方向からの SPAN トラフィック, on page 314 を参照）。

Figure 16: 入力方向からの *SPAN* トラフィック



- 入力送信元（Tx）：この送信元インターフェイスを介してスイッチ ファブリックから送信されるトラフィックは、SD ポートにスパン（コピー）されます（Figure 17: 出力方向からの SPAN トラフィック, on page 315 を参照）。

Figure 17: 出力方向からの *SPAN* トラフィック



IPS 送信元ポート

SPAN 機能は、IP Storage Service（IPS）ポート上の FCIP および iSCSI インターフェイスで利用できます。この SPAN 機能を実装できるのは、IPS ポート自体でなく、FCIP および iSCSI 仮想ファイバ チャンネル インターフェイス上だけです。IPS モジュールで使用可能な 24 個の FCIP インターフェイスのどれでも、入力トラフィック、出力トラフィック、または両方向のトラフィックに SPAN を構成できます。

Note

- イーサネット トラフィックに SPAN を構成するには、Cisco MDS 9000 シリーズ IPS モジュールに接続されたシスコ スイッチまたはルータを使用します。
- Cisco MDS 9200i スイッチは、iSCSI をサポートしていません。

使用可能な送信元インターフェイス タイプ

SPAN 機能を使用できるインターフェイス タイプは、次のとおりです。

- 物理ポート（F ポート、FL ポート、TE ポート、E ポート、および TL ポート）。
- インターフェイス sup-fc0（スーパーバイザに対するトラフィック）
  - sup-fc0 インターフェイスを介してスーパーバイザ モジュールからスイッチ ファブリックに送信されるファイバ チャネル トラフィックを、入力トラフィックと言います。入力送信元ポートとして sup-fc0 が選択されている場合は、このトラフィックがスパンされます。
  - sup-fc0 インターフェイスを介してスイッチ ファブリックからスーパーバイザ モジュールに送信されるファイバチャネルトラフィックを、出力トラフィックと言います。出力送信元ポートとして sup-fc0 が選択されている場合は、このトラフィックがスパンされます。
- ポートチャネル
  - PortChannel 内のすべてのポートが含まれ、送信元としてスパンされます。

- PortChannel 内のポートを SPAN 送信元として個別に指定できません。設定済みの SPAN 固有のインターフェイス情報は廃棄されます。

- IPS モジュール固有のファイバ チャネル インターフェイス
  - iSCSI インターフェイス
  - FCIP インターフェイス

Note Cisco MDS 9700 シリーズ スイッチでは、iSCSI ポートは許可された送信元インターフェイス タイプには適用されません。

送信元としての VSAN

SPAN 送信元とは、トラフィックをモニタリングできるインターフェイスを表します。送信元として VSAN が指定されている場合は、この VSAN 内のすべての物理ポートおよび PortChannel が SPAN 送信元として含まれます。TE ポートが含まれるのは、TE ポートのポート VSAN が送信元 VSAN と一致する場合だけです。設定済みの許可 VSAN リストに送信元 VSAN が含まれている場合でも、ポート VSAN が異なっていれば、TE ポートは除外されます。

同じ SPAN セッション内では、送信元インターフェイス（物理インターフェイス、PortChannel、または sup-fc インターフェイス）と送信元 VSAN を設定できません。

SPAN セッション

各 SPAN セッションは、1 つの宛先と複数の送信元の対応関係、およびネットワーク トラフィックをモニタするために指定されたその他のパラメータを表します。1 つの宛先を 1 つ以上の SPAN セッションで使用することができます。スイッチには最大 16 個の SPAN セッションを設定できます。各セッションには複数の送信元ポートおよび 1 つの宛先ポートを設定できます。

SPAN セッションをアクティブにするには、少なくとも 1 つの送信元および SD ポートを起動して、機能させる必要があります。このようにしないと、トラフィックが SD ポートに転送されません。

Tip 1 つの送信元を 2 つのセッションで共有することは可能です。ただし、各セッションはそれぞれ異なる方向（1 つは入力、1 つは出力）でなければなりません。

SPAN セッションを一時的に非アクティブ（一時停止）にできます。この期間中、トラフィック モニタリングは停止します。

Note Cisco MDS 9250i マルチサービス ファブリック スイッチでは、SPAN ポートが着信フレーム バーストに対応できない場合、パケット ドロップが発生します。これらのパケット ドロップを回避するには、SPAN 宛て先ポートの速度を送信元ポートの最大速度と同じにする必要があります。ただし、送信元が FCIP インターフェイスの場合、FCIP インターフェイスは 10G イーサネット物理インターフェイス上で実行されるため、SPAN 宛て先ポートの速度は 10G を超える必要があります。

フィルタの指定

VSAN ベースのフィルタリングを実行すると、指定された VSAN 上でネットワーク トラフィックを選択的にモニタできます。この VSAN フィルタは、セッション内のすべての送信元に適用できます（を参照）。スパンされるのは、このフィルタ内の VSAN だけです。

指定されたセッション内のすべての送信元に適用されるセッション VSAN フィルタを指定できます。これらのフィルタは双方向であり、セッションに設定されたすべての送信元に適用されます。各 SPAN セッションは、1 つの宛先と複数の送信元の対応関係、およびネットワーク トラフィックをモニタするために指定されたその他のパラメータを表します。

SD ポートの特性

SD ポートには、次の特性があります。

- BB_credits を無視します。
- 出力（Tx）方向のデータ トラフィックだけを許可します。
- デバイスまたはアナライザを物理的に接続する必要はありません。
- 1 Gbps または 2 Gbps の速度だけをサポートします。自動速度オプションは使用できません。
- 複数のセッションで同じ宛先ポートを共有できます。
- SD ポートがシャットダウンされると、共有されたすべてのセッションが SPAN トラフィックの生成を停止します。
- 発信フレームは、Extended Inter-Switch Link（EISL）フォーマットでカプセル化することができます。
- SD ポートにはポート VSAN がありません。
- Storage Services Module（SSM）を使用した SD ポートの設定はできません。
- SPAN セッションで使用中のポート モードは、変更できません。

Note

- SD ポート モードを別のポート モードに変更する必要がある場合は、まずすべてのセッションから SD ポートを削除し、次に **switchport mode** コマンドを使用して、ポート モードを変更する必要があります。
- Cisco MDS 9700 シリーズ スイッチでは、SD ポートは 2 Gbps、4 Gbps、8 Gbps、および 16 Gbps の速度のみをサポートします。自動速度オプションは使用できません。

SPAN 変換動作

（古い任意のリリースで設定された）SPAN 機能は次のように変換されます。

- 指定されたセッションにおいて送信元インターフェイスおよび送信元VSANが設定されている場合は、このセッションからすべての送信元 VSAN が削除されます。

例：Cisco MDS SAN-OS Release 1.0(4) よりも古いリリース

```
Session 1 (active)
   Destination is fc1/9
   No session filters configured
   Ingress (rx) sources are
      vsans 10-11
     fc1/3,
   Egress (tx) sources are
     fc1/3,
```

Cisco MDS SAN-OS Release 1.1(1) にアップグレードした後

```
Session 1 (active)
   Destination is fc1/9
   No session filters configured
   Ingress (rx) sources are
     fc1/3,
   Egress (tx) sources are
     fc1/3,
```

Cisco MDS 9700 シリーズ スイッチ用

```
switch(config-if)# monitor session 1
switch(config-monitor)# source interface fc5/1
switch(config-monitor)# destination interface fc2/9
switch(config-monitor)# no shut
switch(config-monitor)# show monitor session all
session 1
---------------
ssn direction : both
state : up
source intf :
rx : fc5/1
tx : fc5/1
both : fc5/1
```

```
source VLANs :
rx :
tx :
both :
source exception :
rate-limit : Auto
filter VLANs : filter not specified
destination ports : fc2/9
```

アップグレード前は、セッション1に送信元インターフェイスと送信元VSANが両方とも設定されていました。アップグレード後は、送信元 VSAN が削除されました（法則 1）。

- 送信元インターフェイスにインターフェイス レベルの VSAN フィルタが設定されている場合、送信元インターフェイスもセッションから削除されます。このインターフェイスが双方向に設定されている場合、このインターフェイスは双方向で削除されます。

例：Cisco MDS SAN-OS Release 1.0(4) よりも古いリリース

```
Session 2 (active)
   Destination is fc1/9
   No session filters configured
   Ingress (rx) sources are
      vsans 12
     fc1/6 (vsan 1-20),
   Egress (tx) sources are
     fc1/6 (vsan 1-20),
```

Cisco MDS SAN-OS Release 1.1(1) にアップグレードした後

```
Session 2 (inactive as no active sources)
   Destination is fc1/9
   No session filters configured
   No ingress (rx) sources
   No egress (tx) sources
```

Note スイッチオーバーまたは新しいスタートアップ コンフィギュレーションを実装すると、推奨されない設定が固定メモリから削除されます。

セッション 2 には、送信元 VSAN 12 と送信元インターフェイス fc1/6、および Cisco MDS SAN-OS Release 1.0(4) で指定された VSAN フィルタが設定されていました。Cisco MDS SAN-OS Release 1.1(1) にアップグレードすると、次のように変更されます。

- • 送信元 VSAN（VSAN 12）が削除されます（法則 1）。
  • 送信元インターフェイス fc1/6 には VSAN フィルタが指定されていましたが、これも削除されます（法則 2）。

ファイバ チャネル アナライザによるトラフィックのモニタリング

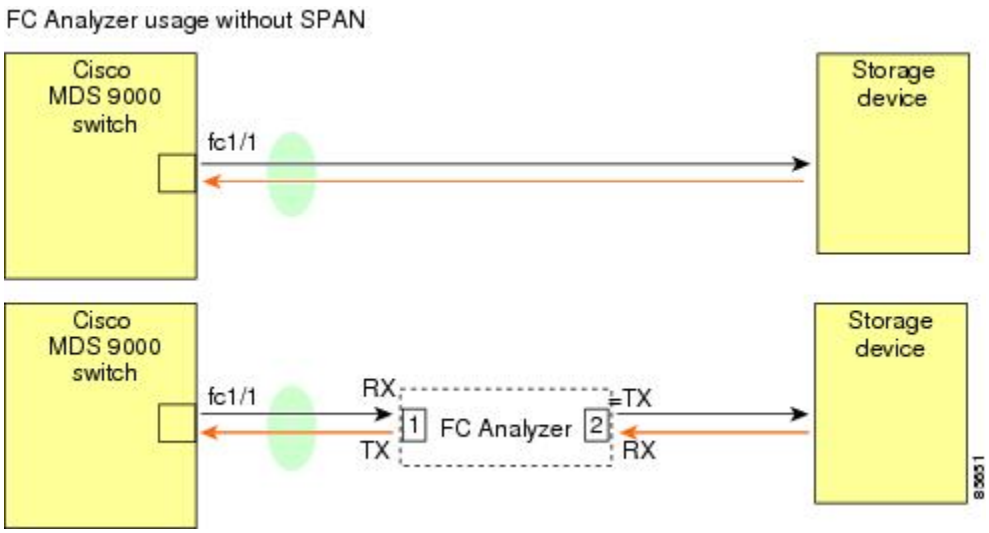
SPAN を使用すると、トラフィックを中断することなく、インターフェイス上でトラフィックをモニタできます。トラブルシューティング時においてトラフィックを中断することによって問題の環境が変更され、問題の再現が困難になる場合には、この機能が特に役立ちます。次の 2 つの方法のいずれかでトラフィックをモニタできます。

- SPAN を使用しない場合
- SPAN を使用する場合

SPAN を使用しないモニタリング

別のスイッチまたはホストに接続された Cisco MDS 9000 ファミリ スイッチのインターフェイス fc1/1 を使用して、トラフィックをモニタできます。インターフェイス fc1/1 を通るトラフィックを分析するには、スイッチとストレージ デバイスをファイバチャネル アナライザで物理的に接続する必要があります（Figure 18: SPAN を使用しない場合のファイバ チャネル アナライザの使用方法, on page 320 を参照）。

***Figure 18: SPAN* を使用しない場合のファイバ チャネル アナライザの使用方法**



この接続タイプには、次のような制約があります。

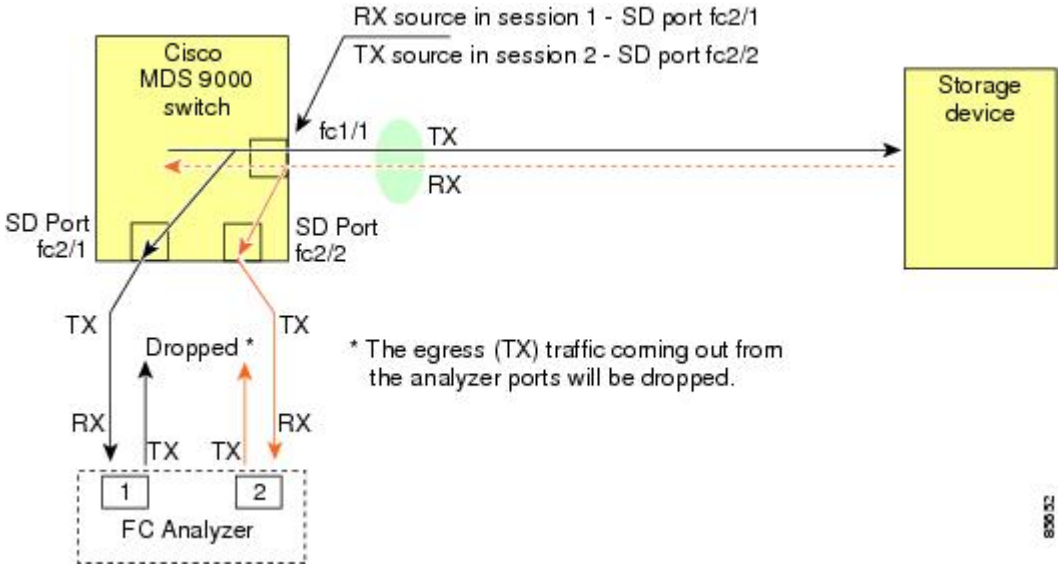
- 2 つのネットワーク デバイス間にファイバ チャネル アナライザを物理的に挿入する必要があります。
- ファイバ チャネル アナライザが物理的に接続されている場合は、トラフィックが中断されます。
- アナライザはポート 1 およびポート 2 の Rx リンクのデータだけをキャプチャします。ポート 1 はインターフェイス fc1/1 からの出力トラフィックを、ポート 2 はインターフェイス fc1/1 への入力トラフィックをキャプチャします。

SPAN を使用するモニタリング

SPAN を使用すると、トラフィックを中断しなくても、同じトラフィック（Figure 18: SPAN を使用しない場合のファイバ チャネル アナライザの使用方法, on page 320 を参照）をキャプチャすることができます。ファイバ チャネルアナライザはポート 1 の入力（Rx）リンクを使用して、インターフェイス fc1/1 から送信されるすべてのフレームをキャプチャします。また、ポート 2 の入力リンクを使用して、インターフェイス fc1/1 へのすべての入力トラフィックをキャプチャします。

SPAN を使用すると、SD ポート fc2/2 で fc1/1 の入力トラフィックをモニタしたり、SD ポート fc2/1 の出力トラフィックをモニタすることができます。このトラフィックは、FC アナライザでシームレスにキャプチャされます（Figure 19: SPAN を使用した場合のファイバ チャネル アナライザの使用方法, on page 321 を参照）。

Figure 19: SPAN を使用した場合のファイバ チャネル アナライザの使用方法

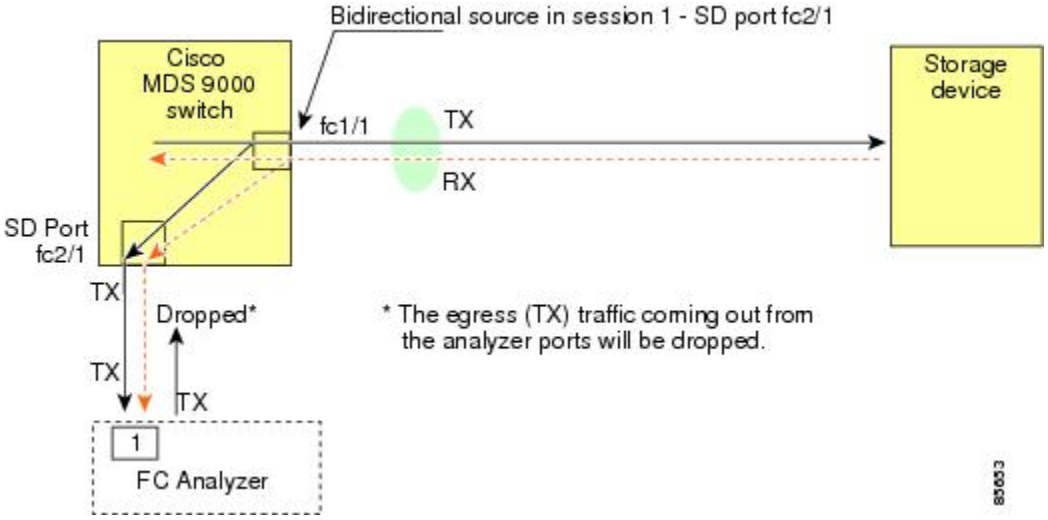


単一 SD ポートによるトラフィックのモニタ

任意のインターフェイス上で双方向トラフィックをモニタする場合、SD ポートを 2 つ使用する必要はありません（Figure 19: SPAN を使用した場合のファイバ チャネル アナライザの使用方法, on page 321 を参照）。同じ SD ポート fc2/1 でこのインターフェイスのトラフィックをモニタすることにより、SD ポートおよびファイバ チャネル アナライザ ポートを 1 つずつ使用することができます。

Figure 20: 単一 SD ポートを使用した場合のファイバ チャネル アナライザ, on page 322 に、宛先ポート fc2/1 および送信元インターフェイス fc1/1 を含む 1 つのセッションを使用して、入力および出力方向のトラフィックをキャプチャする SPAN 設定を示します。この設定には、Figure 19: SPAN を使用した場合のファイバ チャネル アナライザの使用方法, on page 321 に示された設定よりも多くの利点があり、費用対効果に優れています。完全な 2 ポート アナライザを使用する代わりに、1 つの SD ポートとアナライザ上の 1 つのポートが使用されます。

Figure 20: 単一 SD ポートを使用した場合のファイバ チャネル アナライザ

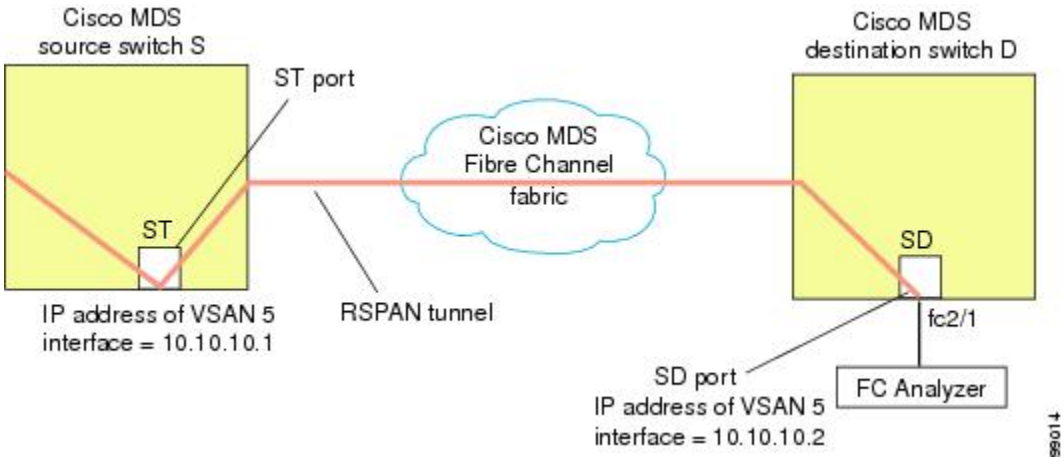


この設定を使用するには、キャプチャされたすべてのフレームの入出力トラフィックを区別する機能がアナライザに必要です。

SD ポート設定

接続先スイッチ内の SD ポートにより、FC アナライザは、ファイバチャネル トンネルからの RSPAN トラフィックを受信できるようになります。Figure 21: RSPAN トンネル設定, on page 322 は、現在トンネル接続先も構成済みである、RSPAN トンネル構成の様子を図示しています。

Figure 21: RSPAN トンネル設定

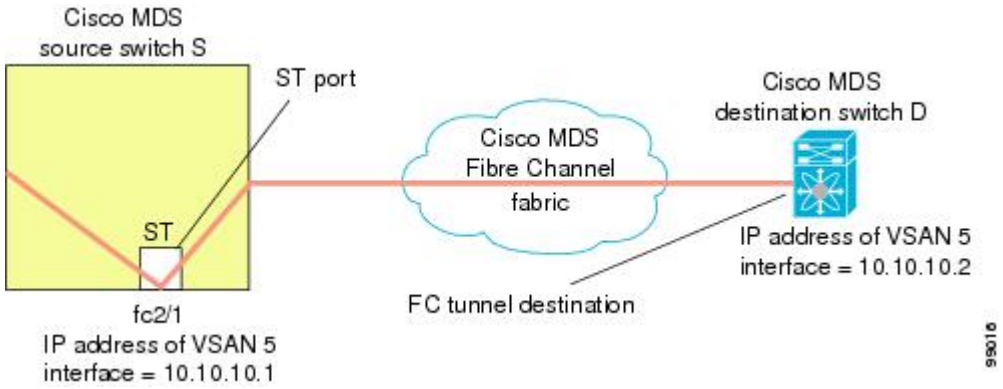


Note Storage Services Module（SSM）を使用した SD ポートの設定はできません。

FC トンネルのマッピング

tunnel-id-map オプションにより、接続先スイッチでのトンネルの出力インターフェイスが指定されます（Figure 22: FC トンネル設定, on page 323 を参照）。

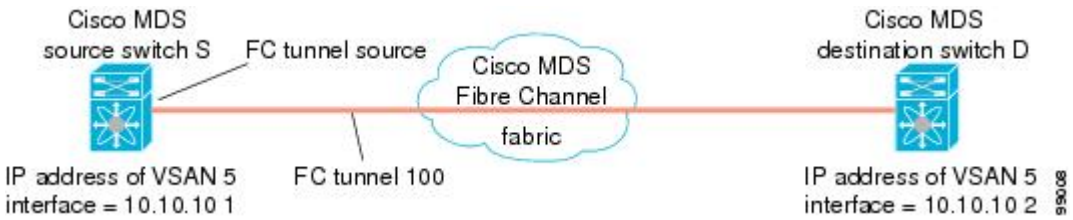
Figure 22: FC トンネル設定



VSAN インターフェイスの作成

Figure 23: FC トンネル設定, on page 323 に、基本的な FC トンネル設定を示します。

Figure 23: FC トンネル設定



Note この例では、VSAN 5 が VSAN データベースですでに設定されているものとします。

リモート SPAN

Note HP C-Class BladeSystem 用シスコ ファブリックスイッチ、IBM BladeSystem 用シスコ ファブリックスイッチ、シスコ ファブリックスイッチ 9250i、およびシスコ ファブリックスイッチ 9100S は、リモート SPAN をサポートしていません。

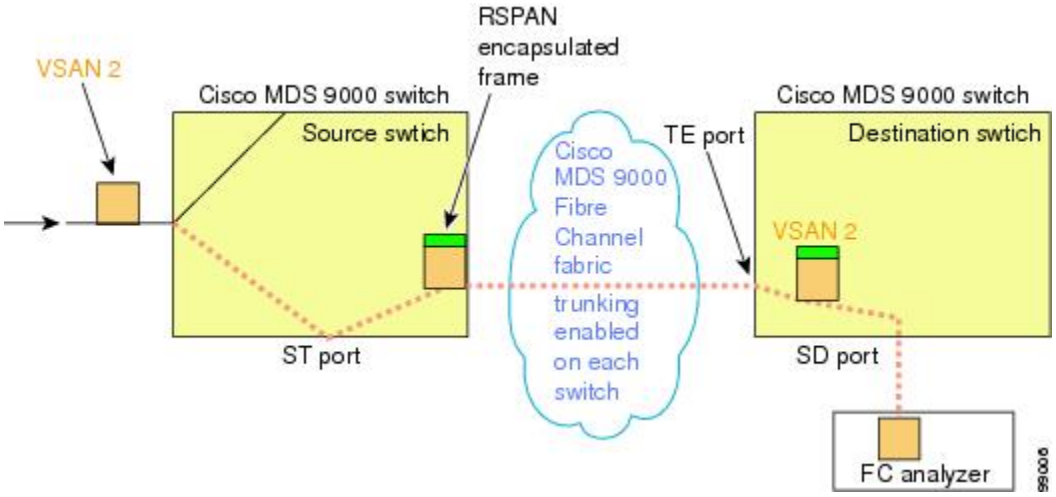
リモート SPAN（RSPAN）機能により、ファイバ チャネル ファブリック内の 1 台以上の送信元スイッチで配信される 1 つ以上の SPAN 送信元のトラフィックをリモートでモニタできるよ

うになります。SPAN 宛先（SD）ポートは、宛先スイッチ内でリモート モニタリング用に使用されます。宛先スイッチは、一般に送信元スイッチとは別に用意されますが、同じファイバ チャネル ファブリックに接続されます。Cisco MDS 送信元スイッチでトラフィックをモニタするのと同様に、任意のリモートの Cisco MDS 9000 ファミリ スイッチまたはディレクタでトラフィックを複製し、モニタすることができます。

RSPAN 機能は他の機能に割り込むことなく、SPAN 送信元ポートのネットワーク トラフィックのスイッチングに影響しません。リモート スイッチ上でキャプチャされたトラフィックは、送信元スイッチから宛先スイッチに至るまでの経路上にあるすべてのスイッチ上でトランキングがイネーブルにされているファイバ チャネル ファブリック上をトンネリングされます。ファイバ チャネル トンネルは、トランク化された ISL（TE）ポートを使用して構造化されます。TE ポート以外にも、RSPAN 機能では他に 2 つのインターフェイス タイプが使用されます（Figure 24: RSPAN の送信, on page 324 を参照）。

- SD ポート：FC アナライザがリモート SPAN トラフィックを取得するために使用できるパッシブ ポート。
- ST ポート：SPAN トンネル（ST）ポートは、RSPAN ファイバ チャネル トンネル用の送信元スイッチ内の入口ポートです。ST ポートは、特別な RSPAN ポートであり、通常のファイバ チャネル トラフィックに使用することはできません。

***Figure 24: RSPAN* の送信**



RSPAN の使用の利点

RSPAN 機能には、次の利点があります。

- 遠隔地での中断のないトラフィック モニタリングが可能になります。
- 複数のスイッチ上でリモート トラフィックをモニタするために 1 つの SD ポートを使用することにより、費用対効果に優れたソリューションを提供します。
- 任意のファイバ チャネル アナライザで動作します。
- Cisco MDS 9000 ポート アナライザ アダプタと互換性があります。

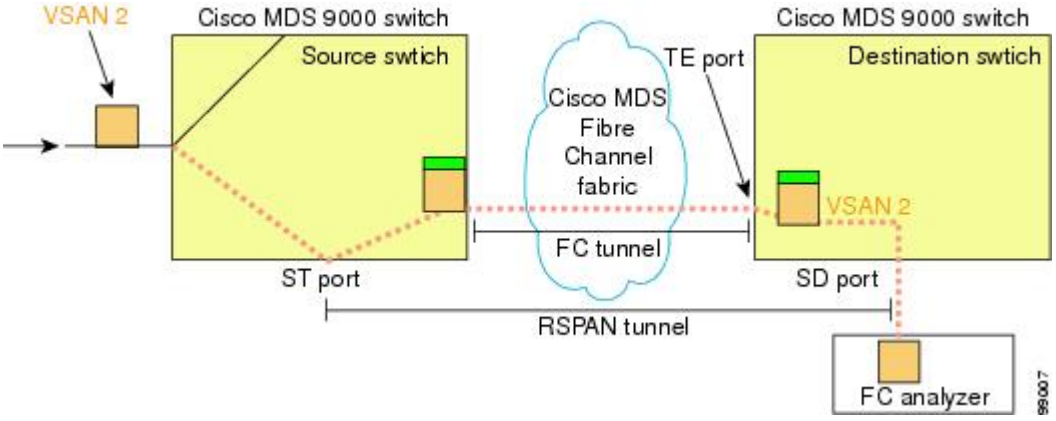
- 送信元スイッチ内のトラフィックに影響を与えません。ただし、ファブリック内の他のポートと ISL 帯域幅を共有します。

FC トンネルと RSPAN トンネル

FC トンネルは、送信元スイッチと宛先スイッチの間の論理的なデータ パスです。FC トンネルは、送信元スイッチから開始し、離れた場所にある宛先スイッチで終端します。

RSPAN では、送信元スイッチ内の ST ポートから開始し、宛先スイッチ内の SD ポートで終端する特別なファイバ チャネル トンネル（FC トンネル）が使用されます。FC トンネルを送信元スイッチ内の ST ポートにバインドし、それと同じ FC トンネルを宛先スイッチ内の SD ポートにマッピングする必要があります。マッピングとバインディングが構成されると、その FC トンネルは RSPAN トンネルと呼ばれます（Figure 25: FC トンネルと RSPAN トンネル, on page 325 を参照）。

Figure 25: FC トンネルと RSPAN トンネル



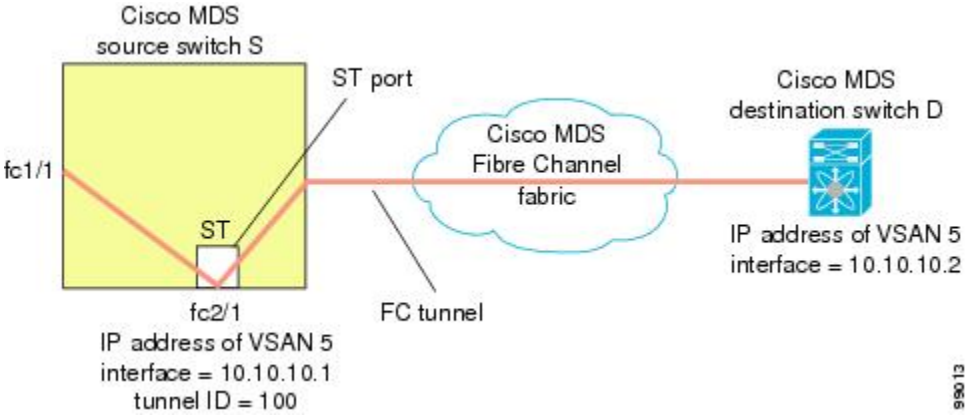
ST ポート設定

Note Cisco MDS 9700 シリーズ スイッチでは、SPAN トンネル ポート（ST ポート）はサポートされていません。

FC トンネルを作成した後、送信元スイッチにおいて、その FC トンネルにバインドされるように ST ポートを設定する必要があります。バインディングとマッピングが完了すると、その FC トンネルは RSPAN トンネルになります。

Figure 26: FC トンネルのバインディング, on page 326 に、基本的な FC トンネル設定を示します。

Figure 26: FC トンネルのバインディング



ST ポートの特性

ST ポートには、次の特性があります。

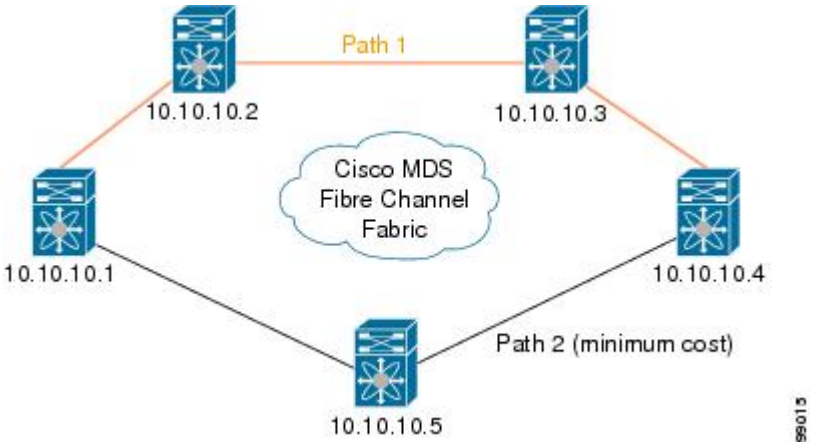
- ST ポートは、FC フレームの RSPAN カプセル化を実行します。
- ST ポートは、BB_credit を使用しません。
- 1 つの ST ポートは、1 つの FC トンネルにしかバインドできません。
- ST ポートは、RSPAN トラフィックの伝送以外には使用できません。
- ST ポートは、Storage Services Module（SSM）を使用して設定することはできません。

明示的なパスの作成

explicit-path オプションを使用して、Cisco MDS ファイバチャネル ファブリックを通過する明示的なパスを指定できます（送信元ベース ルーティング）。たとえば、トンネル宛先に対して複数のパスがある場合、このオプションを使用して、FC トンネルが宛先スイッチまで常に 1 つのパスを使用するように指定できます。この場合、ソフトウェアは、他のパスが使用可能であっても、この指定されたパスを使用します。

このオプションが特に役立つのは、使用可能なパスが他にあるときでも特定のパスにトラフィックを誘導したい場合です。RSPAN の場合、RSPAN トラフィックが既存のユーザ トラフィックの妨げにならないように、明示的なパスを指定できます。1 台のスイッチ内で作成できる明示的なパスの数に制限はありません（Figure 27: 明示的なパスの設定, on page 327 を参照）。

Figure 27: 明示的なパスの設定



注意事項と制約事項

Cisco MDS 9700 シリーズ スイッチの注意事項

Cisco MDS 9700 シリーズ スイッチには、次の注意事項と制限事項が適用されます。

- Cisco MDS 9700 シリーズ スイッチでは、SPAN が Monitor に置き換えられています。
- Cisco MDS 9700 シリーズ スイッチでは、SPAN トンネル ポート（ST ポート）はサポートされていません。
- Cisco MDS 9700 シリーズ スイッチでは、RSPAN はリモート モニタに置き換えられています。
- Cisco MDS 9700 シリーズ スイッチの場合、第 2 世代ファブリック スイッチはサポートされていません

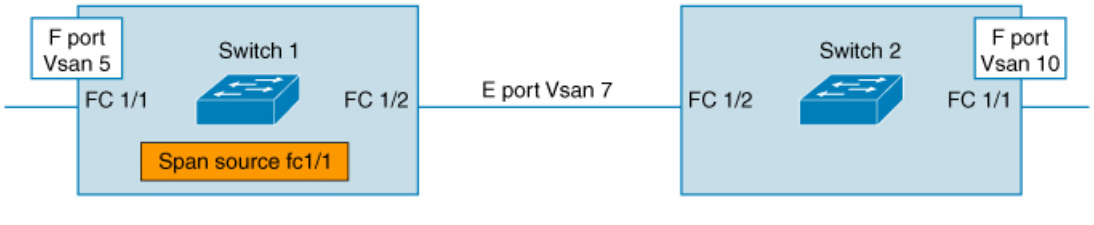
SPAN 設定時の注意事項

SPAN を設定する場合は、次の注意事項と制限が適用されます。

- 複数の入力（Rx）送信元には、最大 16 個の SPAN セッションを設定できます。
- 送信元ポートの数は16以下にする必要があります。ただし、SPANまたはモニタ セッションごとに最大 2 つの送信元ポートのみを構成することが推奨されています。
- 1 つの出力（Tx）ポートには、最大 3 個の SPAN セッションを設定できます。
- 32 ポート スイッチング モジュールでは、1 つのポート グループ（ユニット）内の 4 つのすべてのポートに、同じセッションを設定する必要があります。必要に応じて、このユニット内の 2 つまたは 3 つのポートだけを設定することもできます。

Note これは、Cisco MDS 9700 シリーズ スイッチには適用されません。

- 送信元の合計帯域幅が宛先ポートの速度を超えると、SPAN フレームは廃棄されます。
- 送信元ポートで廃棄されたフレームは、スパンされません。
- SPAN は、Fibre Channel over Ethernet（FCoE）ネットワーク内のポーズ フレームをキャプチャしません。仮想拡張（VE）ポートから送信されるポーズ フレームは、最も外側の MAC レイヤで生成および終端が行われるためです。FCoE の詳細については、『Cisco NX-OS FCoE Configuration Guide for Cisco Nexus 7000 and Cisco MDS 9500』を参照してください。
- IVR 構成およびトポロジの場合、SPAN は送信元ポートの出力（Tx）をキャプチャできません。完全なトラフィック フローをスパンするには、入力（Rx）方向のフローに参加する送信元ポートを追加します。



上の図の FC1/1 を SPAN 送信元ポートとして考えます。この場合、FC1/1 からのトラフィック出力（Tx）はスパンされません。（Rx）FC1/1 に入るパケットだけがスパンされます。完全なフローをキャプチャするには、単一の接続先に向かう単一のセッションで FC1/1（Rx）と FC1/2（Rx）をスパンします。

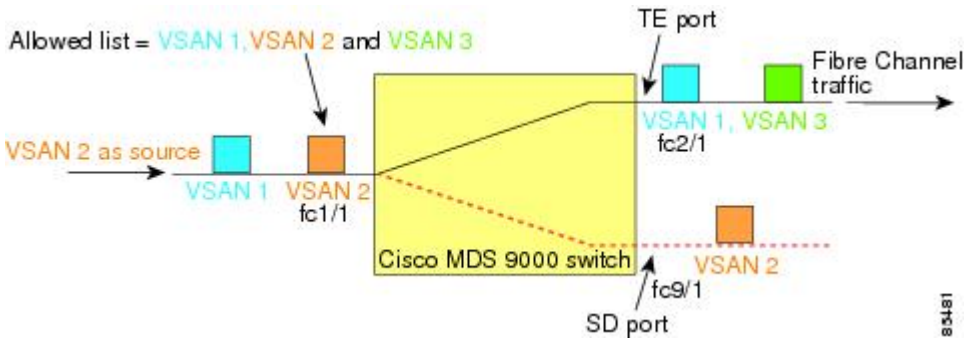
VSAN を送信元として設定する場合の注意事項

VSAN を送信元として設定する場合は、次の注意事項に従ってください。

- 送信元 VSAN に含まれるすべてのインターフェイスのトラフィックは、入力方向の場合にだけスパンされます。
- VSAN が送信元として指定されている場合は、VSAN に含まれるインターフェイス上でインターフェイス レベルの SPAN 設定を実行することができません。設定済みの SPAN 固有のインターフェイス情報は廃棄されます。
- VSAN 内のインターフェイスが送信元として設定されている場合は、この VSAN を送信元として設定できません。VSAN を送信元として設定する前に、まずこのようなインターフェイス上の既存の SPAN 設定を削除する必要があります。

- インターフェイスが送信元として含まれるのは、ポート VSAN が送信元 VSAN と一致する場合だけです。Figure 28: 送信元としての VSAN, on page 329 は、送信元として VSAN 2 を使用する構成を表示しています。
  - スイッチ内のすべてのポートは、fc1/1 を除いて、VSAN 1 内にあります。
  - インターフェイス fc1/1 は、ポート VSAN 2 を含む TE ポートです。VSAN 1、2、および 3 は許可リスト内で設定されます。
  - VSAN 1 および VSAN 2 は、SPAN 送信元として設定されています。

Figure 28: 送信元としての ***VSAN***



この設定では、次のようになります。

- 送信元としての VSAN 2 には、ポート VSAN 2 を持つ TE ポート fc1/1 だけが含まれます。
- ポート VSAN が VSAN 1 と一致しないため、送信元としての VSAN 1 には TE ポート fc1/1 が含まれません。

フィルタを指定する場合の注意事項

SPAN フィルタには、次の注意事項が適用されます。

- PortChannel 設定は、PortChannel 内にあるすべてのポートに適用されます。
- フィルタが指定されていない場合は、該当するインターフェイスのすべてのアクティブ VSAN からのトラフィックがデフォルトでスパンされます。
- セッションでは任意の VSAN フィルタを指定できますが、トラフィックをモニタできるのは、該当するポート VSAN 上、または該当するインターフェイスで許可されているアクティブ VSAN 上だけです。

RSPAN 設定時の注意事項

SPAN を設定する場合は、次の注意事項が適用されます。

- RSPAN トンネルのエンドツーエンドのパス上にあるすべてのスイッチは、Cisco MDS 9000 ファミリに属している必要があります。

- RSPAN トラフィックが含まれるすべての VSAN がイネーブルになっている必要があります。RSPAN トラフィックが含まれる VSAN がイネーブルになっていないと、そのトラフィックはドロップされます。
- RSPAN が実装されるファイバチャネル トンネルのエンドツーエンドのパス内にある *each* スイッチ上で次の構成を実行する必要があります。
  - トランキングをイネーブルにし（デフォルトではイネーブル）、トランク対応リンクをパス内の最低コスト リンクにする必要があります。
  - VSAN インターフェイスを設定する必要があります。
  - ファイバ チャネル トンネル機能をイネーブルにする必要があります（デフォルトではディセーブル）。
  - IPルーティングをイネーブルにする必要があります（デフォルトではディセーブル）。

Note IP アドレスが VSAN と同じサブネット内である場合は、トラフィックがスパンされるすべての VSAN に対して VSAN インターフェイスを設定する必要はありません。

- 単一のファイバ チャネル スイッチ ポートを ST ポート機能専用にする必要があります。
- モニタ対象のポートを ST ポートとして設定してはなりません。
- FC トンネルの IP アドレスは、VSAN インターフェイスと同じサブネット内に存在する必要があります。

SPAN および RSPAN のデフォルト設定

Table 38: SPAN パラメータのデフォルト設定値 , on page 330 に、SPAN パラメータのデフォルト設定を示します。

***Table 38: SPAN* パラメータのデフォルト設定値**

パラメータ	デフォルト
SPAN セッション	Active **Note** Cisco MDS 9700 シリーズ スイッチの場合、モニタ セッションのデフォルト値は Shut です。
フィルタが指定されていない場合	SPAN トラフィックには、すべてのアクティブ VSAN から特定のインターフェイスを経由するトラフィックが含まれます。
カプセル化	ディセーブル
SD ポート	出力フレーム形式はファイバ チャネルです。

Table 39: RSPAN パラメータのデフォルト設定値 , on page 331 に、RSPAN パラメータのデフォルト設定を示します。

***Table 39: RSPAN* パラメータのデフォルト設定値**

パラメータ	デフォルト
FC トンネル	無効
明示パス	未設定
最小コスト パス	明示パスが構成されていない場合に使用されます。

SPAN の設定

SPAN 機能は、Cisco MDS 9000 ファミリ スイッチに特有の機能です。SPAN は、ファイバ チャネル インターフェイスを通じてネットワーク トラフィックをモニタします。

SPAN の SD ポートの設定

SPAN モニタリング用 SD ポートの構成

SPAN モニタリングの SD ポートを構成するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **interface fc9/1**

指定されたインターフェイスを設定します。

ステップ 3 switch(config-if)# **switchport mode SD**

インターフェイス fc9/1 の SD ポート モードを構成します。

ステップ 4 switch(config-if)# **switchport speed 1000**

SD ポート速度を 1000 Mbps に構成します。

Note
Cisco MDS 9700 シリーズ スイッチでは、スイッチ ポートの速度は 8000 Mbps です。

ステップ 5 switch(config-if)# **no shutdown**

このインターフェイスを介したトラフィック フローを有効化します。

SPAN セッションの構成

SPAN セッションを設定する手順は、次のとおりです。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **span session 1**

switch(config-span)#

指定された SPAN セッション（1）を構成します。セッションが存在しない場合は、セッションを作成します。

Note
Cisco MDS 9700 シリーズ スイッチでは、SPAN が Monitor に置き換えられています。

ステップ 3 switch(config)# **no span session 1**

指定された SPAN セッション（1）を削除します。

ステップ 4 switch(config-span)# **destination interface fc9/1**

セッションで指定された接続先インターフェイス（fc 9/1）を構成します。

ステップ 5 switch(config-span)# **no destination interface fc9/1**

指定された接続先インターフェイス（fc 9/1）を削除します。

ステップ 6 switch(config-span)# **source interface fc7/1**

双方向のソース（fc7/1）インターフェイスを構成します。

Note
Cisco MDS 9124 ファブリック スイッチで SPAN 送信元を構成するときは、方向（Rx および Tx）を明示的に指定する必要があります。

ステップ 7 switch(config-span)# **no source interface fc7/1**

指定された接続先インターフェイス（fc 7/1）をこのセッションから削除します。

ステップ 8 switch(config-span)# **source interface sup-fc0**

セッションの送信元インターフェイス（sup-fc0）を構成します。

ステップ 9 switch(config-span)# **source interface fc1/5 - 6, fc2/1 -3**

セッションで指定されたインターフェイス範囲を構成します。

ステップ 10 switch(config-span)# **source vsan 1-2**

セッションで送信元 VSAN 1 および 2 を構成します。

ステップ 11 switch(config-span)# **source interface port-channel 1**

送信元 PortChannel（port-channel 1）を構成します。

ステップ 12 switch(config-span)# **source interface fcip 51**

セッションの送信元 FCIP インターフェイスを構成します。

ステップ 13 switch(config-span)# **source interface iscsi 4/1**

セッションの送信元 iSCSI インターフェイスを構成します。

Note
これは、MDS 9700 シリーズ スイッチには適用されません。

ステップ 14 switch(config-span)# **source interface svc1/1 tx traffic-type initiator**

イニシエータ トラフィック タイプの Tx 方向の送信元 SVC インターフェイスを構成します。

Note
これは、MDS 9700 シリーズ スイッチには適用されません。

ステップ 15 switch(config-span)# **no source interface port-channel 1**

指定された送信元インターフェイス（port-channel 1）を削除します。

ステップ 16 switch(config-span)# **shutdown**

セッションを一時停止します。

Note
これは、MDS 9700 シリーズ スイッチに適用されます。

SPAN フィルタの構成

SPAN フィルタを構成するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **span session 1**

switch(config-span)#

指定されたセッション（1）を構成します。

Note
Cisco MDS 9700 シリーズ スイッチでは、SPAN がモニタ セッション 1 に置き換えられています。

ステップ 3 switch(config-span)# **source interface fc9/1 tx**

送信元 fc9/1 インターフェイスを出力（Tx）方向に構成します。

ステップ 4 switch(config-span)# **source filter vsan 1-2**

VSAN 1 および 2 をセッション フィルタとして構成します。

ステップ 5 switch(config-span)# **source interface fc7/1 rx**

送信元 fc7/1 インターフェイスを入力（Rx）方向に構成します。

第 2 世代ファブリック スイッチ用の SPAN の設定

シスコの第 2 世代ファブリック スイッチ（MDS 9124 など）では、SPAN セッションが両方向（Rx と Tx）でサポートされます。

Note 第 2 世代ファブリック スイッチを使用する場合、アクティブな SPAN セッションは 1 つしか作成できません。

複数の SPAN 送信元インターフェイスを Rx 方向と Tx 方向で指定できます。ただし、方向はコマンドの最後に明示的に指定する必要があります。SPAN は、方向に言及していない送信元インターフェイス構成をすべて拒否します。

入力 SPAN セッションの構成

入力 SPAN セッションを構成する手順は、次のとおりです。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **span session 1**

switch(config-span)#

指定されたセッション（1）を構成します。

ステップ 3 switch(config-span)# **destination interface fc1/1**

インターフェイス fc1/1 を接続先として構成します。

ステップ 4 switch(config-span)# **source interface fc1/2 rx**

送信元インターフェイス fc1/2 を入力方向に構成します。

出力 SPAN セッションの構成

出力 SPAN セッションを構成する手順は、次のとおりです。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **span session 1**

switch(config-span)#

指定されたセッション（1）を構成します。

ステップ 3 switch(config-span)# **destination interface fc1/1**

インターフェイス fc1/1 を接続先として構成します。

ステップ 4 switch(config-span)# **source interface fc1/2 tx**

送信元インターフェイス fc1/2 を出力方向に構成します。

例

この例は、複数の SPAN インターフェイス用に Cisco MDS 9124 を構成する方法を示しています

```
switch(config-span)# span session 1
switch(config-span)# destination interface fc1/1
switch(config-span)# source interface fc1/2 rx
switch(config-span)# source interface fc1/2 tx
```

第 2 世代ファブリック スイッチでは、出力方向において 1 つの VSAN に対してのみ VSAN フィルタがサポートされます。この制限は、入力方向には適用されません。たとえば、TE ポートのインターフェイスで 1 ～ 5 のアクティブな VSAN が存在する場合、VSAN 2 に対して VSAN フィルタを指定すると、VSAN 2 上のトラフィックのみがフィルタリングされます。

```
switch(config-span)# span session 1
switch(config-span)# source filter vsan 2
switch(config-span)# destination interface fc1/1
switch(config-span)# source interface fc1/2 tx
```

ただし、VSAN 1 ～ 2 に VSAN フィルタを指定すると、すべての VSAN（1 ～ 5）からのトラフィックがフィルタリングされ、フィルタが役に立たなくなります。

```
switch(config-span)# span session 1
switch(config-span)# source filter vsan 1-2
switch(config-span)# destination interface fc1/1
switch(config-span)# source interface fc1/2 tx
```

SPAN シリーズの一時停止および再アクティベート

SPAN セッションを一時的に非アクティブ（一時停止）にできます。この期間中、トラフィック モニタリングは停止します。

SPANセッション フィルタを一時的に停止または再アクティブ化するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **span session 1**

switch(config-span)#

指定されたセッション（1）を構成します。

ステップ 3 switch(config-span)# **suspend**

セッションを一時停止します。

ステップ 4 switch(config-span)# **no suspend**

セッションを再開します。

フレームのカプセル化

フレームのカプセル化機能は、デフォルトで無効になっています。カプセル化機能を有効にすると、すべての発信フレームがカプセル化されます。

switchport encap eisl コマンドは、SD ポート インターフェイスにだけ適用されます。カプセル化が有効になっている場合、**show interface** *SD_port_interface* コマンドの出力に新しい行（Encapsulation is eisl）が表示されます。

発信フレームをカプセル化するには（オプション）、次の手順に従います。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **interface fc9/32**

指定されたインターフェイスを設定します。

ステップ 3 switch(config-if)# **switchport mode SD**

インターフェイス fc9/32 の SD ポート モードを構成します。

ステップ 4 switch(config-if)# **switchport encap eisl**

この SD ポートのカプセル化オプションを有効にします。

ステップ 5 switch(config-if)# **no switchport encap eisl**

カプセル化オプションを無効（デフォルト）にします。

SPAN を使用したファイバ チャネル アナライザの設定

送信元および接続先インターフェイスで SPAN を構成するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **span session 1**

switch(config-span)#

SPAN セッション 1 を作成します。

ステップ 3 switch(config-span)## **destination interface fc2/1**

接続先インターフェイス fc2/1 を構成します。

ステップ 4 switch(config-span)# **source interface fc1/1 rx**

送信元インターフェイス fc1/1 を入力方向に構成します。

ステップ 5 switch(config)# **span session 2**

switch(config-span)#

SPAN セッション 2 を作成します。

ステップ 6 switch(config-span)## **destination interface fc2/2**

接続先インターフェイス fc2/2 を構成します。

ステップ 7 switch(config-span)# **source interface fc1/1 tx**

送信元インターフェイス fc1/1 を出力方向に構成します。

SPAN を使用してファイバ チャネル アナライザを設定するには（ の例を使用）、次の手順を実行します。

Procedure

ステップ 1 セッション 1 を使用して SD ポート fc2/1 上でトラフィックを送信するように、インターフェイス fc1/1 の入力（Rx）方向に SPAN を設定します。

ステップ 2 セッション 2 を使用して SD ポート fc2/2 上でトラフィックを送信するように、インターフェイス fc1/1 の出力（Tx）方向に SPAN を設定します。

ステップ 3 ファイバ チャネル アナライザのポート 1 に fc2/1 を物理的に接続します。

ステップ 4 ファイバ チャネル アナライザのポート 2 に fc2/2 を物理的に接続します。

トラフィックのモニタの用シングル SD ポートの構成

シングル SD ポート上の SPAN を構成するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **span session 1**

switch(config-span)#

SPAN セッション 1 を作成します。

ステップ 3 switch(config-span)## **destination interface fc2/1**

接続先インターフェイス fc2/1 を構成します。

ステップ 4 switch(config-span)# **source interface fc1/1**

同じ SD ポートで送信元インターフェイス fc1/1 を構成します。

送信元スイッチの設定

ここでは、送信元スイッチ（スイッチ S）で実行する必要のある作業を示します。

VSAN インターフェイスの作成

のシナリオで送信元スイッチの VSAN インターフェイスを作成するには、次の手順を実行します。

Procedure

ステップ 1 switchS# **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 switchS(config)# **interface vsan 5**

switchS(config-if)#

送信元スイッチ（スイッチ S）で指定された VSAN インターフェイス（VSAN 5）を構成します。

ステップ 3 switchS(config-if)# **ip address 10.10.10.1 255.255.255.0**

送信元スイッチ（スイッチ S）の VSAN インターフェイス 5 の IPv4 アドレスとサブネットを構成します。

ステップ 4 switchS(config-if)# **no shutdown**

このインターフェイスを介したトラフィック フローを有効化します。

FC トンネルの有効化

Note
- FC トンネルは、非トランキング ISL では機能しません。
- 接続先スイッチで FC トンネル マッピングが構成されるまで、インターフェイスは稼働できません。

FC トンネル機能を有効にするには、次の手順を実行します。

Procedure

ステップ 1 switchS# **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 switchS(config)# **fc-tunnel enable**

FC トンネル機能を有効にします（デフォルトでは無効）。

Note
ファブリック内のエンドツーエンド パスの各スイッチで、この機能を必ず有効にしてください。

FC トンネルの開始

のシナリオで送信元スイッチの FC トンネルを開始するには、次の手順を実行します。

Procedure

ステップ 1 switchS# **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 switchS(config)# **interface fc-tunnel 100**

switchS(config-if)#

送信元スイッチ（スイッチ S）で FC トンネル（100）を開始します。トンネル ID の範囲は 1 ～ 255 です。

ステップ 3 switchS(config-if)# **source 10.10.10.1**

送信元スイッチ（スイッチ S）の IPv4 アドレスを FC トンネル（100）にマッピングします。

ステップ 4 switchS(config-if)# **destination 10.10.10.2**

接続先スイッチ（スイッチ D）の IPv4 アドレスを FC トンネル（100）にマッピングします。

ステップ 5 switchS(config-if)# **no shutdown**

このインターフェイスを介したトラフィック フローを有効化します。

ST ポートの構成

Note ST ポートは、Storage Services Module（SSM）を使用して設定することはできません。

ST ポートを構成するには、次の手順を実行します。

Procedure

ステップ 1 switchS# **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 switchS(config)# **interface fc2/1**

指定されたインターフェイスを設定します。

ステップ 3 switchS(config-if)# **switchport mode ST**

インターフェイス fc2/1 の ST ポート モードを構成します。

ステップ 4 switchS(config-if)# **switchport speed 2000**

ST ポート速度を 2000 Mbps に構成します。

ステップ 5 switchS(config-if)# **rspan-tunnel interface fc-tunnel 100**

ST ポートを RSPAN トンネル（100）に関連付けてバインドします。

ステップ 6 switchS(config-if)# **no shutdown**

このインターフェイスを介したトラフィック フローを有効化します。

RSPAN セッションの構成

RSPAN セッションは、接続先インターフェイスが RSPAN トンネルである SPAN セッションに似ています。

のシナリオで送信元スイッチに RSPAN セッションを構成するには、次の手順を実行します。

Procedure

ステップ 1 switchS# **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 switchS(config)# **span session 2**

switchS(config-span)#

指定された SPAN セッション（2）を構成します。セッションが存在しない場合は、セッションを作成します。セッション ID の範囲は 1 ～ 16 です。

ステップ 3 switchS(config-span)# **destination interface fc-tunnel 100**

指定された RSPAN トンネル（100）をセッション内で構成します。

ステップ 4 switchS(config-span)# **source interface fc1/1**

このセッションの送信元インターフェイス（fc1/1）を構成し、インターフェイス fc1/1 から RSPAN トンネル 100 にトラフィックをスパンします。

すべての中間スイッチの設定

ここでは、RSPAN トンネルのエンドツーエンドのパス内にあるすべての中間スイッチで実行する必要のある作業を示します。

VSAN インターフェイスの設定

に、宛先スイッチ（スイッチ D）で終端している RSPAN トンネル設定を示します。

Note この例では、VSAN 5 が VSAN データベースですでに設定されているものとします。

のシナリオで接続先スイッチの VSAN インターフェイスを作成するには、次の手順を実行します。

Procedure

ステップ 1 switchD# **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 switchD(config)# **interface vsan 5**

switchD(config-if)#

接続先スイッチ（スイッチ D）で指定された VSAN インターフェイス（VSAN 5）を構成します。

ステップ 3 switchD(config-if)# **ip address 10.10.10.2 255.255.255.0**

接続先スイッチ（スイッチ D）の VSAN インターフェイス 5 の IPv4 アドレスとサブネットを構成します。

ステップ 4 switchD(config-if)# **no shutdown**

管理上トラフィックを許可するようにトラフィック フローを有効化します（動作ステートは up）。

IP ルーティングの有効化

IP ルーティング機能は、デフォルトではディセーブルになっています。ファブリック内のエンドツーエンドのパス内にある各スイッチ（送信元スイッチと宛先スイッチを含む）において IP ルーティングをイネーブルにする必要があります。この手順は、FC トンネルをセットアップするために必要です。

宛先スイッチの設定

ここでは、宛先スイッチ（スイッチ D）で実行する必要のある作業を示します。

VSAN インターフェイスの設定

に、宛先スイッチ（スイッチ D）で終端している RSPAN トンネル設定を示します。

Note この例では、VSAN 5 が VSAN データベースですでに設定されているものとします。

SD ポートの構成

Note Storage Services Module（SSM）を使用した SD ポートの設定はできません。

のシナリオで SD ポートを構成するには、次の手順を実行します。

Procedure

ステップ 1 switchD# **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 switchD(config)# **interface fc2/1**

指定されたインターフェイスを設定します。

ステップ 3 switchD(config-if)# **switchport mode SD**

インターフェイス fc2/1 の SD ポート モードを構成します。

ステップ 4 switchD(config-if)# **switchport speed 2000**

SD ポート速度を 2000 Mbps に構成します。

ステップ 5 switchD(config-if)# **no shutdown**

このインターフェイスを介したトラフィック フローを有効化します。

FC トンネルのマッピング

のシナリオで接続先スイッチの FC トンネルを終了するには、次の手順を実行します。

Procedure

ステップ 1 switchD# **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 switchD(config)# **fc-tunnel tunnel-id-map 100 interface fc2/1**

接続先スイッチ（switch D）の FC トンネル（100）を終了します。トンネル ID の範囲は 1 ～ 255 です。

明示的なパスの作成

のシナリオの明示的なパスを作成するには、次の手順に従います。

Before you begin

明示的なパスは送信元スイッチに作成する必要があります。明示的なパスを構成するには、最初にパスを作成し、次にいずれか1つのパスを使用するように構成します。明示的なパスが構成されていない場合、デフォルトで最小コストパスが使用されます。明示的なパスが構成されていて、機能している場合は、指定されたパスが使用されます。

Procedure

ステップ 1 switchS# **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 switchS(config)# **fc-tunnel explicit-path Path1**

switch(config-explicit-path)#

パス Path 1 に関する明示的なパスのプロンプトが表示されます。

ステップ 3 switchS(config-explicit-path)# **next-address 10.10.10.2 strict**

switchS(config-explicit-path)# **next-address 10.10.10.3 strict**

switchS(config-explicit-path)# **next-address 10.10.10.4 strict**

明示パスで指定されたネクスト ホップ VSAN インターフェイスの IPv4 アドレスと前のホップが直接接続を必要としないことを指定します。

ステップ 4 switchS(config)# **fc-tunnel explicit-path Path2**

switch(config-explicit-path)#

Path 2 に関する明示的なパスのプロンプトが表示されます。

ステップ 5 switchS(config-explicit-path)# **next-address 10.10.10.5 strict**

Example:

```
switchS(config-explicit-path)# next-address 10.10.10.4 strict
```

明示パスで指定されたネクスト ホップ VSAN インターフェイスの IPv4 アドレスと前のホップが直接接続を必要としないことを指定します。

ステップ 6 switchS(config)# **fc-tunnel explicit-path Path3**

switch(config-explicit-path)#

Path 3 に関する明示的なパスのプロンプトが表示されます。

ステップ 7 switchS(config-explicit-path)# next-address10.10.10.3loose

10.10.10.3 IPv4 アドレスが存在する最小コスト パスを構成します。

Note

では、パス 3 はパス 1 と同じです。パス 1 には 10.10.10.3 が存在します。**loose** オプションを使用すると、ステップ 3 で 3 つのコマンド（**strict** オプションを使用）を発行しなくても、1 のコマンドで同じ結果を達成できます。

明示的パスのリファレンス

明示的なパスを参照するには、次の手順を実行します。

Procedure

ステップ 1 switchS# **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 switchS(config)# **interface fc-tunnel 100**

Path1 のトンネル ID を参照します。

ステップ 3 switchS(config)# **explicit-path Path1**

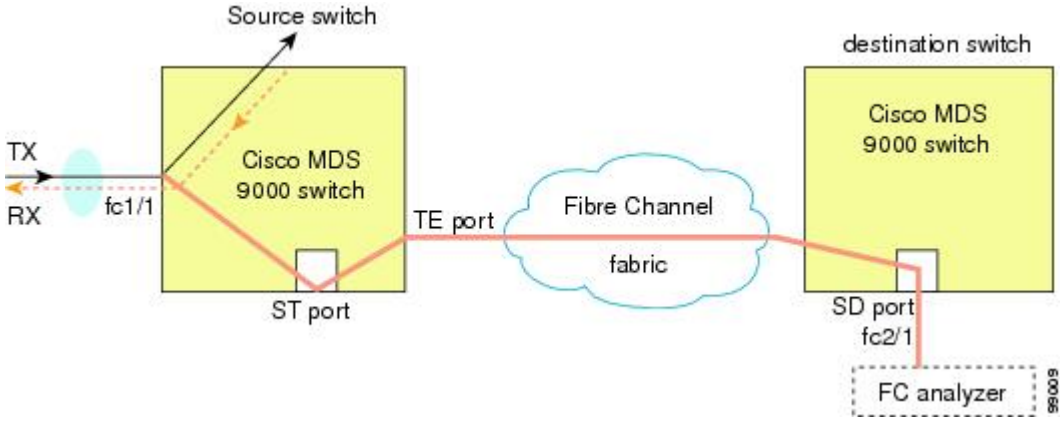
Path1 をトンネル ID にリンクします。

この構成は、RSPAN トラフィックで使用される Path1 を明示的に指定します。明示的なパスおよび送信元ベース ルーティングの詳細については、RFC 3209 を参照してください。

RSPAN トラフィックのモニタリング

セッションが一旦構成されると、このセッションの他の SPAN 送信元も必要に応じて構成することができます。Figure 29: 単一の SD ポートを使用して RSPAN トラフィックをモニタするファイバ チャネル アナライザ, on page 347 に、宛て先ポート fc2/1 および送信元インターフェイス fc1/1 を含む 1 つのセッションを使用して、入力および出力方向のトラフィックをキャプチャする RSPAN 設定を示します。

Figure 29: 単一の *SD* ポートを使用して *RSPAN* トラフィックをモニタするファイバ チャネル アナライザ



この設定を使用するには、キャプチャされたすべてのフレームの入出力トラフィックを区別する機能がアナライザに必要です。

SPAN 構成の確認

SPAN 構成の情報を表示するには、次の作業のいずれかを行います。

コマンド	目的
show span	簡単な形式での SPAN セッションの表示 **Note** Cisco MDS 9700 シリーズ スイッチでは、**show span** コマンドが **show monitor** コマンドに置き換えられています。
show span session 7	指定された SPAN セッションを詳細に表示する **Note** Cisco MDS 9700 シリーズ スイッチでは、**show span session 7** コマンドが **show monitor session 7** コマンドに置き換えられています。
show span session	すべての SPAN セッションの表示 **Note** Cisco MDS 9700 シリーズ スイッチでは、**show span session** コマンドが **show monitor session all** コマンドに置き換えられています。
show int fc9/32	カプセル化が有効になっている SD ポート インターフェイスの表示
show interface brief	ST ポート インターフェイス情報の表示

コマンド	目的
show interface fc1/11	ST ポート インターフェイスの詳細情報の表示
show fc-tunnel	FC トンネルのステータスの表示
show fc-tunnel tunnel-id-map	FC トンネル出力マッピング情報の表示
show fc-tunnel explicit-path	FC トンネルの明示的なマッピング情報の表示
show interface fc-tunnel 200	FC トンネル インターフェイスの表示

これらのコマンドの出力に表示される各フィールドの詳細については、『*Cisco MDS 9000 Family Command Reference*』を参照してください。

SPAN 情報の表示

show span コマンドを使用して、構成された SPAN 情報を表示します。 次の例を参照してください。

簡単なフォーマットの SPAN セッション

次の例は、SPAN セッションを簡単なフォーマットで表示します。

```
switch# show span session brief
-------------------------------------------------------
 Session  Admin          Oper           Destination
          State          State          Interface
-------------------------------------------------------
 7        no suspend     active         fc2/7
 1        suspend        inactive       not configured
 2        no suspend     inactive       fc3/1
```

指定された SPAN セッションの詳細

次の例は、指定された SPAN セッションを詳細に表示します。

```
switch# show span session 7
Session 7 (active)
   Destination is fc2/7
   No session filters configured
   No ingress (rx) sources
   Egress (tx) sources are
     port-channel 7,
```

すべての SPAN セッション

次の例は、すべての SPAN セッションを表示します。

```
switch# show span session
Session 1 (inactive as no destination)
Destination is not specified
   Session filter vsans are 1
   No ingress (rx) sources
   No egress (tx) sources
Session 2 (active)
   Destination is fc9/5
   No session filters configured
   Ingress (rx) sources are
      vsans 1
   No egress (tx) sources
Session 3 (admin suspended)
   Destination is not configured
   Session filter vsans are 1-20
   Ingress (rx) sources are
     fc3/2, fc3/3, fc3/4, fcip 51,
     port-channel 2, sup-fc0,
   Egress (tx) sources are
     fc3/2, fc3/3, fc3/4, sup-fc0,
```

カプセル化が有効になっている SD ポート インターフェイス

次の例では、カプセル化が有効になっている SD ポート インターフェイスを表示します。

```
switch# show int fc9/32
fc9/32 is up
    Hardware is Fibre Channel
    Port WWN is 22:20:00:05:30:00:49:5e
    Admin port mode is SD
    Port mode is SD
    Port vsan is 1
    Speed is 1 Gbps
    Receive Buffer Size is 2112
    Encapsulation is eisl
<----------------
Displays the enabled encapsulation status
    Beacon is turned off
    5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
      0 frames input, 0 bytes, 0 discards
        0 CRC,  0 unknown class
        0 too long, 0 too short
      0 frames output, 0 bytes, 0 discards
      0 input OLS, 0 LRR, 0 NOS, 0 loop inits
```

0 output OLS, 0 LRR, 0 NOS, 0 loop inits

RSPAN 情報の表示

構成された RSPAN 情報を表示するには、**show** コマンドを使用します。次の例を参照してください。

ST ポート インターフェイス情報

次の例は、ST ポート インターフェイス情報を表示します。

```
switch# show interface brief
--------------------------------------------------------------------------------
Interface   Vsan    Admin   Admin   Status      Oper    Oper    Port-channel
                    Mode    Trunk               Mode    Speed
                            Mode                        (Gbps)
--------------------------------------------------------------------------------
fc1/1       1       auto    on      trunking    TE          2       --
...
fc1/14      1       auto    on      trunking    TE          2       --
fc1/15      1       ST      on      up          ST          2       --
...
fc2/9       1       auto    on      trunking    TE          2       port-channel 21
fc2/10      1       auto    on      trunking    TE          2       port-channel 21
...
fc2/13      999     auto    on      up          F           1       --
fc2/14      999     auto    on      up          FL          1       --
fc2/15      1       SD      --      up          SD          2       --
fc2/16      1       auto    on      trunking    TE          2       --
--------------------------------------------------------------------------------
Interface           Status      Speed
                                (Gbps)
--------------------------------------------------------------------------------
sup-fc0             up          1
--------------------------------------------------------------------------------
Interface           Status      IP Address              Speed       MTU
--------------------------------------------------------------------------------
mgmt0               up        172.22.36.175/22          100 Mbps    1500
--------------------------------------------------------------------------------
Interface           Status      IP Address              Speed       MTU--
--------------------------------------------------------------------------------
vsan5               up          10.10.10.1/24           1 Gbps      1500
--------------------------------------------------------------------------------
Interface           Vsan        Admin           Status      Oper    Oper
                                Trunk                       Mode    Speed
                                Mode                                (Gbps)
--------------------------------------------------------------------------------
port-channel 21     1           on              trunking    TE      4
--------------------------------------------------------------------------------
Interface           Status      Dest IP Addr    Src IP Addr     TID    Explicit Path
--------------------------------------------------------------------------------
fc-tunnel 100       up          10.10.10.2      10.10.10.1      100
```

ST ポート インターフェイスの詳細情報

次の例は、ST ポート インターフェイスの詳細情報を表示します。

```
switch# show interface fc1/11
fc1/11 is up
    Hardware is Fibre Channel
    Port WWN is 20:0b:00:05:30:00:59:de
   Admin port mode is ST
    Port mode is ST
    Port vsan is 1
    Speed is 1 Gbps
   Rspan tunnel is fc-tunnel 100
```

```
    Beacon is turned off
    5 minutes input rate 248 bits/sec, 31 bytes/sec, 0 frames/sec
    5 minutes output rate 176 bits/sec, 22 bytes/sec, 0 frames/sec
      6862 frames input, 444232 bytes
        0 discards, 0 errors
        0 CRC, 0 unknown class
        0 too long, 0 too short
      6862 frames output, 307072 bytes
        0 discards, 0 errors
      0 input OLS, 0 LRR, 0 NOS, 0 loop inits
      0 output OLS, 0 LRR, 0 NOS, 0 loop inits
```

FC トンネルのステータス

次の例は、FC トンネルのステータスを表示します。

```
switch# show fc-tunnel
fc-tunnel is enabled
```

FC トンネル出力マッピング情報

次の例は、FC トンネルの出力マッピング情報を表示します。

```
switch# show fc-tunnel tunnel-id-map
tunnel id egress interface
    150     fc3/1
    100     fc3/1
```

Note 複数のトンネル ID を同じインターフェイスで終端させることができます。

FC トンネルの明示的なマッピング情報

次の例は、FC トンネル マッピング情報を表示します。

```
switch# show fc-tunnel explicit-path
Explicit path name: Alternate1
       10.20.1.2 loose
       10.20.1.3 strict
Explicit path name: User2
       10.20.50.1 strict
       10.20.50.4 loose
```

SPAN マッピング情報

次の例は、SPAN マッピング情報を表示します。

```
switch# show span session
Session 2 (active)
```

```
Destination is fc-tunnel 100
No session filters configured
Ingress (rx) sources are
  fc2/16,
Egress (tx) sources are
  fc2/16,
```

FC トンネル インターフェイス

次の例は、FC トンネル インターフェイスを表示します。

```
switch# show interface fc-tunnel 200
fc-tunnel 200 is up
Dest   IP Addr: 200.200.200.7   Tunnel ID: 200
Source IP Addr: 200.200.200.4   LSP ID: 1
Explicit Path Name:
```

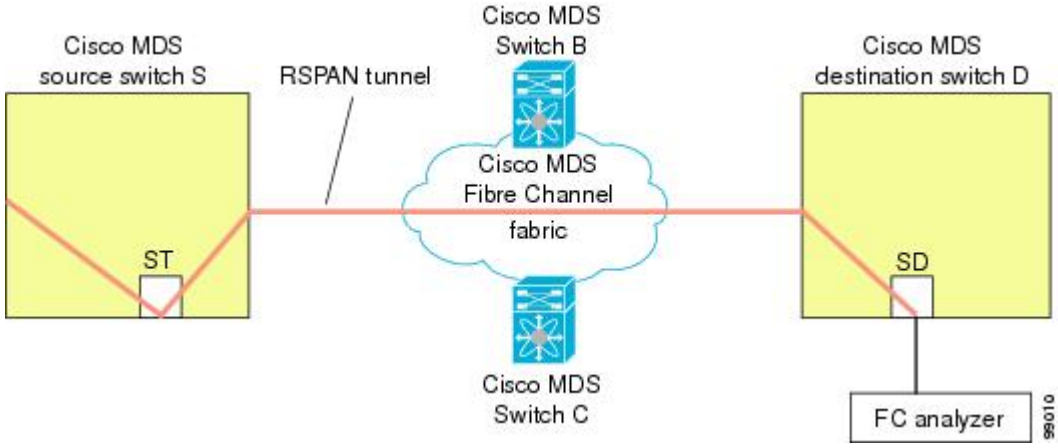
RSPAN の設定例

Note RSPAN は、SD ポートがローカル SPAN トラフィックをリモート SPAN トラフィックと一緒に転送するように、ローカル SPAN 機能と組み合わせることができます。ここでは、さまざまな SPAN 送信元とトンネルのシナリオが説明されます。

単一の送信元と 1 本の RSPAN トンネル

送信元のスイッチ S と宛先のスイッチ D がファイバ チャネル ファブリックを介して相互接続されます。RSPAN トンネルは SPAN セッションの接続先インターフェイスとして構成され、ST ポートは SPAN トラフィックを RSPAN トンネル経由で転送します（Figure 30: 送信元スイッチが 1 台、宛先スイッチが 1 台、トンネルが 1 本の場合の RSPAN シナリオ, on page 353 を参照）。

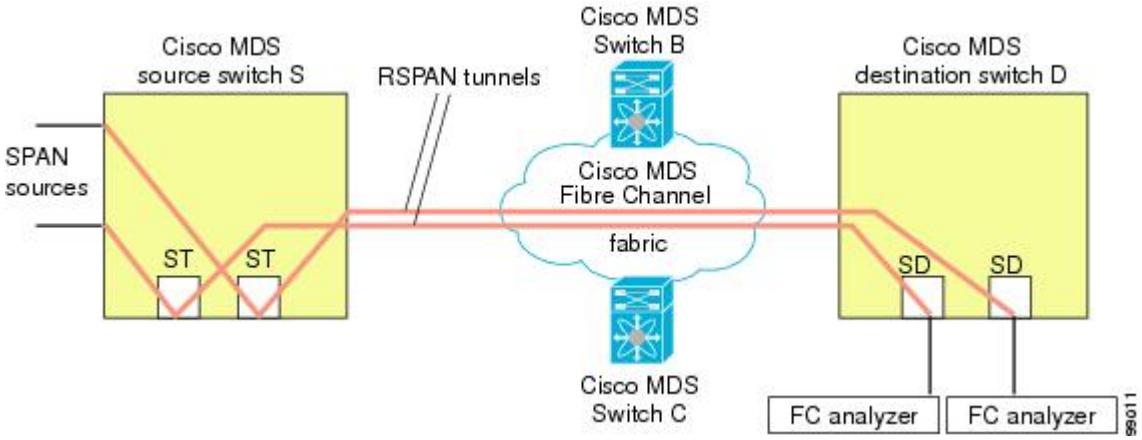
Figure 30: 送信元スイッチが *1* 台、宛先スイッチが *1* 台、トンネルが *1* 本の場合の *RSPAN* シナリオ



単一の送信元と複数の RSPAN トンネル

単一の送信元と複数の RSPAN トンネル , on page 353 はスイッチ S と N 間で構成された 2 つの独立した RSPAN トンネルを表示します。各トンネルの関連 ST ポートは送信元スイッチ内に存在し、独立 SD ポートは接続先スイッチ内に存在します。この設定は、トラブルシューティングの場合に役立ちます。

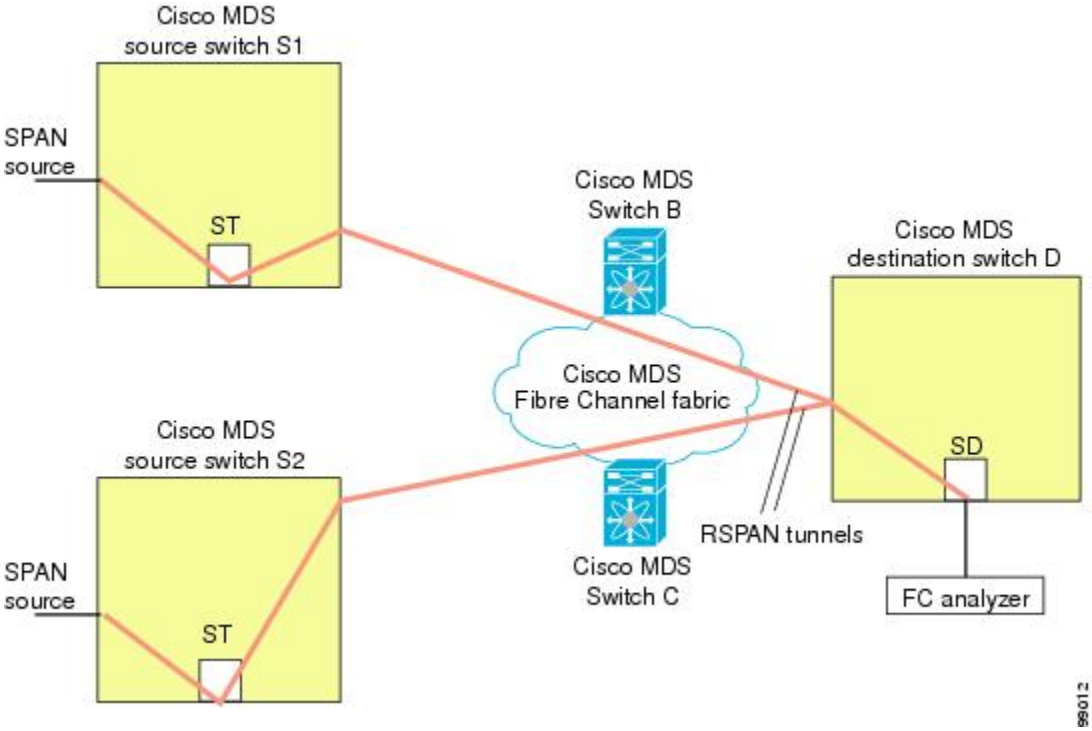
Figure 31: 送信元スイッチが *1* 台、宛先スイッチが *1* 台、トンネルが複数の場合の *RSPAN* シナリオ



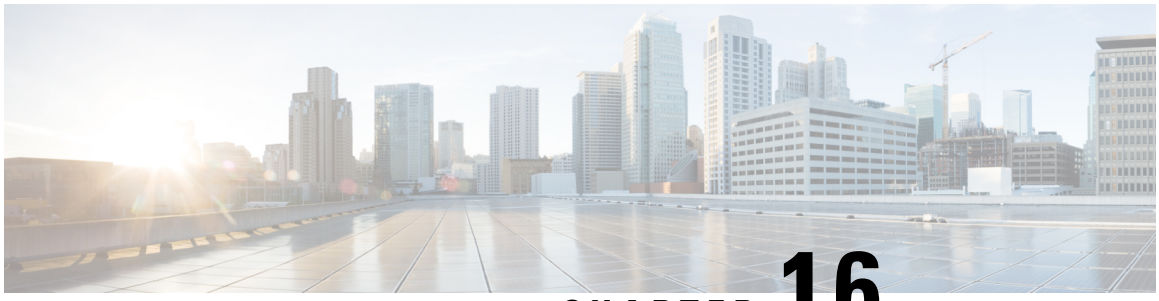
複数の送信元と複数の RSPAN トンネル

Figure 32: 送信元スイッチが 2 台、宛先スイッチが 1 台、トンネルが複数の場合の RSPAN シナリオ, on page 354 に、スイッチ S1 とスイッチ S2 の間に設定された 2 本の独立した RSPAN トンネルを示します。これらのトンネルは、関連 ST ポートがそれぞれ別々の送信元スイッチ内に存在し、両方とも宛先スイッチ内にある同じ SD ポートで終端します。

Figure 32: 送信元スイッチが *2* 台、宛先スイッチが *1* 台、トンネルが複数の場合の *RSPAN* シナリオ



この設定は、リモートモニタリングの場合に役立ちます。たとえば、管理者は宛先スイッチからリモートで 2 台の送信元スイッチをモニタできます。



CHAPTER 16

Fabric Configuration Server の設定

この章では、Cisco MDS 9000 ファミリのディレクタとスイッチで提供されている Fabric Configuration Server（FCS）機能について説明します。

- FCS についての情報, on page 355
- デフォルト設定, on page 357
- FCS の設定, on page 357
- FCS 設定の確認, on page 359
- その他の参考資料, on page 363

FCS についての情報

Fabric Configuration Server（FCS）を使用すると、トポロジ属性を検出したり、ファブリック要素の設定情報リポジトリを維持したりすることができます。通常、管理アプリケーションはNポートを通してスイッチの FCS に接続されます。FCS は次のオブジェクトに基づいて、ファブリック全体を表示します。

- Interconnect Element（IE）オブジェクト：ファブリック内の各スイッチは IE オブジェクトに対応しています。ファブリックは 1 つまたは複数の IE オブジェクトで構成されます。
- ポート オブジェクト：IE の各物理ポートはポート オブジェクトに対応しています。ポート オブジェクトにはスイッチ ポート（xE、Fx、および TL ポート）および接続された Nx ポートが含まれます。
- プラットフォーム オブジェクト：一連のノードをプラットフォーム オブジェクトとして定義して、管理可能な単一のエンティティにできます。これらのノードはファブリックに接続されたエンドデバイス（ホスト システム、ストレージ サブシステム）です。プラットフォーム オブジェクトは、ファブリックのエッジ スイッチ上にあります。

各オブジェクトには、それぞれ独自の属性および値のセットがあります。一部の属性にはヌル値も定義できます。

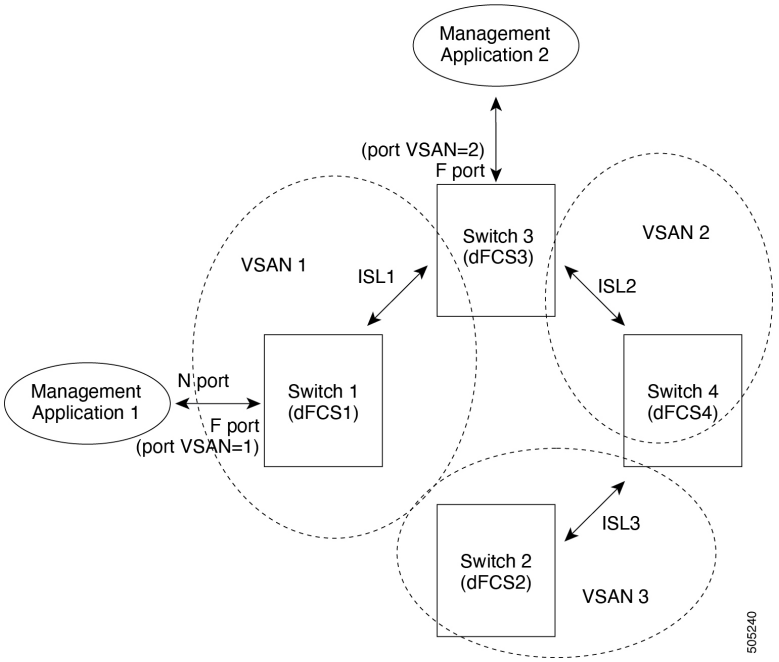
Cisco MDS 9000 ファミリ スイッチ環境では、複数の VSAN がファブリックを構成し、VSAN ごとに 1 つの FCS インスタンスが存在します。

Cisco NX-OS Release 4.1(1) から、FCS は仮想デバイスの検出をサポートしています。FCS 構成サブモードで **fcs virtual-device-add** コマンドを実行すると、特定の VSAN またはすべての VSAN で仮想デバイスを検出できます。IVR 用にゾーン分割されたデバイスは、IVR ゾーンセットをアクティブ化する前に、このコマンドで検出し、Request Domain ID（RDI）をイネーブルにする必要があります。

スイッチに管理アプリケーションが接続されている場合、スイッチの FCS に転送されるすべてのフレームは、スイッチ ポート（Fx ポート）のポート VSAN に属します。管理アプリケーションの表示対象はこの VSAN に限定されます。ただし、このスイッチが属する他の VSAN に関する情報は、SNMP または CLI を使用して取得できます。

次の図では、管理アプリケーション 1（M1）はポート VSAN ID が 1 の F ポートを介して接続され、管理アプリケーション 2（M2）はポート VSAN ID が 2 の F ポートを介して接続されています。M1 はスイッチ S1 および S3 の FCS 情報を、M2 はスイッチ S3 および S4 の FCS 情報をそれぞれ問い合せることができます。スイッチ S2 の情報はどちらにも提供されません。FCS は、VSAN で表示可能なこれらのスイッチ上でだけ動作します。なお、S3 は VSAN 1 にも属していますが、M2 は VSAN 2 にだけ FCS 要求を送信できます。

Figure 33: VSAN* 環境における *FCS



FCS の重要性

ここでは、FCS の重要性について説明します。

- FCS は次のようなネットワーク管理をサポートします。
  - N ポート管理アプリケーションはファブリック要素に関する情報を問い合せて、取得できます。

- SNMP マネージャは FCS 管理情報ベース（MIB）を使用して、ファブリック トポロジ情報の検出を開始して、取得できます。

- FCS は、標準の F ポートおよび E ポートだけでなく、TE ポートと TL ポートもサポートします。
- FCS は、プラットフォームに登録された論理名および管理アドレスを使用して、一連のモードを維持することができます。FCS はすべての登録情報のバックアップをセカンダリ ストレージに維持し、変更があるたびに更新します。再起動またはスイッチオーバーが発生すると、FCS はセカンダリ ストレージ情報を取得し、データベースを再構築します。
- SNMP マネージャは FCS に、ファブリック内のすべての IE、ポート、およびプラットフォームについて問い合せることができます。

デフォルト設定

Table 40: FCS のデフォルト設定値 , on page 357 に、FCSの デフォルト設定値を示します。

***Table 40: FCS* のデフォルト設定値**

パラメータ	デフォルト
プラットフォーム名のグローバル チェック	ディセーブル
プラットフォームのノード タイプ	不明。

FCS の設定

Fabric Configuration Server（FCS）を使用すると、トポロジ属性を検出したり、ファブリック要素の設定情報リポジトリを維持したりすることができます。

FCS 名の指定

一意の名前の確認をファブリック全体（グローバル）に行うのか、または登録されたプラットフォームにローカル（デフォルト）に行うのかを指定できます。

Note このコマンドのグローバル設定は、ファブリック内のすべてのスイッチが Cisco MDS 9000 ファミリのスイッチである場合に限り実行してください。

プラットフォーム名のグローバル チェックを有効にするには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **fcs plat-check-global vsan 1**

プラットフォーム名のグローバル チェックをイネーブルにします。

ステップ 3 switch(config)# **no fcs plat-check-global vsan 1**

プラットフォーム名のグローバル チェックをディセーブル（デフォルト）にします。

プラットフォーム属性の登録

プラットフォーム属性を登録するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch(config)# **fcs register**

switch(config-fcs-register)#

FCS 登録サブモードを開始します。

ステップ 3 switch(config-fcs-register)# **platform name SamplePlatform vsan 1**

switch(config-fcs-register-attrib)#

FCS 登録属性サブモードを開始します。

ステップ 4 switch(config-fcs-register)# **no platform name SamplePlatform vsan 1**

switch(config-fcs-register)#

登録されたプラットフォームを削除します。

ステップ 5 switch(config-fcs-register-attrib)# **mgmt-addr 1.1.1.1**

プラットフォーム管理 IPv4 アドレスを設定します。

ステップ 6 switch(config-fcs-register-attrib)# **no mgmt-addr 1.1.1.1**

プラットフォーム管理 IPv4 アドレスを削除します。

ステップ 7 switch(config-fcs-register-attrib)# **mgmt-addr 2001:0DB8:800:200C::417A**

プラットフォーム管理 IPv6 アドレスを設定します。

ステップ 8 switch(config-fcs-register-attrib)# **no mgmt-addr 2001:0DB8:800:200C::417A**

プラットフォーム管理 IPv6 アドレスを削除します。

ステップ 9 switch(config-fcs-register-attrib)# **nwwn 11:22:33:44:55:66:77:88**

プラットフォーム ノード名を設定します。

ステップ 10 switch(config-fcs-register-attrib)# **no nwwn 11:22:33:44:55:66:77:88**

プラットフォーム ノード名を削除します。

ステップ 11 switch(config-fcs-register-attrib)# **type 5**

定義済みプラットフォーム タイプ fc-gs-3 を設定します。

ステップ 12 switch(config-fcs-register-attrib)# **no type 5**

設定済みのタイプを削除し、スイッチを出荷時の設定（不明なタイプ）に戻します。

ステップ 13 switch(config-fcs-register-attrib)# **exit**

FCS 登録属性サブモードを終了します。

ステップ 14 switch(config-fcs-register)# **exit**

FCS 登録サブモードを終了します。

FCS 設定の確認

FCS の構成情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show fcs database	FCS ローカル データベース情報の表示
show fcs ie vsan 1	特定の VSAN のすべての IE のリストを表示します。
show fcs ie nwwn 20:01:00:05:30:00:16:df vsan 1	特定の nWWN のインターコネクト エレメント オブジェクト情報の表示
show fcs platform name SamplePlatform vsan 1	特定のプラットフォームに関する情報の表示
show fcs platform vsan 1	指定された VSAN のプラットフォームのリストの表示

コマンド	目的
show fcs port vsan 24	指定された VSAN のスイッチポートのリストの表示
show fcs port pwwn 20:51:00:05:30:00:16:de vsan 24	指定された pWWN のポート情報の表示
show fcs statistics	FCS の統計の表示
show fcs vsan	各 VSAN のプラットフォーム設定の表示

これらのコマンドの出力に表示される各フィールドの詳細については、『*Cisco MDS 9000 Family Command Reference*』を参照してください。

FCS 要素の表示

WWN 構成のステータスを表示するには、**show fcs** コマンドを使用します（例 FCS ローカル データベース情報, on page 360 ～ 各 VSAN のプラットフォーム設定, on page 363 を参照）。

FCS ローカル データベース情報

次の例は、FCS ローカル データベース情報を表示します。

```
switch# show fcs database
FCS Local Database in VSAN: 1
-------------------------------
Switch WWN                : 20:01:00:05:30:00:16:df
Switch Domain Id          : 0x7f(127)
Switch Mgmt-Addresses     : snmp://172.22.92.58/eth-ip
                            http://172.22.92.58/eth-ip
Fabric-Name               : 20:01:00:05:30:00:16:df
Switch Logical-Name       : 172.22.92.58
Switch Information List   : [Cisco Systems*DS-C9509*0*20:00:00:05:30:00
Switch Ports:
--------------------------------------------------------------------------
Interface  pWWN                      Type     Attached-pWWNs
--------------------------------------------------------------------------
fc2/1      20:41:00:05:30:00:16:de  TE       20:01:00:05:30:00:20:de
fc2/2      20:42:00:05:30:00:16:de  Unknown  None
fc2/17     20:51:00:05:30:00:16:de  TE       20:0a:00:05:30:00:20:de
FCS Local Database in VSAN: 5
-------------------------------
Switch WWN                : 20:05:00:05:30:00:12:5f
Switch Domain Id          : 0xef(239)
Switch Mgmt-Addresses     : http://172.22.90.171/eth-ip
                            snmp://172.22.90.171/eth-ip
                            http://10.10.15.10/vsan-ip
                            snmp://10.10.15.10/vsan-ip
Fabric-Name               : 20:05:00:05:30:00:12:5f
Switch Logical-Name       : 172.22.90.171
Switch Information List   : [Cisco Systems*DS-C9509**20:00:00:05:30:00:12:5e]
Switch Ports:
--------------------------------------------------------------------------
Interface  pWWN                      Type     Attached-pWWNs
--------------------------------------------------------------------------
fc3/1      20:81:00:05:30:00:12:5e  TE       22:01:00:05:30:00:12:9e
```

```
fc3/2      20:82:00:05:30:00:12:5e  TE       22:02:00:05:30:00:12:9e
fc3/3      20:83:00:05:30:00:12:5e  TE       22:03:00:05:30:00:12:9e
```

Note スイッチ（FCS インターコネクト エレメント）の [FCS スイッチ管理アドレス（FCS Switch Mgmt-Addresses）] フィールドには、スイッチの mgmt0 インターフェイスや IPFC などのダウン インターフェイスにローカル管理アドレスが構成されている場合でも、アップ状態のインターフェイスからの IP アドレスのみが入力されます。

指定された VSAN のすべての IE のリスト

次の例は、指定された VSAN のすべての IE のリストを表示します。

```
switch# show fcs ie vsan 1
IE List for VSAN: 1
--------------------------------------------------------------------------
IE-WWN                   IE-Type                              Mgmt-Id
--------------------------------------------------------------------------
20:01:00:05:30:00:16:df  Switch (Local)                      0xfffc7f
20:01:00:05:30:00:20:df  Switch (Adjacent)                   0xfffc64
[Total 2 IEs in Fabric]
```

特定の nWWN のインターコネクト エレメント オブジェクト情報

次の例は、指定された nWWN のインターコネクト エレメント オブジェクト情報を表示します。

```
switch# show fcs ie nwwn 20:01:00:05:30:00:16:df vsan 1
IE Attributes
-------------
Domain-Id = 0x7f(127)
Management-Id = 0xfffc7f
Fabric-Name = 20:01:00:05:30:00:16:df
Logical-Name = 172.22.92.58
Management Address List =
        snmp://172.22.92.58/eth-ip
        http://172.22.92.58/eth-ip
Information List:
        Vendor-Name = Cisco Systems
        Model Name/Number = DS-C9509
        Release-Code = 0
```

指定されたプラットフォームに関する情報

次の例は、指定されたプラットフォームに関する情報を表示します。

```
switch# show fcs platform name SamplePlatform vsan 1
Platform Attributes
-------------------
Platform Node Names:
        11:22:33:44:55:66:77:88
```

```
Platform Type = Gateway
Platform Management Addresses:
        1.1.1.1
```

指定された VSAN のプラットフォームのリスト

次の例は、指定された VSAN のプラットフォームのリストを表示します。

```
switch# show fcs platform vsan 1
Platform List for VSAN: 1
Platform-Names
--------------
SamplePlatform
[Total 1 Platforms in Fabric]
```

指定された VSAN のスイッチポートのリスト

次の例は、指定された VSAN のスイッチポートのリストを表示します。

```
switch# show fcs port vsan 24
Port List in VSAN: 24
                -- IE WWN: 20:18:00:05:30:00:16:df  --
------------------------------------------------------------------------
Port-WWN                 Type      Module-Type            Tx-Type
------------------------------------------------------------------------
20:41:00:05:30:00:16:de  TE_Port   SFP with Serial Id      Shortwave Laser
20:51:00:05:30:00:16:de  TE_Port   SFP with Serial Id      Shortwave Laser
[Total 2 switch-ports in IE]
                -- IE WWN: 20:18:00:05:30:00:20:df  --
------------------------------------------------------------------------
Port-WWN                 Type      Module-Type            Tx-Type
------------------------------------------------------------------------
20:01:00:05:30:00:20:de  TE_Port   SFP with Serial Id      Shortwave Laser
20:0a:00:05:30:00:20:de  TE_Port   SFP with Serial Id      Shortwave Laser
[Total 2 switch-ports in IE]
```

指定された pWWN のポート情報

次の例は、指定された pWWN のポート情報を表示します。

```
switch# show fcs port pwwn 20:51:00:05:30:00:16:de vsan 24
Port Attributes
---------------
Port Type = TE_Port
Port Number = 0x1090000
Attached-Port-WWNs:
        20:0a:00:05:30:00:20:de
Port State = Online
```

FCS 統計

次の例は、FCS 統計を表示します。

```
switch# show fcs statistics
FCS Statistics for VSAN: 1
---------------------------
FCS Rx Get Reqs   :2
FCS Tx Get Reqs   :7
FCS Rx Reg Reqs   :0
FCS Tx Reg Reqs   :0
FCS Rx Dereg Reqs :0
FCS Tx Dereg Reqs :0
FCS Rx RSCNs      :0
...
FCS Statistics for VSAN: 30
---------------------------
FCS Rx Get Reqs   :2
FCS Tx Get Reqs   :2
FCS Rx Reg Reqs   :0
FCS Tx Reg Reqs   :0
FCS Rx Dereg Reqs :0
FCS Tx Dereg Reqs :0
FCS Rx RSCNs      :0
FCS Tx RSCNs      :0
...
```

各 VSAN のプラットフォーム設定

次の例は、各 VSAN のプラットフォーム設定を表示します。

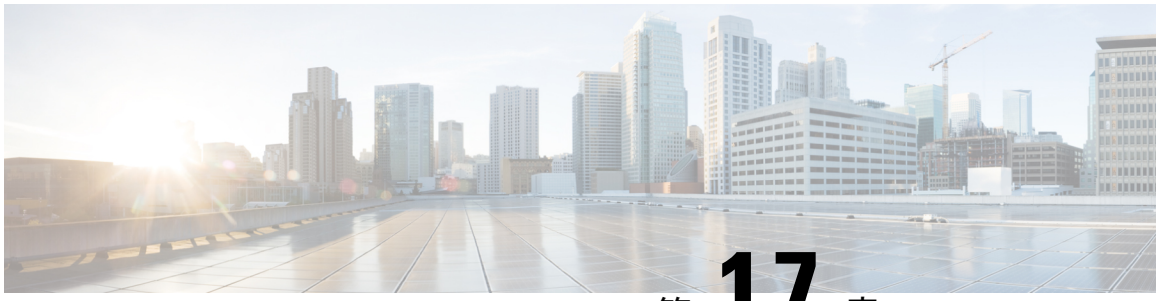
```
switch# show fcs vsan
------------------------------
VSAN    Plat Check fabric-wide
------------------------------
0001    Yes
0010    No
0020    No
0021    No
0030    No
```

その他の参考資料

FCS の実装に関する詳細情報については、次の項を参照してください。

Table 41: MIB

MIB	MIB のリンク
CISCO-FCS-MIB	MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 http://www.cisco.com/en/US/products/ps5989/prod_technical_reference_list.html



第 17 章

ファブリック モジュール エラー モニタリング

この章では、ファブリック モジュール エラー モニタリング（XbarErrorMonitor）とその構成方法について説明します。

- ファブリック モジュール エラー モニタリングの機能履歴 （365 ページ）
- ファブリック モジュール エラー モニタリングについて （365 ページ）
- ファブリック モジュール エラー モニタリングのガイドラインおよび制限事項 （366 ページ）
- ファブリック モジュール エラー モニタリングの構成 （367 ページ）
- 設定例 （368 ページ）

ファブリック モジュール エラー モニタリングの機能履歴

機能名	リリース	機能情報
ファブリック モジュール エラー モニタリング（XbarErrorMonitor）	9.3(1)	この機能が導入されます。

ファブリック モジュール エラー モニタリングについて

Cisco MDS のファブリック モジュールは、一般に Xbar と呼ばれます。これらのファブリック モジュールには、ファブリック 1 とファブリック 3 の 2 つのバージョンがあります。CRC エラーのある FC ポートが受信したフレームはドロップされ、それ以上転送されません。フレームがコンポーネントからコンポーネントへ、およびモジュールからモジュールへ移動すると、エラーが発生する可能性があります。フレームは、スイッチング パスに沿ったいくつかの場所で CRC チェックされます。フレームがエラーとして検出されると、できるだけ早く破棄されます。

既存の「内部 CRC 検出および分離」機能は、これらの内部 CRC エラーが発生した場合に検出し、修正措置を講じることができます。ただし、ファブリック モジュールでは、厳密には内部 CRC エラーではない他のエラーが発生する可能性があります。Cisco MDS リリース 9.3(1) で導入されたファブリック モジュール エラー モニタリング（XbarErrorMonitor）機能は、「内部 CRC 検出および分離」機能を補完し、これらのエラーの存在を検出して修正アクションを実行するように設計されています。この機能により、ネットワーク セットアップで I/O 問題を引き起こす可能性のあるファブリック 1 およびファブリック 3 モジュールのある特定のハードウェア カウンタをモニタできます。

XbarErrorMonitor は、MDS スケジューラ機能を利用してこれらの内部エラーをチェックする Python スクリプトです。これは、スケジューラに定期的に実行させることで機能します（デフォルトは 120 秒）。実行するたびに、「show hardware internal errors」コマンドを発行し、スイッチに存在する特定のファブリック モジュール タイプに対してモニタされた特定のカウンタを記録します。その後、一定時間（デフォルトは 30 秒）スリープ（一時停止）し、別の「ハードウェア内部エラーの表示」コマンドを発行して、特定の各カウンタを前の値と比較します。モニタ対象のカウンタの 1 つ以上がしきい値（デフォルトは 50）以上である場合、指定されたアクション（デフォルトは「ログのみ」）が実行されます。

ファブリック モジュール エラー モニタリングのガイドラインおよび制限事項

- この機能は、Cisco MDS 9700 シリーズ スイッチのみをサポートします。
- この機能は、Cisco MDS リリース 9.3(1) にアップグレードすると自動的に有効になります。この機能にはデフォルト値があります。スケジュール間隔は 120 秒、スリープ時間は 30 秒、カウンタのしきい値は 50、デフォルトのアクションはログのみです。
- この機能は、スイッチ内の次のエラー カウンタをモニタします。
  - ファブリック 1 モジュール カウンタ
    - INTERNAL_ERROR_CNT
    - HIGH_XT_DROP_CNT
    - SAC_XTIMEOUT_INTR_HI
  - ファブリック 3 モジュール カウンタ
    - ポート宛てにドロップされたパケット
    - 受信ポートでパケットがドロップする
    - ダブルビット ECC エラー

（注） これらのカウンタは、**show hardware internal errors** コマンドを使用して表示できます（ゼロ以外の場合）。

- デフォルトでは、この機能はファブリック モジュール 1 およびファブリック モジュール 3 のカウンタを 2 分ごとにモニタします。カウンタがデフォルトのしきい値である 50 を超えると、それぞれのスパインに障害があることを示すsyslogが表示されます。次に例を示します。

```
2022 Jun 28 14:10:38 sw9706-89 %USER-2-SYSTEM_MSG:
xbarErrorMonitor: counter threshold exceeded for xbar 3 for
counter packets dropped destined to port. (Before: 0, After: 128, Delta 128).
```

- XbarErrorMonitor が特定のパラメータ セットで開始された場合は、パラメータを変更するときに、すべての既定以外のパラメータが指定されていることを確認します。次に例を示します。

```
xbarErrorMonitor -si 180 enable
xbarErrorMonitor -a log-and-out-of-service enable
```

- xbarErrorMonitor log-and-out-of-service enable コマンドを使用すると、si パラメータが渡されないため、スケジューリング間隔はデフォルトの 120 秒に戻ります。
- xbarErrorMonitor を有効にすると、xbarErrorMonitor_job という名前のスケジューラ ジョブと XbarErrorMonitor_Schedule という名前のスケジューラ スケジュールが作成されます。これらは削除しないでください。削除すると、xbarErrorMonitor が機能しなくなります。

ファブリック モジュール エラー モニタリングの構成

手順

	コマンドまたはアクション	目的
ステップ 1	switch# xbarErrorMonitor enable	スイッチの XbarErrorMonitor 機能を有効にします。
ステップ 2	switch# xbarErrorMonitor disable	（オプション）XbarErrorMonitor 機能を無効にします。
ステップ 3	switch# xbarErrorMonitor -h	エラー モニタリング パラメータを変更します。 **（注）** ヘルプ オプションには、選択したパラメータに基づいてモニタリングを実行できるように変更できるパラメータのリストが表示されます。このオプションの使用例については、「構成例」セクションを参照してください。
ステップ 4	switch# xbarErrorMonitor show	xbar エラー モニタリングのステータスを確認します。

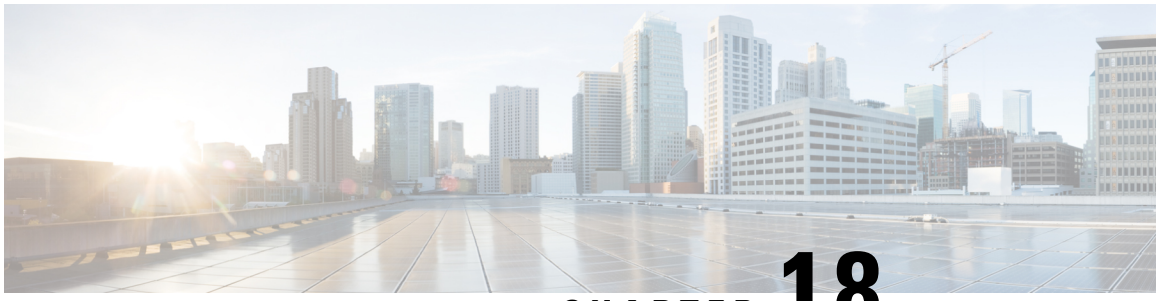
設定例

次の例は、XbarErrorMonitor 機能のステータスを確認する方法を示しています。

```
switch# xbarErrorMonitor show
xbarErrorMonitor 1.0

Status: Enabled
Schedular Interval: 120
Sleep Time: 30
Counter Threshold: 50
Action: log-only
Counters Monitored:
  packets dropped destined to port
  packets drop on receive port
  double bit ecc error
```

次の例は、エラー モニタリング パラメータを変更する方法を示しています。

```
Switch(config)# xbarErrorMonitor --help
usage: xbarErrorMonitor [-h] [-v] [-si] [-st] [-t] [-a]
                        {enable,disable,show,forScheduler} ...

Enable/Disable xbar error monitor on the switch

positional arguments:
  {enable,disable,show,forScheduler}
    enable              Enable xbarErrorMonitor feature
    disable             Disable xbarErrorMonitor feature
    show                Show current status of xbarErrorMonitor feature
    forScheduler        This option is for schedular only, DO NOT USE THIS
                        MANUALLY

optional arguments:
  -h, --help            show this help message and exit
  -v, --version         show program's version number and exit
  -si , --schedular-interval
                        scheduler interval time, value should be between 120s
                        to 3600s. Default value is 120s.
  -st , --sleep-time    sleep time between getting error counters, value
                        should be between 30s to 90s. Default value is 30s.
  -t , --counter-threshold
                        counter threshold value beyond which action will be
                        taken, value should be between 50 to 500. Default
                        value is 50.
  -a , --action         action that needs to be taken when counter breaches
                  the threshold value. 'log-only': Shows only a syslog,
                        'log-and-out-of-service': Shows a syslog as well as
                        puts the xbar out-of-service. Default action is log-
                        only.
```



CHAPTER 18

Port Pacing の構成

この章では、ポート ペーサーを構成する方法について説明します。

- Port Pacing についての情報, on page 369
- 注意事項と制約事項, on page 369
- Port Pacer の構成, on page 370

Port Pacing についての情報

ファイバ チャネル Port Pacer は、Cisco MDS 9513 および MDS 9710 スイッチでのみサポートされています。Port Pacer は、ポートが段階的に起動されるように、同時に起動するモード F ポートの数を調整するように設計されています。

F ポートの起動中に、Port Pacer は F ポート サーバーにポートが起動していることを通知します。Port Pacer は、F ポート サーバーがそのポートで FLOGI と FDISC を受信するのを待ちます。Port Pacer は、同時ポート数のポートを同時に起動しようとします。ただし、F ポート サーバーがそのポートの FLOGI および FDISC を受信したことを Port Pacer に通知した後、Port Pacer はポートの起動を完了し、ポート ステータスを up として更新します。その後、次のポートの起動を試みます。

デフォルトでは、F ポート ペーシングは無効になっています。ポート ペーシングを有効にすると、ポートで受信された FLOGI または FDISC の数が追跡されます。すべての FLOGI または FDISC が正常にログインした場合（これには数秒かかります）、別の一連の同時ポートが起動します。常に、FLOGI は、構成された同時ポートに対してのみ処理されます。この機能は、ホストで FLOGI の再試行がゼロの場合に有用です。

注意事項と制約事項

以下は、ポート ペーサーを有効にするための推奨されるガイドラインと要件です。

- ポート ペーシング構成は、管理ポート モード F でのみサポートされます。
- Concurrent-ports port-number は、トポロジに応じて設定する必要があり、この値を同時に起動できる F ポートの数に設定する必要があります。

Port Pacer の構成

ポート ペーシングの有効化

Note ポート ペーシング構成は、管理ポート モード F でのみサポートされます。

ポート ペーシング コマンドは、すべての管理ポート モード F ポートに適用できるシステム全体のコマンドです。

ポート ペーサーを有効にするには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch# (config)# **system port pacer mode F interface-login-threshold 10 concurrent-ports 1**

同時実行数が 1 でしきい値が 10 に設定されている F ポートのペーサー モードを有効にします。

interface-login-threshold は、ポートで予想される FLOGI または FDISC の数を指定します。

concurrent-ports は、同時に起動できる管理ポート モード F ポートの数を指定します。

Port Pacing 構成の表示

ポート ペーシング構成を無効にするには、次の手順に従います。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

ステップ 2 switch# (config)# **no system port pacer mode F interface-login-threshold 10 concurrent-ports 1**

F ポートのペーサー モードを無効にします。

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。