Cisco Nexus 7000 シリーズ NX-OS システム管理コンフィギュレーション ガイド

初版：2013 年 11 月 20 日

最終更新：2016 年 05 月 12 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/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次

はじめに xxvii

対象読者 xxvii

表記法 xxvii

Cisco Nexus 7000 シリーズ NX-OS ソフトウェアの関連資料 xxix

マニュアルに関するフィードバック xxxi

マニュアルの入手方法およびテクニカル サポート xxxi

新機能および変更された機能に関する情報 1

新機能および変更された機能に関する情報 1

概要 13

Cisco NX-OS デバイス コンフィギュレーション方式 14

CLI または XML 管理インターフェイスによる設定 15

Cisco DCNM または カスタム GUI による設定 15

Cisco Fabric Services 16

ネットワーク タイム プロトコル 16

高精度時間プロトコル 16

Cisco Discovery Protocol 16

システム メッセージ 16

Smart Call Home 16

ロールバック 17

Session Manager 17

スケジューラ 17

SNMP 17

RMON 17

オンライン診断 18

Embedded Event Manager 18

オンボード障害ロギング 18

SPAN 18
ERSPAN 18
LLDP 19
NetFlow 19
FabricPath 19
EEE 19
トラブルシューティング機能 20
CFS の設定 21
機能情報の確認 21
CFS について 22
CFS を使用して設定変更を配信するアプリケーション 22
CFS 配信 22
CFS の配信モード 23
混合ファブリック内での CFS の接続性 24
CFS 結合のサポート 24
ネットワークのロック 25
CFS リージョン 25
ハイ アベイラビリティ 25
CFS のライセンス要件 26
CFS の前提条件 26
CFS の注意事項と制約事項 26
CFS のデフォルト設定 27
CFS 配信の設定 28
アプリケーションの CFS 配信のイネーブル化 28
CFS をイネーブルにして Smart Call Home 設定を配信する 28
CFS をイネーブルにしてデバイス エイリアス設定を配信する 28
CFS をイネーブルにして DPVM 設定を配信する 29
CFS をイネーブルにして FC ドメイン設定を配信する 30
CFS をイネーブルにして FC ポート セキュリティ設定を配信する 31
CFS をイネーブルにして FC タイマー設定を配信する 32
CFS をイネーブルにして IVR 設定を配信する 33
CFS をイネーブルにして NTP 設定を配信する 34
CFS をイネーブルにして RADIUS 設定を配信する 35

CFS をイネーブルにして RSCN 設定を配信する 35
CFS をイネーブルにして TACACS+ 設定を配信する 36
CFS をイネーブルにしてユーザ ロール設定を配信する 37
CFS 配信モードの指定 38
CFSoIP の IP マルチキャスト アドレスの設定 39
CFS リージョンの設定 40
CFS リージョンの作成 40
別の CFS リージョンへのアプリケーションの移動 40
CFS リージョンからのアプリケーションの削除 41
CFS リージョンの削除 42
CFS 設定の作成と配信 43
ロック済みセッションのクリア 45
CFS 設定の破棄 46
CFS 配信のグローバルなディセーブル化 46
CFS 設定の確認 47
CFS に関する追加情報 48
CFS の機能の履歴 49
NTP の設定 51
機能情報の確認 51
NTP について 52
NTP アソシエーション 52
NTP ブロードキャスト アソシエーション 53
NTP マルチキャスト アソシエーション 53
タイム サーバとしての NTP 53
CFS を使用した NTP の配信 53
クロック マネージャ 53
ハイ アベイラビリティ 54
仮想化のサポート 54
NTP のライセンス要件 54
NTP の前提条件 55
NTP の注意事項と制約事項 55
NTP のデフォルト設定 56

NTP の設定 57
VDC での NTP のイネーブル化またはディセーブル化 57
インターフェイスでの NTP のイネーブル化またはディセーブル化 58
正規の NTP サーバとしてのデバイスの設定 59
NTP サーバおよびピアの設定 59
NTP 認証の設定 61
NTP アクセス制限の設定 63
NTP ソース IP アドレスの設定 64
NTP ソース インターフェイスの設定 65
NTP ブロードキャスト サーバの設定 65
NTP マルチキャスト サーバの設定 67
NTP マルチキャスト クライアントの設定 68
セカンダリ（非デフォルト）VDC での NTP 設定 69
NTP ロギングの設定 70
NTP 用の CFS 配信のイネーブル化 70
NTP 設定変更のコミット 71
NTP 設定変更の廃棄 72
CFS セッション ロックの解放 72
NTP の設定確認 73
NTP の設定例 73
その他の参考資料 75
関連資料 75
MIB 75
NTP の機能の履歴 75
PTP の設定 79
機能情報の確認 79
PTP について 80
PTP デバイス タイプ 80
PTP プロセス 81
Pong 82
クロック マネージャ 82
PTP のハイ アベイラビリティ 82
仮想化のサポート 83

PTP のライセンス要件 83
PTP の前提条件 83
PTP の注意事項および制約事項 83
PTP のデフォルト設定 84
PTP の設定 85
PTP のグローバルな設定 85
インターフェイスでの PTP の設定 88
PTP 設定の確認 89
PTP の設定例 90
関連資料 91
関連資料 91
MIB 92
PTP の機能の履歴 92
CDP の設定 95
機能情報の確認 95
CDP について 96
VTP 機能のサポート 97
ハイ アベイラビリティ 97
仮想化のサポート 97
CDP のライセンス要件 97
CDP の前提条件 98
CDP の注意事項と制約事項 98
CDP のデフォルト設定 98
CDP の設定 98
CDP のグローバルなイネーブルまたはディセーブル 99
インターフェイス上での CDP のイネーブルまたはディセーブル 99
CDP オプション パラメータの設定 100
CDP コンフィギュレーションの確認 101
CDP のコンフィギュレーション例 102
その他の参考資料 103
関連資料 103
MIB 103
CDP 機能の履歴 103

システム メッセージ ロギングの設定 105
機能情報の確認 105
システム メッセージ ロギングについて 106
Syslog サーバ 106
仮想化のサポート 107
システム メッセージ ロギングのライセンス要件 107
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 107
システム メッセージ ロギングのデフォルト設定 107
システム メッセージ ロギングの設定 108
ターミナル セッションへのシステム メッセージ ロギングの設定 108
ファイルへのシステム メッセージの記録 110
モジュールおよびファシリティ メッセージのロギングの設定 112
syslog サーバの設定 114
Syslog 転送の宛先ポートの設定 115
UNIX または Linux システムでの Syslog サーバの設定 117
ログ ファイルの表示およびクリア 118
システム メッセージ ロギングの設定確認 119
システム メッセージ ロギングのコンフィギュレーション例 119
その他の参考資料 120
関連資料 120
システム メッセージ ロギングの機能の履歴 120
Smart Call Home の設定 123
機能情報の確認 123
Smart Call Home の概要 124
宛先プロファイル 124
Smart Call Home アラート グループ 125
Smart Call Home のメッセージ レベル 128
Smart Call Home の取得 129
CFS を使用した Smart Call Home の配信 130
データベース マージの注意事項 130
ハイ アベイラビリティ 131
仮想化のサポート 131

Smart Call Home のライセンス要件 131
Smart Call Home の前提条件 131
Smart Call Home の注意事項および制約事項 132
Smart Call Home のデフォルト設定 133
Smart Call Home の設定 134
連絡先情報の設定 134
宛先プロファイルの作成 136
宛先プロファイルの変更 137
アラート グループと宛先プロファイルの関連付け 140
アラート グループへの show コマンドの追加 141
電子メール サーバの設定 142
HTTP を使用したメッセージ送信のための VRF 設定 143
HTTP プロキシ サーバの設定 145
定期的なインベントリ通知の設定 146
重複メッセージ抑制のディセーブル化 147
Smart Call Home のイネーブル化またはディセーブル化 148
Smart Call Home 設定のテスト 149
Smart Call Home 設定の確認 150
Smart Call Home の設定例 151
その他の参考資料 152
イベント トリガー 152
メッセージ フォーマット 154
ショート テキスト メッセージ フォーマット 154
共通のイベント メッセージ フィールド 154
アラート グループ メッセージ フィールド 157
リアクティブおよびプロアクティブ イベント メッセージのフィールド 158
インベントリ イベント メッセージのフィールド 158
ユーザが作成したテスト メッセージのフィールド 159
フル テキスト形式での syslog アラート通知の例 159
XML 形式での syslog アラート通知の例 162
その他の参考資料 166
関連資料 166

MIB 166
Smart Call Home の機能の履歴 166
ロールバックの設定 169
機能情報の確認 169
ロールバックについて 170
自動的に生成されるシステム チェックポイント 170
ハイ アベイラビリティ 171
仮想化のサポート 171
ロールバックのライセンス要件 172
ロールバックの前提条件 172
ロールバックの注意事項と制約事項 172
ロールバックのデフォルト設定 174
ロールバックの設定 174
チェックポイントの作成 174
ロールバックの実装 175
ロールバック コンフィギュレーションの確認 176
ロールバックのコンフィギュレーション例 177
その他の参考資料 177
関連資料 177
ロールバックの機能の履歴 177
Session Manager の設定 179
機能情報の確認 179
Session Manager について 180
ハイ アベイラビリティ 180
仮想化のサポート 180
Session Manager のライセンス要件 180
Session Manager の前提条件 181
Session Manager の注意事項および制約事項 181
Session Manager の設定 181
セッションの作成 181
セッションでの ACL の設定 182
セッションの確認 183

セッションのコミット 183
セッションの保存 184
セッションの廃棄 184
Session Manager 設定の確認 184
Session Manager のコンフィギュレーション例 185
その他の参考資料 185
関連資料 185
Session Manager の機能の履歴 185
スケジューラの設定 187
機能情報の確認 187
スケジューラについて 188
リモート ユーザ認証 188
ログ 189
ハイ アベイラビリティ 189
仮想化のサポート 189
スケジューラのライセンス要件 189
スケジューラの前提条件 189
スケジューラの注意事項および制約事項 190
スケジューラのデフォルト設定 190
スケジューラの設定 190
スケジューラのイネーブル化またはディセーブル化 190
スケジューラ ログ ファイル サイズの定義 191
リモート ユーザ認証の設定 192
ジョブの定義 192
ジョブの削除 193
タイムテーブルの定義 194
スケジューラ ログ ファイルの消去 196
スケジューラの設定確認 196
スケジューラの設定例 196
スケジューラ ジョブの作成 196
スケジューラ ジョブのスケジューリング 197
ジョブ スケジュールの表示 197

スケジューラ ジョブの実行結果の表示 197
関連資料 198
スケジューラの機能の履歴 198
SNMP の設定 199
機能情報の確認 199
SNMP の概要 200
SNMP 機能の概要 200
SNMP 通知 200
SNMPv3 202
SNMPv1、SNMPv2、SNMPv3 のセキュリティ モデルおよびセキュリティ レベル 202
ユーザベースのセキュリティ モデル 204
CLI および SNMP ユーザの同期 204
SNMPv3 サーバの AAA 排他動作 205
グループベースの SNMP アクセス 207
SNMP および EEM 207
マルチインスタンス サポート 207
SNMP のハイ アベイラビリティ 208
SNMP の仮想化サポート 208
SNMP のライセンス要件 208
SNMP の前提条件 209
SNMP の注意事項および制約事項 209
SNMP のデフォルト設定 209
SNMP の設定 209
SNMP ユーザの設定 209
SNMP メッセージ暗号化の適用 210
SNMPv3 ユーザに対する複数のロールの割り当て 211
SNMP コミュニティの作成 212
SNMP 要求のフィルタリング 212
ロケーションに基づく SNMPv3 ユーザの認証 213
SNMP 通知レシーバの設定 214
SNMP 通知用の発信元 インターフェイスの設定 216

通知対象ユーザの設定 217
VRF を使用する SNMP 通知レシーバの設定 218
帯域内ポートを使用してトラップを送信するための SNMP 設定 219
SNMP 通知のイネーブル化 220
インターフェイスでのリンク通知のディセーブル化 234
インターフェイスの SNMP ifIndex の表示 234
TCP による SNMP のワンタイム認証のイネーブル化 235
SNMP デバイスの連絡先およびロケーション情報の割り当て 235
コンテキストとネットワーク エンティティ間のマッピング設定 236
SNMP のディセーブル化 238
AAA 同期時間の変更 238
SNMP の設定の確認 239
SNMP の設定例 240
その他の参考資料 242
関連資料 242
RFC 242
MIB 242
SNMP の機能の履歴 243
RMON の設定 245
機能情報の確認 245
RMON について 246
RMON アラーム 246
RMON イベント 247
RMON のハイ アベイラビリティ 247
RMON の仮想化サポート 247
RMON のライセンス要件 247
RMON の前提条件 248
RMON の注意事項と制約事項 248
RMON のデフォルト設定 248
RMON の設定 248
RMON アラームの設定 249
RMON イベントの設定 250
RMON 設定の確認 251

RMON の設定例 251
その他の参考資料 252
関連資料 252
MIB 252
RMON の機能の履歴 252
オンライン診断の設定 253
機能情報の確認 253
オンライン診断について 254
オンライン診断の概要 254
ブートアップ診断 254
ランタイムまたはヘルス モニタリング診断 256
指定のヘルス モニタリング診断のリカバリ アクション 261
オンデマンド診断 262
ハイ アベイラビリティ 262
仮想化のサポート 263
オンライン診断機能のライセンス要件 263
オンライン診断の注意事項と制約事項 263
オンライン診断のデフォルト設定 264
オンライン診断の設定 264
起動診断レベルの設定 264
診断テストのアクティブ化 265
診断テストを非アクティブとして設定する場合 267
修正アクションの設定 267
オンデマンド診断テストの開始または中止 268
診断結果の消去 269
診断結果のシミュレーション 270
オンライン診断設定の確認 270
オンライン診断のコンフィギュレーション例 272
その他の参考資料 272
関連資料 272
オンライン診断の「機能の履歴」表 272
Embedded Event Manager の設定 275

機能情報の確認 275
EEM について 276
ポリシー 276
イベント文 277
アクション ステートメント 278
VSH スクリプト ポリシー 279
環境変数 279
EEM イベント相関 280
ハイ アベイラビリティ 280
仮想化のサポート 280
EEM のライセンス要件 280
EEM の前提条件 280
EEM の注意事項と制約事項 281
EEM のデフォルト設定 281
EEM の設定 282
環境変数の定義 282
CLI によるユーザ ポリシーの定義 283
イベント文の設定 284
アクション文の設定 291
VSH スクリプトによるポリシーの定義 300
VSH スクリプト ポリシーの登録およびアクティブ化 301
EEM ポリシーのスケジューリング 301
ポリシーの上書き 302
メモリのしきい値の設定 304
EEM パブリッシャとしての syslog の設定 305
EEM 設定の確認 307
EEM のコンフィギュレーション例 308
関連資料 309
EEM の機能の履歴 309
オンボード障害ロギングの設定 311
機能情報の確認 311
OBFL の概要 312

仮想化のサポート 312
OBFL のライセンス要件 312
OBFL の前提条件 313
OBFL の注意事項と制約事項 313
OBFL のデフォルト設定 313
OBFL の設定 313
OBFL コンフィギュレーションの確認 315
OBFL のコンフィギュレーション例 317
その他の参考資料 317
関連資料 317
OBFL の機能の履歴 317
SPAN の設定 319
機能情報の確認 319
SPAN の概要 320
SPAN ソース 320
送信元ポートの特性 320
SPAN 宛先 321
宛先ポートの特性 321
SPAN セッション 321
拡張 SPAN セッション 322
SPAN セッションあたり 4K の VLAN 322
ルール ベース SPAN 323
例外 SPAN 324
仮想 SPAN セッション 325
Network Analysis Module; ネットワーク解析モジュール 325
ハイ アベイラビリティ 326
仮想化のサポート 326
SPAN のライセンス要件 326
SPAN の前提条件 326
SPAN の注意事項および制約事項 326
SPAN の一般的な注意事項と制限事項 326
F1 シリーズ モジュールの注意事項と制約事項 329

F2/F2e シリーズ モジュールの注意事項と制約事項 331
F3 シリーズ モジュールの注意事項と制約事項 332
M1/M1XL シリーズ モジュールの注意事項と制約事項 333
M2/M2XL シリーズ モジュールの注意事項と制約事項 334
M3 シリーズ モジュールの注意事項と制約事項 335
SPAN のデフォルト設定 335
SPAN の設定 335
SPAN セッションの設定 336
F2 シリーズ モジュールでの複数宛先 SPAN の設定 340
SPAN 宛先ポートでの複数 SPAN セッションの設定 343
仮想 SPAN セッションの設定 344
RSPAN VLAN の設定 347
SPAN セッションのシャットダウンまたは再開 348
SPAN セッションごとの MTU の切り捨ての設定 349
各 SPAN セッションのソース レート制限の設定 351
各 SPAN セッションのサンプリングの設定 353
複雑ルール ベース SPAN 354
フィルタの作成 354
フィルタ リストの作成 355
モニタリング セッションへのフィルタ リストの関連付け 356
ルールがイネーブルなセッションの設定 357
SPAN セッションのマルチキャスト ベスト エフォート モードの設定 358
ルール ベース SPAN の設定 360
例外 SPAN の設定 364
FabricPath および VNTAG ヘッダーの削除 366
グローバルなヘッダーの削除 367
ポートごとのヘッダーの削除 367
SPAN の設定確認 368
SPAN のコンフィギュレーション例 368
SPAN セッションのコンフィギュレーション例 368
拡張 SPAN モニタ セッション内のすべての VLAN とポートをモニタする設定例 369
単一方向 SPAN セッションの設定例 370

仮想 SPAN セッションの設定例 370
プライベート VLAN 送信元の SPAN セッションの設定例 371
SPAN の MTU 切り捨ておよび SPAN サンプリングの設定例 372
ルール ベース SPAN の設定例 372
例外 SPAN の設定例 372
関連資料 373
SPAN の機能の履歴 373
ERSPAN の設定 377
機能情報の確認 377
ERSPAN について 378
ERSPAN タイプ 378
ERSPAN 送信元 378
ERSPAN 宛先 379
ERSPAN セッション 379
拡張 ERSPAN セッション 380
ERSPAN セッションあたり 4K の VLAN 380
ルール ベースの ERSPAN 381
例外 ERSPAN 382
Network Analysis Module; ネットワーク解析モジュール 383
ハイ アベイラビリティ 383
仮想化のサポート 383
ERSPAN のライセンス要件 383
ERSPAN の前提条件 383
ERSPAN の注意事項および制約事項 384
デフォルト設定 389
ERSPAN の設定 389
ERSPAN 送信元セッションの設定 389
ERSPAN 宛先セッションの設定 393
ERSPAN セッションのシャットダウンまたはアクティブ化 395
ERSPAN セッションごとの MTU の切り捨ての設定 397
各 ERSPAN セッションのソース レート制限の設定 398
各 ERSPAN セッションのサンプリングの設定 400

ERSPAN セッションのマルチキャスト ベスト エフォート モードの設定 401
ルール ベース ERSPAN の設定 402
例外 ERSPAN の設定 408
ERSPAN 設定の確認 410
ERSPAN の設定例 410
ERSPAN タイプ III 送信元セッションの設定例 410
拡張 ERSPAN モニタ セッション内のすべての VLAN とポートをモニタする設定例 411
単一方向 ERSPAN セッションの設定例 411
ERSPAN 宛先セッションの設定例 412
ERSPAN ACL の設定例 412
ERSPAN の MTU 切り捨ておよび ERSPAN サンプリングの設定例 412
マルチキャスト ベスト エフォート モードを使用した ERSPAN の設定例 413
ルール ベースの ERSPAN の設定例 413
例外 ERSPAN の設定例 413
関連資料 413
ERSPAN の機能の履歴 414
LLDP の設定 417
機能情報の確認 417
LLDP について 418
DCBXP について 418
ハイ アベイラビリティ 419
仮想化のサポート 419
LLDP のライセンス要件 420
LLDP に関する注意事項および制約事項 420
LLDP のデフォルト設定 420
LLDP の設定 421
LLDP のグローバルなイネーブルまたはディセーブル 421
インターフェイス上での LLDP のイネーブルまたはディセーブル 422
LLDP オプション パラメータの設定 423
LLDP コンフィギュレーションの確認 424
LLDP のコンフィギュレーション例 425

関連資料 425
LLDP の機能の履歴 426
NetFlow の設定 427
機能情報の確認 427
NetFlow 428
NetFlow の概要 428
フロー レコード 429
フロー エクスポータ 429
エクスポート フォーマット 430
フロー モニタ 431
サンプラー 431
CoPP インターフェイスでの NetFlow サポート 432
Network Analysis Module; ネットワーク解析モジュール 433
ハイ アベイラビリティ 433
仮想化のサポート 433
NetFlow のライセンス要件 433
NetFlow の前提条件 434
NetFlow に関する注意事項および制約事項 434
NetFlow のデフォルト設定 437
NetFlow の設定 438
NetFlow 機能のイネーブル 438
フロー レコードの作成 439
match パラメータの指定 440
collect パラメータの指定 441
フロー エクスポータの作成 442
フロー モニタの作成 444
サンプラーの作成 445
インターフェイスへのフロー モニタの適用 446
CoPP インターフェイスでの NetFlow サポートの設定 447
VLAN 上でのブリッジ型 NetFlow の設定 448
レイヤ 2 NetFlow の設定 449
NetFlow タイムアウトの設定 451

NetFlow 設定の確認 451
NetFlow のモニタリング 452
NetFlow の設定例 452
NetFlow CoPP インターフェイス サポートの確認例 453
関連資料 454
NetFlow 機能の履歴 454
EEE の設定 457
機能情報の確認 457
EEE について 458
EEE 458
EEE LPI のスリープしきい値 458
EEE 遅延 458
仮想化のサポート 458
EEE のライセンス要件 458
EEE の前提条件 459
注意事項と制約事項 459
デフォルト設定 459
EEE の設定 460
EEE のイネーブル化またはディセーブル化 460
EEE LPI スリープしきい値の設定 461
EEE 設定の確認 461
EEE の設定例 463
関連資料 463
EEE の機能の履歴 463
GIR の設定（Cisco NX-OS Release 7.3(0)D1(1)） 465
GIR について 465
メンテナンス プロファイル 467
計画外メンテナンス 468
メンテナンス モード タイマー 469
Snapshot 469
FIB 保留の抑制 471
GIR の注意事項と制約事項 471

カスタム メンテナンス モード プロファイルおよびカスタム通常モード プロファイルの設定 472
スナップショットの作成 473
スナップショットへの show コマンドの追加 474
スナップショット セクションのダンプ 476
メンテナンス モードの開始 477
通常モードへの復帰 481
メンテナンス プロファイルの削除 482
GIR の設定例 482
GIR の確認 488
プロトコル レベルでの GIR の確認 489
GIR の機能の履歴 491
GIR の設定（Cisco NX-OS Release 7.2(0)D1(1)） 493
GIR について 493
GIR の注意事項と制約事項 494
GIR サイクルの実行 494
通常モード プロファイル ファイルの設定 495
スナップショットの作成 496
メンテナンス モードの開始 497
通常モードへの復帰 498
メンテナンス モード プロファイル ファイルの設定 498
GIR の確認 500
ソフトウェア メンテナンス アップグレードの実行 503
SMU の前提条件 503
SMU の注意事項と制約事項 504
ソフトウェア メンテナンス アップグレードの実行に関する情報 505
SMU の概要 505
パッケージ管理 506
パッケージのアクティブ化と非アクティブ化の影響 506
Cisco NX-OS のソフトウェア メンテナンス アップグレードの実行 507
パッケージ インストールの準備 507
Cisco.com からの SMU パッケージ ファイルのダウンロード 509

ローカル ストレージ デバイスまたはネットワーク サーバへのパッケージ ファイルのコピー 509
パッケージの追加とアクティブ化 512
アクティブなパッケージ セットのコミット 514
パッケージの非アクティブ化と削除 515
インストール ログ情報の表示 517
次の作業 519
その他の参考資料 520
関連資料 520
ソフトウェア メンテナンス アップグレードを実行するための機能情報 521
CLI コマンドのネットワーク設定形式への変換 523
機能情報の確認 523
XMLIN について 524
XMLIN のライセンス要件 524
XMLIN ツールのインストールおよび使用 524
show コマンド出力の XML への変換 525
XMLIN の設定例 526
関連資料 528
XMLIN の機能の履歴 528
Cisco NX-OS システム管理でサポートされている IETF RFC 529
Cisco NX-OS システム管理でサポートされている IETF RFC 529
Embedded Event Manager システム イベントおよびコンフィギュレーション例 531
EEM システム ポリシー 531
EEM イベント 534
EEM ポリシーのコンフィギュレーション例 536
CLI イベントのコンフィギュレーション例 536
インターフェイス シャットダウンのモニタリング 536
モジュール パワーダウンのモニタリング 536
ロールバックを開始するトリガーの追加 536
メジャーしきい値を上書き（ディセーブル）するコンフィギュレーション例 537
メジャーしきい値に達したときにシャットダウンを防ぐ方法 537
1 つの不良センサーをディセーブルにする方法 537

複数の不良センサーをディセーブルにする方法 537
モジュール全体の上書き（ディセーブル） 538
複数のモジュールおよびセンサーの上書き（ディセーブル） 538
1 つのセンサーをイネーブルにして、すべてのモジュールの残りのセンサーをすべてディセーブルにする方法 538
複数のセンサーをイネーブルにして、すべてのモジュールの残りのセンサーをすべてディセーブルにする方法 539
1 つのモジュールのすべてのセンサーをイネーブルにして、残りのモジュールのすべてのセンサーをディセーブルにする方法 539
モジュールのセンサーを組み合わせてイネーブルにして、残りのモジュールのすべてのセンサーをディセーブルにする方法 539
ファントレイ取り外しのためのシャットダウンを上書き（ディセーブル）するコンフィギュレーション例 540
1 つまたは複数のファン トレイを取り外すためのシャットダウンの上書き（ディセーブル） 540
指定したファン トレイを取り外すためのシャットダウンの上書き（ディセーブル） 540
指定した複数のファントレイを取り外すためのシャットダウンの上書き（ディセーブル） 541
1 つを除くすべてのファン トレイを取り外すためのシャットダウンの上書き（ディセーブル） 541
ファントレイの指定したセットを除くファントレイを取り外すためのシャットダウンの上書き（ディセーブル） 541
ファン トレイのセットから 1 台を除くすべてのファン トレイを取り外すためのシャットダウンの上書き（ディセーブル） 542
補足ポリシーを作成するコンフィギュレーション例 542
ファン トレイが存在しないイベントの補足ポリシーの作成 542
温度しきい値イベントの補足ポリシーの作成 542
電力のバジェット超過ポリシーのコンフィギュレーション例 543
モジュールのシャットダウン 543
指定された一連のモジュールのシャットダウン 543
シャットダウンするモジュールを選択するコンフィギュレーション例 543

デフォルトでシャットダウンに非上書きモジュールを選択するポリシーの使用 543
シャットダウンに非上書きモジュールを選択するパラメータ置き換えの使用 544
活性挿抜イベントのコンフィギュレーション例 544
ユーザ syslog を生成するコンフィギュレーション例 545
Syslog メッセージをモニタする設定例 545
SNMP 通知のコンフィギュレーション例 545
SNMP OID のポーリングによる EEM イベントの生成 545
イベント ポリシーのイベントへの応答で SNMP 通知を送信 545
ポート トラッキングのコンフィギュレーション例 546
EEM によって EEM ポリシーを登録する設定例 547
Cisco NX-OS システム管理の設定制限事項 551
Cisco NX-OS システム管理の設定制限事項 551

はじめに

ここでは、次の項について説明します。

- 対象読者，xxvii ページ
- 表記法，xxvii ページ
- Cisco Nexus 7000 シリーズ NX-OS ソフトウェアの関連資料，xxix ページ
- マニュアルに関するフィードバック，xxxi ページ
- マニュアルの入手方法およびテクニカル サポート，xxxi ページ

対象読者

このマニュアルは、Cisco Nexus デバイスのコンフィギュレーションおよびメンテナンスを担当するネットワーク管理者を対象としています。

表記法

（注） お客様のニーズを満たすためにドキュメントを更新するという継続的な取り組みの一環として、シスコでは設定タスクの文書化方法を変更しました。そのため、本ドキュメントには、従来とは異なるスタイルでの設定タスクが説明されている部分もあります。ドキュメントに新たに組み込まれるようになったセクションには、以下のセクションが含まれます。

コマンドの説明には、次のような表記法が使用されます。

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。

表記法	説明
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、角カッコ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。
{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、波カッコで囲み、縦棒で区切って示しています。
[x {y | z}]	角カッコまたは波カッコ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。角カッコ内の波カッコと縦棒は、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、screen 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 screen 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。

Cisco Nexus 7000 シリーズ NX-OS ソフトウェアの関連資料

Cisco Nexus 7000 シリーズ NX-OS 全体のマニュアル セットは、次の URL にあります。
http://www.cisco.com/en/us/products/ps9402/tsd_products_support_series_home.html

リリース ノート

リリース ノートは、次の URL から入手できます。
http://www.cisco.com/en/US/products/ps9402/prod_release_notes_list.html

コンフィギュレーション ガイド

これらのマニュアルは、次の URL から入手できます。
http://www.cisco.com/en/US/products/ps9402/products_installation_and_configuration_guides_list.html
このカテゴリのマニュアルには、次が含まれます。

- 『*Cisco Nexus 7000 Series NX-OS Configuration Examples*』
- 『*Cisco Nexus 7000 Series NX-OS FabricPath Configuration Guide*』
- 『*Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide*』
- 『*Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide*』
- 『*Cisco Nexus 7000 Series NX-OS IP SLAs Configuration Guide*』
- 『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide*』
- 『*Cisco Nexus 7000 Series NX-OS LISP Configuration Guide*』
- 『*Cisco Nexus 7000 Series NX-OS MPLS Configuration Guide*』
- 『*Cisco Nexus 7000 Series NX-OS Multicast Routing Configuration Guide*』
- 『*Cisco Nexus 7000 Series NX-OS OTV Configuration Guide*』
- 『*Cisco Nexus 7000 Series NX-OS Quality of Service Configuration Guide*』

- 『*Cisco Nexus 7000 Series NX-OS SAN Switching Guide*』
- 『*Cisco Nexus 7000 Series NX-OS Security Configuration Guide*』
- *Cisco Nexus 7000* シリーズ *NX-OS* システム管理コンフィギュレーション ガイド
- 『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*』
- 『*Cisco Nexus 7000 Series NX-OS Verified Scalability Guide*』
- 『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』
- 『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Quick Start*』
- 『*Cisco Nexus 7000 Series NX-OS OTV Quick Start Guide*』
- 『*Cisco NX-OS FCoE Configuration Guide for Cisco Nexus 7000 and Cisco MDS 9500*』
- 『*Cisco Nexus 2000 Series Fabric Extender Software Configuration Guide*』

コマンド リファレンス

これらのマニュアルは、次の URL から入手できます。

http://www.cisco.com/en/US/products/ps9402/prod_command_reference_list.html

このカテゴリのマニュアルには、次が含まれます。

- 『*Cisco Nexus 7000 Series NX-OS Command Reference Master Index*』
- 『*Cisco Nexus 7000 Series NX-OS FabricPath Command Reference*』
- 『*Cisco Nexus 7000 Series NX-OS Fundamentals Command Reference*』
- 『*Cisco Nexus 7000 Series NX-OS High Availability Command Reference*』
- 『*Cisco Nexus 7000 Series NX-OS Interfaces Command Reference*』
- 『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference*』
- 『*Cisco Nexus 7000 Series NX-OS LISP Command Reference*』
- 『*Cisco Nexus 7000 Series NX-OS MPLS Configuration Guide*』
- 『*Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference*』
- 『*Cisco Nexus 7000 Series NX-OS OTV Command Reference*』
- 『*Cisco Nexus 7000 Series NX-OS Quality of Service Command Reference*』
- 『*Cisco Nexus 7000 Series NX-OS SAN Switching Command Reference*』
- 『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』
- 『*Cisco Nexus 7000 Series NX-OS System Management Command Reference*』
- 『*Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference*』
- 『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Command Reference*』

- 『*Cisco NX-OS FCoE Command Reference for Cisco Nexus 7000 and Cisco MDS 9500*』

その他のソフトウェアのマニュアル

これらのマニュアルは、以下のランディング ページから検索できます。

http://www.cisco.com/en/us/products/ps9402/tsd_products_support_series_home.html

- 『*Cisco Nexus 7000 Series NX-OS MIB Quick Reference*』
- 『*Cisco Nexus 7000 Series NX-OS Software Upgrade and Downgrade Guide*』
- 『*Cisco Nexus 7000 Series NX-OS Troubleshooting Guide*』
- 『*Cisco NX-OS Licensing Guide*』
- 『*Cisco NX-OS System Messages Reference*』
- 『*Cisco NX-OS XML Interface User Guide*』

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、HTML ドキュメント内のフィードバック フォームよりご連絡ください。ciscodfa-docfeedback@cisco.com。

ご協力をよろしくお願いいたします。

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手、Cisco Bug Search Tool（BST）の使用、サービス要求の送信、追加情報の収集の詳細については、『What's New in Cisco Product Documentation』を参照してください。

新しく作成された、または改訂されたシスコのテクニカル コンテンツをお手元に直接送信するには、『What's New in Cisco Product Documentation』RSS フィードをご購読ください。RSS フィードは無料のサービスです。

第 1 章

新機能および変更された機能に関する情報

この章では、『*Cisco Nexus 7000* シリーズ *NX-OS* システム管理コンフィギュレーション ガイド リリース *6.x*』に記載されている新機能および変更された機能に関するリリース固有の情報について説明します。

- 新機能および変更された機能に関する情報，1 ページ

新機能および変更された機能に関する情報

次の表に、このマニュアルの新機能および変更された機能を要約し、各機能がサポートされているリリースを示します。ご使用のソフトウェア リリースで、本書で説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。

機能	説明	変更されたリリース	参照先
PTP	PTP は M3 モジュールをサポートしません。	7.3(0)DX(1)	第 5 章「PTP の設定」
オンライン診断（GOLD）	M3 モジュールのサポートが追加されました。	7.3(0)DX(1)	第 14 章「オンライン診断の設定」
SPAN	M3 モジュールのサポートが追加されました。	7.3(0)DX(1)	第 17 章「SPAN の設定」
ERSPAN	M3 モジュールのサポートが追加されました。	7.3(0)DX(1)	第 18 章「ERSPAN の設定」

新機能および変更された機能に関する情報

機能	説明	変更されたリリース	参照先
NetFlow	M3 モジュールのサポートが追加されました。	7.3(0)DX(1)	第 20 章「NetFlow の設定」
CoPP インターフェイスでの NetFlow サポート	CoPP インターフェイスでの NetFlow サポート機能が追加されました。	7.3(0)D1(1)	第 5 章「PTP の設定」
SPAN セッションあたり 4K の VLAN	SPAN セッションあたり 4K の VLAN のサポートが追加されました。	7.3(0)D1(1)	第 17 章「SPAN の設定」
ERSPAN セッションあたり 4K の VLAN	ERSPAN セッションあたり 4K の VLAN のサポートが追加されました。	7.3(0)D1(1)	第 18 章「ERSPAN の設定」
NTP 認証キーの長さの拡張	NTP 認証キーの長さが、15 文字から 32 文字の英数字に増加しました。	7.3(0)D1(1)	第 4 章「NTP の設定」
GIR の設定	Cisco NX-OS Release 7.3(0)D1(1) 以降では、GIR のデフォルト モードは isolate です。計画外メンテナンス、メンテナンス モード タイマー、FIB 保留の抑制、スナップショットへの Show コマンドの追加、およびスナップショット セクションのダンプをサポートします。	7.3(0)D1(1)	第 22 章「GIR の設定（Cisco NX-OS Release 7.3(0)D1(1)）」
F3 モジュールでの出力 NetFlow のサポート	F3 モジュールで出力 NetFlow がサポートされます。	7.2(0)D1(1)	第 20 章「NetFlow の設定」
F2、F2e、F3 サブインターフェイスでの NetFlow のサポート	F2、F2e、F3 サブインターフェイスで NetFlow がサポートされます。	7.2(0)D1(1)	第 20 章「NetFlow の設定」
EEM アクション文とスケジューリング文	条件文、文字列、および算術演算で EEM アプレットをプログラムする、アクション ベースのプログラマビリティ。	7.2(0)D1(1)	第 15 章「Embedded Event Manager の設定」
NetFlow	F3 シリーズ モジュールのパケット処理率を 50000 pps に強化しました。	7.2(0)D1(1)	第 20 章「NetFlow の設定」

新機能および変更された機能に関する情報

機能	説明	変更されたリリース	参照先
オンライン診断（GOLD）	オンライン診断のサポートが追加されました。	7.2(0)D1(1)	第 14 章「オンライン診断の設定」
システム メッセージ ロギング	システム メッセージ ログ内で、物理的イーサネット インターフェイスおよびサブインターフェイスに対して説明を追加する機能が追加されました。	7.2(0)D1(1)	第 7 章「システム メッセージ ロギングの設定」
分離およびメンテナンス モードの機能拡張	デバッグやアップグレードを実行できるよう、スイッチを正常に取り出し、ネットワークから分離する機能が提供されています。スイッチは、通常のスイッチング パスから除外され、メンテナンス モードに置かれます。スイッチのメンテナンスが完了したら、スイッチをフル動作モードに設定できます。	7.2(0)D1(1)	第 23 章「メンテナンス モードの設定」
SPAN	SPAN パケットから FabricPath および VLAN タグ ヘッダーを削除するサポートが追加されました。	6.2(10)	第 17 章「SPAN の設定」
オンライン診断（GOLD）	• 中断を伴わないヘルス モニタリング テストとして、InternalPortLoopback テストが追加されました。 • PortLoopback テストに、N77-F348XP-23 モジュールのサポートが追加されました。	6.2(10)	第 14 章「オンライン診断の設定」
CISCO-BGP-MIBv2 のサポート	**cbgp2** キーワードが **snmp-server enable traps** コマンドに追加されました。	6.2(8)	第 12 章「SNMP の設定」
オンライン診断（GOLD）	特定のランタイム診断テストに対してリカバリ アクションを設定する機能が追加されました。	6.2(8)	第 14 章「オンライン診断の設定」

新機能および変更された機能に関する情報

機能	説明	変更されたリリース	参照先
ERSPAN	F2 および F2e シリーズ モジュールの ERSPAN 宛先セッションのサポートが追加されました。	6.2(2)	第 18 章「ERSPAN の設定」
ERSPAN	ERSPAN データ ソースに対する NAM サポートが追加されました。	6.2(2)	第 18 章「ERSPAN の設定」
ERSPAN	拡張 ERSPAN のサポートが追加されました。	6.2(2)	第 18 章「ERSPAN の設定」
ERSPAN	ルール ベースの ERSPAN のサポートが追加されました。	6.2(2)	第 18 章「ERSPAN の設定」
ERSPAN	例外 ERSPAN のサポートが追加されました。	6.2(2)	第 18 章「ERSPAN の設定」
ERSPAN	F2 または F2e シリーズ モジュールで ERSPAN の終端のサポートが追加されました。	6.2(2)	第 18 章「ERSPAN の設定」
NetFlow	同じインターフェイスで設定される入力 NetFlow サンプリングおよび DHCP リレーのサポートが追加されました。	6.2(2)	第 20 章「NetFlow の設定」
NetFlow	NetFlow データ ソースに対する NAM サポートが追加されました。	6.2(2)	第 20 章「NetFlow の設定」
NetFlow	Cisco NetFlow Generation Appliance（NGA）で NetFlow 全体およびサンプリングされた NetFlow のサポートが追加されました。	6.2(2)	第 20 章「NetFlow の設定」
NTP	アクセス グループ オプションを制限の最も緩いものから最も厳しいものの順序でスキャンするための **ntp access-group match-all** コマンドを導入しました。	6.2(2)	第 4 章「NTP の設定」
NTP	NTP がアソシエーションを形成するのを防ぐ **no ntp passive** コマンドを導入しました。	6.2(2)	第 4 章「NTP の設定」

機能	説明	変更されたリリース	参照先
NTP	インターフェイス上で NTP ブロードキャストおよびマルチキャスト サーバおよびマルチキャスト クライアントを設定する機能を追加しました。	6.2(2)	第 4 章「NTP の設定」
NTP	インターフェイス上でNTPをイネーブルまたはディセーブルにする機能を追加しました。	6.2(2)	第 4 章「NTP の設定」
NTP	NTP アクセス グループのオプションは、制限の緩いものから厳しいものの順序でスキャンされるようになりました。	6.2(2)	第 4 章「NTP の設定」
SNMP	場所に基づいてユーザを認証するために SNMPv3 サーバの AAA 排他的動作のサポートが追加されました。	6.2(2)	第 12 章「SNMP の設定」
SNMP	IPv4 および IPv6 ACL の両方を同じ SNMPv3 ユーザまたは SNMPv3 コミュニティに適用する機能が追加されました。	6.2(2)	第 12 章「SNMP の設定」
SPAN	SPAN データ ソースに対する NAM サポートが追加されました。	6.2(2)	第 17 章「SPAN の設定」
SPAN	F2e シリーズ モジュールでのみ、Tx 方向の SPAN 送信元としての FEX ポートのサポートが追加されました。	6.2(2)	第 17 章「SPAN の設定」
SPAN	拡張SPANのサポートが追加されました。	6.2(2)	第 17 章「SPAN の設定」
SPAN	ルール ベースの SPAN のサポートが追加されました。	6.2(2)	第 17 章「SPAN の設定」
SPAN	例外SPANのサポートが追加されました。	6.2(2)	第 17 章「SPAN の設定」

新機能および変更された機能に関する情報

機能	説明	変更されたリリース	参照先
XMLIN	CLI コマンドを Network Configuration（NETCONF）プロトコルに変換するのを可能にする XMLIN ツールが導入されました。	6.2(2)	第 25 章「CLI コマンドのネットワーク設定形式への変換」
EEE	F2e シリーズ モジュールで EEE のサポートが追加されました。	6.2(2)	第 21 章「EEE の設定」
ERSPAN	F2e シリーズ モジュールで ERSPAN のサポートが追加されました。	6.2(2)	第 18 章「ERSPAN の設定」
NetFlow	F2 シリーズおよび F2e シリーズ モジュールでサンプリングされた NetFlow のサポートが追加されました。	6.2(2)	第 20 章「NetFlow の設定」
NetFlow	F2 シリーズおよび F2e シリーズ モジュールで **flow timeout seconds** コマンドが追加されました。	6.2(2)	第 20 章「NetFlow の設定」
ERSPAN	ERSPAN タイプ III のサポートが追加されました。	6.1(1)	第 18 章「ERSPAN の設定」
ERSPAN	スーパーバイザ 2 のサポートが追加されました。	6.1(1)	第 18 章「ERSPAN の設定」
ERSPAN	F2 および M2 シリーズ モジュールのサポートが追加されました。	6.1(1)	第 18 章「ERSPAN の設定」
ERSPAN	ERSPAN サンプリングのサポートが追加されました。	6.1(1)	第 18 章「ERSPAN の設定」
ERSPAN	MTU 切り捨てと各 ERSPAN セッションの送信元レート制限を設定する機能が追加されました。	6.1(1)	第 18 章「ERSPAN の設定」
NTP	NTP 認証キーの長さが、8 文字から 15 文字の英数字に増加しました。	6.1(1)	第 4 章「NTP の設定」
オンライン診断（GOLD）	スーパーバイザ 2 および M2 シリーズ モジュールのサポートが追加されました。	6.1(1)	第 14 章「オンライン診断の設定」

新機能および変更された機能に関する情報

機能	説明	変更されたリリース	参照先
オンライン診断（GOLD）	F2 シリーズ モジュールに Spine path、RewriteEngineLoopback および SnakeLoopback テスト および Spine path テスト に対するサポートが追加されました。	6.1(1)	第 14 章「オンライン診断の設定」
オンライン診断（GOLD）	管理 VDC でオンライン診断設定に対するサポートを追加しました。	6.1(1)	第 14 章「オンライン診断の設定」
PTP	F2、F2e および M2 シリーズ モジュールのレイヤ 3 モードで PTP サポートが追加されました。	6.1(1)	第 5 章「PTP の設定」
PTP	M2 シリーズ モジュールのサポートが追加されました。	6.1(1)	第 5 章「PTP の設定」
PTP	PTP MAC フォーマットが FF:FF から FF:FE に変更されました。	6.1(1)	第 5 章「PTP の設定」
PTP	**vrf** オプションが **ptp source** コマンドで廃止されました。	6.1(1)	第 5 章「PTP の設定」
SPAN	SPAN に、SPAN サンプリングのサポートが追加されました。	6.1(1)	第 17 章「SPAN の設定」
SPAN	帯域内インターフェイスが管理VDC以外の任意の VDC から送信元として追加可能になりました。	6.1(1)	第 17 章「SPAN の設定」
SPAN	スーパーバイザ 2 のサポートが追加されました。	6.1(1)	第 17 章「SPAN の設定」
SPAN	M2 シリーズ モジュールのサポートが追加されました。	6.1(1)	第 17 章「SPAN の設定」
SPAN	ストレージ VDC に対して F2 シリーズ モジュール上で FCoE SPAN サポートが追加されました。	6.1(1)	第 17 章「SPAN の設定」
ERSPAN	ERSPAN および ERSPAN ACL は、F2 シリーズ モジュールではサポートされていません。	6.0(1)	第 18 章「ERSPAN の設定」

新機能および変更された機能に関する情報

機能	説明	変更されたリリース	参照先
NetFlow	NetFlow は、F2 シリーズ モジュールではサポートされません。	6.0(1)	第 19 章「NetFlow の設定」
NetFlow	ACL エントリによって拒否されたフローのコレクションをトリガするために collect routing forwarding-status コマンドのサポートが追加されました。	6.0(1)	第 20 章「NetFlow の設定」
オンライン診断（GOLD）	ポート チャネル メンバ ポートに PTP サポートが追加されました。	6.0(1)	第 14 章「オンライン診断の設定」
PTP	F2 シリーズ モジュールのサポートが追加されました。	6.0(1)	第 5 章「PTP の設定」
PTP	ポート チャネル メンバ ポートに PTP サポートが追加されました。	6.0(1)	第 5 章「PTP の設定」
SPAN	F2 シリーズ モジュールのサポートが追加されました。	6.0(1)	第 17 章「SPAN の設定」
NTP	F2 シリーズ モジュールのサポートが追加されました。		第 4 章「NTP の設定」
CFS プロトコル	デバイス エイリアス、DPVM、FC ドメイン、FC ポート セキュリティ、FC タイマー、IVR、および RSCN に対して CFS over Fibre Channel（CFSoFC）配信サポートが追加されました。	5.2(3)	第 3 章「CFS の設定」
EEM イベント相関	単一の EEM ポリシーで複数のイベント トリガーのサポートが追加されました。	5.2(1)	第 21 章「EEE の設定」
ERSPAN	Cisco Nexus 2000 Series Fabric Extender インターフェイスに対する ERSPAN 送信元サポートが追加されました。	5.2(1)	第 18 章「ERSPAN の設定」

機能	説明	変更されたリリース	参照先
ERSPAN	ERSPANセッションのマルチキャスト ベスト エフォート モードを設定する機能が追加されました。	5.2(1)	第 18 章「ERSPAN の設定」
Smart Call Home に対する HTTP プロキシ サーバ	HTTP プロキシ サーバを経由して HTTP メッセージを送信する機能が追加されました。	5.2(1)	第 8 章「Smart Call Home の設定」
LLDP	Cisco Nexus 2000 シリーズ Fabric Extender に LLDP サポートが追加されました。	5.2(1)	第 19 章「LLDP の設定」
NetFlow	F1 シリーズ ポートのスイッチ仮想インターフェイス（SVI）でNetFlowのサポートが追加されました。	5.2(1)	第 20 章「NetFlow の設定」
NTP	すべての VDC に対する NTP サポートを追加し、VDC はタイム サーバとして機能可能になりました。	5.2(1)	第 4 章「NTP の設定」
NTP	既存のタイム サーバと同期されていない場合でも正規の NTP サーバとしてデバイスを設定する機能が追加され、時間を配信できるようになりました。	5.2(1)	第 4 章「NTP の設定」
NTP	NTPのイネーブルまたはディセーブルに使用するコマンドが [no] ntp enable から [no] feature ntp に変更されました。	5.2(1)	第 4 章「NTP の設定」
NTP アクセス グループ	追加の NTP サービスに対するアクセスをコントロールするために serve、serve-only、query-only アクセス グループ オプションを追加しました。	5.2(1)	第 4 章「NTP の設定」
オンライン診断（GOLD）	追加の NTP サービスに対するアクセスをコントロールするために serve、serve-only、query-only アクセス グループ オプションを追加しました。	5.2(1)	第 14 章「オンライン診断の設定」

新機能および変更された機能に関する情報

機能	説明	変更されたリリース	参照先
オンライン診断（GOLD）	スタンバイ スーパーバイザの SpineControlBus テストがイネーブルになりました。	5.2(1)	第 14 章「オンライン診断の設定」
オンライン診断（GOLD）	F1 シリーズ モジュールの SnakeLoopback テストが非推奨になりました。	5.2(1)	第 14 章「オンライン診断の設定」
PTP	高精度時間プロトコル（PTP）のサポートが追加されました。	5.2(1)	第 5 章「PTP の設定」
SPAN	Cisco Nexus 2000 Series Fabric Extender インターフェイスに対する SPAN 送信元サポートが追加されました。	5.2(1)	第 17 章「SPAN の設定」
SPAN	各 SPAN セッションに対する MTU 切り捨て、送信元レート制限、およびマルチキャスト ベスト エフォートを設定する機能が追加されました。	5.2(1)	第 17 章「SPAN の設定」
システム メッセージ ロギング	システム メッセージ ログ内で、物理的イーサネット インターフェイスおよびサブインターフェイスに対して説明を追加する機能が追加されました。	5.2(1)	第 7 章「システム メッセージ ロギングの設定」
オンライン診断（GOLD）	F1 シリーズ モジュールでの SnakeLoopback テストのサポートが追加されました。	5.1(2)	第 14 章「オンライン診断の設定」
ブリッジ NetFlow	VLAN 上でブリッジ NetFlow を設定する場合に、作成とは独立して VLAN を設定できる VLAN 設定モードのサポートが追加されました。	5.1(1)	第 20 章「NetFlow の設定」
DCBXP	このリンク層プロトコルは、ピア間でノードパラメータを通知、交換、およびネゴシエートするために使用されます。	5.1(1)	第 19 章「LLDP の設定」

新機能および変更された機能に関する情報

機能	説明	変更されたリリース	参照先
ERSPAN および ERSPAN ACL	IP ネットワーク上でトラフィックをモニタするように ERSPAN を設定できます。	5.1(1)	第 18 章「ERSPAN の設定」
オンライン診断（GOLD）	FIPS および BootupPortLoopback テストのサポートが追加されました。	5.1(1)	第 14 章「オンライン診断の設定」
RMON	RMON がデフォルトでイネーブルにされました。	5.1(1)	第 17 章「SPAN の設定」
SPAN	F1 シリーズ モジュールのサポートが追加され、サポートされる SPAN セッションが 18 から 48 に増加されました。	5.1(1)	第 17 章「SPAN の設定」
EEM パブリッシャとしての syslog	スイッチからの syslog メッセージをモニタできます。	5.1(1)	第 21 章「EEE の設定」
Syslog サーバ	サポートされる syslog サーバの数が 3 から 8 に増加されました。	5.1(1)	第 7 章「システム メッセージ ロギングの設定」
Smart Call Home の SMTP サーバ コンフィギュレーション	Smart Call Home に対して複数の SMTP サーバを設定できます。	5.0(2)	第 8 章「Smart Call Home の設定」
Smart Call Home メッセージの HTTP 転送に対する VRF サポート	VRF を使用して、HTTP経由で電子メールおよび他の Smart Call Home メッセージを送信できます。	5.0(2)	第 8 章「Smart Call Home の設定」
Smart Call Home のクラッシュ通知	ラインカード（およびスーパーバイザ モジュール）上でプロセス クラッシュに対してメッセージが送信されます。	5.0(2)	第 8 章「Smart Call Home の設定」
EEM システム ポリシー	ファン EEM ポリシーは、Cisco Nexus 7000 10-Slot Switch に対して変更されました。	5.0(2)	付録 B「Embedded Event Manager システム イベントおよびコンフィギュレーション例」

新機能および変更された機能に関する情報

機能	説明	変更されたリリース	参照先
LLDP	ローカル ネットワーク上の他のデバイスを検出するために、リンク層検出プロトコル（LLDP）を設定できます。	5.0(2)	第 19 章「LLDP の設定」
NetFlow	NetFlow の IPv4 フローおよび NetFlow のテーブル使用率を表示する NetFlow インスタンスを指定できます。	5.0(2)	第 20 章「NetFlow の設定」
NTP アクセス グループ	アクセス グループを使用して、NTP サービスへのアクセスを制御できます。	5.0(2)	第 4 章「NTP の設定」
NTP 認証	ローカル ロックを同期させる時刻源を認証するようデバイスを設定できます。	5.0(2)	第 4 章「NTP の設定」
NTP ロギング	重要な NTP イベントでシステム ログを生成するよう、NTP ロギングを設定できます。	5.0(2)	第 4 章「NTP の設定」
NTP サーバ コンフィギュレーション	NTP サーバとの通信で使用するキーを設定するために、ntp server コマンドにオプションの key キーワードが追加されました。	5.0(2)	第 4 章「NTP の設定」
SNMP 通知	snmp-server enable traps コマンドが更新されました。	5.0(2)	第 12 章「SNMP の設定」

第 2 章

概要

この章では、Cisco NX-OS デバイスのモニタや管理に使用できるシステム管理機能について説明します。

この章の内容は、次のとおりです。

- Cisco NX-OS デバイス コンフィギュレーション方式, 14 ページ
- Cisco Fabric Services, 16 ページ
- ネットワーク タイム プロトコル, 16 ページ
- 高精度時間プロトコル, 16 ページ
- Cisco Discovery Protocol, 16 ページ
- システム メッセージ, 16 ページ
- Smart Call Home, 16 ページ
- ロールバック, 17 ページ
- Session Manager, 17 ページ
- スケジューラ, 17 ページ
- SNMP, 17 ページ
- RMON, 17 ページ
- オンライン診断, 18 ページ
- Embedded Event Manager, 18 ページ
- オンボード障害ロギング, 18 ページ
- SPAN, 18 ページ
- ERSPAN, 18 ページ
- LLDP, 19 ページ
- NetFlow, 19 ページ

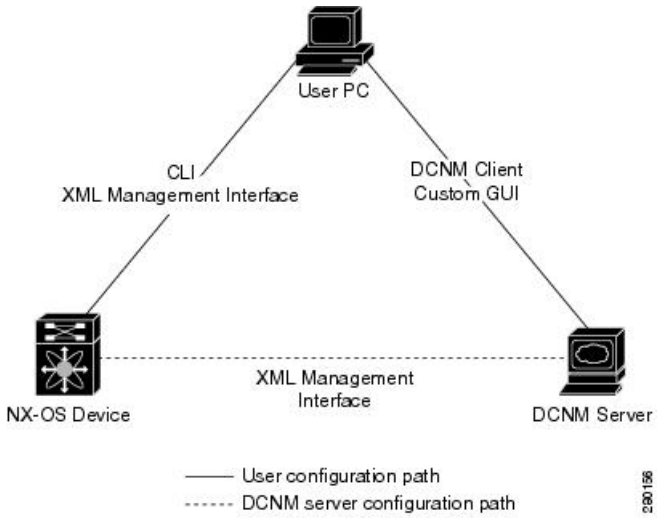
- FabricPath，19 ページ
- EEE，19 ページ
- トラブルシューティング機能，20 ページ

Cisco NX-OS デバイス コンフィギュレーション方式

デバイスは、直接ネットワーク コンフィギュレーション方式または Cisco データセンター ネットワーク管理（DCNM）サーバが提供する Web サービスを使用して設定できます。

次の図は、ネットワーク ユーザが使用できるデバイスのコンフィギュレーション方式を示します。

図 *1*：*Cisco NX-OS* デバイス コンフィギュレーション方式



次の表に、コンフィギュレーション方式と詳しい説明が記載されているマニュアルを示します。

表 *1*：コンフィギュレーション方式および参考資料

コンフィギュレーション方式	マニュアル
セキュア シェル（SSH）セッション、Telnet セッション、またはコンソール ポートからの CLI	『*Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide*』
XML 管理インターフェイス	『*Cisco NX-OS XML Management Interface User Guide*』
Cisco DCNM クライアント	『*Cisco DCNM Fundamentals Guide*』

コンフィギュレーション方式	マニュアル
ユーザ定義の GUI	『*Web Services API Guide, Cisco DCNM for LAN Release 5.x*』

この項では、次のトピックについて取り上げます。

- CLI または XML 管理インターフェイスによる設定
- Cisco DCNM または カスタム GUI による設定

CLI または XML 管理インターフェイスによる設定

次のように SSH からコマンドライン インターフェイス（CLI）または XML 管理インターフェイスを使用して、Cisco NX-OS デバイスを設定できます。

- SSH セッション、Telnet セッション、またはコンソール ポート：SSH セッション、Telnet セッション、またはコンソール ポートから CLI を使用してデバイスを設定できます。SSH ではデバイスへの安全な接続が提供されます。詳細については、『*Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide*』を参照してください。
- SSH を介して XML 管理インターフェイス：XML 管理インターフェイスを使用してデバイスを設定できます。これは、CLI 機能を補完する NETCONF プロトコルに基づくプログラム方式です。詳細については、『*Cisco NX-OS XML Management Interface User Guide*』を参照してください。

Cisco DCNM または カスタム GUI による設定

次のように Cisco DCNM クライアントを使用して、または独自の GUI から Cisco NX-OS デバイスを設定できます。

- **Cisco DCNM クライアント**：Cisco DCNM クライアントを使用してデバイスを設定できます。Cisco DCNM クライアントはユーザのローカル PC 上で動作し、Cisco DCNM サーバの Web サービスを使用します。Cisco DCNM サーバでは XML 管理インターフェイスを使用してデバイスを設定します。Cisco DCNM クライアントの詳細については、『*Fundamentals Configuration Guide, Cisco DCNM for LAN, Release 5.x*』を参照してください。
- **カスタム GUI**：独自の GUI を作成すると、Cisco DCNM サーバ上の Cisco DCNM Web サービス アプリケーション プログラム インターフェイス（API）を使用してデバイスを設定できます。SOAP プロトコルを使用して、Cisco DCNM サーバと XML ベースのコンフィギュレーション メッセージを交換します。Cisco DCNM サーバでは XML 管理インターフェイスを使用してデバイスを設定します。カスタム GUI の作成の詳細については、『*Web Services API Guide, Cisco DCNM for LAN, Release 5.x*』を参照してください。

Cisco Fabric Services

Cisco Fabric Services（CFS）は、設定変更を含むデータをネットワークのすべての Cisco NX-OS デバイスに配信するシスコ独自の機能です。

ネットワーク タイム プロトコル

ネットワーク タイムプロトコル（NTP）は、分散している一連のタイムサーバとクライアント間で 1 日の時間を同期させ、ネットワーク内のデバイスから受信するシステム ログなどの時間関連の情報を相互に関連付けることができます。

高精度時間プロトコル

高精度時間プロトコル（PTP）はネットワークに分散したノードの時刻同期プロトコルです。そのハードウェアのタイムスタンプ機能は、ネットワーク タイムプロトコル（NTP）などの他の時刻同期プロトコルより高い精度を実現します。PTP についての詳細。

Cisco Discovery Protocol

Cisco Discovery Protocol（CDP）を使用して、デバイスに直接接続されているすべてのシスコ製機器を検出し、情報を表示できます。CDP は、ルータ、ブリッジ、アクセス サーバ、コミュニケーション サーバ、スイッチを含む、シスコ製のあらゆる機器で動作します。CDP は、メディアにもプロトコルにも依存せず、ネイバー デバイスのプロトコル アドレスを収集し、各デバイスのプラットフォームを検出します。CDP の動作はデータリンク層上に限定されます。異なるレイヤ 3 プロトコルをサポートする 2 つのシステムで相互学習が可能です。

システム メッセージ

システム メッセージ ロギングを使用して宛先を制御し、システム プロセスが生成するメッセージの重大度をフィルタリングできます。端末セッション、ログファイル、およびリモートシステム上の syslog サーバへのロギングを設定できます。

システム メッセージ ロギングは RFC 3164 に準拠しています。システム メッセージのフォーマットおよびデバイスが生成するメッセージの詳細については、『*Cisco NX-OS System Messages Reference*』を参照してください。

Smart Call Home

Call Home は重要なシステム ポリシーを E メールで通知します。Cisco NX-OS では、ポケットベル サービス、標準的な電子メール、または XML ベースの自動化された解析アプリケーションと

の最適な互換性のために、広範なメッセージ形式が提供されています。この機能を使用して、ネットワーク サポート エンジニアや Network Operations Center を呼び出せます。また、Cisco Smart Call Home サービスを使用して、TAC でケースを自動的に生成することもできます。

ロールバック

ロールバック機能では、デバイスのコンフィギュレーションのスナップショットまたはチェックポイントを使用して、デバイスをリロードせずに、いつでもそのコンフィギュレーションを再適用できます。権限のある管理者であれば、チェックポイントで設定されている機能について専門的な知識がなくても、ロールバック機能を使用して、そのチェックポイント コンフィギュレーションを適用できます。

Session Manager を使用すると、コンフィギュレーション セッションを作成し、そのセッション内のすべてのコマンドを自動的に適用できます。

Session Manager

Session Manager を使用すると、コンフィギュレーションを作成し、すべて正しく設定されていることを確認および検証したあとでバッチ モードで適用できます。

スケジューラ

スケジューラを使用すると、データの定期的なバックアップや Quality of Service（QoS）ポリシーの変更などのジョブを作成し、管理できます。スケジューラでは、ジョブを指定された時間に一度だけ、または定期的な間隔で実行するなど、ニーズに合わせて開始できます。

SNMP

簡易ネットワーク管理プロトコル（SNMP）は、SNMP マネージャとエージェント間の通信用メッセージ フォーマットを提供する、アプリケーション レイヤ プロトコルです。SNMP では、ネットワーク内のデバイスのモニタリングと管理に使用する標準フレームワークと共通言語が提供されます。

RMON

リモート モニタリング（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インターネット技術特別調査委員会（IETF）標準モニタリング仕様です。Cisco NX-OS では、Cisco NX-OS デバイスをモニタするための、RMON アラーム、イベント、およびログをサポートします。

オンライン診断

Cisco Generic Online Diagnostics（GOLD）では、複数のシスコ プラットフォームにまたがる診断操作の共通フレームワークを定義しています。オンライン診断フレームワークでは、中央集中システムおよび分散システムに対応する、プラットフォームに依存しない障害検出アーキテクチャを規定しています。これには共通の診断 CLI とともに、起動時および実行時に診断するための、プラットフォームに依存しない障害検出手順が含まれます。プラットフォーム固有の診断機能は、ハードウェア固有の障害検出テストを行い、診断テストの結果に応じて適切な対策を実行できます。

Embedded Event Manager

Embedded EventManager（EEM）を使用すると、重要なシステム イベントを検出して処理できます。EEM は、イベント発生時点で、またはしきい値を超えた時点でのイベント モニタリングを含め、イベントを検出して回復する機能を提供します。

オンボード障害ロギング

永続ストレージに障害データを記録するように、デバイスを設定できます。あとで記録されたデータを取得して表示し、分析できます。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、障害モジュールの分析に役立ちます。

SPAN

イーサネット スイッチド ポート アナライザ（SPAN）を設定すると、デバイスの入出力トラフィックをモニタできます。SPAN の機能を使用すると、送信元ポートから宛先ポートへのパケットを複製できます。

ERSPAN

Encapsulated Remote Switched Port Analyzer（ERSPAN）は、IP ネットワークでミラーリングされたトラフィックを転送するために使用します。ERSPAN は異なるスイッチ上の送信元ポート、送信元 VLAN、および宛先をサポートし、ネットワーク上にある複数のスイッチのリモート モニタリングを可能にします。ERSPAN は、スイッチ間でトラフィックを伝送するために、総称ルーティング カプセル化（GRE）を使用します。

ERSPAN は、ERSPAN 送信元セッション、ルーティング可能な ERSPAN GRE カプセル化トラフィック、および ERSPAN 宛先セッションで構成されています。異なるスイッチで ERSPAN 送信元セッションおよび宛先セッションを個別に設定します。

ERSPAN 送信元セッションを 1 台のスイッチ上で設定するには、送信元ポートまたは VLAN のセットを、宛先 IP アドレス、ERSPAN ID 番号、および仮想ルーティングおよび転送（VRF）名に対応付けます。ERSPAN 宛先セッションを別のスイッチ上で設定するには、宛先を送信元 IP アドレス、ERSPAN ID 番号、および VRF 名に対応付けます。ERSPAN 送信元セッションは、送信元ポートまたは送信元 VLAN からのトラフィックをコピーし、このトラフィックを、ルーティング可能な GRE カプセル化パケットを使用して ERSPAN 宛先セッションに転送します。ERSPAN 宛先セッションはトラフィックを宛先へスイッチングします。

LLDP

リンク層検出プロトコル（LLDP）はベンダーに依存しない、単一方向のデバイス ディスカバリ プロトコルです。このプロトコルでは、ネットワーク上の他のデバイスにネットワーク デバイスから固有の情報をアドバタイズできます。このプロトコルはデータリンク層で動作するため、異なるネットワーク層プロトコルが稼働する 2 つのシステムで互いの情報を学習できます。LLDP はグローバルに、またはインターフェイスごとにイネーブルにすることができます。

NetFlow

NetFlow は入力 IP パケットと出力 IP パケットの両方について、パケット フローを識別し、各パケット フローに基づいて統計情報を提供します。NetFlow のためにパケットやネットワーキング デバイスを変更する必要はありません。

FabricPath

FabricPath は高度な回復力を持ち、スケーラブルなレイヤ 2 ファブリックを構築するためにレイヤ 3 ルーティングの利点をレイヤ 2 スイッチ ネットワークに適用します。システム マネージャは、FabricPath リソース処理の開始とハートビートのモニタリングを実行します。

EEE

Energy Efficient Ethernet (EEE) は、アイドル時間にイーサネット ネットワークの消費電力を減らすように設計された IEEE 802.3az の標準です。低電力アイドル（LPI）モードをサポートするデバイスで EEE をイネーブルにできます。このようなデバイスは、低い使用率のときに LPI モードを開始して、電力を節約できます。LPI モードでは、リンクの両端にあるシステムは、特定のサービスをシャット ダウンして、電力を節約できます。EEE は上位層プロトコルおよびアプリケーションに対して透過的であるように、LPI モードに移行したり、LPI モードから移行する必要があるプロトコルを提供します。

トラブルシューティング機能

Cisco NX-OS には ping、traceroute、Ethanalyzer、Blue Beacon 機能など、さまざまなトラブルシューティング ツールが揃っています。

サービスで障害が発生すると、システムは障害の原因を判定するために使用できる情報を生成します。次の情報ソースが使用可能です。

- サービスの再起動によって、LOG_ERR レベルの Syslog メッセージが生成されます。
- Smart Call Home サービスがイネーブルになっている場合は、サービスの再起動によって Smart Call Home イベントが生成されます。
- SNMP トラップがイネーブルになっている場合、サービスが再起動されると、SNMP エージェントはトラップを送信します。
- サービスの障害がローカル モジュール上で発生した場合は、そのモジュール内で **show processes log** コマンドを入力することで、イベントのログを表示できます。プロセスのログは、スーパーバイザのスイッチオーバーまたはリセット後も保持されます。
- サービスの障害が発生すると、システムのコア イメージ ファイルが生成されます。最新のコア イメージを表示するには、アクティブなスーパーバイザ上で **show cores** コマンドを入力します。スーパーバイザのスイッチオーバーおよびリセットが生じると、コア ファイルは保持されません。ただし、**system cores** コマンドを入力し、ファイル転送ユーティリティ Trivial File Transfer Protocol（TFTP）を使用して、コア ファイルを外部サーバへエクスポートするようシステムを設定できます。
- CISCO-SYSTEM-MIB には、コアのテーブルが含まれています（cseSwCoresTable）。

第 3 章

CFS の設定

この章では、設定変更を含むデータをネットワークのすべてのCisco NX-OSデバイスに配信するシスコ独自の機能、Cisco Fabric Services（CFS）の使い方を説明します。

この章は、次の項で構成されています。

- 機能情報の確認，21 ページ
- CFS について，22 ページ
- CFS のライセンス要件，26 ページ
- CFS の前提条件，26 ページ
- CFS の注意事項と制約事項，26 ページ
- CFS のデフォルト設定，27 ページ
- CFS 配信の設定，28 ページ
- CFS 設定の確認，47 ページ
- CFS に関する追加情報，48 ページ
- CFS の機能の履歴，49 ページ

機能情報の確認

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

CFS について

Cisco Fabric Services（CFS）を使用して、1 台のシスコ デバイスとネットワークの他のすべてのシスコ デバイスにコンフィギュレーションを配信し、同期させることができます。CFS を使用すると、ネットワークの設定と動作に一貫性をもたせ、ほとんどの場合、同じ設定と動作を維持できます。

CFS を使用して設定変更を配信するアプリケーション

CFS は、次の表に記載するアプリケーションの設定変更を配信します。

表 *2*：*CFS* がサポートするアプリケーション

アプリケーション	デフォルトの状態
デバイス エイリアス	イネーブル
DPVM	イネーブル
FC ドメイン	ディセーブル
FC ポート セキュリティ	ディセーブル
FC タイマー	ディセーブル
IVRivr	ディセーブル
NTP	ディセーブル
RADIUS	ディセーブル
RSCN	ディセーブル
Smart Call Home	ディセーブル
TACACS+	ディセーブル
ユーザ ロール	ディセーブル

CFS 配信

CFS はネットワーク全体に存在する複数のデバイスにコンフィギュレーションの変更を配信します。CFS では、次のタイプの配信がサポートされています。

- CFS over Ethernet（CFSoE）：イーサネット ネットワーク上でアプリケーション データを配信します。
- CFS over IP（CFSoIP）：IPv4 ネットワーク上でアプリケーション データを配信します。

- CFS over Fibre Channel（CFSoFC）：仮想ストレージ エリア ネットワーク（VSAN）などのファイバ チャネル上でアプリケーション データを配信します。デバイスがファイバ チャネル ポートを使用してプロビジョニングされる場合、CFSoFC はデフォルトでイネーブルです。

  Cisco NX-OS Release 5.2 以降では、ファイバ チャネルのトラフィックが物理的イーサネット リンクを介してカプセル化されることを可能にする Fibre Channel over Ethernet（FCoE）を設定できます。Cisco Nexus 7000 シリーズ スイッチで FCoE を実行するには、専用のストレージ仮想デバイス コンテキスト（VDC）を設定する必要があります。FCoE がデバイスでイネーブルになっている場合、CFSoFC サービスを使用できます。ストレージ VDC で CFS 配信がイネーブルにされる必要があるアプリケーションはこの章全体の設定手順で示されています。FCoE およびストレージ VDC の詳細については、『*Cisco NX-OS FCoE Configuration Guide for Cisco Nexus 7000 and Cisco MDS 9500*』および『Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide』を参照してください。

（注） 特に明記されていない限り、この章の情報はすべて、CFSoIP と CFSoFC の両方に適用されます。

CFS の配信モード

CFS では異なる機能要件をサポートするために、3 つの配信モードをサポートします。常に 1 つのモードだけを適用できます。

- 非協調型配信：ピアと競合しないことが期待される情報を配信します。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：複数のデバイス（たとえばポート セキュリティ設定）で操作および配信できる情報を配信します。協調型配信は、いかなる時も 1 つのアプリケーション配信だけ適用できます。CFS はロックを使用してこの機能を実行します。ネットワー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。
  - ネットワーク ロックが取得されます。
  - 設定が配信され、コミットされます。
  - ネットワーク ロックが解除されます。

  CFS は、アプリケーションからの介入またはアプリケーションによる完全な制御なしに、アプリケーション リクエストへの応答としてこれらの段階を実行できます。
- 制限なしの非協調型配信：既存の協調型配信がある場合に複数の並行配信を可能にします。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 7000 シリーズ スイッチ、Cisco Nexus 5000 シリーズ スイッチ、および 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 9000 シリーズ、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 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設定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。

（注） 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 7000 シリーズ、Cisco Nexus 5000 シリーズ、および Cisco MDS 9000 スイッチ用 CFS についての詳細は、『Cisco Nexus 7000 シリーズ NX-OS システム管理コンフィギュレーション ガイド』、『*Cisco Nexus 5000 Series NX-OS System Management Configuration Guide*』、および『*Cisco MDS 9000 Family NX-OS System Management Configuration Guide*』をそれぞれ参照してください。

CFS 結合のサポート

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 つのファブリックが相互に到達可能になった場合、CFS はマージをトリガーします。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 のアプリケーション ピアを持つファブリックが N のアプリケーション ピアを持つ別のファブリックと結合し、アプリケーションが各通知でマージアクションをトリガーすると、リンクアップイベントの結果としてファブリック内の MxN マージが発生します。

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 つのデバイスを選択する作業が伴います。他のデバイスは、マージ プロセスにおいて役割を担いません。

2 つのネットワークのマージ処理中に、指定されたマネージャどうしでコンフィギュレーション データベースが交換されます。一方のアプリケーションによりデータベースがマージされ、マージが成功したかどうかが判断され、他のすべてのデバイスに通知されます。

マージが成功すると、マージされたデータベースは統合されたファブリックの全デバイスに配信され、新しいファブリック全体が一貫性のある状態のままとなります。

ネットワークのロック

CFS のインフラストラクチャを使用するアプリケーションを設定する場合、このアプリケーションは CFS セッションを開始し、ネットワークをロックします。ネットワークがロックされた場合、このアプリケーションへの設定変更は、デバイス ソフトウェアにより、ロックを保持しているデバイスだけから行えます。別のデバイスからアプリケーションへの設定変更を行う場合、ロックされているステータスを知らせるメッセージがデバイスから発行されます。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。

ネットワーク ロックを要求する CFS セッションを開始し、セッションを終了するのを忘れた場合は、管理者がそのセッションをクリアできます。いつでもネットワークをロックした場合、ユーザ名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）別のユーザが設定タスクを実行しようとしても、拒否されます。

CFS リージョン

CFS リージョンとは、ある機能またはアプリケーションに対してユーザが定義したデバイスのサブセットです。通常、互いに近くに存在するデバイスに基づいて配信をローカライズまたは制限する場合にリージョンを定義します。多数の地域で別々の管理者がデバイスのサブセットを担当するネットワークの場合、CFS リージョンを設定して、アプリケーションの範囲を管理できます。

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 リージョンとして予約され、ネットワーク内のすべてのデバイスが含まれます。1 ～ 200 のリージョンを設定できます。

（注） アプリケーションを移動する（つまり新しいリージョンに割り当てる）場合、その範囲はそのリージョンに制限され、他のすべてのリージョンは配信やマージの対象外となります。アプリケーションへのリージョンの割り当ては、配信において初期のスコープよりも優先されます。

複数のアプリケーション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、1 台のデバイスで、特定のアプリケーションのコンフィギュレーションを配信するために設定できる CFS リージョンは一度に 1 つに限られます。アプリケーションを 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。

ハイ アベイラビリティ

CFS のステートレス リスタートがサポートされています。リブート後またはスーパーバイザ スイッチオーバー後に、実行コンフィギュレーションが適用されます。ハイ アベイラビリティの詳細については、『*Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide*』を参照してください。

CFS のライセンス要件

製品	ライセンス要件
Cisco NX-OS	CFS 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。NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

CFS の前提条件

CFS の前提条件は、次のとおりです。

- CFS はデフォルトでイネーブルです。ファブリック内のすべてのデバイスで CFS をイネーブルに設定しないと配信は受信されません。
- アプリケーションに対して CFS がディセーブルになっていると、そのアプリケーションからコンフィギュレーションは配信されず、ファブリック内の他のデバイスからの配信も受け取ることができません。

CFS の注意事項と制約事項

CFS に関するコンフィギュレーションの注意事項および制約事項は、次のとおりです。

- デバイスで仮想ポート チャネル（vPC）機能がイネーブルになっている場合、CFSoE をディセーブルにしないでください。

（注） vPC 機能を動作させるには、CFSoE をイネーブルにする必要があります。

- 同様のマルチキャスト アドレスを持つ CFSoIP がイネーブルになっているすべてのデバイスは 1 つの CFSoIP ファブリックを形成します。
- 設定するアプリケーションについて CFS がイネーブルになっていることを確認してください。
- ファブリックをロックすると、リスタートとスイッチオーバーにわたってユーザ名が記憶されます。
- ファブリックをロックすると、他のユーザによるコンフィギュレーションの変更の試みは拒否されます。

- ファブリックのロック中、アプリケーションでは実行コンフィギュレーションではなく保留データベースまたは一時ストレージにコンフィギュレーションの変更の作業コピーが保持されます。
- まだコミットされていない設定の変更内容（まだ作業中のコピーとして保存されている）は、実行コンフィギュレーションには存在せず、**show** コマンドの出力には表示されません。
- 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。
- 以前コンフィギュレーションの変更が行われていない場合は、空のコミットを行えます。この場合、**commit** コマンドにより、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作成されます。
- **commit** コマンドは、ファブリック ロックが取得されたデバイスだけで使用できます。
- CFSoIP と CFSoE の同時使用はサポートされません。
- CFS リージョンは、CFSoIP アプリケーションにのみ適用できます。
- Cisco MDS 9500 シリーズ スイッチと、Cisco Nexus 7000 シリーズ スイッチに設定されているストレージ VDC 間ではユーザ ロール設定を配信できません。この配信を防ぐには、Cisco MDS および Cisco Nexus 7000 ストレージ VDC のユーザ ロール設定を異なる CFS リージョンにを割り当てます。

CFS のデフォルト設定

表 *3*：デフォルトの *CFS* パラメータ

パラメータ	デフォルト
デバイスでの CFS 配信	イネーブル
CFSoIP	ディセーブル
IPv4 マルチキャスト アドレス	239.255.70.83
CFSoFC	FCoE がある場合、イネーブル
CFSoE	ディセーブル

CFS 配信の設定

アプリケーションの CFS 配信のイネーブル化

CFS をイネーブルにして Smart Call Home 設定を配信する

ネットワーク内のすべての Cisco NX-OS デバイスに Call Home コンフィギュレーションを配信するように CFS をイネーブルにできます。デバイス プライオリティと sysContact 名を除く Call Home コンフィギュレーション全体が配信されます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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	switch(config)# **callhome**	Call Home コンフィギュレーション モードを開始します。
ステップ 3	switch(config-callhome)# **distribute**	CFS をイネーブルにして、Smart Call Home 設定のアップデートを配信します。
ステップ 4	switch(config-callhome)# **show***application-name***status**	（任意） 指定されたアプリケーションについて、CFS 配信ステータスを表示します。
ステップ 5	switch(config-callhome)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

```
switch# configure terminal
switch(config)# callhome
switch(config-callhome)# distribute
switch(config-callhome)# show callhome status
Distribution : Enabled
switch(config-callhome)# copy running-config startup-config
```

CFS をイネーブルにしてデバイス エイリアス設定を配信する

ファブリック内のすべての Cisco NX-OS デバイスを通してデバイス エイリアス データベースを一貫して管理および維持するために、デバイス エイリアス設定を配信するように CFS をイネーブルにできます。

はじめる前に

ストレージ VDC 内にいることを確認します。ストレージ VDC に切り替えるには、**switchto vdc fcoe** コマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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	switch(config)# **device-alias distribute**	デバイスエイリアス設定アップデートを配信するように CFS をイネーブルにします。
ステップ 3	switch(config)# **show cfs application**	（任意） CFS 配信ステータスを表示します。
ステップ 4	switch(config)# **copy running-config startup config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、CFS でのデバイスエイリアス コンフィギュレーションの配信をイネーブルにする例を示します。

```
switch(config)# device-alias distribute
switch(config)# show cfs application
----------------------------------------------
Application Enabled Scope
----------------------------------------------
device-alias Yes Physical-fc
switch(config)# copy running-config startup-config
[########################################] 100%
```

CFS をイネーブルにして DPVM 設定を配信する

ファブリック内のすべての Cisco NX-OS デバイスを通して DPVM データベースを一貫して管理および維持するために、動的ポート VSAN メンバーシップ（DPVM）設定を配信するように CFS をイネーブルにできます。

はじめる前に

ストレージ VDC 内にいることを確認します。ストレージ VDC に切り替えるには、**switchto vdc fcoe** コマンドを使用します。

DPVM 機能をイネーブルにする必要があります。これを実行するには、**feature dpvm** コマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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	switch(config)# **dpvm distribute**	CFS をイネーブルにして、DPVM 設定のアップデートを配信します。
ステップ 3	switch(config)# **show***application-name***status**	（任意） 指定されたアプリケーションについて、CFS 配信ステータスを表示します。
ステップ 4	switch(config)# **copy running-config startup config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

CFS をイネーブルにして、DPVM コンフィギュレーションを配信する例を示します。

```
switch(config)# dpvm distribute
switch(config)# show dpvm status
Distribution is enabled.
switch(config)# copy running-config startup-config
[########################################] 100%
```

CFS をイネーブルにして FC ドメイン設定を配信する

CFS をイネーブルにして、単一の Cisco NX-OS デバイスのコンソールからのファブリック全体で設定を同期するため、また VSAN 内のすべてのデバイス上の許可されるドメイン ID リストの一貫性を保証するためにファイバ チャネル（FC）ドメイン設定を配信できます。

はじめる前に

ストレージ VDC 内にいることを確認します。ストレージ VDC に切り替えるには、**switchto vdc fcoe** コマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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。

	コマンドまたはアクション	目的
ステップ 2	switch(config)# **fcdomain distribute**	CFS をイネーブルにして、FC ドメイン コンフィギュレーションのアップデートを配信します。
ステップ 3	switch(config)# **show***application-name***status**	（任意） 指定されたアプリケーションについて、CFS配信ステータスを表示します。
ステップ 4	switch(config)# **copy running-config startup config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

CFS をイネーブルにして、FC ドメイン コンフィギュレーションを配信する例を示します。

```
switch(config)# fcdomain distribute
switch(config)# show fcdomain status
fcdomain distribution is enabled
switch(config)# copy running-config startup-config
[########################################] 100%
```

CFS をイネーブルにして FC ポート セキュリティ設定を配信する

CFS をイネーブルにして、VSAN 内のファブリック全体に対する単一の設定ポイントを提供するため、またファブリック全体でポート セキュリティ ポリシーを適用するためにファイバ チャネル（FC）ポート セキュリティ設定を配信できます。

はじめる前に

ストレージ VDC 内にいることを確認します。ストレージ VDC に切り替えるには、**switchto vdc fcoe** コマンドを使用します。

FC ポート セキュリティ機能をイネーブルにする必要があります。これを実行するには、**feature fc-port-security** コマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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。

	コマンドまたはアクション	目的
ステップ 2	switch(config)# **fc-port-security distribute**	CFS をイネーブルにして、FC ポート セキュリティ コンフィギュレーションのアップデートを配信します。
ステップ 3	switch(config)# **show cfs application**	（任意） CFS 配信ステータスを表示します。
ステップ 4	switch(config)# **copy running-config startup config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

CFS をイネーブルにして、FC ポート セキュリティ コンフィギュレーションを配信する例を示します。

```
switch(config)# fc-port-security distribute
switch(config)# show cfs application
----------------------------------------------
Application Enabled Scope
----------------------------------------------
fc-port-securi Yes Logical
switch(config)# copy running-config startup-config
[########################################] 100%
```

CFS をイネーブルにして FC タイマー設定を配信する

CFS をイネーブルにして、ファブリック内のすべての Cisco-NX-OS デバイスに対してファイバ チャネル（FC）タイマー設定を配信できます。

はじめる前に

ストレージ VDC 内にいることを確認します。ストレージ VDC に切り替えるには、**switchto vdc fcoe** コマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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	switch(config)# **fctimer distribute**	CFS をイネーブルにして、FC タイマー コンフィギュレーションのアップデートを配信します。

	コマンドまたはアクション	目的
ステップ 3	switch(config)# **show***application-name***status**	（任意） 指定されたアプリケーションについて、CFS配信ステータスを表示します。
ステップ 4	switch(config)# **copy running-config startup config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

CFS をイネーブルにして、FC タイマー コンフィギュレーションを配信する例を示します。

```
switch(config)# fctimer distribute
switch(config)# show fctimer status
Distribution : Enabled
switch(config)# copy running-config startup-config
[########################################] 100%
```

CFS をイネーブルにして IVR 設定を配信する

CFS をイネーブルにして、効率的な IVR 設定管理を実現するため、また VSAN 内のファブリック全体に対する単一ポイントを提供するために内部 VSAN ルーティング（IVR）設定を配信できます。

はじめる前に

ストレージ VDC 内にいることを確認します。ストレージ VDC に切り替えるには、**switchto vdc fcoe** コマンドを使用します。

Advanced SAN Services ライセンスをインストールする必要があります。

IVR 機能をイネーブルにする必要があります。これを実行するには、**feature ivr** コマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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	switch(config)# **ivr distribute**	CFS をイネーブルにして、IVR 設定のアップデートを配信します。 （注） ファブリック内のすべての IVR 対応スイッチ上でIVR配信をイネーブルにする必要があります。

	コマンドまたはアクション	目的
ステップ 3	switch(config)# **show cfs application**	（任意） CFS 配信ステータスを表示します。
ステップ 4	switch(config)# **copy running-config startup config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。

CFS をイネーブルにして、IVR コンフィギュレーションを配信する例を示します。

```
switch(config)# ivr distribute
switch(config)# show cfs application
----------------------------------------------
Application Enabled Scope
----------------------------------------------
ivr Yes Physical-fc
switch(config)# copy running-config startup-config
[########################################] 100%
```

CFS をイネーブルにして NTP 設定を配信する

ネットワーク内のすべての Cisco NX-OS デバイスに NTP コンフィギュレーションを配信するように CFS をイネーブルにできます。

はじめる前に

NTP 機能をイネーブルにします（**feature ntp** コマンドを使用）。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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	switch(config)# **ntp distribute**	CFS をイネーブルにして、NTP コンフィギュレーションのアップデートを配信します。
ステップ 3	switch(config)# **show***application-name***status**	（任意） 指定されたアプリケーションについて、CFS配信ステータスを表示します。
ステップ 4	switch(config)# **copy running-config startup config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

	コマンドまたはアクション	目的

```
switch# configure terminal
switch(config)# ntp distribute
switch(config)# show ntp status
Distribution : Enabled
switch(config)# copy running-config startup-config
```

CFS をイネーブルにして RADIUS 設定を配信する

ネットワーク内のすべての Cisco NX-OS デバイスに RADIUS コンフィギュレーションを配信するように CFS をイネーブルにできます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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	switch(config)# **radius distribute**	CFS をイネーブルにして、RADIUS 設定のアップデートを配信します。
ステップ 3	switch(config)# **show***application-name***status**	（任意） 指定されたアプリケーションについて、CFS 配信ステータスを表示します。
ステップ 4	switch(config)# **copy running-config startup config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

```
switch# configure terminal
switch(config)# radius distribute
switch(config)# show radius status
Distribution : Enabled
switch(config)# copy running-config startup-config
```

CFS をイネーブルにして RSCN 設定を配信する

CFS をイネーブルにして、ファブリック内のすべての Cisco NX-OS デバイスに対して登録状態変更通知（RSCN）設定を配信できます。

はじめる前に

ストレージ VDC 内にいることを確認します。ストレージ VDC に切り替えるには、**switchto vdc fcoe** コマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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	switch(config)# **rscn distribute**	CFS をイネーブルにして、RSCN 設定のアップデートを配信します。
ステップ 3	switch(config)# **show cfs application**	（任意） CFS 配信ステータスを表示します。
ステップ 4	switch(config)# **copy running-config startup config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

CFS をイネーブルにして、RSCN コンフィギュレーションを配信する例を示します。

```
switch(config)# rscn distribute
switch(config)# show cfs application
----------------------------------------------
Application Enabled Scope
----------------------------------------------
rscn Yes Logical
switch(config)# copy running-config startup-config
[########################################] 100%
```

CFS をイネーブルにして TACACS+ 設定を配信する

ネットワーク内のすべての Cisco NX-OS デバイスに TACACS+ コンフィギュレーションを配信するように CFS をイネーブルにできます。

はじめる前に

TACACS+ 機能をイネーブルにします（**feature tacacs+** コマンドを使用）。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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	switch(config)# **tacacs+ distribute**	CFS をイネーブルにして、TACACS+ 設定のアップデートを配信します。
ステップ 3	switch(config)# **show***application-name***status**	（任意） 指定されたアプリケーションについて、CFS 配信ステータスを表示します。
ステップ 4	switch(config)# **copy running-config startup config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

```
switch# configure terminal
switch(config)# tacacs+ distribute
switch(config)# show tacacs+ status
Distribution : Enabled
switch(config)# copy running-config startup-config
```

CFS をイネーブルにしてユーザ ロール設定を配信する

ネットワーク内のすべての Cisco NX-OS デバイスにユーザ ロール コンフィギュレーションを配信するように CFS をイネーブルにできます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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	switch(config)# **role distribute**	CFS をイネーブルにしてユーザ ロール設定を配信します。
ステップ 3	switch(config)# **show***application-name***status**	（任意） 指定されたアプリケーションについて、CFS 配信ステータスを表示します。
ステップ 4	switch(config)# **copy running-config startup config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレー

	コマンドまたはアクション	目的
		ションにコピーして、変更を継続的に保存します。

```
switch# configure terminal
switch(config)# role distribute
switch(config)# show role status
Distribution : Enabled
switch(config)# copy running-config startup-config
```

CFS 配信モードの指定

イーサネットまたは IPv4 での CFS 配信モードを指定して有効にできます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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	switch(config)# **cfs** {**eth** | **ipv4**} **distribute**	デバイス上のすべてのアプリケーションに対するイーサネットまたは IPv4 を介した CFS 配信をグローバルにイネーブルにします。
ステップ 3	switch(config)# **show cfs status**	（任意） 配信モードを含む CFS の現在の状態を表示します。
ステップ 4	switch(config)# **copy running-config startup config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

```
switch# configure terminal
switch(config)# cfs ipv4 distribute
switch(config)# show cfs status
Distribution : Enabled
Distribution over IP : Disabled
Distribution over Ethernet : Enabled
switch(config)# copy running-config startup-config
```

CFSoIP の IP マルチキャスト アドレスの設定

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 メカニズムなど、CFS プロトコル固有の配信では、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。CFSoIPv4 の配信に使用する IP マルチキャスト アドレスを設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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	switch(config)# **no cfs ipv4 distribute**	デバイス上のすべてのアプリケーションに対して CFSoIP配信をグローバルにディセーブルにします。 （注） マルチキャスト アドレスを変更する前に、CFSoIP をディセーブルにする必要があります。
ステップ 3	switch(config)# **cfs ipv4 mcast-address***ip-address*	IPv4 を介した CFS 配信のマルチキャスト 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 4	switch(config)# **cfs ipv4 distribute**	デバイス上のすべてのアプリケーションに対して CFSoIP 配信をグローバルにイネーブルにします。
ステップ 5	switch(config)# **show cfs status**	（任意） イネーブルかどうか、IP モード、マルチキャスト アドレスなど、CFS の現在の状態を表示します。
ステップ 6	switch(config)# **copy running-config startup config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

```
switch# configure terminal
switch(config)# no cfs ipv4 distribute
This will prevent CFS from distributing over IPv4 network.
Are you sure? (y/n) [n] y
switch(config)# cfs ipv4 mcast-address 239.255.1.1
Distribution over this IP type will be affected
Change multicast address for CFS-IP?
Are you sure? (y/n) [n] y
switch(config)# cfs ipv4 distribute
switch(config)# show cfs status
Distribution : Enabled
Distribution over IP : Enabled - mode IPv4
IPv4 multicast address : 239.255.1.1
switch(config)# copy running-config startup-config
```

CFS リージョンの設定

CFS リージョンの作成

CFS リージョンを作成し、Smart Call Home などのアプリケーションを追加できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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	switch(config)#**cfs region***region-number*	リージョンを作成し、指定されたリージョンのコンフィギュレーション モードを開始します。
ステップ 3	switch(config-cfs-region)#*application-name*	指定されたリージョンに対して、指定アプリケーションを追加します。
ステップ 4	switch(config-cfs-region)#**show cfs regions brief**	（任意） 設定されたすべてのリージョンとアプリケーションを表示しますが、ピアは表示されません。
ステップ 5	switch(config-cfs-region)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

```
switch# configure terminal
switch(config)# cfs region 4
switch(config-cfs-region)# callhome
switch(config-cfs-region)# show cfs regions brief
---------------------------------------
Region Application Enabled
---------------------------------------
4      callhome    yes
switch(config-cfs-region)# copy running-config startup-config
```

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異なるリージョンに移動できます。たとえば、NTP をエリア 1 からエリア 2 に移動できます。

（注） アプリケーションを移動すると、その範囲は新しいリージョンに制限されます。配信用またはマージ用の他のすべてのリージョンを無視します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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	switch(config)# **cfs region***region-number*	指定したリージョンの設定モードを開始します。
ステップ 3	switch(config-cfs-region)# *application-name*	移動するアプリケーションを指定します。
ステップ 4	switch(config-cfs-region)# **show cfs regions name***application-name*	（任意） 指定されたアプリケーションのピアおよびリージョン情報を表示します。
ステップ 5	switch(config-cfs-region)# **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。

```
switch# configure terminal
switch(config)# cfs region 2
switch(config-cfs-region)# callhome
switch(config-cfs-region)# show cfs regions name callhome
Region-ID : 2
Application: callhome
Scope : Physical-fc-ip
--------------------------------------------------------------------------------
Switch WWN IP Address
--------------------------------------------------------------------------------
20:00:00:22:55:79:a4:c1 172.28.230.85 [Local]
switch
Total number of entries = 1
switch(config-cfs-region)# copy running-config startup-config
```

CFS リージョンからのアプリケーションの削除

アプリケーションをリージョンから削除できます。アプリケーションをリージョンから削除することは、アプリケーションをデフォルト リージョンに戻すことと同じです。通常、デフォルトの領域は領域 0 です。このアクションにより、ファブリック全体がアプリケーションの配信範囲になります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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	switch(config)# **cfs region***region-number*	指定したリージョンの設定モードを開始します。
ステップ 3	switch(config-cfs-region)# **no***application-name*	指定されたアプリケーションをリージョンから削除します。
ステップ 4	このリージョンから削除するアプリケーションごとにステップ 3 を繰り返します。	（任意）
ステップ 5	switch(config-cfs-region)# **show cfs regions brief**	（任意） 設定されたすべてのリージョンとアプリケーションを表示しますが、ピアは表示されません。
ステップ 6	switch(config-cfs-region)# **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。

```
switch# configure terminal
switch(config)# cfs region 2
switch(config-cfs-region)# no ntp
switch(config-cfs-region)# show cfs regions brief
---------------------------------------
Region Application Enabled
---------------------------------------
4      tacacs+     yes
6      radius      yes
switch(config-cfs-region)# copy running-config startup-config
```

CFS リージョンの削除

リージョンを削除し、リージョン内のすべてのアプリケーションをデフォルト リージョンに戻すことができます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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	switch(config)# **no cfs region***region-number*	この操作によってリージョン内のすべてのアプリケーションがデフォルト リージョンに移されることを伝える警告が表示されたあと、指定されたリージョンが削除されます。 （注） リージョンの削除後、グローバル コンフィギュレーション モードに戻ります。
ステップ 3	switch(config)# **show cfs regions brief**	（任意） 設定されたすべてのリージョンとアプリケーションを表示しますが、ピアは表示されません。
ステップ 4	switch(config)# **show cfs application name***application-name*	（任意） ローカルアプリケーション情報を名前別に表示します。
ステップ 5	switch(config)# **copy running-config startup config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。

```
switch# configure terminal
switch(config)# no cfs region 4
WARNING: All applications in the region will be moved to default region.
Are you sure? (y/n) [n] y
switch(config)# show cfs regions brief
---------------------------------------
Region Application Enabled
---------------------------------------
6      callhome      no
switch(config)# show cfs application name callhome
Enabled : Yes
Timeout : 20s
Merge Capable : Yes
Scope : Physical-fc-ip
Region : Default
switch(config)# copy running-config startup-config
```

CFS 設定の作成と配信

アプリケーションのコンフィギュレーションの変更を作成し、その変更をアプリケーション ピアに配信できます。

注意 変更をコミットしない場合、変更は配信されず、アプリケーション ピア デバイスの実行コンフィギュレーションに保存されません。

注意 配信されたアプリケーション ピア デバイスごとに変更をスタートアップ コンフィギュレーションに保存しない場合、変更は実行コンフィギュレーションだけに保持されます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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	switch(config)# *application-name*	CFS が指定されたアプリケーション名のセッションを開始し、ファブリックをロックすることを指定します。
ステップ 3	switch(config-callhome)# *application-command*	コンフィギュレーションの変更が作業コピーとして保存され、**commit** コマンドを入力するまで実行コンフィギュレーションには保存されないことを指定します。
ステップ 4	追加するコンフィギュレーション コマンドごとにステップ 3 を繰り返します。	（任意）
ステップ 5	switch(config-callhome)# **show***application-name***status**	（任意） 指定されたアプリケーションについて、CFS 配信ステータスを表示します。
ステップ 6	switch(config-callhome)# **commit**	CFS は、コンフィギュレーションの変更を各アプリケーション ピア デバイスの実行コンフィギュレーションに配信します。1 台以上の外部デバイスが成功のステータスを報告すると、ソフトウェアは実行コンフィギュレーションを CFS 作業コピーからの変更で上書きし、ファブリック ロックを解放します。成功のステータスを報告する外部デバイスがない場合、変更は行われず、ファブリック ロックがそのまま適用されます。

	コマンドまたはアクション	目的
ステップ 7	switch(config-callhome)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

```
switch# configure terminal
switch(config)# snmp-server contact personname@companyname.com
switch(config)# callhome
switch(config-callhome)# email-contact admin@Mycompany.com
switch(config-callhome)# phone-contact +1-800-123-4567
switch(config-callhome)# street-address 123 Anystreet st. Anytown,AnyWhere
switch(config-callhome)# show callhome status
Distribution : Enabled
switch(config-callhome)# commit
switch(config-callhome)# copy running-config startup-config
```

ロック済みセッションのクリア

ファブリック内のデバイスから、アプリケーションによって設定されたロックをクリアできます。

注意 ファブリックのロックをクリアすると、そのファブリック内のデバイスで保留されているコンフィギュレーションは破棄されます。

はじめる前に

ロックを解放するには、管理者権限が必要です。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **show** *application-name* **status**	（任意） 現在のアプリケーションの状態を表示します。
ステップ 2	switch# **clear** *application-name* **session**	アプリケーション コンフィギュレーション セッションをクリアし、ファブリックのロックをクリアします。保留中の変更はすべて破棄されます。
ステップ 3	switch# **show** *application-name* **status**	（任意） 現在のアプリケーションの状態を表示します。

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

```
Last operational state: Fabric Locked
switch# clear ntp session
switch# show ntp status
Distribution : Enabled
Last operational state: No session
```

CFS 設定の破棄

コンフィギュレーションの変更を破棄して、ロックを解放できます。

注意 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。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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	switch(config)# *application-name***abort**	アプリケーション設定を打ち切り、設定変更を破棄し、CFS セッションを閉じ、ファブリック ロックを解除します。 （注） **abort** コマンドは、ファブリック ロックを取得したデバイスだけでサポートされます。
ステップ 3	switch(config)# **show***application-name***session status**	（任意） 指定されたアプリケーションについて、CFS セッションのステータスを表示します。

```
switch# configure terminal
switch(config)# ntp abort
This will prevent CFS from distributing the configuration to other switches.
Are you sure? (y/n) [n] y
switch(config)# show ntp session status
Last Action Time Stamp : Wed Aug 14 16:07:25 2013
Last Action : Abort
Last Action Result : Success
Last Action Failure Reason : none
```

CFS 配信のグローバルなディセーブル化

デバイスに対する CFS 配信をディセーブルにして、物理的な接続を維持しながら、CFS を使用してファブリック全体の配信からアプリケーションを分離できます。デバイスで CFS をグローバルにディセーブルにすると、デバイスに対する CFS の操作が制限され、すべての CFS コマンドは、デバイスが物理的に分離されているかのように機能し続けます。

はじめる前に

仮想ポートチャネル（vPC）機能をイネーブルにすると、IP配信だけがディセーブルになります。CFS 配信をディセーブルにする前に、vPC をディセーブルにする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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	switch(config)# **no cfs distribute**	デバイス上のすべてのアプリケーションに対してCFS配信をグローバルにディセーブルにします。
ステップ 3	switch(config)# **show cfs status**	（任意） デバイスに対するグローバルなCFS配信ステータスを表示します。
ステップ 4	switch(config)# **copy running-config startup config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

```
switch# configure terminal
switch(config)# no cfs distribute
This will prevent CFS from distributing the configuration to other switches.
Are you sure? (y/n) [n] y
switch(config)# show cfs status
Distribution : Disabled
Distribution over IP : Disabled
IPv4 multicast address : 239.255.70.83
Distribution over Ethernet : Disabled
switch(config)# copy running-config startup-config
```

CFS 設定の確認

コマンド	目的
show *application-name* **session status**	最終アクション、結果、失敗した場合はその理由を含む、コンフィギュレーションセッションステータスを表示します。
show *application-name* **status**	指定されたアプリケーションについて、CFS配信ステータスを表示します。
show cfs application	現在CFSがイネーブルのアプリケーションを表示します。

コマンド	目的
show cfs application name *application-name*	特定のアプリケーションについて、イネーブルまたはディセーブルの状態、CFS で登録されたタイムアウト、CFS でマージサポートが登録されている場合のマージ機能、配信範囲、配信リージョンなどの詳細を表示します。
show cfs internal	メモリの統計情報、イベント履歴など、CFS 内部の情報を表示します。
show cfs lock	すべてのアクティブ ロックを表示します。
show cfs merge status name *name* [**detail**]	特定のアプリケーションのマージステータスを表示します。
show cfs peers	物理ファブリックのすべてのピアを表示します。
show cfs regions	ピアおよびリージョンの情報とともにすべてのアプリケーションを表示します。
show cfs status	デバイスでの CFS 配信のステータスと IP 配信情報を表示します。
show logging level cfs	CFS ロギングのコンフィギュレーションを表示します。
show tech-support cfs	CFS の問題解決時にテクニカルサポートが必要とする CFS コンフィギュレーションに関する情報を表示します。

CFS に関する追加情報

関連資料

関連項目	マニュアル タイトル
CFS CLI コマンド	『*Cisco Nexus 7000 Series NX-OS System Management Command Reference*』 『*Cisco Nexus 7000 Series NX-OS SAN Switching Command Reference*』

関連項目	マニュアル タイトル
デバイス エイリアスの CFS コンフィギュレーション DPVM の CFS コンフィギュレーション FC ドメインの CFS コンフィギュレーション FC ポート セキュリティの CFS コンフィギュレーション FC タイマーの CFS コンフィギュレーション IVR の CFS コンフィギュレーション RSCN の CFS コンフィギュレーション	『*Cisco Nexus 7000 Series NX-OS SAN Switching Configuration Guide*』
FCoE	『*Cisco NX-OS FCoE Configuration Guide for Cisco Nexus 7000 and Cisco MDS 9500*』
RADIUS	『*Cisco Nexus 7000 Series NX-OS Security Configuration Guide*』
TACACS+	『*Cisco Nexus 7000 Series NX-OS Security Configuration Guide*』
ユーザ ロール	『*Cisco Nexus 7000 Series NX-OS Security Configuration Guide*』

MIB

MIB	MIB のリンク
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/public/sw-center/netmgmt/cmtk/mibs.shtml

CFS の機能の履歴

次の表に、このマニュアルの新機能および変更された機能を要約し、各機能がサポートされているリリースを示します。ご使用のソフトウェア リリースで、本書で説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。

表 *4* : *CFS* の機能の履歴

機能名	リリース	機能情報
CFS プロトコル	5.2(1)	デバイス エイリアス、DPVM、FC ドメイン、FC ポート セキュリティ、FC タイマー、IVR、および RSCN に対して CFS over Fibre Channel（CFSoFC）配信サポートが追加されました。
CFS プロトコル	4.1(2)	この機能が導入されました。

第 4 章

NTP の設定

この章では、Cisco NX-OS デバイスで ネットワーク タイム プロトコル（NTP）を設定する方法について説明します。

この章は、次の項で構成されています。

- 機能情報の確認，51 ページ
- NTP について，52 ページ
- NTP のライセンス要件，54 ページ
- NTP の前提条件，55 ページ
- NTP の注意事項と制約事項，55 ページ
- NTP のデフォルト設定，56 ページ
- NTP の設定，57 ページ
- NTP の設定確認，73 ページ
- NTP の設定例，73 ページ
- その他の参考資料，75 ページ
- NTP の機能の履歴，75 ページ

機能情報の確認

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

NTP について

ネットワーク タイムプロトコル（NTP）は、分散している一連のタイムサーバとクライアント間で1日の時間を同期させ、複数のネットワーク デバイスから受信するシステム ログや時間関連のイベントを相互に関連付けられるようにします。NTP ではトランスポート プロトコルとして、ユーザ データグラム プロトコル（UDP）を使用します。すべての NTP 通信は UTC を使用します。

NTP サーバは通常、タイム サーバに接続されたラジオ クロックやアトミック クロックなどの正規の時刻源から時刻を受信し、ネットワークを介してこの時刻を配信します。NTP はきわめて効率的で、毎分 1 パケット以下で 2 台のマシンを相互に 1 ミリ秒以内に同期します。

NTP では層（stratum）を使用して、ネットワーク デバイスと正規の時刻源の距離を表します。

- ストラタム 1 のタイム サーバは、信頼できる時刻源に直接接続されます（無線時計や原子時計または GPS 時刻源など）。
- ストラタム 2 の NTP サーバは、ストラタム 1 のタイム サーバから NTP を使用して時刻を受信します。

同期の前に、NTP は複数のネットワーク サービスが報告した時刻を比較し、1 つの時刻が著しく異なる場合は、それが Stratum 1 であっても、同期しません。Cisco NX-OS は、無線時計や原子時計に接続できず、ストラタム 1 サーバとして動作することはできないため、インターネット上で利用できるパブリック NTP サーバを使用することを推奨します。ネットワークがインターネットから切り離されている場合、Cisco NX-OS では、NTP によって時刻が同期されていなくても、NTP で同期されているものとして時刻を設定できます。

（注） NTP ピア関係を作成して、サーバで障害が発生した場合に、ネットワーク デバイスを同期させて、正確な時刻を維持するための時刻提供ホストを指定できます。

デバイス上の時刻は重要な情報であるため、NTP のセキュリティ機能を使用して、不正な時刻を誤って（または悪意を持って）設定できないように保護することを強く推奨します。その方法として、アクセス リストベースの制約方式と暗号化認証方式があります。

NTP アソシエーション

N TP アソシエーションは、次のいずれかになります。

- ピア アソシエーション：デバイスが別のデバイスに同期するか、別のデバイスをそのデバイスに同期させることができます。
- サーバ アソシエーション：デバイスは、サーバに同期します。

設定する必要があるのはアソシエーションの片側だけです。他方のデバイスは自動的にアソシエーションを確立できます。

NTP ブロードキャスト アソシエーション

ブロードキャストベースのNTPアソシエーションでは、NTPサーバは、ネットワーク全体でNTPブロードキャストパケットを送信します。ブロードキャストクライアントは、サーバによって送信されるブロードキャスト パケットをリッスンし、ポーリングには関与しません。

NTP ブロードキャスト サーバを使用すると、承認されないメッセージが指定の IPv4 ローカル ブロードキャスト アドレスに送信され、クライアントからのリクエストは通常想定されないため、大量の NTP トラフィックを生成する必要なしに数多くのクライアントを同期できます。

NTP マルチキャスト アソシエーション

NTP マルチキャスト サーバとして動作するデバイスは、NTP マルチキャスト メッセージを所定の IPv4 または IPv6 マルチキャスト グループの IP アドレスに送信します。

NTP マルチキャスト クライアントとして動作するデバイスは、NTP マルチキャスト サーバから所定の IPv4 または IPv6 マルチキャスト グループの IP アドレスに送信される NTP マルチキャスト パケットをリッスンします。

NTP マルチキャスト サーバを使用すると、承認されないメッセージが指定のマルチキャスト グループ アドレスに送信され、通常クライアントからのリクエストは期待されないため、数多くの NTP トラフィックを作成する必要なしに大量のクライアントを同期できます。

タイム サーバとしての NTP

Cisco NX-OS デバイスでは、時刻を配信するために NTP を使用できます。他のデバイスからタイムサーバとして設定できます。デバイスを正規のNTPサーバとして動作するよう設定し、外部の時刻源と同期していないときでも時刻を配信させることもできます。

CFS を使用した NTP の配信

Cisco Fabric Services（CFS）は、ローカル NTP コンフィギュレーションをネットワーク内のすべてのシスコ デバイスに配信します。

デバイス上でCFSをイネーブルにすると、NTPコンフィギュレーションが起動された場合には常に、ネットワーク全体のロックがNTPに適用されます。NTPコンフィギュレーションを変更した後で、これらの変更を破棄することもコミットすることもできます。

いずれの場合でも、CFS のロックはこのときに NTP アプリケーションから解放されます。

クロック マネージャ

クロックはさまざまなプロセス間で共有する必要のあるリソースです。NTP などの複数の時刻同期プロトコルが、システムで稼働している可能性があります。

クロック マネージャを使用して、システム内のさまざまなクロックを制御するプロトコルを指定できます。いったんプロトコルを指定すると、システム クロックの更新が始まります。クロック マネージャの設定の詳細については『*Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide*』を参照してください。

ハイ アベイラビリティ

NTP はステートレス リスタートをサポートします。リブート後またはスーパーバイザ スイッチオーバー後に、実行コンフィギュレーションが適用されます。ハイ アベイラビリティの詳細については、『*Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide*』を参照してください。

NTP ピアを設定すると、NTP サーバ障害の発生時に冗長性が得られます。

仮想化のサポート

5.2 より前の Cisco NX-OS リリースを実行している場合、プラットフォーム全体で 1 つまでの NTP のインスタンスがサポートされます。デフォルトの仮想デバイス コンテキスト（VDC）で NTP を設定する必要があり、他に指定しない限りデフォルトの VDC が自動的に使用されます。

Cisco NX-OS Release 5.2 以降を実行している場合、NTP の複数のインスタンスが、VDC ごとに 1 つのインスタンスでサポートされます。VDC を特別に設定しない限り、デフォルトでは、Cisco NX-OS のデフォルトの VDC が使用されます。システム クロックと同期されるのは常に 1 つの VDC（デフォルトでは、デフォルト VDC）のみです。他のすべての NTP デーモンは、他のデバイスの NTP サーバとしてのみ機能します。システム クロックと同期する VDC を変更するには、clock protocol ntp vdc*vdc-id* コマンドを使用します。

NTP は Virtual Routing and Forwarding（VRF）インスタンスを認識します。NTP サーバおよび NTP ピアに対して特定の VRF を設定していない場合、NTP はデフォルトの VRF を使用します。VRF の詳細情報については、『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

VDC の詳細については、『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』を参照してください。

NTP のライセンス要件

製品	ライセンス要件
Cisco NX-OS	NTP 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 nx-os イメージにバンドルされており、無料で提供されます。NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

NTP の前提条件

NTP の前提条件は、次のとおりです。

- NTP を設定するには、NTP が動作している 1 つ以上のサーバに接続できなければなりません。
- VDC を設定するには、適切なライセンスをインストールする必要があります。設定情報については『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』、ライセンス情報については『*Cisco NX-OS Licensing Guide*』を参照してください。

NTP の注意事項と制約事項

NTP に関する設定時の注意事項および制約事項は、次のとおりです。

- Cisco NX-OS ソフトウェアは、NTP バージョン 4（NTPv4）をサポートしています。
- NTP サーバ機能はサポートされます。
- 別のデバイスとの間にピア アソシエーションを設定できるのは、使用するクロックの信頼性が確実な場合（つまり、信頼できる NTP サーバのクライアントである場合）に限られます。
- 単独で設定したピアは、サーバの役割を担いますが、バックアップとして使用する必要があります。サーバが 2 台ある場合、いくつかのデバイスが一方のサーバに接続し、残りのデバイスが他方のサーバに接続するように設定できます。その後、2 台のサーバ間にピア アソシエーションを設定すると、信頼性の高い NTP 構成になります。
- サーバが 1 台だけの場合は、すべてのデバイスをそのサーバのクライアントとして設定する必要があります。
- NTP サーバを 2 台設定することはお勧めしません。代わりに、1 台、3 台、4 台、またはそれ以上の NTP サーバを設定することをお勧めします。

  すべての NTP サーバは、時間を返す際に同時に現在のエラーの推定値を返します。複数のサーバを使用する場合、NTP ではさらに、それらのサーバ間で時刻を決定することが必要になります。つまり、正しい時刻を含むはずの、1 つの誤差の範囲が存在することになります。NTP サーバが 2 台の場合、どちらのソースがより正しいかを NTP クライアントは決定できず、そのため、2 つのソースで共通の範囲を小さくすることができないという問題が発生する可能性があります。
- 設定できる NTP エンティティ（サーバおよびピア）は、最大 64 です。
- VRF で NTP を設定する場合は、NTP サーバおよびピアが、設定された VRF を介して相互にアクセスできることを確認します。
- ネットワーク全体の NTP サーバおよび Cisco NX-OS デバイスに、NTP 認証キーを手動で配信する必要があります。

- NTP に対して CFS がディセーブルになっていると、その NTP からコンフィギュレーションは配信されず、ネットワーク内の他のデバイスからの配信も受け取られません。
- NTP に対して CFS 配信をイネーブルにしても、**commit** コマンドを入力するまで、NTP コンフィギュレーション コマンドのエントリはNTP コンフィギュレーションに対してネットワークをロックします。ロック中は、ネットワーク内の（ロックを保持しているデバイス以外の）すべてのデバイスは NTP コンフィギュレーションを変更できません。
- CFS を使用して NTP をディセーブルにする場合、ネットワーク内のすべてのデバイスは、NTP に対して使用するよう設定したものと同じ VRF を持っている必要があります。
- VRF で NTP を設定する場合は、NTP サーバおよびピアが、設定された VRF を介して相互にアクセスできることを確認します。
- ネットワーク全体の NTP サーバおよび Cisco NX-OS デバイスに、NTP 認証キーを手動で配信する必要があります。
- 時刻の精度および信頼性要件が厳密ではない場合、NTPブロードキャストまたはマルチキャスト アソシエーションを使用すると、ネットワークがローカル化され、ネットワークは 20 以上のクライアントを持ちます。帯域幅、システム メモリ、または CPU リソースが限られているネットワークでは NTP ブロードキャストまたはマルチキャスト アソシエーションの使用をお勧めします。

（注） 情報の流れが一方向に限定されるため、NTPブロードキャストアソシエーションでは、時刻の精度がわずかに低下します。

- NTP ソースインターフェイスおよびソース設定には、クライアントで設定された場合のみ適用されるという制限があります。サーバ（NTPマスターを備えたスイッチ）で設定を行った場合、出力パケットの送信元アドレスは受信した宛先アドレスのままとなります。

NTP のデフォルト設定

次の表に、NTP パラメータのデフォルト設定を示します。

パラメータ	デフォルト
NTP	すべての VDC およびすべてのインターフェイスに対してイネーブルにします。デフォルトで、NTPはサーバおよびクライアントとしてイネーブルです。
NTP passive（アソシエーションを形成するために NTP をイネーブルにする）	イネーブル
NTP 認証	ディセーブル
NTP アクセス	イネーブル

パラメータ	デフォルト
NTP access group match all	ディセーブル
NTP broadcast server	ディセーブル
NTP multicast server	ディセーブル
NTP multicast client	ディセーブル
NTP ロギング	ディセーブル

NTP の設定

（注） この機能の Cisco NX-OS コマンドは、Cisco IOS のコマンドとは異なる場合があるので注意してください。

VDC での NTP のイネーブル化またはディセーブル化

特定の VDC で NTP をイネーブルまたはディセーブルにできます。NTP は、デフォルトではすべての VDC でイネーブルです。

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	[**no**] **feature ntp** 例： `switch(config)# feature ntp`	NTP をイネーブルまたはディセーブルにします。

ステップ 3	**show ntp status**
	
	例：
	`switch(config)# show ntp status`
	`Distribution: Enabled`
	`Last operational state: Fabric Locked`
		（任意）
		NTP アプリケーションのステータスを表示します。

	コマンドまたはアクション	目的
ステップ 4	**copy running-config startup-config** 例： `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。

インターフェイスでの NTP のイネーブル化またはディセーブル化

特定のインターフェイスで NTP をイネーブルまたはディセーブルにできます。NTP は、デフォルトではすべての VDC でイネーブルです。

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# config t`
	`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	**interface***type slot/port*
	
	例：
	`switch(config)# interface ethernet 6/1`
	`switch(config-if)#`
		インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**[no]ntp disable{ip | ipv6}** 例： `switch(config-if)# ntp disable ip`	（任意） 指定のインターフェイスで NTP IPv4 または IPv6 をディセーブルにします。インターフェイス上で NTP を再度イネーブルにするにはこのコマンドの no 形式を使用します。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

正規の NTP サーバとしてのデバイスの設定

デバイスを正規のNTPサーバとして動作するよう設定し、既存のタイムサーバと同期していないときでも時刻を配信させることができます。

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	[**no**] **ntp master** [*stratum*] 例： `switch(config)# ntp master`	正規の NTP サーバとしてデバイスを設定します。 NTP クライアントがこれらの時間を同期するのと別の階層レベルを指定できます。指定できる範囲は 1 ～ 15 です。
ステップ 3	**show running-config ntp** 例： `switch(config)# show running-config ntp`	（任意） NTP コンフィギュレーションを表示します。
ステップ 4	**copy running-config startup-config** 例： `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。

NTP サーバおよびピアの設定

NTP サーバおよびピアを設定できます。

はじめる前に

使用している NTP サーバと、そのピアの IP アドレスまたはドメイン ネーム システム（DNS）名がわかっていることを確認します。

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	[**no**] **ntp server** {*ip-address* | *ipv6-address* | *dns-name*} [**key** *key-id*] [**maxpoll** *max-poll*] [**minpoll** *min-poll*] [**prefer**] [**use-vrf** *vrf-name*] 例： `switch(config)# ntp server 192.0.2.10`	1 つのサーバと 1 つのサーバ アソシエーションを形成します。 NTP サーバとの通信で使用するキーを設定するには、**key** キーワードを使用します。*key-id* 引数の範囲は 1 ～ 65535 です。 サーバをポーリングする最大および最小の間隔を設定するには、**maxpoll** および **minpoll** キーワードを使用します。*max-poll* および *min-poll* 引数の範囲は 4 ～ 16 秒で、デフォルト値はそれぞれ 6 秒と 4 秒です。 このサーバをデバイスの優先 NTP サーバにするには、**prefer** キーワードを使用します。 指定された VRF を介して通信するように NTP サーバを設定するには、**use-vrf** キーワードを使用します。*vrf-name* 引数として、**default**、**management**、または大文字と小文字を区別した 32 文字までの任意の英数字の文字列を使用できます。 （注） NTP サーバとの通信で使用するキーを設定する場合は、そのキーが、デバイス上の信頼できるキーとして存在していることを確認してください。
ステップ 3	[**no**] **ntp peer** {*ip-address* | *ipv6-address* | *dns-name*} [**key** *key-id*] [**maxpoll** *max-poll*] [**minpoll** *min-poll*] [**prefer**] [**use-vrf** *vrf-name*] 例： `switch(config)# ntp peer 2001:0db8::4101`	1 つのピアと 1 つのピア アソシエーションを形成します。複数のピア アソシエーションを指定できます。 NTP ピアとの通信で使用するキーを設定するには、**key** キーワードを使用します。*key-id* 引数の範囲は 1 ～ 65535 です。 ピアをポーリングする最大および最小の間隔を設定するには、**maxpoll** および **minpoll** キーワードを使用します。*max-poll* および *min-poll* 引数の範囲は 4 ～ 17 秒で、デフォルト値はそれぞれ 6 秒と 4 秒です。 このピアをデバイスの優先 NTP ピアにするには、**prefer** キーワードを使用します。

	コマンドまたはアクション	目的
		指定された VRF を介して通信するように NTP ピアを設定するには、**use-vrf** キーワードを使用します。*vrf-name* 引数として、**default**、**management**、または大文字と小文字を区別した 32 文字までの任意の英数字の文字列を使用できます。
ステップ 4	**show ntp peers** 例： `switch(config)# show ntp peers`	（任意） 設定されたサーバおよびピアを表示します。 （注） ドメイン名が解決されるのは、DNS サーバが設定されている場合だけです。
ステップ 5	**copy running-config startup-config** 例： `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。

NTP 認証の設定

ローカル ロックを同期させる時刻源を認証するようデバイスを設定できます。NTP 認証をイネーブルにすると、**ntp trusted-key** コマンドによって指定されたいずれかの認証キーを時刻源が保持している場合のみ、デバイスはその時刻源と同期します。デバイスは、認証チェックに失敗したすべてのパケットをドロップし、それらのパケットでローカル クロックがアップデートされないようにします。NTP 認証はデフォルトでディセーブルになっています。

はじめる前に

NTP サーバおよび NTP ピアの認証は、**ntp server** および **ntp peer** コマンドのそれぞれで key キーワードを使用して、アソシエーションごとに設定します。すべての NTP サーバとピアのアソシエーションを、指定する認証キーによって設定するようにしてください。**ntp server** または **ntp peer** コマンドで key キーワードを指定しない場合、認証なしでの動作が続けられます。

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。

	コマンドまたはアクション	目的
ステップ 2	[**no**] **ntp authentication-key***number***md5***md5-string* 例： `switch(config)# ntp authentication-key 42 md5 aNiceKey`	認証キーを定義します。デバイスが時刻源と同期するのは、時刻源がこれらの認証キーのいずれかを持ち、**ntp trusted-key***number* コマンドによってキー番号が指定されている場合だけです。 認証キーの範囲は 1 ～ 65535 です。MD5 文字列の場合は、最大 8 文字の英数字を指定できます。 Cisco NX-OS Release 7.3(0)D1(1) 以降では、MD5 文字列に最大 32 文字の英数字を入力できます。
ステップ 3	**show ntp authentication-keys** 例： `switch(config)# show ntp authentication-keys`	（任意） 設定済みの NTP 認証キーを表示します。

ステップ 4	[**no**] **ntp trusted-key***number*
	
	例：
	`switch# config t`
	`Enter configuration commands, one per line. End with CNTL/Z.`
	`switch(config)# ntp authentication-key 42 md5 aNiceKey`
	`switch(config)# ntp server 10.1.1.1 key 42`
	`switch(config)# ntp trusted-key 42`
	`switch(config)# ntp authenticate`
	`switch(config)# copy running-config startup-config`
	`[##########################################] 100%`
	`switch(config)#`
		1 つ以上のキー（ステップ 2 で定義されているもの）を指定します。デバイスが時刻源と同期するために、時刻源はこのキーを NTP パケット内に提供する必要があります。Trusted Key の範囲は 1 ～ 65535 です。
		このコマンドにより、デバイスが、信頼されていない時刻源と誤って同期する、ということが防止されます。

ステップ 5	**show ntp trusted-keys** 例： `switch(config)# show ntp trusted-keys`	（任意） 設定済みの NTP の信頼されているキーを表示します。
ステップ 6	[**no**] **ntp authenticate** 例： `switch(config)# ntp authenticate`	NTP 認証機能をイネーブルまたはディセーブルにします。NTP 認証はデフォルトでディセーブルになっています。
ステップ 7	**show ntp authentication-status** 例： `switch(config)# show ntp authentication-status`	（任意） NTP 認証の状況を表示します。

	コマンドまたはアクション	目的
ステップ 8	**copy running-config startup-config** 例： `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。

NTP アクセス制限の設定

アクセス グループを使用して、NTP サービスへのアクセスを制御できます。具体的には、デバイスを許可する要求のタイプ、およびデバイスが応答を受け取るサーバを指定できます。

アクセス グループを設定しない場合は、すべてのデバイスに NTP アクセス権が付与されます。何らかのアクセス グループを設定した場合は、ソース IP アドレスがアクセス リストの基準をパスしたリモート デバイスに対してだけ、NTP アクセス権が付与されます。

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	[**no**] **ntp access-group** {**peer** | **serve** | **serve-only** | **query-only**} *access-list-name* 例： `switch(config)# ntp access-group peer accesslist1`	NTP のアクセスを制御し、基本の IP アクセス リストを適用するためのアクセス グループを作成または削除します。 NTP がピアに設定されている拒否 ACL ルールに一致した場合、ACL の処理は停止し、次のアクセス グループ オプションに継続されません。 • **peer** キーワードは、デバイスが時刻要求と NTP 制御クエリーを受信し、アクセス リストで指定されているサーバと同期するようにします。 • **serve** キーワードは、アクセス リストに指定されているサーバからの時刻要求と NTP 制御クエリーをデバイスが受信できるようにしますが、指定されたサーバとは同期しないようにします。 • **serve-only** キーワードは、アクセス リストで指定されたサーバからの時刻要求のみをデバイスが受信できるようにします。

	コマンドまたはアクション	目的
		• **query-only** キーワードは、デバイスがアクセス リストで指定されたサーバからの NTP 制御クエリーのみを受信するようにします。
ステップ 3	**show ntp access-groups** 例： `switch(config)# show ntp access-groups`	（任意） NTP アクセス グループのコンフィギュレーションを表示します。
ステップ 4	**copy running-config startup-config** 例： `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。

NTP ソース IP アドレスの設定

NTP は、NTP パケットが送信されたインターフェイスのアドレスに基づいて、すべての NTP パケットにソース IP アドレスを設定します。特定のソース IP アドレスを使用するよう NTP を設定できます。

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	[**no**] **ntp source** *ip-address* 例： `switch(config)# ntp source 192.0.2.1`	すべての NTP パケットにソース IP アドレスを設定します。*ip-address* には IPv4 または IPv6 形式を使用できます。
ステップ 3	**copy running-config startup-config** 例： `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。

NTP ソース インターフェイスの設定

特定のインターフェイスを使用するよう NTP を設定できます。

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	[**no**] **ntp source-interface** *interface* 例： `switch(config)# ntp source-interface ethernet 2/1`	すべての NTP パケットに対してソースインターフェイスを設定します。**?** キーワードを使用して、サポートされるインターフェイスを表示します。
ステップ 3	**copy running-config startup-config** 例： `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。

NTP ブロードキャスト サーバの設定

インターフェイス上で NTP IPv4 ブロードキャスト サーバを設定できます。デバイスは、そのインターフェイスを介してブロードキャスト パケットを定期的に送信します。クライアントは応答を送信する必要はありません。

はじめる前に

switchto vdc コマンドを使用して特定の非デフォルトの VDC に変更します。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure t**
	
	例：
	`switch# config t`
	`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。

	コマンドまたはアクション	目的

ステップ 2	**interface***type slot/port*
	
	例：
	`switch(config)# interface ethernet 6/1`
	`switch(config-if)#`
		インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	[**no**] **ntp broadcast** [**destination***ip-address*] [**key***key-id*] [**version***number*] 例： `switch(config-if)# ntp broadcast destination 192.0.2.10`	指定されたインターフェイスの IPv4 NTP ブロードキャスト サーバをイネーブルにします。 • destination*ip-address*：ブロードキャスト宛先 IP アドレスを設定します。 • key *key-id*：ブロードキャスト認証キー番号を設定します。有効な範囲は 1 ～ 65535 です。 • version*number*：NTP バージョンを設定します。範囲は 2 ～ 4 です。

ステップ 4	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス コンフィギュレーション モードを終了します。

ステップ 5	（任意）[**no**] **ntp broadcastdelay***delay* 例： `switch(config)# ntp broadcastdelay 100`	（任意）推定ブロードキャスト ラウンドトリップ遅延をマイクロ秒単位で設定します。範囲は 1 ～ 999999 です。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） （任意）リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、NTP ブロードキャスト パケットを送信するようにイーサネット インターフェイスを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet6/1
switch(config-if)# ntp broadcast 192.0.2.10
```

NTP マルチキャスト サーバの設定

インターフェイスに対して NTP IPv4 または IPv6 マルチキャスト サーバを設定できます。デバイスは、そのインターフェイスを介してマルチキャスト パケットを定期的に送信します。

はじめる前に

switchto vdc コマンドを使用して特定の非デフォルトの VDC に変更します。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure t**
	
	例：
	`switch# config t`
	`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	**interface***type slot/port*
	
	例：
	`switch(config)# interface`
	`ethernet 6/1`
	`switch(config-if)#`
		インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	[**no**] **ntp multicast** [*ipv4-address* | *ipv6-address*] [**key***key-id*] [**ttl***value*] [**version***number*]
	
	例：
	`switch(config-if)# ntp multicast`
	`FF02:1::FF0E:8C6C`
		指定されたインターフェイスの NTP IPv6 ブロードキャスト サーバをイネーブルにします。
		• destination*ip-address*：ブロードキャスト宛先 IP アドレスを設定します。
		• key*key-id*：ブロードキャスト認証キー番号を設定します。有効な範囲は 1 ～ 65535 です。
		• ttl*value*：マルチキャスト パケットの存続可能時間値。範囲は 1 ～ 255 です。
		• version*number*：NTP バージョンを設定します。
		（注） IPv4 マルチキャスト サーバで指定できる範囲は 2 ～ 4 です。

ステップ 4	**copy running-config startup-config**
	
	例：
	`switch(config)# copy`
	`running-config startup-config`
		（任意）
		（任意）リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、NTPマルチキャストパケットを送信するようにイーサネットインターフェイスを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet2/2
switch(config-if)# ntp multicast FF02::1:FF0E:8C6C
```

NTP マルチキャスト クライアントの設定

インターフェイス上で NTP マルチキャスト クライアントを設定できます。デバイスは NTP マルチキャスト メッセージをリッスンし、マルチキャストが設定されていないインターフェイスからのメッセージを廃棄します。

はじめる前に

switchto vdc コマンドを使用して特定の非デフォルトの VDC に変更します。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure t**
	
	例：
	`switch# config t`
	`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	**interface***type slot/port*
	
	例：
	`switch(config)# interface ethernet 6/1`
	`switch(config-if)#`
		インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	[**no**] **ntp multicast client** [*ipv4-address* | *ipv6-address*] 例： `switch(config-if)# ntp multicast FF02:1::FF0E:8C6C`	指定されたインターフェイスの NTP IPv6 ブロードキャスト サーバをイネーブルにします。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） （任意）リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

セカンダリ（非デフォルト）VDC での NTP 設定

同期のためにデフォルトの VDC とそのクライアントから時間更新を受信するように非デフォルト VDC を設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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	switch(config)# **feature ntp**	非デフォルト VDC の NTP をイネーブルにします。
ステップ 3	switch(config)# **ntp master**	正規の NTP サーバとしてデバイスを設定します。
ステップ 4	switch(config)# **ntp source-interface** *interface*	（任意） すべての NTP パケットに対してソースインターフェイスを設定します。次のリストに、*interface* として有効な値を示します。 • ethernet • loopback • mgmt • port-channel • vlan
ステップ 5	[**no**] **ntp source** *ip-address*	（任意） すべての NTP パケットにソース IP アドレスを設定します。*ip-address* には IPv4 または IPv6 形式を使用できます。
ステップ 6	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。

次に、セカンダリ（非デフォルト）VDC で NTP を設定する例を示します。

```
switch# configure terminal
switch(config)# feature ntp
switch(config)# ntp master
switch(config)# ntp source-interface ethernet
switch(config)# ntp source 192.0.2.2
switch(config)# copy running-config startup-config
```

NTP ロギングの設定

重要な NTP イベントでシステム ログを生成するよう、NTP ロギングを設定できます。NTP ロギングはデフォルトでディセーブルになっています。

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	[**no**] **ntp logging** 例： `switch(config)# ntp logging`	重要な NTP イベントでシステム ログを生成することをイネーブルまたはディセーブルにします。NTP ロギングはデフォルトでディセーブルになっています。
ステップ 3	**show ntp logging-status** 例： `switch(config)# show ntp logging-status`	（任意） NTP ロギングのコンフィギュレーション状況を表示します。
ステップ 4	**copy running-config startup-config** 例： `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。

NTP 用の CFS 配信のイネーブル化

NTP コンフィギュレーションを他の CFS 対応デバイスに配信するために、NTP 用の CFS 配信をイネーブルにできます。

はじめる前に

デバイスの CFS 配信をイネーブルにしていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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	switch(config)# [**no**] **ntp distribute**	CFS を介して配信される NTP コンフィギュレーションのアップデートをデバイスが受信することを、イネーブルまたはディセーブルにします。
ステップ 3	switch(config)# **show ntp status**	（任意） NTP CFS の配信状況を表示します。
ステップ 4	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、デバイスが CFS を介して NTP 設定の更新を受信できるようにする例を示します。

```
switch# configure terminal
switch(config)# ntp distribute
switch(config)# copy running-config startup-config
```

NTP 設定変更のコミット

NTP コンフィギュレーションの変更をコミットすると、保留データベースのコンフィギュレーション変更によって有効なデータベースが上書きされ、ネットワーク内のすべてのデバイスが同じコンフィギュレーションを受け取ります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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	switch(config)# **ntp commit**	ネットワーク内のすべての Cisco NX-OS デバイスに NTP コンフィギュレーションの変更を配信し、CFS ロックを解放します。このコマンドは、保留データベースに対して行われた変更によって、有効なデータベースを上書きします。

NTP 設定変更の廃棄

コンフィギュレーション変更の後で、これらの変更をコミットせずに、破棄するよう選択することもできます。変更を破棄すると、Cisco NX-OS によって保留データベースの変更が削除され、CFS ロックが解放されます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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	switch(config)# **ntp abort**	保留データベースでNTP コンフィギュレーションの変更を破棄して、CFS ロックを解放します。このコマンドは、NTP コンフィギュレーションを起動したデバイスで使用します。

CFS セッション ロックの解放

NTP コンフィギュレーションを実行したが、変更をコミットまたは破棄してロックを解放し忘れた場合は、自分で、または他の管理者がネットワーク内の任意のデバイスからロックを解放できます。また、この操作では、保留データベースの変更が破棄されます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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	switch(config)# **clear ntp session**	保留データベースでNTP コンフィギュレーションの変更を破棄して、CFS ロックを解放します。

NTP の設定確認

NTP の設定を表示するには、次のいずれかの作業を行います。

コマンド	目的
show ntp access-groups	NTP アクセス グループのコンフィギュレーションを表示します。
show ntp authentication-keys	設定済みの NTP 認証キーを表示します。
show ntp authentication-status	NTP 認証の状況を表示します。
show ntp internal	内部の NTP 情報を表示します。
show ntp logging-status	NTP のロギング状況を表示します。
show ntp peer-status	すべての NTP サーバおよびピアのステータスを表示します。
show ntp peers	すべての NTP ピアを表示します。
show ntp rts-update	RTS アップデートの状況を表示します。
show ntp source	設定済みの NTP ソース IP アドレスを表示します。
show ntp source-interface	設定済みの NTP ソース インターフェイスを表示します。
show ntp statistics {**io** | **local** | **memory** | **peer** {**ipaddr** {*ipv4-addr* | *ipv6-addr*} | **name** *peer-name*}}	NTP 統計情報を表示します。
show ntp trusted-keys	設定済みの NTP の信頼されているキーを表示します。
show running-config ntp	NTP 情報を表示します。

NTP セッションをクリアするには、**clear ntp session** コマンドを使用します。

NTP 統計情報を消去するには、**clear ntp statistics** コマンドを使用します。

NTP の設定例

次に、NTP サーバおよびピアを設定し、NTP 認証をイネーブルにして、NTP ロギングをイネーブルにした後で、その設定をスタートアップに保存し、リブートとリスタートを通して保存されるようにする例を示します。

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ntp server 192.0.2.105 key 42
```

```
switch(config)# ntp peer 2001:0db8::4101
switch(config)# show ntp peers
-------------------------------------------------
Peer IP Address Serv/Peer
-------------------------------------------------
2001:db8::4101 Peer (configured)
192.0.2.105 Server (configured)
switch(config)# ntp authentication-key 42 md5 aNiceKey
switch(config)# show ntp authentication-keys
-----------------------------
Auth key MD5 String
-----------------------------
42 aNicekey
switch(config)# ntp trusted-key 42
switch(config)# show ntp trusted-keys
Trusted Keys:
42
switch(config)# ntp authenticate
switch(config)# show ntp authentication-status
Authentication enabled.
switch(config)# ntp logging
switch(config)# show ntp logging
NTP logging enabled.
switch(config)# copy running-config startup-config
[########################################] 100%
switch(config)#
```

次に、以下の制約事項のある NTP アクセス グループの設定の例を示します。

- peer の制約事項は、「peer-acl」というアクセス リストの条件を満たす IP アドレスに適用されます。
- serve の制約事項は、「serve-acl」というアクセス リストの条件を満たす IP アドレスに適用されます。
- serve-only の制約事項は、「serve-only-acl」というアクセス リストの条件を満たす IP アドレスに適用されます。
- query-only の制約事項は、「query-only-acl」というアクセス リストの条件を満たす IP アドレスに適用されます。

```
switch# configure terminal
switch(config)# ntp peer 10.1.1.1
switch(config)# ntp peer 10.2.2.2
switch(config)# ntp peer 10.3.3.3
switch(config)# ntp peer 10.4.4.4
switch(config)# ntp peer 10.5.5.5
switch(config)# ntp peer 10.6.6.6
switch(config)# ntp peer 10.7.7.7
switch(config)# ntp peer 10.8.8.8
switch(config)# ntp access-group peer peer-acl
switch(config)# ntp access-group serve serve-acl
switch(config)# ntp access-group serve-only serve-only-acl
switch(config)# ntp access-group query-only query-only-acl
switch(config)# ip access-list peer-acl
switch(config-acl)# 10 permit ip host 10.1.1.1 any
switch(config-acl)# 20 permit ip host 10.8.8.8 any
switch(config)# ip access-list serve-acl
switch(config-acl)# 10 permit ip host 10.4.4.4 any
switch(config-acl)# 20 permit ip host 10.5.5.5 any
switch(config)# ip access-list serve-only-acl
switch(config-acl)# 10 permit ip host 10.6.6.6 any
switch(config-acl)# 20 permit ip host 10.7.7.7 any
switch(config)# ip access-list query-only-acl
switch(config-acl)# 10 permit ip host 10.2.2.2 any
```

```
switch(config-acl)# 20 permit ip host 10.3.3.3 any
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Clock Manager	『*Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide*』
NTP CLI コマンド	『*Cisco Nexus 7000 Series NX-OS System Management Command Reference*』
VDC および VRF	『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』

MIB

MIB	MIB のリンク
NTP に関連する MIB	サポートされている 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/public/sw-center/netmgmt/cmtk/mibs.shtml

NTP の機能の履歴

次の表に、このマニュアルの新機能および変更された機能を要約し、各機能がサポートされているリリースを示します。ご使用のソフトウェア リリースで、本書で説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。

表 *5* : *NTP* の機能の履歴

機能名	リリース	機能情報

NTP	7.3(0)D1(1)	NTP 認証キーの長さが、15 文字から 32 文字の英数字に増加しました。
NTP	6.2(2)	アクセス グループ オプションを制限の最も緩いものから最も厳しいものの順序でスキャンするための **ntp access-group match-all** コマンドを導入しました。
NTP	6.2(2)	NTP がアソシエーションを形成するのを防ぐ **no ntp passive** コマンドを導入しました。
NTP	6.2(2)	インターフェイス上で NTP ブロードキャストおよびマルチキャスト サーバおよびマルチキャスト クライアントを設定する機能を追加しました。
NTP	6.2(2)	インターフェイス上で NTP をイネーブルまたはディセーブルにする機能を追加しました。
NTP	6.1(1)	NTP アクセス グループのオプションは、制限の緩いものから厳しいものの順序でスキャンされるようになりました。
NTP	6.1(1)	NTP認証キーの長さが、8文字から15 文字の英数字に増加しました。
NTP	5.2(3)	NTP認証キーの長さが、8文字から15 文字の英数字に増加しました。
NTP	5.2(1)	すべてのVDCに対するNTPサポートを追加し、VDCはタイム サーバとして機能可能になりました。
NTP	5.2(1)	NTP のイネーブルまたはディセーブルに使用するコマンドが [**no**] **ntp enable** から [**no**] feature ntp に変更されました。

NTP	5.2(1)	既存のタイム サーバと同期されていない場合でも正規の NTP サーバとしてデバイスを設定する機能が追加され、時間を配信できるようになりました。
NTP アクセス グループ	5.2(1)	追加の NTP サービスに対するアクセスをコントロールするために **serve**、**serve-only**、**query-only** アクセス グループ オプションを追加しました。
NTP アクセス グループ	5.0(2)	アクセス グループを使用して、NTP サービスへのアクセスを制御する機能が追加されました。
NTP 認証	5.0(2)	NTP 認証をイネーブルまたはディセーブルにする機能が追加されました。
NTP ロギング	5.0(2)	NTP 認証をイネーブルまたはディセーブルにする機能が追加されました。
NTP サーバ コンフィギュレーション	5.0(2)	NTP サーバとの通信で使用するキーを設定するために、**ntp server** コマンドにオプションの **key** キーワードが追加されました。
CFS サポート	4.2(1)	CFS を使用して NTP コンフィギュレーションを配信する機能が追加されました。
NTP ソース IP アドレスまたはインターフェイス	4.1(3)	ピアに送信したすべての NTP パケットに NTP が含めるソース IP アドレスまたはソース インターフェイスを設定する機能が追加されました。
NTP	4.0(3)	NTP をディセーブルにする機能が追加されました。

第 5 章

PTP の設定

この章では、Cisco NX-OS デバイスで高精度時間プロトコル（PTP）を設定する方法について説明します。

この章は、次の項で構成されています。

- 機能情報の確認，79 ページ
- PTP について，80 ページ
- 仮想化のサポート，83 ページ
- PTP のライセンス要件，83 ページ
- PTP の前提条件，83 ページ
- PTP の注意事項および制約事項，83 ページ
- PTP のデフォルト設定，84 ページ
- PTP の設定，85 ページ
- PTP 設定の確認，89 ページ
- PTP の設定例，90 ページ
- 関連資料，91 ページ
- PTP の機能の履歴，92 ページ

機能情報の確認

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

PTP について

PTP はネットワークに分散したノードの時刻同期プロトコルです。そのハードウェアのタイムスタンプ機能は、ネットワーク タイム プロトコル（NTP）などの他の時刻同期プロトコルよりも高い精度を実現します。

Cisco NX-OS Release 7.3(0)D1(1) では、PTP はさらに IEEE 802.1AS を実装しており、F3 ラインカード用に Nexus 7700 プラットフォームでオーディオ ビデオ ブリッジング（AVB）をサポートしています。AVB 設定の詳細については、『*Cisco Nexus 7000 Audio Video Bridging Configuration Guide*』を参照してください。

PTP システムは、PTP および非 PTP デバイスの組み合わせで構成できます。PTP デバイスには、オーディナリ クロック、境界クロック、およびトランスペアレント クロックが含まれます。非 PTP デバイスには、通常のネットワーク スイッチやルータなどのインフラストラクチャ デバイスが含まれます。

PTP は、システムのリアルタイム PTP クロックが相互に同期する方法を指定する分散プロトコルです。これらのクロックは、グランドマスター クロック（階層の最上部にあるクロック）を持つマスター/スレーブ同期階層に編成され、システム全体の時間基準を決定します。同期は、タイミング情報を使用して階層のマスターの時刻にクロックを調整するメンバーと、PTP タイミング メッセージを交換することによって実現されます。PTP は、PTP ドメインと呼ばれる論理範囲内で動作します。

PTP デバイス タイプ

次のクロックは、一般的な PTP デバイスです。

オーディナリ クロック

エンドホストと同様に、単一の物理ポートに基づいてネットワークと通信します。オーディナリ クロックはグランドマスター クロックとして動作できます。

境界クロック

通常、複数の物理ポートがあり、各ポートはオーディナリ クロックのポートのように動作します。ただし、各ポートはローカル クロックを共有し、クロックのデータ セットはすべてのポートに共通です。各ポートは、境界クロックのその他すべてのポートから使用可能な最善のクロックに基づいて、個々の状態を、マスター（それに接続されている他のポートを同期する）またはスレーブ（ダウンストリーム ポートに同期する）に決定します。同期とマスター/スレーブ階層の確立に関するメッセージは、境界クロックのプロトコル エンジンで終了し、転送されません。

トランスペアレント クロック

通常のスイッチやルータなどのすべての PTP メッセージを転送しますが、スイッチでのパケットの滞留時間（パケットがトランスペアレント クロックを通過するために要した時間）と、場合によってはパケットの入力ポートのリンク遅延を測定します。トランスペアレント クロックはグランドマスター クロックに同期する必要がないため、ポートの状態はありません。

次の 2 種類のトランスペアレント クロックがあります。

エンドツーエンド トランスペアレント クロック

PTP メッセージの滞留時間を測定し、PTP メッセージまたは関連付けられたフォローアップ メッセージの修正フィールドの時間を収集します。

ピアツーピア トランスペアレント クロック

PTP メッセージの滞留時間を測定し、各ポートと、リンクを共有する他のノードの同じように装備されたポートとの間のリンク遅延を計算します。パケットの場合、この着信リンクの遅延は、PTP メッセージまたは関連付けられたフォローアップ メッセージの修正フィールドの滞留時間に追加されます。

（注） Cisco NX-OS Release 7.3(0)D1(1) 以降では、汎用 PTP クロック モードが導入されており、AVB 機能をサポートしています。

（注） PTP は境界クロック モードのみで動作します。シスコでは、スイッチに接続された、同期を必要とするクロックが含まれるサーバを使用して、グランドマスタークロック（10MHz）アップストリームを配置することを推奨します。

エンドツーエンド トランスペアレント クロック モードとピアツーピア トランスペアレント クロック モードはサポートされません。

PTP プロセス

PTP プロセスは、マスター/スレーブ階層の確立とクロックの同期の 2 つのフェーズで構成されます。

PTP ドメイン内では、オーディナリ クロックまたは境界クロックの各ポートが、次のプロセスに従ってステートを決定します。

- 受信したすべての（マスター ステートのポートによって発行された）アナウンス メッセージの内容を検査します

- 外部マスターのデータ セット（アナウンス メッセージ内）とローカル クロックで、優先順位、クロック クラス、精度などを比較します
- 自身のステートがマスターまたはスレーブのいずれであるかを決定します

マスター/スレーブ階層が確立されると、クロックは次のように同期されます。

- マスターはスレーブに同期メッセージを送信し、送信された時刻を記録します。
- スレーブは同期メッセージを受信し、受信した時刻を記録します。すべての同期メッセージには、フォローアップ メッセージがあります。そのため、同期メッセージの数は、フォローアップ メッセージの数と同じである必要があります。
- スレーブはマスターに遅延要求メッセージを送信し、送信された時刻を記録します。
- マスターは遅延要求メッセージを受信し、受信した時刻を記録します。
- マスターはスレーブに遅延応答メッセージを送信します。遅延要求メッセージの数は、遅延応答メッセージの数と同じある必要があります。
- スレーブは、これらのタイムスタンプを使用して、クロックをマスターの時刻に調整します。

Pong

ネットワーク モニタリング ツール Pong はネットワークの状態を診断するために、PTP の時刻同期インフラストラクチャを使用します。Pong はポートツーポートの遅延を測定し、ネットワーク監視ユーティリティ Ping と同様ですが、より詳細なネットワーク診断を提供します。Pong の詳細については、『*Cisco Nexus 7000 Series NX-OS Troubleshooting Guide*』を参照してください。

クロック マネージャ

クロックは、異なるプロセスおよび異なる VDC を通して共有される必要のあるリソースです。（NTP や PTP などの）複数同期プロトコルがシステムで実行されている場合があり、同じプロトコルの複数のインスタンスが異なる VDC で実行されている場合があります。クロック マネージャによってプロトコルおよびそのプロトコルが実行されている VDC を特定し、システム内のさまざまなクロックを制御することができます。クロック マネージャの設定の詳細については『*Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide*』を参照してください。

PTP のハイ アベイラビリティ

PTP のステートフル リスタートがサポートされています。リブート後またはスーパーバイザ スイッチオーバー後に、実行コンフィギュレーションが適用されます。ハイ アベイラビリティの詳細については、『*Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide*』を参照してください。

仮想化のサポート

Cisco NX-OS は、仮想デバイス コンテキスト（VDC）ごとに 1 インスタンスずつ、複数の PTP インスタンスをサポートします。VDC を特別に設定しない限り、デフォルトでは、Cisco NX-OS のデフォルトの VDC が使用されます。VDC の詳細については、『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』を参照してください。

PTP のライセンス要件

PTP 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。NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

PTP の前提条件

PTP には、次の前提条件があります。

- VDC を設定するには、適切なライセンスをインストールする必要があります。設定情報については『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』、ライセンス情報については『*Cisco NX-OS Licensing Guide*』を参照してください。

PTP の注意事項および制約事項

- PTP は境界クロック モードでのみ動作します（AVB をサポートする場合は gPTP モードで動作）。エンドツーエンド トランスペアレント クロック モードとピアツーピア トランスペアレント クロック モードはサポートされません。
- 1 つの PTP プロセスだけがクロック マネージャを通してすべてのポート クロックを制御できます。
- PTP はユーザ データグラム プロトコル（UDP）上の転送をサポートします。
- イーサネットを介したトラフィックは、AVB アプリケーションでサポートされます。
- PTP はマルチキャスト通信だけをサポートします。ネゴシエートされたユニキャスト通信は、AVB アプリケーションでサポートされます。
- PTP はネットワークごとに 1 つのドメインに制限されます。
- すべての管理メッセージは PTP がイネーブルのポートに転送されます。管理メッセージの処理はサポートされていません。

- PTP 対応ポートは、ポート上で PTP をイネーブルにしない場合、PTP パケットを識別せず、これらのパケットにタイムスタンプを適用したり、パケットをリダイレクトしたりしません。
- PTP は F1、F2、F2e、F3 および M2 シリーズ モジュール ポート上でのみイネーブルにできます。
- PTP は FEX インターフェイスではサポートされません。
- F1 シリーズ モジュールに対して、プライオリティ フロー制御がイネーブルの場合は PTP はポートでサポートされません。同様に、PTP が同じポート上でイネーブルの場合はプライオリティ フロー制御はサポートされません。
- F1 シリーズ モジュールに対して、プライオリティ フロー制御が同じ VDC のいずれかのポートでイネーブルの場合は Pong は VDC でサポートされません。同様に、Pong が同じ VDC上でイネーブルの場合はプライオリティ フロー制御はサポートされません。
- Cisco NX-OS Release 6.1 以降では、PTP が F2、F2e および M2 シリーズ モジュールのレイヤ 3 モードでサポートされます。
- Cisco NX-OS Release 6.2.6 以降では、PTP は、F3 シリーズ モジュールでサポートされます。
- PTP のカプセル化は、Cisco Nexus 7.3.0 以降でサポートされます。デフォルト値はレイヤ 3 です。
- FabricPath を介した PTP はサポートされません。
- PTP および Pong は、M3 シリーズ モジュールではサポートされません。

PTP のデフォルト設定

次の表に、PTP パラメータのデフォルト設定を示します。

表 *6*：デフォルトの *PTP* パラメータ

パラメータ	デフォルト
PTP	ディセーブル
PTP バージョン	2
PTP ドメイン	0
クロックをアドバタイズする場合、PTP プライオリティ 1 値	255
クロックをアドバタイズする場合、PTP プライオリティ 2 値	255

パラメータ	デフォルト
PTP アナウンス間隔	1 ログ秒
PTP アナウンス タイムアウト	3 アナウンス間隔
PTP 最小遅延要求間隔	0 ログ秒
PTP VLAN	1

PTP の設定

PTP のグローバルな設定

デバイスで PTP をグローバルにイネーブルまたはディセーブルにできます。また、ネットワーク内のどのクロックがグランドマスターとして選択される優先順位が最も高いかを判別するために、さまざまな PTP クロック パラメータを設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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	switch(config) # [**no**] **feature ptp**	デバイス上で PTP をイネーブルまたはディセーブルにします。 （注） スイッチの PTP をイネーブルにしても、各インターフェイスの PTP はイネーブルになりません。
ステップ 3	switch(config) # [**no**] **ptp source***ip-address* [**vrf***vrf*]	すべての PTP パケットのソース IP アドレスを設定します。 *ip-address* には IPv4 または IPv6 形式を使用できます。
ステップ 4	switch(config) # [**no**] **ptp domain***number*	（任意） このクロックで使用するドメイン番号を設定します。PTP ドメインを使用すると、1 つのネットワーク上で、複数の独立した PTP クロッキング サブドメインを使用できます。 *number* の範囲は 0 ～ 128 です。

	コマンドまたはアクション	目的
ステップ 5	switch(config) # [**no**] **ptp priority1***value*	（任意） このクロックをアドバタイズするときに使用する priority1 の値を設定します。この値はベストマスタークロック選択のデフォルトの基準（クロック品質、クロック クラスなど）を上書きします。低い値が優先されます。 *value* の範囲は 0 ～ 255 です。
ステップ 6	switch(config) # [**no**] **ptp priority2***value*	（任意） このクロックをアドバタイズするときに使用する priority2 の値を設定します。この値は、デフォルトの基準では同等に一致する 2 台のデバイスのうち、どちらを優先するかを決めるために使用されます。たとえば、priority2 値を使用して、特定のスイッチが他の同等のスイッチよりも優先されるようにすることができます。 *value* の範囲は 0 ～ 255 です。
ステップ 7	switch(config) # [**no**] **ptp encapsulation {layer-2 | layer-3}**	（任意） PTP に使用するカプセル化を設定します。レイヤ 3 カプセル化では、PTP パケットは IP + UDP フレームでカプセル化されます。レイヤ 2 カプセル化では、PTP パケットはイーサネット フレーム内でカプセル化されます。デフォルトの PTP カプセル化はレイヤ 3 で、PTP モードは Boundary です。レイヤ 2 カプセル化は AVB でのみサポートされます。
ステップ 8	switch(config) # [**no**] **ptp mode {boundary-clock | generalized-PTP | transparent-clock peer-to-peer}**	（任意） PTP デバイス モードを設定します。デフォルト モードは *boundary-clock* です。generalized-PTP モードは AVB に使用されます。*transparent-clock peer-to-peer mode* は、実験目的で追加されたもので、公式にはサポートされません。
ステップ 9	switch(config) # [**no**] **ptp switchlatency-estimated***value*	（任意） スイッチ遅延の最大推定値をナノ秒（ns）で設定します。この値は AVB で使用されます。範囲は 0 ～ 2147483647 です。デフォルト値は 5000 です。
ステップ 10	switch(config) # [**no**] **show ptp clock foreign-masters record[interface ethernet***slot/port*	（任意） 外部マスターに関する情報を表示します。

	コマンドまたはアクション	目的
ステップ 11	switch(config) # [**no**] **show ptp delay summary**	（任意） すべてのインターフェイスのリンク遅延と滞留遅延の情報を表示します。これはAVB で使用されます。
ステップ 12	switch(config) # [**no**] **show ptp parent**	（任意） 親クロックの情報を表示します。
ステップ 13	switch(config) # [**no**] **show ptp time-property**	（任意） ローカル クロック タイムのプロパティ情報を表示します。
ステップ 14	switch(config) # [**no**] **show ptp corrections**	（任意） このノードへの最新の修正を数件表示します。
ステップ 15	switch(config) # **show ptp brief**	（任意） PTP のステータスを表示します。
ステップ 16	switch(config) # **show ptp clock**	（任意） ローカル クロックのプロパティを表示します。
ステップ 17	switch(config) # **show ptp clock**	（任意） ローカル クロックのプロパティを表示します。

次に、デバイス上で PTP をグローバルに設定し、PTP 通信用の送信元 IP アドレスを指定し、クロックの優先レベルを設定する例を示します。

```
switch# configure terminal
switch(config)# feature ptp
switch(config)# ptp source 10.10.10.1
switch(config)# ptp priority1 1
switch(config)# ptp priority2 1
switch(config)# show ptp brief
PTP port status
-----------------------
Port State
------- --------------
switch(config)# show ptp clock
PTP Device Type: Boundary clock
Clock Identity : 0:22:55:ff:ff:79:a4:c1
Clock Domain: 0
Number of PTP ports: 0
Priority1 : 1
Priority2 : 1
Clock Quality:
Class : 248
Accuracy : 254
Offset (log variance) : 65535
Offset From Master : 0
Mean Path Delay : 0
Steps removed : 0
Local clock time:Sun Jul 3 14:13:24 2011
switch(config)#
```

インターフェイスでの PTP の設定

PTP をグローバルにイネーブルにしても、デフォルトで、サポートされているすべてのインターフェイス上でイネーブルになりません。PTP インターフェイスは個別にイネーブルに設定する必要があります。

はじめる前に

スイッチ上でグローバルに PTP をイネーブルにし、PTP 通信の送信元 IP アドレスを設定したことを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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	switch(config) # **interface ethernet***slot/port*	PTP をイネーブルにするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if) # [**no**] **ptp**	インターフェイスで PTP をイネーブルまたはディセーブルにします。
ステップ 4	switch(config-if) # [**no**] **ptp announce** {**interval***log seconds* | **timeout***count*}	（任意） インターフェイス上の PTP アナウンス メッセージ間の間隔またはタイムアウトがインターフェイスで発生する前の PTP 間隔の数を設定します。 PTP アナウンス間隔の範囲は 0 ～ 4 秒で、間隔のタイムアウトの範囲は 2 ～ 10 です。
ステップ 5	switch(config-if) # [**no**] **ptp delay request minimum interval***log seconds*	（任意） ポートがマスター ステートの場合に PTP 遅延要求メッセージ間で許可される最小間隔を設定します。 範囲はログ（-6）～ログ（1）秒です。ログ（-2）は、1 秒あたり 2 フレームです。
ステップ 6	switch(config-if) # [**no**] **ptp sync interval***log seconds*	（任意） インターフェイス上の PTP 同期メッセージの送信間隔を設定します。
ステップ 7	switch(config-if) # [**no**] **ptp vlan***vlan-id*	（任意） PTP をイネーブルにするインターフェイスの VLAN を指定します。インターフェイスの 1 つの VLAN でイネーブルにできるのは、1 つの PTP のみです。

	コマンドまたはアクション	目的
		指定できる範囲は 1 ～ 4094 です。
ステップ 8	switch(config-if) # **show ptp brief**	（任意） PTP のステータスを表示します。
ステップ 9	switch(config-if) # **show ptp port interface***interface slot/port*	（任意） PTP ポートのステータスを表示します。
ステップ 10	switch(config-if)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。

次に、インターフェイス上で PTP を設定し、アナウンス、遅延要求、および同期メッセージの間隔を設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# ptp
switch(config-if)# ptp announce interval 3
switch(config-if)# ptp announce timeout 2
switch(config-if)# ptp delay-request minimum interval 4
switch(config-if)# ptp sync interval -1
switch(config-if)# show ptp brief
PTP port status
-----------------------
Port State
------- --------------
Eth2/1 Master
switch(config-if)# show ptp port interface ethernet 2/1
PTP Port Dataset: Eth2/1
Port identity: clock identity: 0:22:55:ff:ff:79:a4:c1
Port identity: port number: 1028
PTP version: 2
Port state: Master
Delay request interval(log mean): 4
Announce receipt time out: 2
Peer mean path delay: 0
Announce interval(log mean): 3
Sync interval(log mean): -1
Delay Mechanism: End to End
Peer delay request interval(log mean): 0
switch(config-if)#
```

PTP 設定の確認

次のいずれかのコマンドを使用して、設定を確認します。

表 *7* : ***PTP Show*** コマンド

コマンド	目的
show ptp brief	PTP のステータスを表示します。

コマンド	目的
show ptp clock	ローカル クロックのプロパティ（クロック ID など）を表示します。
show ptp clock foreign-masters-record	PTP プロセスが認識している外部マスターの状態を表示します。外部マスターごとに、出力に、クロック ID、基本的なクロック プロパティ、およびクロックがグランドマスターとして使用されているかどうかが表示されます。
show ptp corrections	最後の数個の PTP 修正を表示します。
show ptp parent	PTP ペアレントのプロパティを表示します。
show ptp port interface ethernet *slot/port*	スイッチの PTP ポートのステータスを表示します。

PTP の設定例

次に、デバイス上で PTP をグローバルに設定し、PTP 通信用の送信元 IP アドレスを指定し、クロックの優先レベルを設定する例を示します。

```
switch# config t
switch(config)# feature ptp
switch(config)# ptp source 10.10.10.1
switch(config)# ptp priority1 1
switch(config)# ptp priority2 1
switch(config)# show ptp brief
PTP port status
-----------------------
Port         State
-------  --------------
switch(config)# show ptp clock
PTP Device Type: Boundary clock
Clock Identity : 0:22:55:ff:fe:79:a4:c1
Clock Domain: 0
Number of PTP ports: 0
Priority1 : 1
Priority2 : 1
Clock Quality:
  Class : 248
  Accuracy : 254
  Offset (log variance) : 65535
Offset From Master : 0
Mean Path Delay : 0
Steps removed : 0
Local clock time:Sun Jul 3 14:13:24 2011
```

次に、インターフェイス上で PTP を設定し、アナウンス、遅延要求、および同期メッセージの間隔を設定する例を示します。

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# ptp
```

```
switch(config-if)# ptp announce interval 3
switch(config-if)# ptp announce timeout 2
switch(config-if)# ptp delay-request minimum interval 4
switch(config-if)# ptp sync interval -1
switch(config-if)# show ptp brief
PTP port status
-----------------------
Port     State
------- --------------
Eth2/1    Master
switch(config-if)# show ptp port interface ethernet 2/1
PTP Port Dataset: Eth2/1
Port identity: clock identity: 0:22:55:ff:fe:79:a4:c1
Port identity: port number: 1028
PTP version: 2
Port state: Master
Delay request interval(log mean): 4
Announce receipt time out: 2
Peer mean path delay: 0
Announce interval(log mean): 3
Sync interval(log mean): -1
Delay Mechanism: End to End
Peer delay request interval(log mean): 0
```

関連資料

関連項目	マニュアル タイトル
PTP CLI コマンド	『*Cisco Nexus 7000 Series NX-OS System Management Command Reference*』
Pong	『*Cisco Nexus 7000 Series NX-OS Troubleshooting Guide*』
Clock Manager	『*Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide*』
VDC	『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』

関連資料

関連項目	マニュアル タイトル
PTP CLI コマンド	『*Cisco Nexus 7000 Series NX-OS System Management Command Reference*』
VDC	『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』

関連項目	マニュアル タイトル
Pong	『*Cisco Nexus 7000 Series NX-OS Troubleshooting Guide*』
Clock Manager	『*Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide*』

MIB

MIB	MIB リンク
CISCO-PTP-MIB	サポートされている 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。 ftp://ftp.cisco.com/pub/mibs/supportlists/nexus7000/Nexus7000MIBSupportList.html

PTP の機能の履歴

次の表に、このマニュアルの新機能および変更された機能を要約し、各機能がサポートされているリリースを示します。ご使用のソフトウェア リリースで、本書で説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。

表 *8* : *PTP* の機能の履歴

機能名	リリース	機能情報
PTP	7.3(0)D1(1)	Nexus 7700 シャーシの F3 ライン カードでのみ、AVB、802.1AS、汎用 PTP モード、ピア遅延応答メカニズム、レイヤ 2 カプセル化のサポートが追加されました。詳細については、『*Cisco Nexus AVB configuration Guide*』を参照してください。
PTP	6.2(6)	F3 シリーズ モジュールのサポートが追加されました。

PTP	6.1(1)	F2、F2e および M2 シリーズ モジュールのレイヤ 3 モードで PTP サポートが追加されました。
PTP	6.1(1)	M2 シリーズ モジュールのサポートが追加されました。
PTP	6.1(1)	PTP MAC フォーマットが FF:FF から FF:FE に変更されました。
PTP	6.1(1)	**vrf** オプションが **ptp source** コマンドで廃止されました。
PTP	6.0(1)	ポート チャネル メンバ ポートに PTP サポートが追加されました。
PTP	6.0(1)	F2 シリーズ モジュールのサポートが追加されました。
PTP	5.2(1)	この機能が導入されました。

第 6 章

CDP の設定

この章では、Cisco NX-OS デバイス上で Cisco Discovery Protocol（CDP）を設定する方法について説明します。

この章は、次の項で構成されています。

- 機能情報の確認，95 ページ
- CDP について，96 ページ
- CDP のライセンス要件，97 ページ
- CDP の前提条件，98 ページ
- CDP の注意事項と制約事項，98 ページ
- CDP のデフォルト設定，98 ページ
- CDP の設定，98 ページ
- CDP コンフィギュレーションの確認，101 ページ
- CDP のコンフィギュレーション例，102 ページ
- その他の参考資料，103 ページ
- CDP 機能の履歴，103 ページ

機能情報の確認

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

CDP について

Cisco Discovery Protocol（CDP）は、ルータ、ブリッジ、アクセス サーバ、コミュニケーション サーバ、スイッチを含め、シスコ製のあらゆる機器で動作する、メディア独立型およびプロトコル独立型のプロトコルです。CDP を使用すると、デバイスに直接接続されているすべてのシスコ デバイスの情報を検出して表示できます。

CDP はネイバーデバイスのプロトコルアドレスを収集し、各デバイスのプラットフォームを検出します。CDP の動作はデータリンク層上に限定されます。異なるレイヤ 3 プロトコルをサポートする 2 つのシステムで相互学習が可能です。

CDP が設定された各デバイスは、マルチキャストアドレスに定期的にアドバタイズメントを送信します。各デバイスは、SNMP メッセージを受信できるアドレスを少なくとも 1 つアドバタイズします。アドバタイズメントには保持時間情報も含まれます。保持時間は、受信デバイスが CDP 情報を削除するまでに保持する時間の長さを表します。アドバタイズメントまたはリフレッシュ タイマーおよびホールド タイマーを設定できます。

CDP Version-2（CDPv2）では、接続デバイスとの間でネイティブ VLAN ID またはポート デュプレックス ステートが一致していないインスタンスを追跡できます。

CDP では、次の Type-Length-Value（TLV）フィールドがアドバタイズされます。

- Device ID
- Address
- Port ID
- Capabilities
- Version
- Platform
- Native VLAN
- Full/Half Duplex
- MTU
- SysName
- SysObjectID
- Management Address
- Physical Location
- VTP

すべての CDP パケットに VLAN ID が含まれます。レイヤ 2 アクセス ポート上で CDP を設定した場合、そのアクセス ポートから送信される CDP パケットには、アクセス ポートの VLAN ID が含まれます。レイヤ 2 トランク ポート上で CDP を設定した場合は、そのトランク ポートから送信される CDP パケットに、トランク ポート上で許可設定されている最小の VLAN ID が含まれます。トランク ポートは、そのトランク ポートの許可 VLAN リストに指定されている VLAN ID で

あれば、どの VLAN ID が含まれている CDP パケットでも受信できます。VLAN の詳細については、『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide*』を参照してください。

VTP 機能のサポート

次の条件に当てはまる場合、CDP は VLAN トランキング プロトコル（VTP）の type-length-value（TLV）フィールドを送信します。

- CDP バージョン 2 がイネーブルになっている
- VTP 機能がイネーブルになっている
- VTP ドメイン名が設定されている

show cdp neighbors detail コマンドを使用すると、VTP 情報を参照できます。

ハイ アベイラビリティ

Cisco NX-OS は、CDP のステートフルおよびステートレス両方のリスタートとスイッチオーバーをサポートします。ハイ アベイラビリティの詳細については、『*Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide*』を参照してください。

仮想化のサポート

Cisco NX-OS は、仮想デバイス コンテキスト（VDC）ごとに 1 インスタンスずつ、複数の CDP インスタンスをサポートします。VDC を特別に設定しない限り、デフォルトでは、Cisco NX-OS のデフォルトの VDC が使用されます。VDC の詳細については、『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』を参照してください。

CDP のライセンス要件

製品	ライセンス要件
Cisco NX-OS	CDP 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 nx-os イメージにバンドルされており、無料で提供されます。NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

CDP の前提条件

VDC を設定する場合は、適切なライセンスをインストールし、所定の VDC を開始する必要があります。設定情報については『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』、ライセンス情報については『*Cisco NX-OS Licensing Guide*』を参照してください。

CDP の注意事項と制約事項

CDP に関する設定時の注意事項および制約事項は、次のとおりです。

- 接続数が 256 のハブにポートを接続した場合、CDP はポートあたり最大 256 のネイバーを検出できます。
- デバイス上でCDPをイネーブルにする必要があります。イネーブルにしておかないと、インターフェイス上で CDP をイネーブルにできません。
- CDP を設定できるのは、物理インターフェイスおよびポート チャネル上に限られます。
- CDP は Cisco Nexus 2000 シリーズ Fabric Extender ではサポートされません。

CDP のデフォルト設定

次の表に、CDP パラメータのデフォルト設定を示します。

パラメータ	デフォルト
CDP	グローバルおよびすべてのインターフェイスでイネーブル
CDP version	Version 2
CDP device ID	Serial number
CDP timer	60 秒
CDP hold timer	180 秒

CDP の設定

（注） この機能の Cisco NX-OS コマンドは、Cisco IOS のコマンドとは異なる場合があるので注意してください。

CDP のグローバルなイネーブルまたはディセーブル

CDP はデフォルトで有効になっています。CDP をディセーブルにしてから、もう一度イネーブルにできます。

インターフェイス上で CDP をイネーブルにするには、先にデバイス上で CDP をイネーブルにしておく必要があります。CDP がグローバルなディセーブルになっているときに、特定のインターフェイス上で CDP をイネーブルにしても、これらのインターフェイス上で CDP がアクティブになることはなく、エラー メッセージが戻ります。

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	[**no**] **cdp enable** 例： `switch(config)# cdp enable`	デバイス全体で CDP 機能をイネーブルまたはディセーブルにします。デフォルトではイネーブルです。
ステップ 3	**copy running-config startup-config** 例： `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。

インターフェイス上での CDP のイネーブルまたはディセーブル

CDP はデフォルトで、インターフェイス上でイネーブルです。インターフェイス上で CDP をディセーブルにできます。

CDP がグローバルなディセーブルになっているときに、特定のインターフェイス上で CDP をイネーブルにしても、これらのインターフェイス上で CDP がアクティブになることはなく、エラー メッセージが戻ります。

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	**interface***interface slot*/*port*
	
	例：
	`switch(config)# interface ethernet 1/2`
	`switch(config-if)#`
		インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	[**no**] **cdp enable** 例： `switch(config-if)# cdp enable`	このインターフェイスで CDP をイネーブルまたはディセーブルにします。デフォルトではイネーブルです。 （注） CDP がデバイス上でグローバルにイネーブルになっていることを確認します。
ステップ 4	**show cdp interface***interface slot*/*port* 例： `switch(config-if)# show cdp interface ethernet 1/2`	（任意） インターフェイスの CDP 情報を表示します。
ステップ 5	**copy running-config startup-config** 例： `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。

CDP オプション パラメータの設定

この手順でオプションのコマンドを使用して CDP 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。

	コマンドまたはアクション	目的
ステップ 2	**cdp advertise** {**v1** | **v2**} 例： `switch(config)# cdp advertise v1`	（任意） デバイスがサポートする CDP のバージョンを設定します。デフォルトは v2 です。
ステップ 3	**cdp format device-id** {**mac-address** | **serial-number** | **system-name**} 例： `switch(config)# cdp format device-id mac-address`	（任意） CDP デバイス ID を設定します。オプションは次のとおりです。 • **mac-address**：シャーシの MAC アドレス。 • **serial-number**：シャーシのシリアル番号/組織固有識別子（OUI） • **system-name**：システム名または完全修飾ドメイン名。 デフォルトでは **system-name** です。
ステップ 4	**cdp holdtime** *seconds* 例： `switch(config)# cdp holdtime 150`	（任意） CDP ネイバー情報を削除するまでに保持する時間を設定します。範囲は 10 ～ 255 秒です。デフォルト値は 180 秒です。
ステップ 5	**cdp timer** *seconds* 例： `switch(config)# cdp timer 50`	（任意） CDP がネイバーにアドバタイズメントを送信するリフレッシュ タイムを設定します。範囲は 5 ～ 254 秒です。デフォルトは 60 秒です。
ステップ 6	**copy running-config startup-config** 例： `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。

CDP コンフィギュレーションの確認

CDP の設定を表示するには、次のいずれかの作業を行います。

コマンド	目的
show cdp all	CDP がイネーブルになっているすべてのインターフェイスを表示します。
show cdp entry {**all** | **name***entry-name*}	CDP データベース エントリを表示します。

コマンド	目的
show cdp global	CDP グローバル パラメータを表示します。
show cdp interface*interfaceslot*/*port*	CDPインターフェイスのステータスを表示します。
show cdp neighbors {**device-id** | **interface***interfaceslot*/*port*} [**detail**]	CDP ネイバーのステータスを表示します。
show cdp interface*interfaceslot*/*port*	インターフェイスの CDP トラフィック統計を表示します。

インターフェイスの CDP 統計情報を消去するには、**clear cdp counters** コマンドを使用します。

1 つまたはすべてのインターフェイスの CDP キャッシュを消去するには、**clear cdp table** コマンドを使用します。

CDP のコンフィギュレーション例

CDP機能をイネーブルにして、リフレッシュ タイマーおよびホールドタイマーを設定する例を示します。

```
config t
cdp enable
cdp timer 50
cdp holdtime 100
```

次に、CDP グローバル パラメータを表示する例を示します。

```
switch# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute
Device-ID           Local Intrfce    Hldtme Capability    Platform        Port ID
Mgmt-switch
                    mgmt0             148    R S I         WS-C4948-10GE Gig1/37
switch88(FOX1518GRE6)
                    Eth1/25           164    R S I s       N5K-C5596UP   Eth1/25
switch89(FOX1518GQJ2)
                    Eth1/26           163    R S I s       N5K-C5596UP   Eth1/25
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
CDP CLI コマンド	『*Cisco Nexus 7000 Series NX-OS System Management Command Reference*』
VDC および VRF	『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』

MIB

MIB	MIB のリンク
CDP に関連する MIB	サポートされている 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/public/sw-center/netmgmt/cmtk/mibs.shtml

CDP 機能の履歴

次の表に、このマニュアルの新機能および変更された機能を要約し、各機能がサポートされているリリースを示します。ご使用のソフトウェア リリースで、本書で説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。

表 *9* : *CDP* 機能の履歴

機能名	リリース	機能情報
VTP ドメイン名に対する CDP サポート	4.2(1)	CDP は、CDP バージョン 2 パケット内の VLAN トランキング プロトコル（VTP）の type-length-value（TLV）フィールドを通知します。

第 7 章

システム メッセージ ロギングの設定

この章では、Cisco NX-OS デバイス上でシステム メッセージ ロギングを設定する方法について説明します。

この章の内容は、次のとおりです。

- 機能情報の確認，105 ページ
- システム メッセージ ロギングについて，106 ページ
- システム メッセージ ロギングのライセンス要件，107 ページ
- 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，107 ページ
- システム メッセージ ロギングのデフォルト設定，107 ページ
- システム メッセージ ロギングの設定，108 ページ
- システム メッセージ ロギングの設定確認，119 ページ
- システム メッセージ ロギングのコンフィギュレーション例，119 ページ
- その他の参考資料，120 ページ
- システム メッセージ ロギングの機能の履歴，120 ページ

機能情報の確認

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

システム メッセージ ロギングについて

システム メッセージ ロギングを使用して宛先を制御し、システム プロセスが生成するメッセージの重大度をフィルタリングできます。端末セッション、ログ ファイル、およびリモート システム上の Syslog サーバへのロギングを設定できます。

システム メッセージ ロギングは RFC 3164 に準拠しています。システム メッセージのフォーマットおよびデバイスが生成するメッセージの詳細については、『*Cisco NX-OS System Messages Reference*』を参照してください。

デフォルトでは、デバイスはターミナル セッションにメッセージを出力し、ログ ファイルにシステム メッセージをログします。

次の表に、システム メッセージで使用されている重大度を示します。重大度を設定する場合、システムはそのレベル以下のメッセージを出力します。

表 *10*： システム メッセージの重大度

レベル	説明
0：緊急	システムが使用不可
1：アラート	即時処理が必要
2：クリティカル	クリティカル状態
3：エラー	エラー状態
4：警告	警告状態
5：通知	正常だが注意を要する状態
6：情報	単なる情報メッセージ
7：デバッグ	デバッグ実行時にのみ表示

デバイスは重大度 0、1、または 2 のメッセージのうち、最新の 100 メッセージを NVRAM ログに記録します。NVRAM へのロギングは設定できません。

メッセージを生成したファシリティと重大度に基づいて記録するシステム メッセージを設定できます。

Syslog サーバ

syslog サーバは、syslog プロトコルに基づいてシステム メッセージを記録するリモート システム上で動作します。IPv4 または IPv6 の Syslog サーバを最大 8 つ設定できます。

ファブリック内のすべてのスイッチでsyslogサーバの同じ設定をサポートするために、Cisco Fabric Services（CFS）を使用して syslog サーバ設定を配布できます。

（注） 最初のデバイス初期化時に、メッセージがsyslogサーバに送信されるのは、ネットワークの初期化後です。

仮想化のサポート

仮想デバイス コンテキスト（VDC）は、一連のシステム リソースを論理的に表現する用語です。システム メッセージ ロギングが適用されるのは、コマンドが入力された VDC に限られます。

VDC の設定方法については、『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』を参照してください。

システム メッセージ ロギングのライセンス要件

製品	ライセンス要件
Cisco NX-OS	システム メッセージ ロギング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 nx-os イメージにバンドルされており、無料で提供されます。NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

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 メッセージは、デフォルトでコンソールおよびログ ファイルに記録されます。

システム メッセージ ロギングのデフォルト設定

次の表に、システム メッセージ ロギング パラメータのデフォルト設定を示します。

表 *11*： デフォルトのシステム メッセージ ロギング パラメータ

パラメータ	デフォルト
コンソール ロギング	重大度 2 でイネーブル

パラメータ	デフォルト
モニタ ロギング	重大度 5 でイネーブル
ログ ファイル ロギング	重大度 5 のメッセージ ロギングがイネーブル
モジュール ロギング	重大度 5 でイネーブル
ファシリティ ロギング	イネーブル
タイムスタンプ単位	Seconds
Syslog サーバ ロギング	ディセーブル
Syslog サーバ設定の配布	ディセーブル

システム メッセージ ロギングの設定

（注） この機能の Cisco NX-OS コマンドは、Cisco IOS のコマンドとは異なる場合があるので注意してください。

ターミナル セッションへのシステム メッセージ ロギングの設定

重大度に基づいて、コンソール、Telnet、および SSH セッションにメッセージを記録するようにデバイスを設定できます。

デフォルトでは、ターミナル セッションでロギングはイネーブルです。

（注） 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。

手順

	コマンドまたはアクション	目的
ステップ 1	**terminal monitor** 例： `switch# terminal monitor`	デバイスがコンソールにメッセージを記録できるようにします。

ステップ 2	**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 3	[**no**] **logging console** [*severity-level*] 例： `switch(config)# logging console 3`	指定された重大度とそれより上位の重大度のメッセージをコンソールセッションに記録するように、デバイスを設定します。小さい値は、より高い重大度を示します。重大度は 0 ～ 7 の範囲です。 • 0：緊急 • 1：アラート • 2：クリティカル • 3：エラー • 4：警告 • 5：通知 • 6：情報 • 7：デバッグ 重大度が指定されていない場合、デフォルトの 2 が使用されます。**no** オプションは、メッセージをコンソールにログするデバイスの機能をディセーブルにします。
ステップ 4	**show logging console** 例： `switch(config)# show logging console`	（任意） コンソール ロギング設定を表示します。
ステップ 5	[**no**] **logging monitor** [*severity-level*] 例： `switch(config)# logging monitor 3`	デバイスが指定された重大度とそれより上位の重大度のメッセージをモニタに記録できるようにします。小さい値は、より高い重大度を示します。重大度は 0 ～ 7 の範囲です。 • 0：緊急

	コマンドまたはアクション	目的
		• 1：アラート • 2：クリティカル • 3：エラー • 4：警告 • 5：通知 • 6：情報 • 7：デバッグ 設定はTelnetおよびSSHセッションに適用されます。 重大度が指定されていない場合、デフォルトの2が使用されます。**no** オプションは、メッセージを Telnet および SSH セッションにログするデバイスの機能をディセーブルにします。
ステップ 6	**show logging monitor** 例： `switch(config)# show logging monitor`	（任意） モニタ ロギング設定を表示します。
ステップ 7	**[no] logging message interface type ethernet description** 例： `switch(config)# logging message interface type ethernet description`	システム メッセージ ログ内で、物理的なイーサネット インターフェイスおよびサブインターフェイスに対して説明を追加できるようにします。この説明は、インターフェイスで設定された説明と同じものです。 **no** オプションは、物理イーサネット インターフェイスのシステム メッセージ ログ内のインターフェイス説明の印刷をディセーブルにします。
ステップ 8	**copy running-config startup-config** 例： `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。

ファイルへのシステム メッセージの記録

システム メッセージをファイルに記録するようにデバイスを設定できます。デフォルトでは、システム メッセージはファイル log:messages に記録されます。

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	[**no**] **logging logfile** *logfile-name severity-level* [**size** *bytes*] 例： `switch(config)# logging logfile my_log 6`	システム メッセージを保存するのに使用するログ ファイルの名前と、記録する最小重大度を設定します。小さい値は、より高い重大度を示します。重大度は 0 ～ 7 の範囲です。 • 0：緊急 • 1：アラート • 2：クリティカル • 3：エラー • 4：警告 • 5：通知 • 6：情報 • 7：デバッグ 任意で最大ファイル サイズを指定できます。 デフォルトの重大度は 5 です。ファイル サイズは 10485760 です。ファイル サイズは 4096 ～ 4194304 バイトです。

ステップ 3	**logging event** {**link-status** | **trunk-status**} {**enable** | **default**}
	
	例：
	`switch# logging event link-status default`
	`switch(config)#`
		インターフェイス イベントをロギングします。
		• **link-status**：すべての UP/DOWN メッセージおよび CHANGE メッセージをログに記録します。
		• **trunk-status**：すべての TRUNK ステータス メッセージをログに記録します。
		• **enable**：ポート レベルのコンフィギュレーションを上書きしてロギングをイネーブルにするよう、指定します。
		• **default**：ロギングが明示的に設定されてないインターフェイスで、デフォルトのロギング設定を使用するよう、指定します。

	コマンドまたはアクション	目的
ステップ 4	**show logging info** 例： `switch(config)# show logging info`	（任意） ロギング設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `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。

モジュールおよびファシリティ メッセージのロギングの設定

モジュールおよびファシリティに基づいて記録するメッセージの重大度およびタイムスタンプの単位を設定できます。

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	[**no**] **logging module** [*severity-level*] 例： `switch(config)# logging module 3`	指定された重大度またはそれ以上の重大度であるモジュール ログ メッセージをイネーブルにします。重大度は 0 ～ 7 の範囲です。 • 0：緊急 • 1：アラート • 2：クリティカル • 3：エラー • 4：警告 • 5：通知 • 6：情報 • 7：デバッグ

	コマンドまたはアクション	目的
		重大度が指定されていない場合、デフォルトの 5 が使用されます。**no** オプションを使用すると、モジュール ログ メッセージがディセーブルになります。
ステップ 3	**show logging module** 例： `switch(config)# show logging module`	（任意） モジュール ロギング設定を表示します。
ステップ 4	[**no**] **logging level***facility severity-level* 例： `switch(config)# logging level aaa 2`	指定された重大度またはそれ以上の重大度である指定のファシリティからのロギング メッセージをイネーブルにします。重大度は 0 ～ 7 の範囲です。 • 0：緊急 • 1：アラート • 2：クリティカル • 3：エラー • 4：警告 • 5：通知 • 6：情報 • 7：デバッグ 同じ重大度をすべてのファシリティに適用するには、**all** ファシリティを使用します。デフォルト値については、**show logging level** コマンドを参照してください。 **no** オプションを使用すると、指定されたファシリティのロギング重大度がデフォルトのレベルにリセットされます。ファシリティおよび重大度を指定しなかった場合、すべてのファシリティがそれぞれのデフォルト重大度にリセットされます。
ステップ 5	**show logging level** [*facility*] 例： `switch(config)# show logging level aaa`	（任意） ファシリティごとに、ロギング レベル設定およびシステムのデフォルト レベルを表示します。ファシリティを指定しなかった場合は、すべてのファシリティのレベルが表示されます。
ステップ 6	[**no**] **logging timestamp** {**microseconds** | **milliseconds** | **seconds**}	ロギング タイムスタンプ単位を設定します。デフォルトでは、単位は秒です。

	コマンドまたはアクション	目的
	例： `switch(config)# logging timestamp milliseconds`	（注） このコマンドは、スイッチ内で保持されているログに適用されます。また、外部のロギング サーバには適用されません。
ステップ 7	**show logging timestamp** 例： `switch(config)# show logging timestamp`	（任意） 設定されたロギング タイムスタンプ単位を表示します。
ステップ 8	**copy running-config startup-config** 例： `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。

syslog サーバの設定

システム メッセージを記録する、リモート システムを参照する syslog サーバを最大で 8 台設定できます。

（注） シスコは、管理仮想ルーティングおよび転送（VRF）インスタンスを使用するサーバとして、syslog サーバを設定することを推奨します。VRF の詳細情報については、『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

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	[**no**] **logging server***host* [*severity-level* [**use-vrf***vrf-name*]] 例： `switch(config)# logging server 192.0.2.253`	指定されたホスト名、あるいは IPv4 または IPv6 アドレスで Syslog サーバを設定します。**use-vrf** キーワードを使用すると、メッセージ ロギングを特定の VRF に限定できます。重大度は 0 ～ 7 の範囲です。

	コマンドまたはアクション	目的
	例： `switch(config)# logging server 2001:db8::3 5 use-vrf red`	• 0：緊急 • 1：アラート • 2：クリティカル • 3：エラー • 4：警告 • 5：通知 • 6：情報 • 7：デバッグ デフォルトの発信ファシリティは local7 です。 **no** オプションは、指定したホストのロギング サーバを削除します。 最初の例では、ファシリティ local 7 のすべてのメッセージを転送します。2 番目の例では、VRF red で重大度が 5 以下のメッセージを転送します。
ステップ 3	**logging source-interface***interface* 例： `switch(config)# logging source-interface loopback 5`	ログ メッセージに IP アドレスを表示する送信元インターフェイスを設定します。このスタティックな設定により、個々の Cisco NX-OS デバイスから送信されるすべてのメッセージ ログに、同じ IP アドレスが表示されます。
ステップ 4	**show logging server** 例： `switch(config)# show logging server`	（任意） Syslog サーバ設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `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。

Syslog 転送の宛先ポートの設定

ロギング先となるリモート サーバにシステム メッセージを転送する際、使用する宛先ポートを指定できます。

（注） 指定したユーザ定義のポートをリッスンするように、リモート サーバの syslog 設定ファイルを変更する必要があります。デフォルトでは、システム メッセージは UDP ペイロードとして 514 番ポートによりリモート サーバに送信され、ロギングされます。

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	[**no**] **logging server***host* [*severity-level* [**use-vrf***vrf-name*]]
	
	例：
	`switch(config)# logging server 192.0.2.253 port 600`
	
	例：
	`switch(config)# logging server 192.0.2.253 5 port 600`
		syslog をリモート サーバに転送するのに使用される宛先ポートを指定します。ポート番号の範囲は 1 ～ 65535 です。
		デフォルトの宛先ポート番号は 514 です。
		（注） カスタム宛先ポートを削除するかまたはデフォルト値にリセットするには、ポート番号を指定せずに **logging server** コマンドを使用します。任意で、ポート番号を 514 に指定できます。
		最初の例では、ユーザ定義の 600 番ポートですべてのメッセージを転送します。2 番目の例では、ユーザ定義の 600 番ポートで、重大度が 5 以下のメッセージを転送します。

ステップ 3	**show logging server** 例： `switch(config)# show logging server`	（任意） Syslog サーバ設定を表示します。
ステップ 4	**copy running-config startup-config** 例： `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。

UNIX または Linux システムでの Syslog サーバの設定

/etc/syslog.conf ファイルに次の行を追加して、UNIX または Linux システム上に Syslog サーバを設定できます。

facility.level `<five tab characters>` *action*

次の表に、設定可能な syslog フィールドを示します。

表 *12*：*syslog.conf* の *Syslog* フィールド

フィールド	説明
ファシリティ	メッセージの作成者。auth、authpriv、cron、daemon、kern、lpr、mail、mark、news、syslog、user、local0 ～ local7 です。アスタリスク（*）を使用するとすべてを指定します。これらのファシリティ指定により、発信元に基づいてメッセージの宛先を制御できます。 （注） ローカル ファシリティを使用する前に設定をチェックします。
レベル	メッセージを記録する最小重大度。debug、info、notice、warning、err、crit、alert、emerg です。アスタリスク（*）を使用するとすべてを指定します。none を使用するとファシリティをディセーブルにできます。
Action	メッセージの宛先。ファイル名、前に @ 記号を加えたホスト名、ユーザをカンマで区切ったリスト、またはすべてのログイン ユーザを表すアスタリスク（*）を使用できます。

手順

ステップ 1 /etc/syslog.conf ファイルに次の行を追加して、ファイル /var/log/myfile.log に local7 ファシリティのデバッグ メッセージを記録します。

例：
```
debug.local7 var/log/myfile.log
```

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

例：
```
$ touch /var/log/myfile.log
$ chmod 666 /var/log/myfile.log
```

ステップ 3 次のコマンドを入力して、システム メッセージ ロギング デーモンが myfile.log をチェックして、新しい変更を取得するようにします。

例：
```
$ kill -HUP ~cat /etc/syslog.pid~
```

ログ ファイルの表示およびクリア

ログ ファイルおよび NVRAM のメッセージを表示したり消去したりできます。

手順

	コマンドまたはアクション	目的
ステップ 1	**show logging last***number-lines* 例： `switch# show logging last 40`	ロギングファイルの最終行番号を表示します。最終行番号には 1 ～ 9999 を指定できます。
ステップ 2	**show logging logfile** [**start-time***yyyymmm dd hh:mm:ss*] [**end-time***yyyy mmm dd hh:mm:ss*] 例： `switch# show logging logfile start-time 2013 oct 1 15:10:0`	入力されたスパン内にタイムスタンプがあるログ ファイルのメッセージを表示します。終了時間を入力しないと、現在の時間が使用されます。月の時間フィールドには 3 文字を、年と日の時間 フィールドには数値を入力します。
ステップ 3	**show logging nvram** [**last***number-lines*] 例： `switch# show logging nvram last 10`	NVRAM のメッセージを表示します。表示される行数を制限するには、表示する最終行番号を入力できます。最終行番号には 1 ～ 100 を指定できます。
ステップ 4	**clear logging logfile** 例： `switch# clear logging logfile`	ログ ファイルの内容をクリアします。
ステップ 5	**clear logging nvram** 例： `switch# clear logging nvram`	NVRAM の記録されたメッセージをクリアします。

システム メッセージ ロギングの設定確認

システム メッセージ ロギングの設定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 console	コンソール ロギング設定を表示します。
show logging info	ロギング設定を表示します。
show logging last*number-lines*	ログ ファイルの末尾から指定行数を表示します。
show logging level [*facility*]	ファシリティ ロギング重大度設定を表示します。
show logging logfile [**start-time***yyyymmmddhh:mm:ss*] [**end-time***yyyymmmddhh:mm:ss*]	ログ ファイルのメッセージを表示します。
show logging module	モジュール ロギング設定を表示します。
show logging monitor	モニタ ロギング設定を表示します。
show logging nvram [**last***number-lines*]	NVRAM ログのメッセージを表示します。
show logging server	Syslog サーバ設定を表示します。
show logging timestamp	ロギング タイムスタンプ単位設定を表示します。

システムメッセージロギングのコンフィギュレーション例

システム メッセージ ロギングのコンフィギュレーション例を示します。

```
configure terminal
 logging console 3
 logging monitor 3
 logging logfile my_log 6
 logging module 3
 logging level aaa 2
 logging timestamp milliseconds
 logging server 172.28.254.253
```

```
logging server 172.28.254.254 5 facility local3
copy running-config startup-config
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
システム メッセージの CLI コマンド	『*Cisco Nexus 7000 Series NX-OS System Management Command Reference*』
システム メッセージ	『*Cisco NX-OS System Messages Reference*』

システム メッセージ ロギングの機能の履歴

次の表に、このマニュアルの新機能および変更された機能を要約し、各機能がサポートされているリリースを示します。ご使用のソフトウェア リリースで、本書で説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。

表 *13*：システム メッセージ ロギングの機能の履歴

機能名	リリース	機能情報
システム メッセージ ロギング	7.2(0)D1(1)	この機能が導入されました。
システム メッセージ ロギング	5.2(1)	システム メッセージ ログ内で、物理的イーサネット インターフェイスおよびサブインターフェイスに対して説明を追加する機能が追加されました。
Syslog サーバ	5.1(1)	サポートされる syslog サーバの数が 3 から 8 に増加されました。
IPv6 サポート	4.2(1)	IPv6 syslog ホストに対するサポートが追加されました。
システム メッセージ ロギング	4.0(1)	この機能が導入されました。

第 8 章

Smart Call Home の設定

この章では、Cisco NX-OS デバイスの Smart Call Home 機能を設定する方法について説明します。この章の内容は、次のとおりです。

- 機能情報の確認，123 ページ
- Smart Call Home の概要，124 ページ
- Smart Call Home のライセンス要件，131 ページ
- Smart Call Home の前提条件，131 ページ
- Smart Call Home の注意事項および制約事項，132 ページ
- Smart Call Home のデフォルト設定，133 ページ
- Smart Call Home の設定，134 ページ
- Smart Call Home 設定の確認，150 ページ
- Smart Call Home の設定例，151 ページ
- その他の参考資料，152 ページ
- Smart Call Home の機能の履歴，166 ページ

機能情報の確認

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

Smart Call Home の概要

Smart Call Home では、重要なシステム ポリシーに対して電子メールベースの通知が提供されます。豊富なメッセージ フォーマットから選択できるので、ポケットベル サービス、標準 E 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最適な互換性が得られます。この機能を使用して、ネットワーク サポート エンジニアにポケットベルで連絡したり、ネットワーク オペレーション センターに電子メールを送信したりできます。また、Cisco Smart Call Home サービスを使用して TAC のケースを自動的に生成できます。

Smart Call Home には、次の機能があります。

- 関連する CLI コマンド出力の実行および添付が自動化されます。
- 次のような、複数のメッセージ フォーマット オプションがあります。
  - 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。
  - フルテキスト：人間が判読しやすいように完全にフォーマットされたメッセージ情報です。
  - XML：Extensible Markup Language（XML）および Adaptive Messaging Language（AML）XML Schema Definition（XSD）を使用する、調和の取れた判読可能なフォーマット。AML XSD は Cisco.com の Web サイトで公開されています。XML フォーマットでは、TAC との通信が可能になります。
- 複数のメッセージ宛先への同時配信が可能。それぞれの宛先プロファイルには、最大 50 個の電子メール宛先アドレスを設定できます。

宛先プロファイル

宛先プロファイルには、次の情報が含まれます。

- 1 つ以上のアラート グループ：アラートの発生時に、特定の Smart Call Home メッセージを送信するアラートのグループ。
- 1 つ以上の電子メール宛先：この宛先プロファイルに割り当てられたアラート グループによって生成された Smart Call Home メッセージの受信者リスト。
- メッセージフォーマット：Smart Call Home メッセージのフォーマット（ショートテキスト、フル テキスト、または XML）。
- メッセージ重大度：Cisco NX-OS が宛先プロファイル内のすべての電子メール アドレスに対して Smart Call Home メッセージを生成するまで、アラートが満たす必要がある Smart Call Home 重大度。アラートの Smart Call Home 重大度が宛先プロファイルに設定されたメッセージの重大度に満たない場合、Cisco NX-OS はアラートを生成しません。

定期メッセージを日別、週別、月別で送信するコンポーネントアラートグループを使用して、定期的なコンポーネントアップデートメッセージを許可するよう宛先プロファイルを設定することもできます。

Cisco NX-OS は、次の定義済み宛先プロファイルをサポートします。

- CiscoTAC-1：XML メッセージ フォーマットの Cisco-TAC アラート グループをサポートします。このプロファイルは、callhome@cisco.com という E メール コンタクト、最大メッセージ サイズ、およびメッセージ重大度 0 で設定済みです。このプロファイルのデフォルト情報はどれも変更できません。
- full-text-destination：フル テキスト メッセージ フォーマットをサポートします。
- short-text-destination：ショート テキスト メッセージ フォーマットをサポートします。

Smart Call Home アラート グループ

アラート グループは、すべての Cisco Nexus デバイスでサポートされる Smart Call Home アラートの定義済みサブセットです。アラート グループを使用すると、定義済みまたはカスタム宛先プロファイルに送信する一連の Smart Call Home アラートを選択できます。Smart Call Home アラートが宛先プロファイルにアソシエートされたいずれかのアラート グループに属する場合、およびアラートで、Smart Call Home メッセージ重大度が宛先プロファイルに設定されているメッセージ重大度と同じか、それ以上である場合のみ、デバイスは Smart Call Home アラートを宛先プロファイルの電子メールの宛先に送信します。

次の表に、サポートされるアラート グループと、アラート グループ用に生成された Smart Call Home メッセージに含まれるデフォルトの CLI コマンド出力を示します。

アラート グループ	説明	実行されるコマンド
Cisco-TAC	Smart Call Home 宛ての、他のアラート グループからのすべてのクリティカル アラート。	アラートを発信するアラート グループに基づいてコマンドを実行します。
Configuration	設定に関連した定期的なイベント。	**show module** **show version**

アラート グループ	説明	実行されるコマンド
Diagnostic	診断によって生成されたイベント。	**show diagnostic result module all detail** **show diagnostic result module***number***detail** **show hardware** **show logging last 200** **show module** **show sprom all** **show tech-support gold** **show tech-support ha** **show tech-support platform** **show version**
EEM	EEM によって生成されるイベント	**show diagnostic result module all detail** **show diagnostic result module***number***detail** **show module** **show tech-support gold** **show tech-support ha** **show tech-support platform**
Environmental	電源、ファン、および温度アラームなどの環境検知要素に関連するイベント。	**show environment** **show logging last 200** **show module** **show version**
Inventory	装置がコールド ブートした場合、または FRU の取り付けまたは取り外しを行った場合に示されるコンポーネント ステータス。このアラートは重要でないイベントであり、情報はステータスおよび使用権に使用されます。	**show inventory** **show license usage** **show module** **show sprom all** **show system uptime** **show version**
License	ライセンスおよびライセンス違反に関連するイベント	**show logging last 200**

アラート グループ	説明	実行されるコマンド
Linecard hardware	標準またはインテリジェント スイッチング モジュールに関連するイベント。	**show diagnostic result module all detail** **show diagnostic result module***number***detail** **show hardware** **show logging last 200** **show module** **show sprom all** **show tech-support ethpm** **show tech-support gold** **show tech-support ha** **show tech-support platform** **show version**
Supervisor hardware	スーパーバイザ モジュールに関連するイベント。	**show diagnostic result module all detail** **show hardware** **show logging last 200** **show module** **show sprom all** **show tech-support ethpm** **show tech-support gold** **show tech-support ha** **show tech-support platform** **show version**
Syslog port group	syslog PORT ファシリティによって生成されるイベント	**show license usage** **show logging last 200**

アラート グループ	説明	実行されるコマンド
System	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 diagnostic result module all detail** **show hardware** **show logging last 200** **show module** **show sprom all** **show tech-support ethpm** **show tech-support gold** **show tech-support ha** **show tech-support platform**
Test	ユーザが作成したテスト メッセージ	**show module** **show version**

Smart Call Home は、syslog の重大度を、syslog ポート グループ メッセージの対応する Smart Call Home の重大度に対応させます。

特定のイベントが発生し、Smart Call Home メッセージを含む **show** 出力を送信した場合に、追加の CLI **show** コマンドを実行するために、定義済みのアラート グループをカスタマイズできます。

show コマンドは、フルテキストおよびXML宛先プロファイルにのみ追加できます。ショートテキスト宛先プロファイルは、128バイトのテキストに制限されているため、追加の **show** コマンドをサポートしていません。

Smart Call Home のメッセージ レベル

Smart Call Home を使用すると、緊急度に基づいてメッセージをフィルタリングできます。各定義済みまたはユーザ定義宛先プロファイルを、0（最小緊急度）～9（最大緊急度）までの Smart Call Home しきい値と関連付けることができます。デフォルトは 0（全メッセージを送信）です。

Syslog 重大度は、Smart Call Home メッセージ レベルにマッピングされています。

（注） Smart 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。

次の表に、各 Smart Call Home メッセージ レベルのキーワードと、syslog ポート アラート グループの対応する syslog レベルを一覧表示します。

表 *14*：重大度と *syslog* レベルのマッピング

Smart Call Home レベル	キーワード	Syslog レベル	説明
9	Catastrophic	該当なし	ネットワーク全体に壊滅的な障害が発生しています。
8	Disaster	該当なし	ネットワークに重大な影響が及びます。
7	Fatal	緊急（0）	システムが使用不可能な状態。
6	Critical	アラート（1）	クリティカルな状況で、すぐに対応する必要があります。
5	Major	重要（2）	重大な状態。
4	Minor	エラー（3）	軽微な状態。
3	Warning	警告（4）	警告状態。
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。
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。
0	Debugging	デバッグ（7）	デバッグ メッセージ。

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 サービスに登録できます。Smart Call Home は、Smart Call Home メッセージを分析し、背景説明と推奨措置を提供します。既知の問題、特にオンライン診断障害については、TAC に Automatic Service Request が作成されます。

Smart Call Home には、次の機能があります。

- 継続的なデバイス ヘルス モニタリングとリアルタイムの診断アラート。

- Smart Call Home メッセージの分析。必要に応じて、自動サービス要求（詳細な診断情報が含まれる）が作成され、該当する TAC チームにルーティングされるため、問題解決を高速化できます。
- セキュアなメッセージが、ご使用のデバイスから直接、HTTP プロキシ サーバを経由して転送されるか、またはダウンロード可能な転送ゲートウェイ（TG）から転送されます。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。
- あらゆる Smart Call Home デバイスの Smart Call Home メッセージおよび推奨事項、インベントリ情報、設定情報への Web アクセス。この機能によって、関連する現場の注意事項、セキュリティ勧告、および廃止情報にアクセスできます。

登録には次の情報が必要です。

- デバイスの SMARTnet 契約番号
- 電子メール アドレス
- Cisco.com ID

Smart Call Home の詳細については、次の Smart Call Home のページを参照してください。 https://supportforums.cisco.com/community/netpro/solutions/smart_services/smartcallhome

CFS を使用した Smart Call Home の配信

Cisco Fabric Services（CFS）を使用して、ネットワーク内のすべての CFS 対応デバイスに Smart Call Home コンフィギュレーションを配信できます。デバイス プライオリティと sysContact 名を除く Smart Call Home コンフィギュレーション全体が配信されます。

CFS の詳細については、「CFS の設定」の項を参照してください。

データベース マージの注意事項

2 つの Smart 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。

- マージされるデータベースには、次の情報が含まれます。
  - マージ側デバイスからの全宛先プロファイルのスーパーセット。
  - 宛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。
  - マージ側デバイスにあるその他の設定情報（メッセージスロットリング、定期的なインベントリなど）。
- 宛先プロファイル名は、マージするデバイス内で重複しないようにしてください。コンフィギュレーションが異なっても、同じ名前は使用できません。プロファイル名が重複している場合、重複するプロファイルの 1 つを削除する必要があります。そうしなければマージ処理が失敗します。

ハイ アベイラビリティ

ステートフルおよびステートレスの両方のリスタートが、Smart Call Home でサポートされます。

仮想化のサポート

仮想デバイス コンテキスト（VDC）ごとに Smart Call Home インスタンスが 1 つサポートされます。Smart Call Home では、最初に登録された VDC のコンタクト情報を物理デバイス上のすべての VDC の管理者コンタクトとして使用します。たとえば、Smart Call Home でデフォルト VDC のコンタクト情報が使用されるようにするには、その VDC を使用して登録する必要があります。この情報は次の URL から、Smart Call Home の Web サイトでアップデートできます。

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

Smart Call Home は他のすべての VDC のコンタクトを、物理デバイスのすべての Smart Call Home データを参照できるけれども、管理者として動作することはできないユーザとして登録します。すべての登録ユーザおよび登録管理者は、物理デバイス上のすべての VDC からすべての Smat Call Home 通知を受け取ります。

デフォルトでは、デフォルトの VDC が使用されます。デフォルト VDC では、**callhome send** および **callhome test** コマンドを使用して Smart Call Home をテストできます。デフォルト以外の VDC では、**callhome test** コマンドのみ使用できます。VDC の詳細については、『Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide』を参照してください。

Smart Call Home は、仮想ルーティングおよびフォワーディング（VRF）を認識します。特定の VRF を使用して Smart Call Home SMTP サーバに接続するように Smart Call Home を設定できます。

Smart Call Home のライセンス要件

製品	ライセンス要件
Cisco NX-OS	Smart Call Home 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 nx-os イメージにバンドルされており、無料で提供されます。NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

Smart Call Home の前提条件

Smart Call Home には、次の前提条件があります。

- 電子メール アドレスにメッセージを送信するには、まず電子メール サーバを設定する必要があります。HTTP を使用してメッセージを送信するには、HTTPS サーバにアクセスでき、Cisco Nexus デバイスに有効な証明書がインストールされている必要があります。

- デバイスは E メール サーバまたは HTTPS サーバと IP 接続している必要があります。
- まず、コンタクト名（SNMP サーバのコンタクト）、電話番号、および住所情報を設定する必要があります。この手順は、受信メッセージの送信元を判別するために必要です。
- Smart Call Home サービスを使用する場合、設定中のデバイスに対応している現在のサービス契約が必要です。
- VDC を設定する場合は、適切なライセンスをインストールします。設定情報については『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』、ライセンス情報については『*Cisco NX-OS Licensing Guide*』を参照してください。

Smart Call Home の注意事項および制約事項

Smart Call Home には、次の注意事項および制限事項があります。

- IP 接続がない場合、またはプロファイル宛先への仮想ルーティングおよび転送（VRF）インスタンス内のインターフェイスがダウンしている場合、デバイスは Smart Call Home メッセージを送信できません。
- Smart Call Home はあらゆる SMTP サーバで動作します。
- Smart Call Home に対して最大 5 つの SMTP サーバを設定できます。
- CFS を使用して Smart Call Home コンフィギュレーションを配信すると、デバイス プライオリティと sysContact 名を除く Smart Call Home コンフィギュレーション全体が配信されます。
- CoPP は現在、インバンドの接続性が必要な場合に HTTP/HTTPS または SMTP 方式を使用する Smart Call Home のパケットを保護しません。これらのサービスのリターン トラフィックには、CoPP の class-default クラスが適用され、接続がほぼできなくなります。
- HTTPS 方式または SMTP 方式の明示的なクラスがコントロール プレーン ポリシングで定義されておらず、CoPP の class-default クラスで継続的な違反が起きている場合、Smart Call Home（SCH）機能が設定されたシステムでは、レポートの途中で接続障害が起きる場合があります。この問題は、SCH からの設定済みの宛先が既知のインバンドである場合にのみ発生します。
- 非標準の宛先ポートが使用されている SCH にインバンドを使用する場合、ユーザにそれらのポートを追加するよう警告する syslog を出力する必要があります。非管理ポートで HTTP または HTTPS プロキシ サーバを使用してシスコの Web サーバへの到達可能性を許可する場合にも、syslog での警告を考慮する必要があります。
- CFS がイネーブルになっている混合ファブリック環境では、Cisco NX-OS Release 5.x を実行しているシスコ デバイスは、5.x のコンフィギュレーション（複数の SMTP サーバ サポート、HTTP VRF サポート、および HTTP プロキシ サポート）を、CFS を介してファブリック内の他の 5.x デバイスへ配信できます。ただし、既存のデバイスを 5.x へアップグレードしても、これらの新しいコンフィギュレーションはデバイスへは配信されません。これは、アップグレード時に CFS マージがトリガーされないためです。したがって、シスコでは、ファブリック内のすべてのデバイスが新しいコンフィギュレーションをサポートしている場

合に限り、新しいコンフィギュレーションを適用するか、または（新しくアップグレードされたデバイスではなく）、新しいコンフィギュレーションを保持している既存の 5.x デバイスから空のコミットを実行することを推奨します。

Smart Call Home のデフォルト設定

このテーブルは、Smart Call Home パラメータのデフォルト設定を示します。

表 *15*：デフォルトの *Smart Call Home* パラメータ

パラメータ	デフォルト
フルテキストフォーマットで送信するメッセージの宛先メッセージ サイズ	2,500,000
XML フォーマットで送信するメッセージの宛先メッセージ サイズ	2,500,000
ショートテキストフォーマットで送信するメッセージの宛先メッセージ サイズ	4000
ポートを指定しなかった場合の SMTP サーバ ポート	25
プライオリティを指定しなかった場合の SMTP サーバのプライオリティ	50
プロファイルとアラート グループの関連付け	フルテキスト宛先プロファイルおよびショートテキスト宛先プロファイルの場合はすべて。CiscoTAC-1 宛先プロファイルの場合は cisco-tac アラート グループ
フォーマット タイプ	XML
Smart 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ない

Smart Call Home の設定

（注） Cisco NX-OS コマンドは Cisco IOS コマンドと異なる場合があるので注意してください。

次の順序で Smart Call Home 設定を行うことを推奨します。

1. 連絡先情報の設定, （134 ページ）
2. 宛先プロファイルの作成, （136 ページ）
3. アラート グループと宛先プロファイルの関連付け, （140 ページ）
4. （任意） アラート グループへの show コマンドの追加, （141 ページ）
5. Smart Call Home のイネーブル化またはディセーブル化, （148 ページ）
6. （任意） Smart Call Home 設定のテスト, （149 ページ）

連絡先情報の設定

Smart Call Home には、電子メール、電話番号、住所の各情報を指定する必要があります。契約 ID、カスタマー ID、サイト ID、およびスイッチ プライオリティ情報を任意で指定できます。

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 contact***sys-contact* 例： `switch(config)# snmp-server contact personname@companyname.com`	SNMP sysContact を設定します。

ステップ 3	**callhome**
	
	例：
	`switch(config)# callhome`
	`switch(config-callhome)#`
		Smart Call Home コンフィギュレーション モードを開始します。

ステップ 4	**email-contact***email-address*
	
	例：
	`switch(config-callhome)#`
	`email-contact admin@Mycompany.com`
		デバイスの主要責任者の電子メール アドレスを設定します。
		
		email-address には、電子メール アドレスの形式で、最大 255 の英数字を使用できます。

	コマンドまたはアクション	目的
		（注） 有効な電子メールアドレスを使用できます。アドレスには、空白を含めることはできません。
ステップ 5	**phone-contact***international-phone-number* 例： `switch(config-callhome)# phone-contact +1-800-123-4567`	デバイスの主要責任者の電話番号を国際電話フォーマットで設定します。 *international-phone-number* は、最大 17 文字の英数字で、国際電話フォーマットにする必要があります。 （注） 電話番号には、空白を含めることはできません。番号の前にプラス（+）プレフィックスを使用します。
ステップ 6	**streetaddress***address* 例： `switch(config-callhome)# streetaddress 123 Anystreet st. Anytown,AnyWhere`	デバイスの主要責任者の住所を空白の含まれる英数字ストリングとして設定します。 *address* には、最大 255 の英数字を使用できます。スペースを使用できます。
ステップ 7	**contract-id***contract-number* 例： `switch(config-callhome)# contract-id Contract5678`	（任意） サービス契約からこのデバイスの契約番号を設定します。 *contract-number* は、最大 255 文字の英数字を自由なフォーマットで指定できます。
ステップ 8	**customer-id***customer-number* 例： `switch(config-callhome)# customer-id Customer123456`	（任意） サービス契約からこのデバイスの顧客番号を設定します。 *customer-number* は、最大 255 文字の英数字を自由なフォーマットで指定できます。
ステップ 9	**site-id***site-number* 例： `switch(config-callhome)# site-id Site1`	（任意） このデバイスのサイト番号を設定します。 *site-number* は、最大 255 文字の英数字を自由なフォーマットで指定できます。
ステップ 10	**switch-priority***number* 例： `switch(config-callhome)# switch-priority 3`	（任意） このデバイスのスイッチ プライオリティを設定します。 指定できる範囲は 0 ～ 7 です。0 は最高のプライオリティを、7 は最低のプライオリティを示します。デフォルト値は 7 です。

	コマンドまたはアクション	目的
		（注） スイッチ 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。
ステップ 11	**commit** 例： `switch(config-callhome)# commit`	Smart Call Home 設定コマンドをコミットします。
ステップ 12	**show callhome** 例： `switch(config-callhome)# show callhome`	（任意） Smart Call Home コンフィギュレーションの概要を表示します。
ステップ 13	**copy running-config startup-config** 例： `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。

次の作業

宛先プロファイルを作成します。

宛先プロファイルの作成

ユーザ定義宛先プロファイルを作成し、メッセージ フォーマットを設定できます。

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。

	コマンドまたはアクション	目的

ステップ 2	**callhome**
	
	例：
	`switch(config)# callhome`
	`switch(config-callhome)#`
		Smart Call Home コンフィギュレーション モードを開始します。

ステップ 3	**destination-profile** *name* 例： `switch(config-callhome)# destination-profile Noc101`	新しい宛先プロファイルを作成します。名前は、最大 31 文字の英数字で指定できます。
ステップ 4	**destination-profile** *name* **format** {**XML** | **full-txt** | **short-txt**} 例： `switch(config-callhome)# destination-profile Noc101 format full-txt`	プロファイルのメッセージフォーマットを設定します。名前は、最大 31 文字の英数字で指定できます。
ステップ 5	**commit** 例： `switch(config-callhome)# commit`	Smart Call Home 設定コマンドをコミットします。
ステップ 6	**show callhome destination-profile** [**profile** *name*] 例： `switch(config-callhome)# show callhome destination-profile profile Noc101`	（任意） 1 つまたは複数の宛先プロファイルに関する情報を表示します。
ステップ 7	**copy running-config startup-config** 例： `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。

次の作業

宛先プロファイルに 1 つまたは複数のアラート グループを関連付けます。

宛先プロファイルの変更

定義済みまたはユーザ定義の宛先プロファイルの次の属性を変更できます。

- 宛先電子メール 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）。
- 宛先 URL：アラートの送信先となる HTTP または HTTPS URL。

- 転送方式：電子メールまたは HTTP 転送によって、使用される宛先アドレスのタイプが決まります。
- 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）。
- メッセージ レベル：この宛先プロファイルの Smart Call Home メッセージの重大度
- メッセージ サイズ：この宛先プロファイルの電子メール アドレスに送信された Smart Call Home メッセージの許容長さ。

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	**callhome**
	
	例：
	`switch(config)# callhome`
	`switch(config-callhome)#`
		Smart Call Home コンフィギュレーション モードを開始します。

ステップ 3	**destination-profile** {*name* | **CiscoTAC-1** | **full-txt-destination** | **short-txt-destination**} **email-addr***address* 例： `switch(config-callhome)# destination-profile full-txt-destination email-addr person@place.com`	ユーザ定義または定義済みの宛先プロファイルに電子メールアドレスを設定します。宛先プロファイルには、最大 50 個の電子メール アドレスを設定できます。
ステップ 4	**destination-profile** {*name* | **CiscoTAC-1** | **full-txt-destination** | **short-txt-destination**} **http***address* 例： `switch(config-callhome)# destination-profile CiscoTAC-1 http http://site.com/service/callhome`	ユーザ定義または定義済み宛先プロファイルの HTTP または HTTPS URL を設定します。URL の最大文字数は 255 文字です。
ステップ 5	**destination-profile** {*name* | **CiscoTAC-1** | **full-txt-destination** | **short-txt-destination**} **transport-method** {**email** | **http**} 例： `switch(config-callhome)# destination-profile CiscoTAC-1 transport-method http`	ユーザ定義または定義済み宛先プロファイルに対応する電子メールまたはHTTP転送方式を設定します。選択する転送方式のタイプによって、そのタイプに設定された宛先アドレスが決まります。

	コマンドまたはアクション	目的
ステップ 6	**destination-profile** {*name* | **CiscoTAC-1** | **full-txt-destination** | **short-txt-destination**} **message-level***number* 例： `switch(config-callhome)# destination-profile full-txt-destination message-level 5`	この宛先プロファイルの Smart Call Home メッセージの重大度を設定します。Cisco NX-OS がこのプロファイルの宛先に送信するのは、Smart Call Home の重大度が同じか、それ以上のアラートだけです。指定できる範囲は 0 ～ 9 です。9 は最大の重大度を示します。
ステップ 7	**destination-profile** {*name* | **CiscoTAC-1** | **full-txt-destination** | **short-txt-destination**} **message-size***number* 例： `switch(config-callhome)# destination-profile full-txt-destination message-size 100000`	この宛先プロファイルの最大メッセージ サイズを設定します。範囲は 0 ～ 5000000 です。デフォルト値は 2500000 です。
ステップ 8	**commit** 例： `switch(config-callhome)# commit`	Smart Call Home 設定コマンドをコミットします。
ステップ 9	**show callhome destination-profile** [**profile***name*] 例： `switch(config-callhome)# show callhome destination-profile profile full-text-destination`	（任意） 1 つまたは複数の宛先プロファイルに関する情報を表示します。
ステップ 10	**copy running-config startup-config** 例： `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。

次の作業

宛先プロファイルに 1 つまたは複数のアラート グループを関連付けます。

アラート グループと宛先プロファイルの関連付け

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	**callhome**
	
	例：
	`switch(config)# callhome`
	`switch(config-callhome)#`
		Smart Call Home コンフィギュレーション モードを開始します。

ステップ 3	**destination-profile** {*name* | **CiscoTAC-1** | **full-txt-destination** | **short-txt-destination**} **alert-group** {**All** | **Cisco-TAC** | **Configuration** | **Diagnostic** | **EEM** | **Environmental** | **Inventory** | **License** | **Supervisor-Hardware** | **Syslog-group-port** | **System** | **Test**} 例： `switch(config-callhome)# destination-profile Noc101 alert-group All`	アラート グループをこの宛先プロファイルにアソシエートします。キーワード **All** を使用して、すべてのアラート グループをこの宛先プロファイルにアソシエートします。
ステップ 4	**commit** 例： `switch(config-callhome)# commit`	Smart Call Home 設定コマンドをコミットします。
ステップ 5	**show callhome destination-profile** [**profile***name*] 例： `switch(config-callhome)# show callhome destination-profile profile Noc101`	（任意） 1 つまたは複数の宛先プロファイルに関する情報を表示します。
ステップ 6	**copy running-config startup-config** 例： `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。

次の作業

任意で **show** コマンドをアラート グループに追加し、SMTP 電子メール サーバを設定します。

アラート グループへの show コマンドの追加

1 つのアラート グループにユーザ定義の CLI **show** コマンドを 5 つまで割り当てることができます。

（注） CiscoTAC-1 宛先プロファイルには、ユーザ定義の CLI **show** コマンドを追加できません。

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	**callhome**
	
	例：
	`switch(config)# callhome`
	`switch(config-callhome)#`
		Smart Call Home コンフィギュレーション モードを開始します。

ステップ 3	**alert-group** {**Configuration** | **Diagnostic** | **EEM** | **Environmental** | **Inventory** | **License** | **Supervisor-Hardware** | **Syslog-group-port** | **System** | **Test**} **user-def-cmd***show-cmd* 例： `switch(config-callhome)# alert-group Configuration user-def-cmd show ip route`	**show** コマンド出力を、このアラート グループに送信された Smart Call Home メッセージに追加します。有効な **show** コマンドだけが受け入れられます。
ステップ 4	**commit** 例： `switch(config-callhome)# commit`	Smart Call Home 設定コマンドをコミットします。
ステップ 5	**show callhome user-def-cmds** 例： `switch(config-callhome)# show callhome user-def-cmds`	（任意） アラート グループに追加されたすべてのユーザ定義 **show** コマンドに関する情報を表示します。
ステップ 6	**copy running-config startup-config** 例： `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。

次の作業

SMTP 電子メール サーバに接続するように Smart Call Home を設定します。

電子メール サーバの設定

Smart Call Home 機能が動作するよう SMTP サーバ アドレスを設定します。送信元および返信先電子メール アドレスも設定できます。

Smart Call Home に対して最大 5 つの SMTP サーバを設定できます。サーバは、プライオリティに基づいて試行されます。最もプライオリティの高いサーバが最初に試行されます。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が試行されます。2 つのサーバのプライオリティが同じ場合は、先に設定された方が最初に試行されます。

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	**callhome**
	
	例：
	`switch(config)# callhome`
	`switch(config-callhome)#`
		Smart Call Home コンフィギュレーション モードを開始します。

ステップ 3	**transport email mail-server***ip-address* [**port***number*] [**priority***number*] [**use-vrf***vrf-name*] 例： `switch(config-callhome)# transport email mail-server 192.0.2.1 use-vrf Red`	ドメイン ネーム サーバ（DNS）名、IPv4 アドレス、または IPv6 アドレスのいずれかとして SMTP サーバを設定します。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 25 です。 任意で、SMTP サーバのプライオリティを設定します。プライオリティの範囲は 1 ～ 100 で、1 が最高、100 が最低のプライオリティです。プライオリティを指定しない場合、デフォルト値の 50 が使用されます。 また、この SMTP サーバと通信する際に使用するよう任意で VRF を設定します。指定された VRF は、HTTP を使用したメッセージの送信には使用されません。

	コマンドまたはアクション	目的
ステップ 4	**transport email from***email-address* 例： `switch(config-callhome)# transport email from person@company.com`	（任意） Smart Call Home メッセージの送信元電子メール フィールドを設定します。
ステップ 5	**transport email reply-to***email-address* 例： `switch(config-callhome)# transport email reply-to person@company.com`	（任意） Smart Call Home メッセージの返信先電子メール フィールドを設定します。
ステップ 6	**commit** 例： `switch(config-callhome)# commit`	Smart Call Home 設定コマンドをコミットします。
ステップ 7	**show callhome transport** 例： `switch(config-callhome)# show callhome transport`	（任意） Smart Call Home に対する転送関係のコンフィギュレーションを表示します。
ステップ 8	**copy running-config startup-config** 例： `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。

次の作業

任意で、VRF を使用して HTTP で Smart Call Home メッセージを送信します。

HTTP を使用したメッセージ送信のための VRF 設定

VRF を使用して、HTTP で Smart Call Home メッセージを送信できます。HTTP VRF が設定されていない場合は、デフォルトの VRF を使用して HTTP でメッセージが転送されます。

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	**callhome**
	
	例：
	`switch(config)# callhome`
	`switch(config-callhome)#`
		Smart Call Home コンフィギュレーション モードを開始します。

ステップ 3	**transport http use-vrf** *vrf-name* 例： `switch(config-callhome)# transport http use-vrf Blue`	HTTP で電子メールおよび他の Smart Call Home メッセージを送信するための VRF を設定します。
ステップ 4	**commit** 例： `switch(config-callhome)# commit`	Smart Call Home 設定コマンドをコミットします。
ステップ 5	**show callhome** 例： `switch(config-callhome)# show callhome`	（任意） Smart Call Home に関する情報を表示します。
ステップ 6	**copy running-config startup-config** 例： `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。

次の作業

任意で、HTTP プロキシ サーバから HTTP メッセージを送信するように Smart Call Home を設定します。

HTTP プロキシ サーバの設定

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	**callhome**
	
	例：
	`switch(config)# callhome`
	`switch(config-callhome)#`
		Smart Call Home コンフィギュレーション モードを開始します。

ステップ 3	**transport http proxy server***ip-address* [**port** *number*] 例： `switch(config-callhome)# transport http proxy server 192.0.2.1`	HTTP プロキシ サーバのドメイン ネーム サーバ（DNS）の名前、IPv4 アドレス、または IPv6 アドレスを設定します。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 ポート番号は、8080 です。
ステップ 4	**transport http proxy enable** 例： `switch(config-callhome)# transport http proxy enable`	Smart Call Home で、HTTP プロキシ サーバ経由ですべての HTTP メッセージを送信できるようにします。 （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。 （注） プロキシサーバを経由してメッセージを転送するために使用する VRF は、**transport http use-vrf** コマンドを使用して設定したものと同じです。
ステップ 5	**commit** 例： `switch(config-callhome)# commit`	Smart Call Home 設定コマンドをコミットします。
ステップ 6	**show callhome transport** 例： `switch(config-callhome)# show callhome transport`	（任意） Smart Call Home に対する転送関係のコンフィギュレーションを表示します。

	コマンドまたはアクション	目的
ステップ 7	**copy running-config startup-config** 例： `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。

次の作業

任意で、定期的にインベントリ通知を送信するようにデバイスを設定します。

定期的なインベントリ通知の設定

デバイス上で現在イネーブルにされて動作しているすべてのソフトウェア サービスのインベントリとともに、ハードウェア インベントリ情報を示すメッセージを定期的に送信するように、デバイスを設定できます。デバイスは、2 種類の Smart Call Home 通知を生成します。定期的コンフィギュレーション メッセージと定期的インベントリ メッセージです。

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	**callhome**
	
	例：
	`switch(config)# callhome`
	`switch(config-callhome)#`
		Smart Call Home コンフィギュレーション モードを開始します。

ステップ 3	**periodic-inventory notification** [**interval***days*] [**timeofday***time*] 例： `switch(config-callhome)# periodic-inventory notification interval 20`	定期的なインベントリ メッセージを設定します。間隔の範囲は 1 ～ 30 日で、デフォルトは 7 です。*time* 引数は HH:MM の形式です。これは、*X* 日ごとに更新が送信される日の時間を定義します（ここで *X* は更新間隔です）。
ステップ 4	**commit** 例： `switch(config-callhome)# commit`	Smart Call Home 設定コマンドをコミットします。

	コマンドまたはアクション	目的
ステップ 5	**show callhome** 例： `switch(config-callhome)# show callhome`	（任意） Smart Call Home に関する情報を表示します。
ステップ 6	**copy running-config startup-config** 例： `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。

次の作業

任意で重複メッセージ スロットリングをディセーブルにします。

重複メッセージ抑制のディセーブル化

同じイベントについて受信する重複メッセージの数を制限できます。デフォルトでは、デバイスは同じイベントについて受信する重複メッセージの数を制限します。2 時間の時間枠内で送信された重複メッセージの数が 30 メッセージを超えると、デバイスは同じアラート タイプの以降のメッセージを廃棄します。

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	**callhome**
	
	例：
	`switch(config)# callhome`
	`switch(config-callhome)#`
		Smart Call Home コンフィギュレーション モードを開始します。

ステップ 3	**no duplicate-message throttle** 例： `switch(config-callhome)# no duplicate-message throttle`	Smart Call Home の重複メッセージ抑制をディセーブルにします。 重複メッセージ抑制はデフォルトでイネーブルです。

	コマンドまたはアクション	目的
ステップ 4	**commit** 例： `switch(config-callhome)# commit`	Smart Call Home 設定コマンドをコミットします。
ステップ 5	**copy running-config startup-config** 例： `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。

次の作業

Smart Call Home をイネーブルにします。

Smart Call Home のイネーブル化またはディセーブル化

担当者情報を設定した場合、Smart Call Home 機能をイネーブルにできます。

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	**callhome**
	
	例：
	`switch(config)# callhome`
	`switch(config-callhome)#`
		Smart Call Home コンフィギュレーション モードを開始します。

ステップ 3	[**no**] **enable** 例： `switch(config-callhome)# enable`	Smart Call Home をイネーブルまたはディセーブルにします。 Smart Call Home は、デフォルトでディセーブルです。
ステップ 4	**commit** 例： `switch(config-callhome)# commit`	Smart Call Home 設定コマンドをコミットします。

	コマンドまたはアクション	目的
ステップ 5	**copy running-config startup-config** 例： `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。

次の作業

任意でテスト メッセージを生成します。

Smart Call Home 設定のテスト

テスト メッセージを生成して Smart Call Home 通信をテストできます。

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	**callhome**
	
	例：
	`switch(config)# callhome`
	`switch(config-callhome)#`
		Smart Call Home コンフィギュレーション モードを開始します。

ステップ 3	**callhome send** [**configuration** | **diagnostic**] 例： `switch(config-callhome)# callhome send diagnostic`	設定されたすべての宛先に、指定された Smart Call Home テスト メッセージを送信します。
ステップ 4	**callhome test** 例： `switch(config-callhome)# callhome test`	設定されたすべての宛先にテストメッセージを送信します。
ステップ 5	**copy running-config startup-config** 例： `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。

Smart Call Home 設定の確認

Smart Call Home 設定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 callhome	Smart Call Home 設定を表示します。
show callhome destination-profile*name*	1 つまたは複数の Smart Call Home 宛先プロファイルを表示します。
show callhome merge	Smart Call Home の最後の CFS マージ処理のステータスを表示します。
show callhome pending	保留中の CFS データベースの Smart Call Home 設定変更を表示します。
show callhome pending-diff	保留中の Smart Call Home 設定と実行中の Smart Call Home 設定の違いを表示します。
show callhome session-status	最後の CFS コミットまたは打ち切り操作のステータスを表示します。
show callhomestatus	Smart Call Home の CFS 配信状態（イネーブルまたはディセーブル）を表示します。
show callhome transport	Smart Call Home に対する転送関係のコンフィギュレーションを表示します。
show callhome user-def-cmds	任意のアラート グループに追加された CLI コマンドを表示します。
show running-config callhome [**all**]	Smart Call Home の実行コンフィギュレーションを表示します。

コマンド	目的
show startup-config callhome	Smart Call Home のスタートアップ コンフィギュレーションを表示します。
show tech-support callhome	Smart Call Home のテクニカル サポート出力を表示します。

Smart Call Home の設定例

Noc101 という宛先プロファイルを作成し、コンフィギュレーションのアラート グループをこのプロファイルに関連付けて、連絡先情報と電子メールの情報を設定した後で、HTTP を介して Smart Call Home メッセージを送信するための VRF を指定する例を示します。

```
configure terminal
snmp-server contact person@company.com
callhome
distribute
email-contact admin@Mycompany.com
phone-contact +1-800-123-4567
streetaddress 123 Anystreet st. Anytown,AnyWhere
destination-profile Noc101 format full-txt
destination-profile full-text-destination email-addr person@company.com
destination-profile full-text-destination message-level 5
destination-profile Noc101 alert-group Configuration
alert-group Configuration user-def-cmd show ip route
transport email mail-server 192.0.2.10 priority 1
transport http use-vrf Blue
enable
commit
```

Smart Call Home メッセージに対して複数の SMTP サーバを設定する例を示します。

```
configure terminal
callhome
transport email mail-server 192.0.2.10 priority 4
transport email mail-server 172.21.34.193
transport email smtp-server 10.1.1.174
transport email mail-server 64.72.101.213 priority 60
transport email from person@company.com
transport email reply-to person@company.com
commit
```

上記のコンフィギュレーションに基づいて、SMTP サーバはこの順序で試行されます。

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（プライオリティ 50、デフォルト）

64.72.101.213（プライオリティ 60）

（注） **transport email smtp-server** コマンドのプライオリティは、最大の 0 です。このコマンドで指定されたサーバは最初に試行され、次に、**transport email mail-server** コマンドで指定されたサーバが、プライオリティの順に試行されます。

次に、HTTP プロキシ サーバからの HTTP メッセージを送信するように、Smart Call Home を設定する例を示します。

```
configure terminal
callhome
transport http proxy server 10.10.10.1 port 4
transport http proxy enable
commit
```

その他の参考資料

イベント トリガー

次の表に、イベント トリガーおよび Smart Call Home メッセージの重大度を示します。

アラート グループ	イベント名	説明	Smart Call Home 重大度
設定	PERIODIC_CONFIGURATION	定期的コンフィギュレーション アップデート メッセージ	2
診断	DIAGNOSTIC_MAJOR_ALERT	GOLD が生成したメジャー アラート	7
	DIAGNOSTIC_MINOR_ALERT	GOLD が生成したマイナー アラート	4
	DIAGNOSTIC_NORMAL_ALERT	Smart Call Home が生成した通常の診断アラート	2

アラート グループ	イベント名	説明	Smart Call Home 重大度
環境および CISCO_TAC	FAN_FAILURE	冷却ファンが障害になりました。	5
	POWER_SUPPLY_ALERT	電源モジュールに関する警告の発生	6
	POWER_SUPPLY_FAILURE	電源モジュールの故障	6
	POWER_SUPPLY_SHUTDOWN	電源モジュールのシャットダウン	6
	TEMPERATURE_ALARM	温度センサーの障害	6
	TEMPERATURE_MAJOR_ALARM	温度が動作メジャーしきい値を超えたことを示す温度センサーの表示	6
	TEMPERATURE_MINOR_ALARM	温度が動作マイナーしきい値を超えたことを示す温度センサーの表示	4
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	シャーシへの新しいハードウェア コンポーネントの追加	2
	HARDWARE_REMOVAL	シャーシからのハードウェアの取り外し	2
	PERIODIC_INVENTORY	定期的インベントリ メッセージの作成	2
ライセンス	LICENSE_VIOLATION	使用中の機能にライセンスがなく、猶予期間を経てオフになった場合	6
ライン モジュール ハードウェアおよび CISCO_TAC	LINEmodule_FAILURE	モジュールの動作障害	7
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 モジュールの動作障害	7

アラート グループ	イベント名	説明	Smart Call Home 重大度
Syslog グループ ポート	PORT_FAILURE	ポート ファシリティに対応する syslog メッセージの生成	6
	SYSLOG_ALERT	syslog アラート メッセージの生成	5
システムおよび CISCO_TAC	SW_CRASH	ステートレス リスタートによるソフトウェア プロセス障害、つまりサービスの停止スーパーバイザ モジュールでのプロセス クラッシュに対してメッセージが送信されます。	5
	SW_SYSTEM_INCONSISTENT	ソフトウェアまたはファイル システムにおける不整合の検出	5
テストおよび CISCO_TAC	TEST	ユーザが作成したテストの発生	2

メッセージ フォーマット

Smart Call Home では、次のメッセージ フォーマットがサポートされます。

ショート テキスト メッセージ フォーマット

次の表に、すべてのメッセージ タイプのショート テキスト書式設定オプションを示します。

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）

共通のイベント メッセージ フィールド

次の表では、フル テキストまたは XML メッセージに共通するイベント メッセージ フィールドの最初のセットについて説明します。

データ項目（プレーン テキストおよび XML）	説明（プレーン テキストおよび XML）	XML タグ（XML のみ）
Timestamp	ISO 時刻通知でのイベントの日付/タイム スタンプ YYYY-MM-DD HH:MM:SS GMT+HH:MM.	/aml/header/time
メッセージ名	メッセージの名前。	/aml/header/name
メッセージ タイプ	リアクティブまたはプロアクティブなどのメッセージ タイプの名前	/aml/header/type
メッセージ グループ	Syslog などのアラート グループの名前	/aml/header/group
重大度	メッセージの重大度。	/aml/header/level
送信元 ID	ルーティング製品タイプ（Catalyst 6500 シリーズ スイッチなど）	/aml/header/source
デバイス ID	メッセージを生成したエンド デバイスの固有デバイス識別情報（UDI）。メッセージがデバイスに対して固有でない場合は、このフィールドを空にする必要があります。形式は、*type@Sid@serial*。 • *type* はバックプレーン IDPROM 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：WS-C6509@C@12345678	/aml/ header/deviceId

データ項目（プレーン テキストおよび XML）	説明（プレーン テキストおよび XML）	XML タグ（XML のみ）
Customer ID	サポート サービスによって契約情報やその他の ID 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。	/aml/ header/customerID
契約 ID	サポート サービスによって契約情報やその他の ID 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。	/aml/ header /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。	/aml/ header/siteId
Server ID	デバイスからメッセージが生成された場合、この ID はデバイスの Unique Device Identifier（UDI）フォーマットです。形式は、*type@Sid@serial*。 • *type* はバックプレーン IDPROM 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：WS-C6509@C@12345678	/aml/header/serverId
メッセージの説明	エラーを説明するショート テキスト	/aml/body/msgDesc
デバイス名	イベントが発生したノード（デバイスのホスト名）	/aml/body/sysName

データ項目（プレーン テキストおよび XML）	説明（プレーン テキストおよび XML）	XML タグ（XML のみ）
担当者名	イベントが発生したノード関連の問題について問い合わせる担当者名	/aml/body/sysContact
Contact email	このユニットの連絡先として識別される担当者の電子メールアドレス。	/aml/body/sysContactEmail
Contact phone number	このユニットの連絡先である人物の電話番号。	/aml/body/sysContactPhone Number
住所	この装置関連の返品許可（RMA）部品の送付先住所を保存するオプション フィールド	/aml/body/sysStreetAddress
モデル名	デバイスのモデル名（製品ファミリ名に含まれる具体的なモデル）	/aml/body/chassis/name
Serial number	ユニットのシャーシのシリアル番号。	/aml/body/chassis/serialNo
シャーシの部品番号	シャーシの最上アセンブリ番号。	/aml/body/chassis/partNo

アラート グループ メッセージ フィールド

次の表に、フル テキストおよびXML のアラート グループ メッセージに固有のフィールドについて説明します。1 つのアラート グループに対して複数の CLI コマンドが実行される場合は、これらのフィールドが繰り返されることがあります。

データ項目（プレーン テキストおよび XML）	説明（プレーン テキストおよび XML）	XML タグ（XML のみ）
コマンド出力名	実行されたCLI コマンドの正確な名前	/aml/attachments/attachment/name
添付タイプ	特定のコマンド出力	/aml/attachments/attachment/type
MIME タイプ	プレーン テキストまたは符号化タイプ	/aml/attachments/attachment/mime

データ項目（プレーン テキストおよび XML）	説明（プレーン テキストおよび XML）	XML タグ（XML のみ）
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。	/aml/attachments/attachment/atdata

リアクティブおよびプロアクティブ イベント メッセージのフィールド

次の表では、フル テキストまたは XML メッセージのリアクティブおよびプロアクティブ イベント メッセージ形式について説明します。

データ項目（プレーン テキストおよび XML）	説明（プレーン テキストおよび XML）	XML タグ（XML のみ）
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。	/aml/body/chassis/hwVersion
スーパーバイザ モジュール ソフトウェア バージョン	最上レベルのソフトウェア バージョン。	/aml/body/chassis/swVersion
影響のある FRU の名前	イベント メッセージを生成する関連 FRU の名前	/aml/body/fru/name
影響のある FRU のシリアル番号	関連 FRU のシリアル番号	/aml/body/fru/serialNo
影響のある FRU の製品番号	関連 FRU の部品番号	/aml/body/fru/partNo
FRU スロット	イベント メッセージを生成する FRU のスロット番号	/aml/body/fru/slot
FRU ハードウェア バージョン	関連 FRU のハードウェア バージョン	/aml/body/fru/hwVersion
FRU ソフトウェア バージョン	関連 FRU で稼働しているソフトウェア バージョン	/aml/body/fru/swVersion

インベントリ イベント メッセージのフィールド

次の表では、フル テキストまたは XML メッセージのインベントリ イベント メッセージ形式について説明します。

データ項目（プレーン テキストおよび XML）	説明（プレーン テキストおよび XML）	XML タグ（XML のみ）
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	/aml/body/chassis/hwVersion
スーパーバイザ モジュール ソフトウェア バージョン	最上レベルのソフトウェア バージョン。	/aml/body/chassis/swVersion
FRU name	イベント メッセージを生成する関連 FRU の名前	/aml/body/fru/name
FRU s/n	FRU のシリアル番号	/aml/body/fru/serialNo
FRU 製品番号	FRU の部品番号	/aml/body/fru/partNo
FRU スロット	FRU のスロット番号	/aml/body/fru/slot
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	/aml/body/fru/hwVersion
FRU ソフトウェア バージョン	FRUで稼働しているソフトウェア バージョン	/aml/body/fru/swVersion

ユーザが作成したテスト メッセージのフィールド

次の表に、フル テキストまたは XML のユーザが作成したテスト メッセージ形式について説明します。

データ項目（プレーン テキストおよび XML）	説明（プレーン テキストおよび XML）	XML タグ（XML のみ）
プロセス ID	固有のプロセス ID。	/aml/body/process/id
Process state	プロセスの状態（実行中、中止など）。	/aml/body/process/processState
Process exception	原因コードの例外。	/aml/body/process/exception

フル テキスト形式での syslog アラート通知の例

次の例では、Syslog ポート アラート グループ通知のフル テキスト形式を示します。

```
Severity Level:5
Series:Nexus7000
Switch Priority:0
Device Id:N7K-C7010@C@TXX12345678
Server Id:N7K-C7010@C@TXX12345678
Time of Event:2008-01-17 16:31:33 GMT+0000 Message Name:
```

```
Message Type:syslog
System Name:dc3-test
Contact Name:Jay Tester
Contact Email:contact@example.com
Contact Phone:+91-80-1234-5678
Street Address:#1 Any Street
Event Description:SYSLOG_ALERT 2008 Jan 17 16:31:33 dc3-test %ETHPORT-2-IF_SEQ_ERROR: Error
 (0x20) while
communicating with component MTS_SAP_ELTM opcode:MTS_OPC_ETHPM_PORT_PHY_CLEANUP (for:RID_PORT:
 Ethernet3/1)

syslog_facility:ETHPORT
start chassis information:
Affected Chassis:N7K-C7010
Affected Chassis Serial Number:TXX12345678 Affected Chassis Hardware Version:0.405 Affected
 Chassis Software
Version:4.1(1) Affected Chassis Part No:73-10900-04 end chassis information:
start attachment
name:show logging logfile | tail -n 200
type:text
data:
2008 Jan 17 10:57:51 dc3-test %SYSLOG-1-SYSTEM_MSG : Logging logfile (messages) cleared by
 user
2008 Jan 17 10:57:53 dc3-test %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configuring console from
/dev/ttyS0 /dev/ttyS0_console
2008 Jan 17 10:58:35 dc3-test %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configuring console from
/dev/ttyS0 /dev/ttyS0_console
2008 Jan 17 10:59:00 dc3-test %DAEMON-3-SYSTEM_MSG: error: setsockopt IP_TOS 16: Invalid
argument: - sshd[14484]
2008 Jan 17 10:59:05 dc3-test %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configuring console from
/dev/ttyS0 /dev/ttyS0_console
2008 Jan 17 12:11:18 dc3-test %SYSMGR-STANDBY-5-SUBPROC_TERMINATED: "System Manager (gsync
 controller)" (PID 12000)
has finished with error code SYSMGR_EXITCODE_GSYNCFAILED_NONFATAL (12).
2008 Jan 17 16:28:03 dc3-test %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configuring console from
/dev/ttyS0 /dev/ttyS0_console
2008 Jan 17 16:28:44 dc3-test %SYSMGR-3-BASIC_TRACE: core_copy: PID 2579 with message Core
 not generated by system
for eltm(0). WCOREDUMP(9) returned zero .
2008 Jan 17 16:28:44 dc3-test %SYSMGR-2-SERVICE_CRASHED: Service "eltm" (PID 3504) hasn't
caught signal 9 (no core).
2008 Jan 17 16:29:08 dc3-test %SYSMGR-3-BASIC_TRACE: core_copy: PID 2579 with message Core
 not generated by system
for eltm(0). WCOREDUMP(9) returned zero.
2008 Jan 17 16:29:08 dc3-test %SYSMGR-2-SERVICE_CRASHED: Service "eltm" (PID 23210) hasn't
 caught signal 9 (no core).
2008 Jan 17 16:29:17 dc3-test %SYSMGR-3-BASIC_TRACE: core_copy: PID 2579 with message Core
 not generated by system
for eltm(0). WCOREDUMP(9) returned zero.
2008 Jan 17 16:29:17 dc3-test %SYSMGR-2-SERVICE_CRASHED: Service "eltm" (PID 23294) hasn't
 caught signal 9 (no core).
2008 Jan 17 16:29:25 dc3-test %SYSMGR-2-HASWITCHOVER_PRE_START: This supervisor is becoming
 active (pre-start phase).
2008 Jan 17 16:29:25 dc3-test %SYSMGR-2-HASWITCHOVER_START: This supervisor is becoming
active.
2008 Jan 17 16:29:26 dc3-test %USER-3-SYSTEM_MSG: crdcfg_get_srvinfo: mts_send failed -
device_test
2008 Jan 17 16:29:27 dc3-test %NETSTACK-3-IP_UNK_MSG_MAJOR: netstack [4336] Unrecognized
message from MRIB. Major
type 1807
2008 Jan 17 16:29:27 dc3-test %IM-5-IM_INTF_STATE: mgmt0 is DOWN in vdc 1
2008 Jan 17 16:29:27 dc3-test %IM-5-IM_INTF_STATE: mgmt0 is DOWN in vdc 2
2008 Jan 17 16:29:27 dc3-test %IM-5-IM_INTF_STATE: mgmt0 is DOWN in vdc 3
2008 Jan 17 16:29:27 dc3-test %IM-5-IM_INTF_STATE: mgmt0 is DOWN in vdc 4
2008 Jan 17 16:29:28 dc3-test %SYSMGR-2-SWITCHOVER_OVER: Switchover completed.
2008 Jan 17 16:29:28 dc3-test %DAEMON-3-SYSTEM_MSG: ntp:socket family : 2 - ntpd[19045]
2008 Jan 17 16:29:28 dc3-test %DAEMON-3-SYSTEM_MSG: ntp:socket family : 10 - ntpd[19045]
2008 Jan 17 16:29:28 dc3-test %DAEMON-3-SYSTEM_MSG: ntp:ipv6 only defined - ntpd[19045]
2008 Jan 17 16:29:28 dc3-test %DAEMON-3-SYSTEM_MSG: ntp:bindv6 only defined - ntpd[19045]
2008 Jan 17 16:29:28 dc3-test %DAEMON-3-SYSTEM_MSG: ntp:socket family : 2 - ntpd[19045]
2008 Jan 17 16:29:28 dc3-test %DAEMON-3-SYSTEM_MSG: ntp:socket family : 0 - ntpd[19045]
2008 Jan 17 16:29:28 dc3-test %DAEMON-3-SYSTEM_MSG: ntp:socket family : 0 - ntpd[19045]
2008 Jan 17 16:29:28 dc3-test %NETSTACK-3-CLIENT_GET: netstack [4336] HA client filter
```

```
recovery failed (0)
2008 Jan 17 16:29:28 dc3-test %NETSTACK-3-CLIENT_GET: netstack [4336] HA client filter
recovery failed (0)
2008 Jan 17 16:29:29 dc3-test %DAEMON-3-SYSTEM_MSG: ssh disabled, removing -
dcos-xinetd[19072]
2008 Jan 17 16:29:29 dc3-test %DAEMON-3-SYSTEM_MSG: Telnet disabled, removing -
dcos-xinetd[19072]
2008 Jan 17 16:29:31 dc3-test %DAEMON-3-SYSTEM_MSG: Telnet disabled, removing -
dcos-xinetd[19073]
2008 Jan 17 16:29:32 dc3-test %DAEMON-3-SYSTEM_MSG: ssh disabled, removing -
dcos-xinetd[19079]
2008 Jan 17 16:29:32 dc3-test %DAEMON-3-SYSTEM_MSG: Telnet disabled, removing -
dcos-xinetd[19079]
2008 Jan 17 16:29:34 dc3-test %IM-5-IM_INTF_STATE: mgmt0 is UP in vdc 1
2008 Jan 17 16:29:34 dc3-test %IM-5-IM_INTF_STATE: mgmt0 is UP in vdc 2
2008 Jan 17 16:29:34 dc3-test %IM-5-IM_INTF_STATE: mgmt0 is UP in vdc 3
2008 Jan 17 16:29:34 dc3-test %IM-5-IM_INTF_STATE: mgmt0 is UP in vdc 4
2008 Jan 17 16:29:34 dc3-test %DAEMON-3-SYSTEM_MSG: ssh disabled, removing -
dcos-xinetd[19105]
2008 Jan 17 16:29:34 dc3-test %DAEMON-3-SYSTEM_MSG: Telnet disabled, removing -
dcos-xinetd[19105]
2008 Jan 17 16:29:35 dc3-test %PLATFORM-2-PS_AC_IN_MISSING: Power supply 2 present but all
 AC inputs are not
connected, ac-redundancy might be affected
2008 Jan 17 16:29:35 dc3-test %PLATFORM-2-PS_AC_IN_MISSING: Power supply 3 present but all
 AC inputs are not
connected, ac-redundancy might be affected
2008 Jan 17 16:29:38 dc3-test %CALLHOME-2-EVENT: SUP_FAILURE
2008 Jan 17 16:29:46 dc3-test vsh[19166]: CLIC-3-FAILED_EXEC: Can not exec command <more>
return code <14>
2008 Jan 17 16:30:24 dc3-test vsh[23810]: CLIC-3-FAILED_EXEC: Can not exec command <more>
return code <14>
2008 Jan 17 16:30:24 dc3-test vsh[23803]: CLIC-3-FAILED_EXEC: Can not exec command <more>
return code <14>
2008 Jan 17 16:30:24 dc3-test vsh[23818]: CLIC-3-FAILED_EXEC: Can not exec command <more>
return code <14>
2008 Jan 17 16:30:47 dc3-test %SYSMGR-3-BASIC_TRACE: core_copy: PID 2630 with message Core
 not generated by
system for eltm(0). WCOREDUMP(9) returned zero .
2008 Jan 17 16:30:47 dc3-test %SYSMGR-2-SERVICE_CRASHED: Service "eltm" (PID 4820) hasn't
caught signal 9
(no core).
2008 Jan 17 16:31:02 dc3-test %SYSMGR-3-BASIC_TRACE: core_copy: PID 2630 with message Core
 not generated by
system for eltm(0). WCOREDUMP(9) returned zero .
2008 Jan 17 16:31:02 dc3-test %SYSMGR-2-SERVICE_CRASHED: Service "eltm" (PID 24239) hasn't
 caught signal 9
(no core).
2008 Jan 17 16:31:14 dc3-test %SYSMGR-3-BASIC_TRACE: core_copy: PID 2630 with message Core
 not generated by
system for eltm(0). WCOREDUMP(9) returned zero .
2008 Jan 17 16:31:14 dc3-test %SYSMGR-2-SERVICE_CRASHED: Service "eltm" (PID 24401) hasn't
 caught signal 9
(no core).
2008 Jan 17 16:31:23 dc3-test %CALLHOME-2-EVENT: SW_CRASH alert for service: eltm
2008 Jan 17 16:31:23 dc3-test %SYSMGR-3-BASIC_TRACE: core_copy: PID 2630 with message Core
 not generated by
system for eltm(0). WCOREDUMP(9) returned zero .
2008 Jan 17 16:31:23 dc3-test %SYSMGR-2-SERVICE_CRASHED: Service "eltm" (PID 24407) hasn't
 caught signal 9
(no core).
2008 Jan 17 16:31:24 dc3-test vsh[24532]: CLIC-3-FAILED_EXEC: Can not exec command <more>
return code <14>
2008 Jan 17 16:31:24 dc3-test vsh[24548]: CLIC-3-FAILED_EXEC: Can not exec command <more>
return code <14>
2008 Jan 17 16:31:24 dc3-test vsh[24535]: CLIC-3-FAILED_EXEC: Can not exec command <more>
return code <14>
2008 Jan 17 16:31:33 dc3-test %NETSTACK-3-INTERNAL_ERROR: netstack [4336] (null)
2008 Jan 17 16:31:33 dc3-test %ETHPORT-2-IF_SEQ_ERROR: Error (0x20) while communicating
with component MTS_SAP_ELTM
opcode:MTS_OPC_ETHPM_PORT_PHY_CLEANUP (for:RID_PORT: Ethernet3/1) end attachment start
attachment
name:show vdc membership
```

```
type:text
data:
vdc_id: 1 vdc_name: dc3-test interfaces:
Ethernet3/1 Ethernet3/2 Ethernet3/3
Ethernet3/4 Ethernet3/5 Ethernet3/6
Ethernet3/7 Ethernet3/8 Ethernet3/9
Ethernet3/10 Ethernet3/11 Ethernet3/12
Ethernet3/13 Ethernet3/14 Ethernet3/15
Ethernet3/16 Ethernet3/17 Ethernet3/18
Ethernet3/19 Ethernet3/20 Ethernet3/21
Ethernet3/22 Ethernet3/23 Ethernet3/24
Ethernet3/25 Ethernet3/26 Ethernet3/27
Ethernet3/28 Ethernet3/29 Ethernet3/30
Ethernet3/31 Ethernet3/32 Ethernet3/33
Ethernet3/34 Ethernet3/35 Ethernet3/36
Ethernet3/37 Ethernet3/38 Ethernet3/39
Ethernet3/40 Ethernet3/41 Ethernet3/42
Ethernet3/43 Ethernet3/44 Ethernet3/45
Ethernet3/46 Ethernet3/47 Ethernet3/48
vdc_id: 2 vdc_name: dc3-aaa interfaces:
vdc_id: 3 vdc_name: dc3-rbac interfaces:
vdc_id: 4 vdc_name: dc3-call interfaces:
end attachment
start attachment
name:show vdc current-vdc
type:text
data:
Current vdc is 1 - dc3-test
end attachment
start attachment
name:show license usage
type:text
data:
Feature Ins Lic Status Expiry Date Comments
Count
--------------------------------------------------------------------------------
LAN_ADVANCED_SERVICES_PKG Yes - In use Never -
LAN_ENTERPRISE_SERVICES_PKG Yes - Unused Never -
--------------------------------------------------------------------------------
end attachment
```

XML 形式での syslog アラート通知の例

次の例では、Syslog ポート アラート グループ通知の XML を示します。

```
<?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:TXX12345678:478F82E6</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>2008-01-17 16:31:33 GMT+0000</aml-block:CreationDate>
<aml-block:Builder>
<aml-block:Name>DC3</aml-block:Name>
<aml-block:Version>4.1</aml-block:Version>
</aml-block:Builder>
<aml-block:BlockGroup>
```

```
<aml-block:GroupId>1005:TXX12345678:478F82E6</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>5</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>2008-01-17 16:31:33 GMT+0000</ch:EventTime> <ch:MessageDescription>SYSLOG_ALERT
 2008 Jan 17 16:31:33
dc3-test %ETHPORT-2-IF_SEQ_ERROR: Error (0x20) while communicating with component MTS_SAP_ELTM
opcode:MTS_OPC_ETHPM_PORT_PHY_CLEANUP
(for:RID_PORT: Ethernet3/1) </ch:MessageDescription> <ch:Event> <ch:Type>syslog</ch:Type>
<ch:SubType></ch:SubType>
<ch:Brand>Cisco</ch:Brand> <ch:Series>Nexus7000</ch:Series> </ch:Event> <ch:CustomerData>
<ch:UserData>
<ch:Email>contact@example.com</ch:Email>
</ch:UserData>
<ch:ContractData>
<ch:DeviceId>N7K-C7010@C@TXX12345678</ch:DeviceId>
</ch:ContractData>
<ch:SystemInfo>
<ch:Name>dc3-test</ch:Name>
<ch:Contact>Jay Tester</ch:Contact> <ch:ContactEmail>contact@example.com</ch:ContactEmail>
<ch:ContactPhoneNumber>+91-80-1234-5678</ch:ContactPhoneNumber>
<ch:StreetAddress>#1, Any Street</ch:StreetAddress> </ch:SystemInfo> </ch:CustomerData>
<ch:Device>
<rme:Chassis xmlns:rme="http://www.cisco.com/rme/4.1">
<rme:Model>N7K-C7010</rme:Model>
<rme:HardwareVersion>0.405</rme:HardwareVersion>
<rme:SerialNumber>TXX12345678</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">
2008 Jan 17 10:57:51 dc3-test %SYSLOG-1-SYSTEM_MSG : Logging logfile (messages) cleared by
 user
2008 Jan 17 10:57:53 dc3-test %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configuring console from
/dev/ttyS0 /dev/ttyS0_console
2008 Jan 17 10:58:35 dc3-test %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configuring console from
/dev/ttyS0 /dev/ttyS0_console
2008 Jan 17 10:59:00 dc3-test %DAEMON-3-SYSTEM_MSG: error: setsockopt IP_TOS 16: Invalid
argument: - sshd[14484]
2008 Jan 17 10:59:05 dc3-test %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configuring console from
/dev/ttyS0 /dev/ttyS0_console
2008 Jan 17 12:11:18 dc3-test %SYSMGR-STANDBY-5-SUBPROC_TERMINATED: \"System Manager (gsync
 controller)\"
(PID 12000) has finished with error code SYSMGR_EXITCODE_GSYNCFAILED_NONFATAL (12).
2008 Jan 17 16:28:03 dc3-test %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configuring console from
/dev/ttyS0 /dev/ttyS0_console
2008 Jan 17 16:28:44 dc3-test %SYSMGR-3-BASIC_TRACE: core_copy: PID 2579 with message Core
 not generated by system
for eltm(0). WCOREDUMP(9) returned zero .
2008 Jan 17 16:28:44 dc3-test %SYSMGR-2-SERVICE_CRASHED: Service \"eltm\" (PID 3504)
hasn&apos;t caught signal 9
(no core).
2008 Jan 17 16:29:08 dc3-test %SYSMGR-3-BASIC_TRACE: core_copy: PID 2579 with message Core
 not generated by system
for eltm(0). WCOREDUMP(9) returned zero .
2008 Jan 17 16:29:08 dc3-test %SYSMGR-2-SERVICE_CRASHED: Service \"eltm\" (PID 23210)
hasn&apos;t caught signal 9
(no core).
2008 Jan 17 16:29:17 dc3-test %SYSMGR-3-BASIC_TRACE: core_copy: PID 2579 with message Core
 not generated by system
for eltm(0). WCOREDUMP(9) returned zero .
2008 Jan 17 16:29:17 dc3-test %SYSMGR-2-SERVICE_CRASHED: Service \"eltm\" (PID 23294)
hasn&apos;t caught signal 9
```

```
(no core).
2008 Jan 17 16:29:25 dc3-test %SYSMGR-2-HASWITCHOVER_PRE_START: This supervisor is becoming
 active (pre-start phase).
2008 Jan 17 16:29:25 dc3-test %SYSMGR-2-HASWITCHOVER_START: This supervisor is becoming
active.
2008 Jan 17 16:29:26 dc3-test %USER-3-SYSTEM_MSG: crdcfg_get_srvinfo: mts_send failed -
device_test
2008 Jan 17 16:29:27 dc3-test %NETSTACK-3-IP_UNK_MSG_MAJOR: netstack [4336] Unrecognized
message from MRIB.
Major type 1807
2008 Jan 17 16:29:27 dc3-test %IM-5-IM_INTF_STATE: mgmt0 is DOWN in vdc 1
2008 Jan 17 16:29:27 dc3-test %IM-5-IM_INTF_STATE: mgmt0 is DOWN in vdc 2
2008 Jan 17 16:29:27 dc3-test %IM-5-IM_INTF_STATE: mgmt0 is DOWN in vdc 3
2008 Jan 17 16:29:27 dc3-test %IM-5-IM_INTF_STATE: mgmt0 is DOWN in vdc 4
2008 Jan 17 16:29:28 dc3-test %SYSMGR-2-SWITCHOVER_OVER: Switchover completed.
2008 Jan 17 16:29:28 dc3-test %DAEMON-3-SYSTEM_MSG: ntp:socket family : 2 - ntpd[19045]
2008 Jan 17 16:29:28 dc3-test %DAEMON-3-SYSTEM_MSG: ntp:socket family : 10 - ntpd[19045]
2008 Jan 17 16:29:28 dc3-test %DAEMON-3-SYSTEM_MSG: ntp:ipv6 only defined - ntpd[19045]
2008 Jan 17 16:29:28 dc3-test %DAEMON-3-SYSTEM_MSG: ntp:bindv6 only defined - ntpd[19045]
2008 Jan 17 16:29:28 dc3-test %DAEMON-3-SYSTEM_MSG: ntp:socket family : 2 - ntpd[19045]
2008 Jan 17 16:29:28 dc3-test %DAEMON-3-SYSTEM_MSG: ntp:socket family : 0 - ntpd[19045]
2008 Jan 17 16:29:28 dc3-test %DAEMON-3-SYSTEM_MSG: ntp:socket family : 0 - ntpd[19045]
2008 Jan 17 16:29:28 dc3-test %NETSTACK-3-CLIENT_GET: netstack [4336] HA client filter
recovery failed (0)
2008 Jan 17 16:29:28 dc3-test %NETSTACK-3-CLIENT_GET: netstack [4336] HA client filter
recovery failed (0)
2008 Jan 17 16:29:29 dc3-test %DAEMON-3-SYSTEM_MSG: ssh disabled, removing -
dcos-xinetd[19072]
2008 Jan 17 16:29:29 dc3-test %DAEMON-3-SYSTEM_MSG: Telnet disabled, removing -
dcos-xinetd[19072]
2008 Jan 17 16:29:31 dc3-test %DAEMON-3-SYSTEM_MSG: Telnet disabled, removing -
dcos-xinetd[19073]
2008 Jan 17 16:29:32 dc3-test %DAEMON-3-SYSTEM_MSG: ssh disabled, removing -
dcos-xinetd[19079]
2008 Jan 17 16:29:32 dc3-test %DAEMON-3-SYSTEM_MSG: Telnet disabled, removing -
dcos-xinetd[19079]
2008 Jan 17 16:29:34 dc3-test %IM-5-IM_INTF_STATE: mgmt0 is UP in vdc 1
2008 Jan 17 16:29:34 dc3-test %IM-5-IM_INTF_STATE: mgmt0 is UP in vdc 2
2008 Jan 17 16:29:34 dc3-test %IM-5-IM_INTF_STATE: mgmt0 is UP in vdc 3
2008 Jan 17 16:29:34 dc3-test %IM-5-IM_INTF_STATE: mgmt0 is UP in vdc 4
2008 Jan 17 16:29:34 dc3-test %DAEMON-3-SYSTEM_MSG: ssh disabled, removing -
dcos-xinetd[19105]
2008 Jan 17 16:29:34 dc3-test %DAEMON-3-SYSTEM_MSG: Telnet disabled, removing -
dcos-xinetd[19105]
2008 Jan 17 16:29:35 dc3-test %PLATFORM-2-PS_AC_IN_MISSING: Power supply 2 present but all
 AC inputs are not
connected, ac-redundancy might be affected
2008 Jan 17 16:29:35 dc3-test %PLATFORM-2-PS_AC_IN_MISSING: Power supply 3 present but all
 AC inputs are not
connected, ac-redundancy might be affected
2008 Jan 17 16:29:38 dc3-test %CALLHOME-2-EVENT: SUP_FAILURE
2008 Jan 17 16:29:46 dc3-test vsh[19166]: CLIC-3-FAILED_EXEC: Can not exec command
&lt;more&gt; return code &lt;14&gt;
2008 Jan 17 16:30:24 dc3-test vsh[23810]: CLIC-3-FAILED_EXEC: Can not exec command
&lt;more&gt; return code &lt;14&gt;
2008 Jan 17 16:30:24 dc3-test vsh[23803]: CLIC-3-FAILED_EXEC: Can not exec command
&lt;more&gt; return code &lt;14&gt;
2008 Jan 17 16:30:24 dc3-test vsh[23818]: CLIC-3-FAILED_EXEC: Can not exec command
&lt;more&gt; return code &lt;14&gt;
2008 Jan 17 16:30:47 dc3-test %SYSMGR-3-BASIC_TRACE: core_copy: PID 2630 with message Core
 not generated by system
for eltm(0). WCOREDUMP(9) returned zero .
2008 Jan 17 16:30:47 dc3-test %SYSMGR-2-SERVICE_CRASHED: Service \"eltm\" (PID 4820)
hasn&apos;t caught signal 9
(no core).
2008 Jan 17 16:31:02 dc3-test %SYSMGR-3-BASIC_TRACE: core_copy: PID 2630 with message Core
 not generated by system
for eltm(0). WCOREDUMP(9) returned zero .
2008 Jan 17 16:31:02 dc3-test %SYSMGR-2-SERVICE_CRASHED: Service \"eltm\" (PID 24239)
hasn&apos;t caught signal 9
(no core).
2008 Jan 17 16:31:14 dc3-test %SYSMGR-3-BASIC_TRACE: core_copy: PID 2630 with message Core
 not generated by system
```

```
for eltm(0). WCOREDUMP(9) returned zero .
2008 Jan 17 16:31:14 dc3-test %SYSMGR-2-SERVICE_CRASHED: Service \"eltm\" (PID 24401)
hasn&apos;t caught signal 9
(no core).
2008 Jan 17 16:31:23 dc3-test %CALLHOME-2-EVENT: SW_CRASH alert for service: eltm
2008 Jan 17 16:31:23 dc3-test %SYSMGR-3-BASIC_TRACE: core_copy: PID 2630 with message Core
 not generated by system
for eltm(0). WCOREDUMP(9) returned zero .
2008 Jan 17 16:31:23 dc3-test %SYSMGR-2-SERVICE_CRASHED: Service \"eltm\" (PID 24407)
hasn&apos;t caught signal 9
(no core).
2008 Jan 17 16:31:24 dc3-test vsh[24532]: CLIC-3-FAILED_EXEC: Can not exec command
&lt;more&gt; return code &lt;14&gt;
2008 Jan 17 16:31:24 dc3-test vsh[24548]: CLIC-3-FAILED_EXEC: Can not exec command
&lt;more&gt; return code &lt;14&gt;
2008 Jan 17 16:31:24 dc3-test vsh[24535]: CLIC-3-FAILED_EXEC: Can not exec command
&lt;more&gt; return code &lt;14&gt;
2008 Jan 17 16:31:33 dc3-test %NETSTACK-3-INTERNAL_ERROR: netstack [4336] (null)
2008 Jan 17 16:31:33 dc3-test %ETHPORT-2-IF_SEQ_ERROR: Error (0x20) while communicating
with component
MTS_SAP_ELTM opcode:MTS_OPC_ETHPM_PORT_PHY_CLEANUP (for:RID_PORT: Ethernet3/1)
</aml-block:Data>
</aml-block:Attachment> <aml-block:Attachment type="inline"> <aml-block:Name>show vdc
membership</aml-block:Name>
<aml-block:Data encoding="plain">
vdc_id: 1 vdc_name: dc3-test interfaces:
Ethernet3/1 Ethernet3/2 Ethernet3/3
Ethernet3/4 Ethernet3/5 Ethernet3/6
Ethernet3/7 Ethernet3/8 Ethernet3/9
Ethernet3/10 Ethernet3/11 Ethernet3/12
Ethernet3/13 Ethernet3/14 Ethernet3/15
Ethernet3/16 Ethernet3/17 Ethernet3/18
Ethernet3/19 Ethernet3/20 Ethernet3/21
Ethernet3/22 Ethernet3/23 Ethernet3/24
Ethernet3/25 Ethernet3/26 Ethernet3/27
Ethernet3/28 Ethernet3/29 Ethernet3/30
Ethernet3/31 Ethernet3/32 Ethernet3/33
Ethernet3/34 Ethernet3/35 Ethernet3/36
Ethernet3/37 Ethernet3/38 Ethernet3/39
Ethernet3/40 Ethernet3/41 Ethernet3/42
Ethernet3/43 Ethernet3/44 Ethernet3/45
Ethernet3/46 Ethernet3/47 Ethernet3/48
vdc_id: 2 vdc_name: dc3-aaa interfaces:
vdc_id: 3 vdc_name: dc3-rbac interfaces:
vdc_id: 4 vdc_name: dc3-call interfaces:


</aml-block:Data>
</aml-block:Attachment>
<aml-block:Attachment type="inline">
<aml-block:Name>show vdc current-vdc</aml-block:Name> <aml-block:Data encoding="plain">
Current vdc
is 1 - dc3-test  </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">
Feature Ins Lic Status Expiry Date Comments
Count
--------------------------------------------------------------------------------
LAN_ADVANCED_SERVICES_PKG Yes - In use Never -
LAN_ENTERPRISE_SERVICES_PKG Yes - Unused Never -
--------------------------------------------------------------------------------

</aml-block:Data>
</aml-block:Attachment>
</aml-block:Attachments>
</aml-block:Block>
</soap-env:Body>
</soap-env:Envelope>
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Smart Call CLI コマンド	『*Cisco Nexus 7000 Series NX-OS System Management Command Reference*』
VDC および VRF	『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』

MIB

MIB	MIB のリンク
Smart Call Home に関連する MIB	サポートされている 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。 ftp://ftp.cisco.com/pub/mibs/supportlists/nexus7000/Nexus7000MIBSupportList.html

Smart Call Home の機能の履歴

次の表に、このマニュアルの新機能および変更された機能を要約し、各機能がサポートされているリリースを示します。ご使用のソフトウェア リリースで、本書で説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。

表 *16* : ***Smart Call Home*** の機能の履歴

機能名	リリース	機能情報
HTTP プロキシ サーバ	5.2(1)	HTTP プロキシ サーバを経由して HTTP メッセージを送信する機能が追加されました。
SMTP サーバ コンフィギュレーション	5.0(2)	複数の SMTP サーバを設定する機能が追加されました。

Smart Call Home メッセージの HTTP 転送に対する VRF サポート	5.0(2)	VRF を使用して、HTTP 経由で電子メールおよび他の Smart Call Home メッセージを送信できます。
クラッシュ通知	4.0(1)	オンラインカードでのプロセスクラッシュに対してメッセージが送信されます。
宛先プロファイルのコンフィギュレーション	4.1(3)	コマンド **destination-profile http** と **destination-profile transport-method** は配信できません。

第 9 章

ロールバックの設定

この章では、Cisco NX-OS デバイスでロールバックを設定する方法について説明します。

この章の内容は、次のとおりです。

- 機能情報の確認，169 ページ
- ロールバックについて，170 ページ
- ロールバックのライセンス要件，172 ページ
- ロールバックの前提条件，172 ページ
- ロールバックの注意事項と制約事項，172 ページ
- ロールバックのデフォルト設定，174 ページ
- ロールバックの設定，174 ページ
- ロールバック コンフィギュレーションの確認，176 ページ
- ロールバックのコンフィギュレーション例，177 ページ
- その他の参考資料，177 ページ
- ロールバックの機能の履歴，177 ページ

機能情報の確認

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

ロールバックについて

ロールバックを使用すると、Cisco NX-OS コンフィギュレーションのスナップショットまたはユーザ チェックポイントを使用して、デバイスをリロードしなくても、いつでもそのコンフィギュレーションをデバイスに再適用できます。権限のある管理者であれば、チェックポイントで設定されている機能について専門的な知識がなくても、ロールバック機能を使用して、そのチェックポイント コンフィギュレーションを適用できます。

Cisco NX-OS は、システムのチェックポイントを自動的に作成します。ユーザまたはシステムのチェックポイントのいずれかを使用して、ロールバックを実行できます。

いつでも、現在の実行コンフィギュレーションのチェックポイント コピーを作成できます。Cisco NX-OS はこのチェックポイントを ASCII ファイルとして保存するので、将来、そのファイルを使用して、実行コンフィギュレーションをチェックポイント コンフィギュレーションにロールバックできます。複数のチェックポイントを作成すると、実行コンフィギュレーションのさまざまなバージョンを保存できます。

実行コンフィギュレーションをロールバックするとき、次のロールバック タイプを発生させることができます。

- atomic：エラーが発生しなかった場合に限り、ロールバックを実装します。
- best-effort：ロールバックを実装し、エラーがあってもスキップします。
- stop-at-first-failure：エラーが発生した場合は中止されるロールバックを実装します。

デフォルトのロールバック タイプは atomic です。

チェックポイント コンフィギュレーションにロールバック可能になった時点で、現在の実行コンフィギュレーションに適用される変更を確認してから、ロールバック操作にコミットできます。ロールバック操作時にエラーが発生した場合は、操作を取り消すか、またはエラーを無視してロールバック操作を続行するかを選択できます。操作を取り消した場合、Cisco NX-OS はエラーが発生する前に適用した変更のリストを提示します。これらの変更は手動で処理する必要があります。

自動的に生成されるシステム チェックポイント

Cisco NX-OS ソフトウェアは、コンフィギュレーション情報が消失しないよう、システム チェックポイントを自動的に生成します。システム チェックポイントは次のイベントによって生成されます。

- **no feature** コマンドで、イネーブルになっている機能をディセーブルにする
- **no router bgp** コマンドや **no ip pim sparse-mode** コマンドで、レイヤ 3 プロトコルのインスタンスを削除する
- 機能のライセンスの有効期限が切れる

これらのイベントのいずれかによってシステム コンフィギュレーションの変更が生じると、この機能ソフトウェアによって、システム チェックポイントが作成されます。これを使用すると、以

前のシステム コンフィギュレーションへロールバックできます。システムで生成されたチェックポイント ファイルの名前は「system-」で始まり、機能名が含まれています。たとえば、EIGRP 機能を最初にディセーブルにすると、システムは、system-fm-__inst_1__eigrp という名前のチェックポイントを作成します。

ハイ アベイラビリティ

checkpoint または checkpoint checkpoint_name コマンドを使用してチェックポイントが作成されるときは必ず、チェックポイントはスタンバイ ユニットと同期されます。

ロールバックではチェックポイント操作の状況を記憶しています。このためチェックポイント操作が中断された場合、およびシステムが不整合の状態になった場合には、ロールバック操作を続行する前に、ロールバックでチェックポイント操作（スタンバイ ユニットへのチェックポイントの同期化）を完了できます。

チェックポイント ファイルは、プロセスのリスタート後またはスーパーバイザのスイッチオーバー後も引き続き使用できます。プロセスの再起動中またはスーパーバイザのスイッチオーバー中に中断された場合でも、操作を続行する前にチェックポイントが正常に完了します。スーパーバイザのスイッチオーバーでは、チェックポイントは新しいアクティブ ユニットで完了します。

ロールバック操作中にプロセスの再起動またはスーパーバイザのスイッチオーバーが生じた場合は、再起動またはスイッチオーバーが完了した後で、ロールバックが以前の状態から再開し、正常に終了します。

仮想化のサポート

Cisco NX-OS は、ユーザがログインした仮想デバイス コンテキスト（VDC）で、実行コンフィギュレーションのチェックポイントを作成します。VDC ごとにさまざまなチェックポイント コピーを作成できます。ある VDC のチェックポイントを別の VDC に適用することはできません。デフォルトでは、Cisco NX-OS はデフォルト VDC に配置します。『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』を参照してください。

VDC の設定は、VDC の作成、VDC の削除、VDC の停止、VDC のリロード、VDC の名前変更、VDC のインターフェイス割り当て、共有インターフェイス割り当て、FCoE VLAN 割り当て、リソースの割り当て、およびリソース テンプレートをはじめとした操作（ただし、これらに限定されません）に対してチェックポイントをサポートしません。チェックポイントは特定の VDC から作成する必要があります。

ロールバックのライセンス要件

製品	ライセンス要件
Cisco NX-OS	ロールバック機能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nx-osイメージにバンドルされており、無料で提供されます。NX-OSライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

ロールバックの前提条件

ロールバックを設定するには、network-admin のユーザ権限が必要です。

VDC を設定する場合は、適切なライセンスをインストールしてから、設定する VDC にアクセスします。設定情報については『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』、ライセンス情報については『*Cisco NX-OS Licensing Guide*』を参照してください。

ロールバックの注意事項と制約事項

ロールバック設定時の注意事項と制限事項は次のとおりです。

- 作成できるチェックポイント コピーの最大数は 10 です。
- チェックポイント ファイル名の長さは、最大 80 文字です。
- チェックポイントコンフィギュレーションと比較した場合に、実行コンフィギュレーションのグローバル コンフィギュレーション部分に変更がある場合、非デフォルト VDC のチェックポイント コンフィギュレーションは適用できません。
- チェックポイント ファイル名の長さは、最大 80 文字です。
- チェックポイントのファイル名の先頭を *system* にすることはできません。
- Cisco NX-OS Release 4.2(1) 以降は、チェックポイントのファイル名の先頭を *auto* にできます。
- Cisco NX-OS Release 4.2(1) 以降は、チェックポイントのファイル名を *summary*、または *summary* の何らかの省略形にすることもできます。
- チェックポイント、ロールバック、または実行コンフィギュレーションからスタートアップ コンフィギュレーションへのコピーを同時に実行できるのは、1 ユーザだけです。
- システムで **write erase** または **reload** コマンドを実行すると、チェックポイントが削除されます。**clear checkpoint database** コマンドを使用すると、すべてのチェックポイント ファイルを削除できます。

- ロールバック中、ハードウェアでプログラムされているレコードを変更しようとすると、NetFlow のロールバックは失敗します。
- 異なるソフトウェアバージョン間でのチェックポイントのロールバックはサポートされていませんが、ユーザは自己判断でロールバックを実行し、best-effort モードでエラーから回復できます。
- ブートフラッシュでチェックポイントを作成した場合、ロールバックの実行前は実行システム コンフィギュレーションとの違いは実行できず、「変更なし」と報告されます。
- チェックポイントは、VDC に対してローカルなものになります。
- **checkpoint** および **checkpoint***checkpoint_name* コマンドを使用して作成されるチェック ポイントは、スイッチオーバーの直後に出現します。
- デフォルトの VDC で作成されたチェックポイントは、リロードの前に **write-erase** コマンドを発行しない限り、リロードに対して存在します。
- **copy running-config startup-config** コマンドが、適用可能な VDC およびデフォルト VDC で発行された場合に限り、デフォルト以外の VDC で作成されたチェックポイントはリロードに対して存在します。
- **checkpoint***checkpoint_name* コマンドを使用して作成されたファイルで、その他の ASCII タイプのファイルではない場合に限り、ブートフラッシュ時のファイルへのロールバックがサポートされます。
- チェックポイントの名前は一意にする必要があります。以前に保存したチェックポイントを同じ名前で上書きすることはできません。
- ストレージ VDC ではロールバックはサポートされていません。
- ロールバックは、管理仮想デバイス コンテキスト（VDC）機能ではサポートされません。
- チェックポイントに対して **rollback** コマンドを実行する前に、**terminal dont-ask** コマンドを設定してください。ロールバック パッチでは、ロールバック プロセスはユーザ インタラクションで停止せず、インタラクティブ コマンドのデフォルト値が使用されます。**rollback** コマンドを実行する前に **terminal dont-ask** コマンドを設定すると、この問題を解決できます。
- ロールバックは自動設定のコンテキストではサポートされません。チェックポイントは自動設定を保存しません。したがって、ロールバックを実行した後、対応する自動設定は存在しないことになります。
- ロールバックを実行する際に、そのモジュールの設定コマンドとともに対応するモジュールに対する **reload** コマンドがパッチに含まれていると、ロールバックは失敗します。これは、ロールバック アクションが、モジュールがオンラインになるのを待たず、リロード プロセスが進行中であっても、モジュール上で設定コマンドの実行を開始するためです。この問題を解決するには、モジュールがオンラインになった後に、手動で設定コマンドを実行します。

  例：

  - ロールバックは、**bfd hw-offload-module** コマンドまたはこのコマンドの **no** 形式を実行すると失敗します。この場合の失敗は、BFD セッションの一部であるスイッチインター

フェイスに電源が投入されると、ロールバックはこれらのコマンドを実行できないためです。この問題を解決するには、**bfd hw-offload-module** コマンドまたはこのコマンドの **no** 形式を実行する前に、**shutdown** コマンドを使用して、BFD セッションの一部であるインターフェイスをすべてシャットダウンします。

- ロールバック vPC がインターフェイスに適用される際に FEX が設定されている場合、FEX が一時的にオフラインになります。これが起こると、ロールバックは、FEX がオンラインになるのを待たずにインターフェイスに対して設定コマンドを実行し、その結果、対応する FEX がまだプロビジョニングされていないため、失敗します。この問題を解決するには、FEX がオンラインになった後に、手動で FEX 関連の設定コマンドを実行します。

ロールバックのデフォルト設定

次の表に、ロールバック パラメータのデフォルト設定を示します。

パラメータ	デフォルト
ロールバック タイプ	アトミック

ロールバックの設定

（注） Cisco NX-OS コマンドは Cisco IOS コマンドと異なる場合があるので注意してください。

チェックポイントの作成

設定には、最大 10 個のチェック ポイントを作成できます。

手順

	コマンドまたはアクション	目的
ステップ 1	[**no**] **checkpoint** {[*cp-name*] [**description** *descr*] | **file***file-name*} **例**： `switch# checkpoint stable`	ユーザ チェックポイント名またはファイルのいずれかに対して、実行中のコンフィギュレーションのチェックポイントを作成します。チェックポイント名には最大 80 文字の任意の英数字を使用できますが、スペースを含めることはできません。チェックポイント名を指定しなかった場合、Cisco NX-OS はチェックポイント名を user-checkpoint-*number* に設定します。ここで *number* は 1 ～ 10 の値です。

	コマンドまたはアクション	目的
		description には、スペースも含めて最大 80 文字の英数字を指定できます。 **checkpoint** コマンドの **no** 形式を使用すると、チェックポイント名を削除できます。**delete** コマンドを使用して、チェックポイント ファイルを削除できます。
ステップ 2	**show checkpoint** *cp-name* [**all**] 例： `switch# show checkpoint stable`	（任意） チェックポイント名の内容を表示します。

ロールバックの実装

チェックポイント名またはファイルにロールバックを実装できます。ロールバックを実装する前に、現在のコンフィギュレーションまたは保存されているコンフィギュレーションを参照しているソースと宛先のチェックポイント間の差異を表示できます。

（注） atomic ロールバック中に設定を変更すると、ロールバックは失敗します。

手順

	コマンドまたはアクション	目的
ステップ 1	**show diff rollback-patch** {**checkpoint** *src-cp-name* | **running-config** | **startup-config** | **file** *source-file*} {**checkpoint** *dest-cp-name* | **running-config** | **startup-config** | **file** *dest-file*} 例： `switch# show diff rollback-patch checkpoint stable running-config`	ソースと宛先のチェックポイント間の差異を表示します。
ステップ 2	**rollback running-config** {**checkpoint** *cp-name* | **file** *cp-file*} [**atomic** | **best-effort** | **stop-at-first-failure**] 例： `switch# rollback running-config checkpoint stable`	指定されたチェックポイント名またはファイルへのロールバックを作成します。次のロールバック タイプを実装できます。 • atomic：エラーが発生しなかった場合に限り、ロールバックを実装します。

	コマンドまたはアクション	目的
		• best-effort：ロールバックを実装し、エラーがあってもスキップします。 • stop-at-first-failure：エラーが発生した場合は中止されるロールバックを実装します。 デフォルトは atomic です。 次に、ユーザ チェックポイント名に対するロールバックを実装する例を示します。

ロールバック コンフィギュレーションの確認

ロールバックの設定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 checkpoint*name* [**all**]	チェックポイント名の内容を表示します。
show checkpoint all [**user** | **system**]	すべてのチェック ポイントの内容を表示します。表示されるチェックポイントを、ユーザまたはシステムで生成されるチェックポイントに限定できます。
show checkpoint summary [**user** | **system**]	すべてのチェック ポイントの一覧を表示します。表示されるチェックポイントを、ユーザまたはシステムで生成されるチェックポイントに限定できます。
show diff rollback-patch {**checkpoint***src-cp-name* | **running-config** | **startup-config** | **file***source-file*} {**checkpoint***dest-cp-name* | **running-config** | **startup-config** | **file***dest-file*}	ソースと宛先のチェックポイント間の差異を表示します。
show rollback log [**exec** | **verify**]	ロールバック ログの内容を表示します。

すべてのチェックポイント ファイルを削除するには、**clear checkpoint database** コマンドを使用します。

（注） **checkpoint** が作成されたら、**show run all** コマンドを使用して、デフォルト設定 **priority-flow-control mode auto** を表示できます。インターフェイスに対して **show run** コマンドを使用して設定 **priority-flow-control mode auto** を表示することはできません。

ロールバックのコンフィギュレーション例

次に、チェックポイントファイルを作成して、ユーザチェックポイント名に対する best-effort ロールバックを実装する例を示します。

```
checkpoint stable
rollback running-config checkpoint stable best-effort
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
ロールバック CLI コマンド	『*Cisco Nexus 7000 Series NX-OS System Management Command Reference*』
VDC	『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』
コンフィギュレーション ファイル	『*Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide*』

ロールバックの機能の履歴

次の表に、このマニュアルの新機能および変更された機能を要約し、各機能がサポートされているリリースを示します。ご使用のソフトウェア リリースで、本書で説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。

表 *17*：ロールバックの機能の履歴

機能名	リリース	機能情報
ハイ アベイラビリティ	4.2(1)	チェックポイントおよびロールバック動作でハイ アベイラビリティをサポートしました。

注意事項と制約事項	4.2(1)	チェックポイントファイルの命名規則が変更されました。
システム チェックポイントの自動生成	4.2(1)	機能をディセーブルにしたり、ライセンスを失効したりしてコンフィギュレーション情報を損失する可能性がある場合に、ソフトウェアがシステム チェックポイントを自動的に生成します。
注意事項と制約事項	4.1(3)	ロールバック中、ハードウェアでプログラムされているレコードを変更しようとすると、NetFlow のロールバックは失敗します。 異なるソフトウェア バージョン間でのチェックポイントのロールバックはサポートされていません。

第 10 章

Session Manager の設定

この章では、Cisco NX-OS デバイスで Session Manager を設定する方法について説明します。

この章の内容は、次のとおりです。

- 機能情報の確認，179 ページ
- Session Manager について，180 ページ
- Session Manager のライセンス要件，180 ページ
- Session Manager の前提条件，181 ページ
- Session Manager の注意事項および制約事項，181 ページ
- Session Manager の設定，181 ページ
- Session Manager 設定の確認，184 ページ
- Session Manager のコンフィギュレーション例，185 ページ
- その他の参考資料，185 ページ
- Session Manager の機能の履歴，185 ページ

機能情報の確認

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

Session Manager について

Session Manager を使用すると、設定変更をバッチ モードで実行できます。Session Manager は次のフェーズで機能します。

- コンフィギュレーションセッション：Session Managerモードで実行するコマンドのリストを作成します。
- 検証：設定の基本的なセマンティック チェックを行います。Cisco NX-OS は、設定の一部でセマンティクス検査が失敗した場合にエラーを返します。
- 検証：既存のハードウェア設定、ソフトウェア設定、およびリソースに基づいて、設定全体を確認します。Cisco NX-OS は、設定がこの確認フェーズで合格しなかった場合にエラーを返します。
- コミット：Cisco NX-OS はコンフィギュレーション全体を確認して、デバイスに対する変更を実行します。障害が発生した場合、Cisco NX-OS は元の設定に戻ります。
- 打ち切り：設定変更を実行しないで廃棄します。

任意で、変更をコミットしないでコンフィギュレーション セッションを終了できます。また、コンフィギュレーション セッションを保存することもできます。

ハイ アベイラビリティ

Session Manager セッションは、スーパーバイザのスイッチオーバー後も引き続き使用できます。セッションはソフトウェア リロード後までは維持されません。

仮想化のサポート

デフォルトでは、Cisco NX-OS はデフォルト VDC に配置します。『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』を参照してください。

Session Manager のライセンス要件

製品	ライセンス要件
Cisco NX-OS	Session Manager 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nx-osイメージにバンドルされており、無料で提供されます。NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

Session Manager の前提条件

使用する予定の Session Manager コマンドをサポートする権限があることを確認してください。

VDC を設定する場合は、適切なライセンスをインストールしてから、設定する VDC にアクセスします。設定情報については『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』、ライセンス情報については『*Cisco NX-OS Licensing Guide*』を参照してください。

Session Manager の注意事項および制約事項

Session Manager には、次の注意事項および制限事項があります。

- Session Manager は、アクセス コントロール リスト（ACL）および Quality of Service（QoS）機能だけをサポートします。
- 作成できるコンフィギュレーション セッションの最大数は 32 です。
- アクティブ セッションの進行中にインサービス ソフトウェア アップグレード（ISSU）を実行することはできません。セッションをコミットして保存するか、または打ち切ってから ISSU を実行する必要があります。
- すべてのセッションで設定できるコマンドの最大数は 20,000 です。
- 複数のコンフィギュレーション セッションまたはコンフィギュレーション ターミナル モードで、コンフィギュレーション コマンドを同時に実行することはできません。パラレル コンフィギュレーション（1 つのコンフィギュレーション セッションと 1 つのコンフィギュレーション ターミナルのようなもの）は、コンフィギュレーション セッションで確認または検証が失敗する原因になることがあります。
- コンフィギュレーションセッションであるインターフェイスを設定中に、そのインターフェイスをリロードすると、そのときにインターフェイスがデバイス上になくても Session Manager コマンドを受け取ることができます。

Session Manager の設定

（注） Cisco NX-OS コマンドは Cisco IOS コマンドと異なる場合があるので注意してください。

セッションの作成

作成できるコンフィギュレーション セッションの最大数は 32 です。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure session***name*
	
	例：
	`switch# configure session myACLs`
	`switch(config-s)#`
		コンフィギュレーション セッションを作成し、セッション コンフィギュレーション モードを開始します。名前は任意の英数字ストリングです。
		セッションの内容を表示します。

ステップ 2	**show configuration session** [*name*] 例： `switch(config-s)# show configuration session myACLs`	（任意） セッションの内容を表示します。
ステップ 3	**save***location* 例： `switch(config-s)# save bootflash:sessions/myACLs`	（任意） セッションをファイルに保存します。保管場所には bootflash:、slot0:、または volatile: を指定できます。

セッションでの ACL の設定

コンフィギュレーション セッションで ACL を設定できます。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure session***name*
	
	例：
	`switch# configure session myacls`
	`switch(config-s)#`
		コンフィギュレーションセッションを作成し、セッション コンフィギュレーション モードを開始します。名前は任意の英数字ストリングです。

ステップ 2	**ip access-list***name*
	
	例：
	`switch(config-s)# ip access-list acl1`
	`switch(config-s-acl)#`
		ACL を作成し、その ACL のコンフィギュレーション モードを開始します。

ステップ 3	**permit***protocol source destination* 例： `switch(config-s-acl)# permit tcp any any`	（任意） ACL に許可文を追加します。

	コマンドまたはアクション	目的

ステップ 4	**interface***interface-type number*
	
	例：
	`switch(config-s-acl)# interface e 2/1`
	`switch(config-s-if)#`
		インターフェイス コンフィギュレーション モードを開始します。

ステップ 5	**ip access-group***name* {**in** | **out**}
	
	例：
	`switch(config-s-acl)# interface e 2/1`
	`switch(config-s-if)#`
		アクセス グループを適用するトラフィックの方向を指定します。

ステップ 6	**show configuration session** [*name*] 例： `switch(config-s)# show configuration session myacls`	（任意） セッションの内容を表示します。

セッションの確認

セッション モードで次のコマンドを使用して、セッションを確認します。

コマンド	目的
verify [**verbose**] 例： `switch(config-s)# verify`	既存のハードウェアおよびソフトウェアのコンフィギュレーションおよびリソースに基づいて、コンフィギュレーション全体を確認します。Cisco NX-OS は、設定がこの確認で合格しなかった場合にエラーを返します。

セッションのコミット

セッション モードで次のコマンドを使用して、セッションをコミットします。

コマンド	目的
commit [**verbose**] 例： `switch(config-s)# commit`	現在のセッションで行われたコンフィギュレーションの変更を検証し、有効な変更をデバイスに適用します。検証に失敗した場合、Cisco NX-OS は元の設定に戻ります。

セッションの保存

セッション モードで次のコマンドを使用して、セッションを保存します。

コマンド	目的
save*location* 例： `switch(config-s)# save bootflash:sessions/myACLs`	（任意）セッションをファイルに保存します。保管場所には bootflash:、slot0:、または volatile: を指定できます。

セッションの廃棄

セッション モードで次のコマンドを使用して、セッションを廃棄します。

コマンド	目的

abort
例：
`switch(config-s)# abort`
`switch#`
	コマンドを適用しないで、コンフィギュレーション セッションを廃棄します。

Session Manager 設定の確認

Session Manager 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 configuration session [*name*]	コンフィギュレーション ファイルの内容を表示します。
show configuration session status [*name*]	コンフィギュレーション セッションのステータスを表示します。
show configuration session summary	すべてのコンフィギュレーション セッションのサマリーを表示します。

Session Manager のコンフィギュレーション例

Session Manager を使用して ACL コンフィギュレーションを作成し、コミットする例を示します。

```
switch# configure session ACL_tcp_in
Config Session started, Session ID is 1
Enter configuration commands, one per line. End with CNTL/Z.
switch(config-s)# ip access-list ACL1
switch(config-s-acl)# permit tcp any any
switch(config)# interface e 7/1
switch(config-if)# ip access-group ACL1 in
switch(config-if)# exit
switch(config)# exit
switch# config session ACL_tcp_in
Config Session started, Session ID is 1
Enter configuration commands, one per line. End with CNTL/Z.
switch(config-s)# verify
Verification Successful
switch(config-s)# commit
Commit Successful
switch#
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Session Manager CLI コマンド	『*Cisco Nexus 7000 Series NX-OS System Management Command Reference*』
VDC	『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』
コンフィギュレーション ファイル	『*Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide*』

Session Manager の機能の履歴

次の表に、このマニュアルの新機能および変更された機能を要約し、各機能がサポートされているリリースを示します。ご使用のソフトウェア リリースで、本書で説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。

表 *18* : *Session Manager* の機能の履歴

機能名	リリース	機能情報
Session Manager	4.0(1)	この機能が導入されました。

第 11 章

スケジューラの設定

この章では、Cisco NX-OS デバイス上でスケジューラを設定する方法について説明します。

この章は、次の項で構成されています。

- 機能情報の確認，187 ページ
- スケジューラについて，188 ページ
- スケジューラのライセンス要件，189 ページ
- スケジューラの前提条件，189 ページ
- スケジューラの注意事項および制約事項，190 ページ
- スケジューラのデフォルト設定，190 ページ
- スケジューラの設定，190 ページ
- スケジューラの設定確認，196 ページ
- スケジューラの設定例，196 ページ
- 関連資料，198 ページ
- スケジューラの機能の履歴，198 ページ

機能情報の確認

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

スケジューラについて

スケジューラを使用すると、次のようなメンテナンス作業のタイムテーブルを定義し、設定することができます。

- Quality of Service（QoS）ポリシーの変更
- データのバックアップ
- 設定の保存

ジョブは、定期的な作業を定義する単一または複数のコマンドで構成されています。ジョブは、1 回だけ、または定期的な間隔でスケジューリングすることができます。

スケジューラでは、ジョブと、そのタイムテーブルを次のように定義できます。

- ジョブ：コマンドリストとして定義され、特定のスケジュールに従って実行される定期的なタスク。
- スケジュール：ジョブを実行するタイムテーブル1 つのスケジュールに複数のジョブを割り当てることができます。1 つのスケジュールは、定期的、または 1 回だけ実行するように定義されます。
  - 定期モード：ジョブを削除するまで、ジョブの実行が定期的な間隔で繰り返されます。次のタイプの定期的な間隔を設定できます。
    - Daily：ジョブは 1 日 1 回実行されます。
    - Weekly：ジョブは毎週 1 回実行されます。
    - Monthly：ジョブは毎月 1 回実行されます。
    - Delta：ジョブは、指定した時間に開始され、以後、指定した間隔（days:hours:minutes）で実行されます。
  - One-time mode：ジョブは、指定した時間に 1 回だけ実行されます。

リモート ユーザ認証

ジョブの開始前に、スケジューラはジョブを作成したユーザを認証します。リモート認証で得たユーザ クレデンシャルは短時間しか保有されないため、スケジューリングされたジョブをサポートできません。ジョブを作成するユーザの認証パスワードをローカルで設定する必要があります。これらのパスワードは、スケジューラのコンフィギュレーションに含まれ、ローカル設定のユーザとは見なされません。

ジョブを開始する前に、スケジューラはローカル パスワードとリモート認証サーバに保存されたパスワードを照合します。

ログ

スケジューラはジョブ出力を含むログファイルを管理します。ジョブ出力のサイズがログ ファイルのサイズより大きい場合、出力内容は切り捨てられます。

ハイ アベイラビリティ

スケジューリングされたジョブは、スーパバイザのスイッチオーバーまたはソフトウェアのリロード後も使用可能です。

仮想化のサポート

ジョブは、ログインした仮想デバイス コンテキスト（Virtual Device Context）で作成されます。デフォルトでは、Cisco NX-OS はデフォルト VDC に配置します。詳細については、『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』を参照してください。

スケジューラのライセンス要件

製品	ライセンス要件
Cisco NX-OS	スケジューラ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 nx-os イメージにバンドルされており、無料で提供されます。NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

スケジューラの前提条件

スケジューラの前提条件は次のとおりです。

- 条件付き機能をイネーブルにしてからでなければ、ジョブでそれらの機能を設定できません。
- ライセンスの必要な機能をジョブで設定するには、各機能の有効なライセンスをインストールしておく必要があります。
- スケジューリングされたジョブを設定するには、network-admin ユーザ特権が必要です。

スケジューラの注意事項および制約事項

スケジューラに関する設定時の注意事項および制約事項は、次のとおりです。

- ジョブの実行中に次のいずれかの状況が発生した場合、スケジューラは失敗する可能性があります。
  - 機能のライセンスが、その機能を使用するジョブがスケジューリングされている時間に失効している場合。
  - 機能が、その機能を使用するジョブがスケジューリングされている時間に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にもかかわらず、そのスロットを対象にしたジョブがスケジューリングされている場合。
- 時刻が設定されていることを確認します。スケジューラはデフォルトのタイムテーブルを適用しません。スケジュールを作成し、ジョブを割り当てても、時刻を設定しなければ、ジョブは開始しません。
- ジョブは開始されると非インタラクティブ方式で実行されるため、ジョブの定義中、インタラクティブなコマンドや中断を伴うコマンド（例：**copy bootflash:***file***ftp:***URI*、**write erase**、その他類似のコマンド）が指定されていないことを確認してください。

スケジューラのデフォルト設定

この表は、スケジューラのデフォルト設定を示します。

パラメータ	デフォルト
スケジューラの状態	ディセーブル
ログ ファイル サイズ	16 KB

スケジューラの設定

スケジューラのイネーブル化またはディセーブル化

ジョブを設定してスケジュールできるようにスケジューラ機能をイネーブルにすることができ、または、スケジューラをイネーブルにした後にスケジューラ機能をディセーブルにすることもできます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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	switch(config)# [**no**] **feature scheduler**	スケジューラをイネーブルまたはディセーブルにします。
ステップ 3	switch(config)# **show scheduler config**	（任意） スケジューラ設定を表示します。
ステップ 4	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。

スケジューラ ログ ファイル サイズの定義

ジョブ、スケジュール、およびジョブ出力をキャプチャするログ ファイルのサイズを設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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	switch(config)# **scheduler logfile size***value*	スケジューラ ログ ファイル サイズをキロバイト（KB）で定義します。範囲は 16 ～ 1024 です。デフォルトは 16 です。 （注） ジョブ出力のサイズがログ ファイルのサイズより大きい場合、出力内容は切り捨てられます。
ステップ 3	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。

リモート ユーザ認証の設定

ジョブの設定およびスケジューリングを行うユーザにリモート認証を使用するように、スケジューラを設定できます。

（注） リモート ユーザは、ジョブを作成および設定する前に、クリア テキスト パスワードを使用して認証する必要があります。

（注） **show running-config** コマンドの出力では、リモート ユーザ パスワードは常に暗号化された状態で表示されます。コマンドの暗号化オプション（**7**）は、ASCII デバイス設定をサポートします。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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	switch(config)# **scheduler aaa-authentication password** [**0** | **7**] *password*	現在ログインしているユーザ用のクリア 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 username***name***password** [**0** | **7**] *password*	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)# **show running-config** | **include "scheduler aaa-authentication"**	（任意） スケジューラのパスワード情報を表示します。
ステップ 5	switch(config)# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ジョブの定義

ジョブを定義して、ジョブ名とコマンド シーケンスを指定することができます。

注意 一旦ジョブを定義すると、コマンドの変更、削除はできません。ジョブを変更するには、そのジョブを削除して新しいジョブを作成する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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	switch(config)# **scheduler job name***string*	ジョブを作成し、ジョブ コンフィギュレーション モードを開始します。 backup-cfg という名前のスケジューラ ジョブを作成する例を示します。
ステップ 3	switch(config-job)# *command1* ;[*command2* ;*command3* ;...]	特定のジョブに対応するコマンド シーケンスを定義します。複数のコマンドは、スペースとセミコロン（「;」）で区切る必要があります。 実行コンフィギュレーションを bootflash 内のファイルに保存し、ファイルを bootflash から TFTP サーバにコピーするスケジューラ ジョブを作成する例を示します。ファイル名は現在のタイムスタンプとスイッチ名を使用して作成されます。
ステップ 4	switch(config-job)# **show scheduler job** [**name***name*]	（任意） ジョブ情報を表示します。
ステップ 5	switch(config)# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ジョブの削除

スケジューラからジョブを削除できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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。

	コマンドまたはアクション	目的
ステップ 2	switch(config)# **no scheduler job name***string*	特定のジョブおよびそこで定義されたすべてのコマンドを削除します。
ステップ 3	switch(config-job)# **show scheduler job** [**name***name*]	（任意） ジョブ情報を表示します。
ステップ 4	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。

タイムテーブルの定義

1 つまたは複数のジョブで使用するタイムテーブルをスケジューラで定義できます。

time コマンドで時刻を設定しない場合は、スケジューラは現在の時刻を使用します。たとえば、現在の時刻が 2013 年 3 月 24 日の 22 時 00 分である場合、ジョブは次のように開始されます。

- スケジューラは、**time start 23:00 repeat 4:00:00** コマンドの開始時刻が 2013 年 3 月 24 日 23 時 00 分であると見なします。
- スケジューラは、**time daily 55** コマンドの開始時刻が、毎日 22 時 55 分であると見なします。
- スケジューラは、**time weekly 23:00** コマンドの開始時刻が、毎週金曜日の 23 時 00 分であると見なします。
- スケジューラは、**time monthly 23:00** コマンドの開始時刻が、毎月 24 日の 23 時 00 分であると見なします。

（注） スケジューラは、1 つ前のジョブが完了しない限り、次のジョブを開始しません。たとえば、1 分間隔で実行するジョブを 22 時 00 分に開始するようジョブをスケジューリングしたが、ジョブを完了するには2分間必要である場合、ジョブは次のように実行されます。スケジューラは 22 時 00 分に最初のジョブを開始し、22 時 02 分に完了します。次に 1 分間待機し、22 時 03 分に次のジョブを開始します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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。

	コマンドまたはアクション	目的
ステップ 2	switch(config)# **scheduler schedule name***string*	スケジュールを作成し、スケジュール コンフィギュレーション モードを開始します。
ステップ 3	switch(config-schedule)# **job name***string*	このスケジュールにジョブを関連付けます。1 つのスケジュールに複数のジョブを追加できます。
ステップ 4	switch(config-schedule)# **time daily***time*	ジョブが毎日 HH:MM の形式で指定された時刻に開始することを意味します。
ステップ 5	switch(config-schedule)# **time weekly** [[*dow*:]*HH*:]*MM*	ジョブが週の指定された曜日に開始することを意味します。 曜日（dow）は次のいずれかの方法で指定されます。 • 曜日を表す整数。たとえば 1 = 日曜日、2 = 月曜日。 • 曜日の省略形。たとえば Sun = Sunday。 引数全体の最大長は 10 です。
ステップ 6	switch(config-schedule)# **time monthly** [[*dm*:]*HH*:]*MM*	ジョブが月の特定の日（dm）に開始することを意味します。29、30 または 31 のいずれかを指定した場合、そのジョブは各月の最終日に開始されます。
ステップ 7	switch(config-schedule)# **time start** {**now repeat***repeat-interval* | *delta-time* [**repeat***repeat-interval*]}	ジョブが定期的に開始することを意味します。 start-time の形式は [[[[yyyy:]mmm:]dd:]HH]:MM です。 • *delta-time*：スケジュールの設定後、ジョブの開始までの待機時間を指定します。 • **now**：ジョブを今すぐ開始することを指定します。 • **repeat***repeat-interval*：ジョブを反復する回数を指定します。 この例では、ただちにジョブが開始され、48 時間間隔で反復されます。
ステップ 8	switch(config)# **show scheduler config**	（任意） スケジューラ設定を表示します。
ステップ 9	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。

スケジューラ ログ ファイルの消去

スケジューラ ログ ファイルを消去できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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	switch(config)# **clear scheduler logfile**	スケジューラ ログ ファイルの消去

スケジューラの設定確認

スケジューラの設定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	スケジューラ設定を表示します。
show scheduler job [**name** *string*]	設定されているジョブを表示します。
show scheduler logfile	スケジューラ ログ ファイルの内容を表示します。
show scheduler schedule [**name** *string*]	設定されているスケジュールを表示します。

スケジューラの設定例

スケジューラ ジョブの作成

次に、実行中のコンフィギュレーションを bootflash 内のファイルに保存し、ファイルを bootflash から TFTP サーバにコピーするスケジューラ ジョブを作成する例を示します（ファイル名は、現在のタイム スタンプとスイッチ名を使用して作成されます）。

```
switch# configure terminal
switch(config)# scheduler job name backup-cfg
switch(config-job)# cli var name timestamp $(TIMESTAMP) ;copy running-config
bootflash:/$(SWITCHNAME)-cfg.$(timestamp) ;copy bootflash:/$(SWITCHNAME)-cfg.$(timestamp)
```

```
tftp://1.2.3.4/ vrf management
switch(config-job)# end
switch(config)#
```

スケジューラ ジョブのスケジューリング

次に、backup-cfg という名前のスケジューラ ジョブを、毎日午前 1 時に実行するようスケジューリングする例を示します。

```
switch# configure terminal
switch(config)# scheduler schedule name daily
switch(config-if)# job name backup-cfg
switch(config-if)# time daily 1:00
switch(config-if)# end
switch(config)#
```

ジョブ スケジュールの表示

次に、ジョブ スケジュールを表示する例を示します。

```
switch# show scheduler schedule
Schedule Name : daily
---------------------------
User Name : admin
Schedule Type : Run every day at 1 Hrs 00 Mins
Last Execution Time : Fri Jan 2 1:00:00 2013
Last Completion Time: Fri Jan 2 1:00:01 2013
Execution count : 2
----------------------------------------------
Job Name Last Execution Status
----------------------------------------------
back-cfg Success (0)
switch#
```

スケジューラ ジョブの実行結果の表示

次に、スケジューラによって実行されたスケジューラ ジョブの結果を表示する例を示します。

```
switch# show scheduler logfile
Job Name : back-cfg Job Status: Failed (1)
Schedule Name : daily User Name : admin
Completion time: Fri Jan 1 1:00:01 2013
-------------------------------- Job Output ---------------------------------
`cli var name timestamp 2013-01-01-01.00.00`
`copy running-config bootflash:/$(HOSTNAME)-cfg.$(timestamp)`
`copy bootflash:/switch-cfg.2013-01-01-01.00.00 tftp://1.2.3.4/ vrf management `
copy: cannot access file '/bootflash/switch-cfg.2013-01-01-01.00.00'
==============================================================================
Job Name : back-cfg Job Status: Success (0)
Schedule Name : daily User Name : admin
Completion time: Fri Jan 2 1:00:01 2013
-------------------------------- Job Output ---------------------------------
`cli var name timestamp 2013-01-02-01.00.00`
`copy running-config bootflash:/switch-cfg.2013-01-02-01.00.00`
`copy bootflash:/switch-cfg.2013--01-02-01.00.00 tftp://1.2.3.4/ vrf management `
Connection to Server Established.
[ ] 0.50KBTrying to connect to tftp server......
[###### ] 24.50KB
TFTP put operation was successful
```

```
================================================================================
switch#
```

関連資料

関連項目	マニュアル タイトル
スケジューラの CLI コマンド	『*Cisco Nexus 7000 Series NX-OS System Management Command Reference*』
VDC	『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』

スケジューラの機能の履歴

次の表に、このマニュアルの新機能および変更された機能を要約し、各機能がサポートされているリリースを示します。ご使用のソフトウェア リリースで、本書で説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。

表 *19*：スケジューラの機能の履歴

機能名	リリース	機能情報
Scheduler	4.0(1)	この機能が導入されました。

第 12 章

SNMP の設定

この章では、Cisco NX-OS デバイス上で SNMP 機能を設定する方法について説明します。

この章の内容は、次のとおりです。

- 機能情報の確認，199 ページ
- SNMP の概要，200 ページ
- SNMP のライセンス要件，208 ページ
- SNMP の前提条件，209 ページ
- SNMP の注意事項および制約事項，209 ページ
- SNMP のデフォルト設定，209 ページ
- SNMP の設定，209 ページ
- SNMP の設定の確認，239 ページ
- SNMP の設定例，240 ページ
- その他の参考資料，242 ページ
- SNMP の機能の履歴，243 ページ

機能情報の確認

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

SNMP の概要

簡易ネットワーク管理プロトコル（SNMP）は、SNMPマネージャとエージェント間の通信用メッセージフォーマットを提供する、アプリケーションレイヤプロトコルです。SNMP では、ネットワーク内のデバイスのモニタリングと管理に使用する標準フレームワークと共通言語が提供されます。

SNMP 機能の概要

SNMP フレームワークは 3 つの部分で構成されます。

- SNMP マネージャ：SNMP を使用してネットワーク デバイスのアクティビティを制御し、モニタリングするシステム
- SNMP エージェント：デバイスのデータを維持し、必要に応じてこれらのデータを管理システムに報告する、管理対象デバイス内のソフトウェア コンポーネント。Cisco Nexus デバイスはエージェントおよびMIB をサポートします。SNMPエージェントをイネーブルにするには、マネージャとエージェントの関係を定義する必要があります。
- 管理情報ベース（Management Information Base）：SNMP エージェントの管理対象オブジェクトのコレクション

SNMP は、RFC 3411 ～ 3418 で規定されています。

デバイスは、SNMPv1、SNMPv2c、および SNMPv3 をサポートします。SNMPv1 および SNMPv2c はどちらも、コミュニティベース形式のセキュリティを使用します。

Cisco NX-OS は IPv6 による SNMP をサポートしています。

SNMP 通知

SNMP の重要な機能の 1 つは、SNMP エージェントから通知を生成できることです。これらの通知では、要求を SNMP マネージャから送信する必要はありません。通知は、不正なユーザ認証、再起動、接続の切断、隣接ルータとの接続の切断、その他の重要なイベントを表示します。

Cisco NX-OS は、トラップまたはインフォームとして SNMP 通知を生成します。トラップは、エージェントからホスト レシーバ テーブルで指定された SNMP マネージャに送信される、非同期の非確認応答メッセージです。応答要求は、SNMP エージェントから SNMP マネージャに送信される非同期メッセージで、マネージャは受信したという確認応答が必要です。

トラップの信頼性はインフォームより低くなります。SNMP マネージャはトラップを受信しても確認応答（ACK）を送信しないからです。デバイスは、トラップが受信されたかどうかを判断できません。インフォーム要求を受信する SNMP マネージャは、SNMP 応答プロトコル データ ユニット（PDU）でメッセージの受信を確認応答します。デバイスが応答を受信しない場合、インフォーム要求を再度送信できます。

複数のホスト レシーバーに通知を送信するよう Cisco NX-OS を設定できます。

次の表は、デフォルトでイネーブルになっている SNMP トラップを示します。

トラップ タイプ	説明
generic	: coldStart
generic	: warmStart
entity	: entity_mib_change
entity	: entity_module_status_change
entity	: entity_power_status_change
entity	: entity_module_inserted
entity	: entity_module_removed
entity	: entity_unrecognised_module
entity	: entity_fan_status_change
entity	: entity_power_out_change
link	: linkDown
link	: linkUp
link	: extended-linkDown
link	: extended-linkUp
link	: cieLinkDown
link	: cieLinkUp
link	: delayed-link-state-change
rf	: redundancy_framework
license	: notify-license-expiry
license	: notify-no-license-for-feature
license	: notify-licensefile-missing
license	: notify-license-expiry-warning
upgrade	: UpgradeOpNotifyOnCompletion
upgrade	: UpgradeJobStatusNotify
rmon	: risingAlarm
rmon	: fallingAlarm
rmon	: hcRisingAlarm

トラップ タイプ	説明
rmon	: hcFallingAlarm
entity	: entity_sensor

SNMPv3

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 が提供す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。

SNMPv1、SNMPv2、SNMPv3 のセキュリティ モデルおよびセキュリティ レベル

セキュリティ レベルは、SNMP メッセージを開示から保護する必要があるかどうか、およびメッセージを認証するかどうか判断します。セキュリティ モデル内のさまざまなセキュリティ レベルは、次のとおりです。

- noAuthNoPriv：認証または暗号化を実行しないセキュリティ レベル。
- authNoPriv：認証は実行するが、暗号化を実行しないセキュリティ レベル。
- authPriv：認証と暗号化両方を実行するセキュリティ レベル。

SNMPv1、SNMPv2c、および SNMPv3 の 3 つのセキュリティ モデルを使用できます。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 メッセージの処理中に適用されるセキュリティ メカニズムが決まります。次の表に、セキュリティ モデルとレベルの組み合わせの意味を示します。

（注） noAuthnoPriv は、SNMPv3 でサポートされません。

表 *20* : ***SNMP*** セキュリティ モデルおよびセキュリティ レベル

モデル	レベル	認証	暗号化	結果
v1	noAuthNoPriv	コミュニティ ストリング	No	コミュニティ ストリングの照合を使用して認証します。
v2c	noAuthNoPriv	コミュニティ ストリング	No	コミュニティ ストリングの照合を使用して認証します。
v3	noAuthNoPriv	Username	No	ユーザ名の照合を使用して認証します。
v3	authNoPriv	HMAC-MD5 または HMAC-SHA	No	Hash-Based Message Authentication Code（HMAC）メッセージ ダイジェスト 5（MD5）アルゴリズムまたは HMAC Secure Hash Algorithm（SHA）アルゴリズムに基づいて認証します。
v3	authPriv	HMAC-MD5 または HMAC-SHA	DES	HMAC-MD5 アルゴリズムまたは HMAC-SHA アルゴリズムに基づいて認証します。データ暗号規格（DES）の 56 ビット暗号化、および暗号ブロック連鎖（CBC）DES（DES-56）標準に基づいた認証を提供します。

ユーザベースのセキュリティ モデル

SNMPv3 ユーザベース セキュリティ モデル（USM） は SNMP メッセージレベル セキュリティを参照し、次のサービスを提供します。

- メッセージの完全性：メッセージが不正な方法で変更または破壊されず、データ シーケンスが悪意なく起こり得る範囲を超えて変更されていないことを保証します。
- メッセージ発信元の認証：受信データを発信したユーザのアイデンティティが確認されたことを保証します。
- メッセージの機密性：情報が使用不可であること、または不正なユーザ、エンティティ、またはプロセスに開示されないことを保証します。

SNMPv3 は、設定済みユーザによる管理動作のみを許可し、SNMP メッセージを暗号化します。

Cisco NX-OSは、次の 2 つの SNMPv3 認証プロトコルを使用します。

- HMAC-MD5-96 認証プロトコル
- HMAC-SHA-96 認証プロトコル

Cisco NX-OS は、SNMPv3 メッセージ暗号化用プライバシー プロトコルの 1 つとして、Advanced Encryption Standard（AES）を使用し、RFC 3826 に準拠します。

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。**priv** オプションおよび **aes-128** トークンは、128 ビットの AES キーを生成するためのプライバシー パスワードであることを示します。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は、大文字と小文字を区別して、最大 64 文字の英数字を指定できます。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。

（注） 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 を指定する必要があります。

CLI および SNMP ユーザの同期

SNMPv3 ユーザ管理は、Access Authentication and Accounting（AAA）サーバ レベルで集中化できます。この中央集中型ユーザ管理により、Cisco NX-OSの SNMP エージェントは 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。AAAサーバはユーザ グループ名の格納にも使用されます。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。

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。

Cisco NX-OS は、次のようにユーザ設定を同期化します。

- **snmp-server user** コマンドで指定された認証パスフレーズが CLI ユーザのパスワードになります。
- **username** コマンドで指定されたパスワードが SNMP ユーザの認証およびプライバシー パスフレーズになります。
- SNMP または CLI を使用してユーザを作成または削除すると、SNMP と CLI の両方でユーザが作成または削除されます。
- 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。
- CLI から行ったロール変更（削除または変更）は、SNMP と同期します。

（注） パスフレーズまたはパスワードをローカライズしたキーおよび暗号形式で設定した場合、Cisco NX-OS はユーザ情報（パスワードやロールなど）を同期させません。

Cisco NX-OS はデフォルトで、同期したユーザ設定を 60 分間維持します。

SNMPv3 サーバの 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。

一意の SNMPv3 ユーザが存在し、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、ユーザは検証されません。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 の排他的な動作がイネーブルになっているかどうかに基づいて許可または拒否されます。

表 *21*：*AAA* の排他的な動作のシナリオ

User Location	AAA Server	AAA Exclusive Behavior	User Authentication
Local User Database	ディセーブル	イネーブル	ユーザが認証されます。
Local User Database	イネーブル	イネーブル	ユーザは認証されません。
Local User Database	イネーブル	ディセーブル	ユーザが認証されます。

リモートおよびローカル ユーザ データベース（同一ユーザ名）	イネーブル	イネーブル	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。 （注） ユーザ クレデンシャルを自動的に N7k スイッチに同期し、その結果、想定された SNMP ウォークを出力する、NMS サーバからの FM/DM コンセプトがある場合のみ機能します。これがない場合、ユーザ クレデンシャルはスイッチに同期しないため、スイッチで非表示の CLI を使用して手動で同期する必要があります。
リモートおよびローカル ユーザ データベース（同一ユーザ名）	ディセーブル	イネーブル	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 データベース（同一ユーザ名）	ディセーブル	ディセーブル	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 データベース（同一ユーザ名）	イネーブル	ディセーブル	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。

（注） AAA サーバが到達不能な場合、ユーザがローカル ユーザ 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で設定することができます。ユーザがローカル データベースにない場合、SNMPv3 サーバはエラーを返します。ユーザがリモート ユーザのデータベースに存在しない場合、SNMPv3 サーバは AAA サーバの可用性をチェックせずに「Unknown user」のメッセージを返します。

グループベースの SNMP アクセス

（注） グループは業界全体で使用されている標準的な SNMP 用語なので、SNMP に関する説明では、「ロール」ではなく「グループ」を使用します。

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。各グループは読み取りアクセス権または読み取りと書き込みアクセス権を指定して定義します。

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。

SNMP および EEM

Embedded Event Manager（EEM）機能は、SNMP MIB オブジェクトを含むイベントをモニタし、これらのイベントに基づいてアクションを開始します。SNMP 通知の送信もアクションの 1 つです。EEM は SNMP 通知として、CISCO-EMBEDDED-EVENT-MGR-MIB の cEventMgrPolicyEvent を送信します。

マルチインスタンス サポート

デバイスは、プロトコル インスタンスや仮想ルーティングおよびフォワーディング（VRF）インスタンスなどの論理ネットワーク エンティティの複数のインスタンスをサポートできます。大部分の既存 MIB は、これら複数の論理ネットワーク エンティティを識別できません。たとえば、元々の OSPF-MIB ではデバイス上のプロトコル インスタンスが 1 つであることが前提になりますが、現在はデバイス上で複数の OSPF インスタンスを設定できます。

SNMPv3 ではコンテキストを使用して、複数のインスタンスを識別します。SNMP コンテキストは管理情報のコレクションであり、SNMP エージェントを通じてアクセスできます。デバイスは、さまざまな論理ネットワーク エンティティの複数のコンテキストをサポートできます。SNMP コンテキストによって、SNMP マネージャはさまざまな論理ネットワーク エンティティに対応するデバイス上でサポートされる、MIB モジュールの複数のインスタンスの 1 つにアクセスできます。

Cisco NX-OS は、SNMP コンテキストと論理ネットワーク エンティティ間のマッピングのために、CISCO-CONTEXT-MAPPING-MIB をサポートします。SNMP コンテキストは VRF、プロトコル インスタンス、またはトポロジに関連付けることができます。

SNMPv3 は、SNMPv3 PDU の contextName フィールドでコンテキストをサポートします。この contextName フィールドを特定のプロトコル インスタンスまたは VRF にマッピングできます。

SNMPv2c の場合は、SNMP-COMMUNITY-MIB の snmpCommunityContextName MIB オブジェクトを使用して、SNMP コミュニティをコンテキストにマッピングできます（RFC 3584）。さらに CISCO-CONTEXT-MAPPING-MIB または CLI を使用すると、この snmpCommunityContextName を特定のプロトコル インスタンスまたは VRF にマッピングできます。

SNMP のハイ アベイラビリティ

Cisco NX-OS は、SNMP 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。

SNMP の仮想化サポート

Cisco NX-OS は、仮想デバイス コンテキスト（VDC）ごとに SNMP インスタンスを 1 つずつサポートします。デフォルトでは、Cisco NX-OS はデフォルト VDC に配置します。詳細については、『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』を参照してください。

SNMP は複数の MIB モジュール インスタンスをサポートし、それらを論理ネットワーク エンティティにマッピングします。詳細については、「マルチインスタンス サポート」の項を参照してください。

SNMP も VRF を認識します。特定の VRF を使用して、SNMP 通知ホスト レシーバに接続するように SNMP を設定できます。通知が発生した VRF に基づいて、SNMP ホスト レシーバへの通知をフィルタリングするように SNMP を設定することもできます。詳細については、「VRF を使用する SNMP 通知レシーバの設定」の項を参照してください。

SNMP のライセンス要件

製品	ライセンス要件
Cisco NX-OS	SNMP 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 nx-os イメージにバンドルされており、無料で提供されます。NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

SNMP の前提条件

VDC を設定する場合は、適切なライセンスをインストールし、所定の VDC を開始する必要があります。設定情報については『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』、ライセンス情報については『*Cisco NX-OS Licensing Guide*』を参照してください。

SNMP の注意事項および制約事項

SNMP には、次の注意事項および制限事項があります。

- アクセス コントロール リスト（ACL）は、スイッチに設定されたローカル SNMPv3 ユーザのみに適用できます。ACL は、認証、許可、アカウンティング（AAA）サーバに保存されるリモート SNMPv3 ユーザに適用できません。
- Cisco NX-OS は、一部の SNMP MIB への読み取り専用アクセスをサポートします。詳細については次の URL にアクセスして、Cisco NX-OS の MIB サポート リストを参照してください。ftp://ftp.cisco.com/pub/mibs/supportlists/nexus7000/Nexus7000MIBSupportList.html

SNMP のデフォルト設定

次の表に、SNMP パラメータのデフォルト設定を示します。

パラメータ	デフォルト
ライセンス通知	イネーブル

SNMP の設定

（注） この機能の Cisco NX-OS コマンドは、Cisco IOS のコマンドとは異なる場合があるので注意してください。

（注） デバイス上に最大 10 の SNMP ホストを設定できます。

SNMP ユーザの設定

SNMP ユーザを設定できます。

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 user***name* [**auth** {**md5** | **sha**} *passphrase* [**auto**] [**priv** [**aes-128**] *passphrase*] [**engineID***id*] [**localizedkey**]] 例： `switch(config)# snmp-server user Admin auth sha abcd1234 priv abcdefgh`	認証およびプライバシー パラメータのある SNMP ユーザを設定します。パスフレーズには最大 64 文字の英数字を使用できます。大文字と小文字が区別されます。**localizedkey** キーワードを使用する場合は、パスフレーズに大文字と小文字を区別した英数字を 130 文字まで使用できます。 engineID の形式は、12 桁のコロンで区切った 10 進数字です。
ステップ 3	**show snmp user** 例： `switch(config) # show snmp user`	（任意） 1 人または複数の SNMP ユーザに関する情報を表示します。
ステップ 4	**copy running-config startup-config** 例： `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。

SNMP メッセージ暗号化の適用

着信要求に認証または暗号化が必要となるよう SNMP を設定できます。デフォルトでは、SNMP エージェントは認証および暗号化を行わないでも SNMPv3 メッセージを受け付けます。プライバシーを適用する場合、Cisco NX-OS は、**noAuthNoPriv** または **authNoPriv** のいずれかのセキュリティ レベル パラメータを使用しているすべての SNMPv3 PDU 要求に対して、許可エラーで応答します。

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 user***name***enforcePriv** 例： `switch(config)# snmp-server user Admin enforcePriv`	このユーザに対して SNMP メッセージ暗号化を適用します。
ステップ 3	**snmp-server globalEnforcePriv** 例： `switch(config)# snmp-server globalEnforcePriv`	すべてのユーザに対して SNMP メッセージ暗号化を適用します。
ステップ 4	**copy running-config startup-config** 例： `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。

SNMPv3 ユーザに対する複数のロールの割り当て

SNMP ユーザを作成した後で、そのユーザに複数のロールを割り当てることができます。

（注） 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。

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。

	コマンドまたはアクション	目的
ステップ 2	**snmp-server user***namegroup* 例： `switch(config)# snmp-server user Admin superuser`	この SNMP ユーザと設定されたユーザ ロールをアソシエートします。
ステップ 3	**copy running-config startup-config** 例： `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。

SNMP コミュニティの作成

SNMPv1 または SNMPv2c の SNMP コミュニティを作成できます。

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 community***name* {**group** *group* | **ro** | **rw**} 例： `switch(config)# snmp-server community public ro`	SNMP コミュニティ ストリングを作成します。
ステップ 3	**copy running-config startup-config** 例： `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。

SNMP 要求のフィルタリング

アクセス コントロール リスト（ACL）を SNMPv3 ユーザまたは SNMPv3 コミュニティに割り当てて、着信 SNMP 要求にフィルタを適用できます。割り当てた ACL により着信要求パケットが

許可される場合、SNMP はその要求を処理します。ACL により要求が拒否される場合、SNMP はその要求を廃棄して、システム メッセージを送信します。

ACL は次のパラメータで作成します。

- 送信元 IP アドレス
- 宛先 IP アドレス
- 送信元ポート
- 宛先ポート
- プロトコル（UDP または TCP）

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 user***name* [**use-ipv4acl** *ipv4acl-name*] [**use-ipv6acl** *ipv6acl-name*] 例： `switch(config)# snmp-server community public use-ipv4acl myacl`	SNMPv3 ユーザに IPv4 ACL または IPv6 ACL を割り当てて SNMP 要求をフィルタします。 （注） AAA サーバは、SNMPv3 ユーザの作成をサポートする必要があります。
ステップ 3	**snmp-server community***name* [**use-ipv4acl** *ipv4acl-name*] [**use-ipv6acl** *ipv6acl-name*] 例： `switch(config)# snmp-server community public use-ipv4acl myacl`	SNMPv3 コミュニティに IPv4 ACL または IPv6 ACL を割り当てて SNMP 要求をフィルタします。
ステップ 4	**copy running-config startup-config** 例： `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。

ロケーションに基づく SNMPv3 ユーザの認証

ロケーションに基づいて、ローカルまたはリモートの SNMPv3 ユーザを認証できます。

SNMPv3 サーバの AAA の排他的な動作をイネーブルにするには、グローバル コンフィギュレーション 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	ロケーションに基づいてユーザを認証するために SNMPv3 サーバの AAA 排他的動作をイネーブルにします。 ユーザのロケーションおよび AAA サーバがイネーブルかどうかによって、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 サーバがイネーブルの場合、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 サーバがディセーブルの場合、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 ユーザおよびリモート AAA ユーザの両方で、 AAA サーバがイネーブルの場合、リモート クレデンシャルを持つクエリは成功し、ローカル クレデンシャル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 サーバがディセーブルの場合、ローカル リモート クレデンシャルを持つクエリは成功し、リモート クレデンシャル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 通知レシーバの設定

複数のホスト レシーバーに対して SNMP 通知を生成するよう Cisco NX-OSを設定できます。

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 host***ip-address***traps version 1***community* [**udp_port***number*] 例： `switch(config)# snmp-server host 192.0.2.1 traps version 1 public`	SNMPv1 トラップのホスト レシーバを設定します。*ip-address* は IPv4 または IPv6 アドレスを使用できます。*community* には最大 255 の英数字を使用できます。UDP ポート番号の範囲は 0 ～ 65535 です。
ステップ 3	**snmp-server host***ip-address* {**traps** | **informs**} **version 2c***community* [**udp_port***number*] 例： `switch(config)# snmp-server host 192.0.2.1 informs version 2c public`	SNMPv2c トラップまたはインフォームのホスト レシーバを設定します。*ip-address* は IPv4 または IPv6 アドレスを使用できます。*community* には最大 255 の英数字を使用できます。UDP ポート番号の範囲は 0 ～ 65535 です。
ステップ 4	**snmp-server host***ip-address* {**traps** | **informs**} **version 3** {**auth** | **noauth** | **priv**} *username* [**udp_port***number*] 例： `switch(config)# snmp-server host 192.0.2.1 informs version 3 auth NMS`	SNMPv3 トラップまたは応答要求のホスト レシーバを設定します。*ip-address* は IPv4 または IPv6 アドレスを使用できます。*username* には最大 255 の英数字を使用できます。UDP ポート番号の範囲は 0 ～ 65535 です。 （注） SNMP マネージャは、SNMPv3 メッセージを認証して復号化するために、Cisco NX-OS デバイスの SNMP エンジン ID に基づいてユーザ クレデンシャル（authKey/PrivKey）を調べる必要があります。
ステップ 5	**copy running-config startup-config** 例： `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。

SNMP 通知用の発信元 インターフェイスの設定

通知の送信元 IP アドレスとしてインターフェイスの IP アドレスを使用するよう、SNMP を設定できます。通知が生成される場合、送信元 IP アドレスは、この設定済みインターフェイスの IP アドレスに基づいています。

次のように発信元インターフェイスを設定できます。

- すべての通知が、すべての SNMP 通知レシーバへ送信される。
- すべての通知が、特定の SNMP 通知レシーバへ送信される。このコンフィギュレーションは、グローバル発信元インターフェイスのコンフィギュレーションよりも優先されます。

（注） 発信トラップパケットの送信元インターフェイス IP アドレスを設定すると、デバイスがトラップの送信に同じインターフェイスを使用することが保証されません。送信元インターフェイス IP アドレスは、SNMP トラップの内部で送信元アドレスを定義し、出力インターフェイス アドレスを送信元として接続が開きます。

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 host** *ip-address* **source-interface** *if-type if-number* [**udp_port** *number*] 例： `switch(config)# snmp-server host 192.0.2.1 source-interface ethernet 2/1`	SNMPv2c トラップまたはインフォームのホスト レシーバを設定します。*ip-address* は IPv4 または IPv6 アドレスを使用できます。**?** を使用して、サポートされているインターフェイス タイプを特定します。UDP ポート番号の範囲は 0 ～ 65535 です。 このコンフィギュレーションは、グローバル発信元インターフェイスのコンフィギュレーションよりも優先されます。
ステップ 3	**snmp-server source-interface** {**traps** | **informs**} *if-type if-number* 例： `switch(config)# snmp-server source-interface traps ethernet 2/1`	SNMPv2c トラップまたは応答要求を送信するよう発信元インターフェイスを設定します。**?** を使用して、サポートされているインターフェイス タイプを特定します。

	コマンドまたはアクション	目的
ステップ 4	**show snmp source-interface** 例： `switch(config)# show snmp source-interface`	設定した発信元インターフェイスの情報を表示します。

通知対象ユーザの設定

SNMPv3 インフォーム通知を通知ホスト レシーバに送信するには、デバイスに通知ターゲット ユーザを設定する必要があります。

Cisco NX-OS は通知ターゲット ユーザのクレデンシャルを使用して、設定された通知ホスト レシーバへの SNMPv3 インフォーム通知メッセージを暗号化します。

（注） 受信した INFORM PDU を認証して復号化する場合、Cisco NX-OS で設定されているのと同じ、応答要求を認証して解読するユーザ クレデンシャルが通知ホスト レシーバに必要です。

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 user** *name* [**auth** {**md5** | **sha**} *passphrase* [**auto**] [**priv** [**aes-128**] *passphrase*] [**engineID** *id*] 例： `switch(config)# snmp-server user NMS auth sha abcd1234 priv abcdefgh engineID 00:00:00:63:00:01:00:10:20:15:10:03`	通知ホスト レシーバのエンジン ID を指定して、通知ターゲット ユーザを設定します。エンジン ID の形式は、12 桁のコロンで区切った 10 進数字です。
ステップ 3	**copy running-config startup-config** 例： `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。

VRF を使用する SNMP 通知レシーバの設定

SNMP 通知レシーバの VRF 到達可能性およびフィルタリング オプションを設定すると、SNMP によって CISCO-SNMP-TARGET-EXT-MIB の cExtSnmpTargetVrfTable にエントリが追加されます。

（注） VRF 到達可能性またはフィルタリング オプションを設定する前に、ホストを設定する必要があります。

ホスト レシーバに到達するように設定した VRF を使用したり、または通知が発生した VRF に基づいて通知をフィルタするように Cisco NX-OS を設定できます。

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	[**no**] **snmp-server host***ip-address***use-vrf***vrf-name* [**udp_port***number*] 例： `switch(config)# snmp-server host 192.0.2.1 use-vrf Blue`	特定の VRF を使用してホスト レシーバと通信するように SNMP を設定します。*ip-address* は IPv4 または IPv6 アドレスを使用できます。VRF 名には最大 255 の英数字を使用できます。UDP ポート番号の範囲は 0 ～ 65535 です。このコマンドによって、CISCO-SNMP-TARGET-EXT-MB の ExtSnmpTargetVrfTable にエントリが追加されます。 このコマンドの **no** 形式は、設定されたホストの VRF 到達可能性情報を削除し、CISCO-SNMP-TARGET-EXT-MB の ExtSnmpTargetVrfTable からエントリを削除します。 （注） このコマンドによってホスト設定は削除されません。
ステップ 3	[**no**] **snmp-server host***ip-address***filter-vrf***vrf-name* [**udp_port***number*] 例： `switch(config)# snmp-server host 192.0.2.1 filter-vrf Red`	設定された VRF に基づいて、通知ホスト レシーバへの通知をフィルタリングします。*ip-address* は IPv4 または IPv6 アドレスを使用できます。VRF 名には最大 255 の英数字を使用できます。UDP ポート番号の範囲は 0 ～ 65535 です。 このコマンドによって、CISCO-SNMP-TARGET-EXT-MB の ExtSnmpTargetVrfTable にエントリが追加されます。 このコマンドの **no** 形式は、設定されたホストの VRF フィルタ情報を削除し、CISCO-SNMP-TARGET-EXT-MB の ExtSnmpTargetVrfTable からエントリを削除します。

	コマンドまたはアクション	目的
		（注） このコマンドによってホスト設定は削除されません。
ステップ 4	**copy running-config startup-config** 例： `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。

帯域内ポートを使用してトラップを送信するための SNMP 設定

帯域内ポートを使用してトラップを送信するよう SNMP を設定できます。このようにするには、（グローバルまたはホスト レベルで）発信元インターフェイスを設定し、トラップを送信するための VRF を設定します。

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 source-interface traps** *if-type if-number* 例： `switch(config)# snmp-server source-interface traps ethernet 1/2`	SNMP トラップを送信するための発信元インターフェイスをグローバルに設定します。? を使用して、サポートされているインターフェイス タイプを特定します。 グローバル レベルまたはホスト レベルで発信元インターフェイスを設定できます。発信元インターフェイスをグローバルに設定すると、新しいホストコンフィギュレーションはグローバルなコンフィギュレーションを使用してトラップを送信します。 （注） 発信元インターフェイスをホスト レベルで設定するには、**snmp-server host** *ip-address* **source-interface** *if-type if-number* コマンドを使用します。

	コマンドまたはアクション	目的
ステップ 3	**show snmp source-interface** 例： `switch(config)# show snmp source-interface`	（任意） 設定した発信元インターフェイスの情報を表示します。
ステップ 4	**snmp-server host** *ip-address* **use-vrf** *vrf-name* [**udp_port** *number*] 例： `switch(config)# snmp-server host 171.71.48.164 use-vrf default`	特定の VRF を使用してホスト レシーバと通信するように SNMP を設定します。*ip-address* は IPv4 または IPv6 アドレスを使用できます。VRF 名には最大 255 の英数字を使用できます。UDP ポート番号の範囲は 0 ～ 65535 です。このコマンドによって、CISCO-SNMP-TARGET-EXT-MB の ExtSnmpTargetVrfTable にエントリが追加されます。 （注） デフォルトでは、SNMP は管理 VRF を使用してトラップを送信します。管理 VRF を使用しない場合は、このコマンドを使用して対象の VRF を指定する必要があります。
ステップ 5	**show snmp host** 例： `switch(config)# show snmp host`	（任意） 設定した SNMP ホストの情報を表示します。
ステップ 6	**copy running-config startup-config** 例： `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。

SNMP 通知のイネーブル化

通知をイネーブルまたはディセーブルにできます。通知名を指定しないと、Cisco NX-OSは通知をすべてイネーブルにします。

（注） **snmp-server enable traps** コマンドを使用すると、設定されている通知ホスト レシーバに応じて、トラップおよび応答要求の両方がイネーブルになります。

次の表に、Cisco NX-OS MIB の通知をイネーブルにするコマンドを示します。

表 *22* : *SNMP* 通知のイネーブル化

MIB	関連コマンド
すべての通知	**snmp-server enable traps**
CISCO-AAA-SERVER-MIB	**snmp-server enable traps aaa** **snmp-server enable traps aaa server-state-change**
CISCO-BGP4-MIB	**snmp-server enable traps bgp**
CISCO-BGP-MIBv2	**snmp-server enable traps bgp cbgp2**
CISCO-STP-BRIDGE-MIB	**snmp-server enable traps bridge** **snmp-server enable traps bridge newroot** **snmp-server enable traps bridge topologychange**
CISCO-CALLHOME-MIB	**snmp-server enable traps callhome** **snmp-server enable traps callhome event-notify** **snmp-server enable traps callhome smtp-send-fail**
CISCO-CFS-MIB	**snmp-server enable traps cfs** **snmp-server enable traps cfs merge-failure** **snmp-server enable traps cfs state-change-notif**
CISCO-CONFIG-MAN-MIB	**snmp-server enable traps config** **snmp-server enable traps config ccmCLIRunningConfigChanged**
CISCO-EIGRP-MIB	**snmp-server enable traps eigrp**[*tag*]

MIB	関連コマンド
ENTITY-MIB, CISCO-ENTITY-SENSOR-MIB	**snmp-server enable traps entity** **snmp-server enable traps entity entity_fan_status_change** **snmp-server enable traps entity entity_mib_change** **snmp-server enable traps entity entity_module_inserted** **snmp-server enable traps entity entity_module_removed** **snmp-server enable traps entity entity_module_status_change** **snmp-server enable traps entity entity_power_out_change** **snmp-server enable traps entity entity_power_status_change** **snmp-server enable traps entity entity_unrecognised_module**
CISCO-FEATURE-CONTROL-MIB	**snmp-server enable traps feature-control** **snmp-server enable traps feature-control FeatureOpStatusChange**
CISCO-HSRP-MIB	**snmp-server enable traps hsrp** **snmp-server enable traps hsrp state-change**
CISCO-LICENSE-MGR-MIB	**snmp-server enable traps license** **snmp-server enable traps license notify-license-expiry** **snmp-server enable traps license notify-license-expiry-warning** **snmp-server enable traps license notify-licensefile-missing** **snmp-server enable traps license notify-no-license-for-feature**
CISCO-INTERFACE-XCVR MONITOR-MIB	**snmp-server enable traps link cisco-xcvr-mon-status-chg**

MIB	関連コマンド
IF-MIB	**snmp-server enable traps link** **snmp-server enable traps link IETF-extended-linkDown** **snmp-server enable traps link IETF-extended-linkUp** **snmp-server enable traps link cisco-extended-linkDown** **snmp-server enable traps link cisco-extended-linkUp** **snmp-server enable traps link linkDown** **snmp-server enable traps link Up**
OSPF-MIB, OSPF-TRAP-MIB	**snmp-server enable traps ospf**[*tag*] **snmp-server enable traps ospf lsa** **snmp-server enable traps ospf rate-limit***rate*
CISCO-PORT-SECURITY-MIB	**snmp-server enable traps port-security** **snmp-server enable traps port-security** **access-secure-mac-violation** **snmp-server enable traps port-security** **trunk-secure-mac-violation**
CISCO-RF-MIB	**snmp-server enable traps rf** **snmp-server enable traps rf redundancy_framework**
CISCO-RMON-MIB	**snmp-server enable traps rmon** **snmp-server enable traps rmon fallingAlarm** **snmp-server enable traps rmon hcFallingAlarm** **snmp-server enable traps rmon hcRisingAlarm** **snmp-server enable traps rmon risingAlarm**

MIB	関連コマンド
SNMPv2-MIB	**snmp-server enable traps snmp** **snmp-server enable traps snmp authentication**
CISCO-STPX-MIB	**snmp-server enable traps stpx** **snmp-server enable traps stpx inconsistency** **snmp-server enable traps stpx loop-inconsistency** **snmp-server enable traps stpx root-inconsistency**
CISCO-SYSTEM-EXT-MIB	**snmp-server enable traps sysmgr** **snmp-server enable traps sysmgr cseFailSwCoreNotifyExtended**
UPGRADE-MIB	**snmp-server enable traps upgrade** **snmp-server enable traps upgrade UpgradeJobStatusNotify** **snmp-server enable traps upgrade UpgradeOpNotifyOnCompletion**
ZONE-MIB	**zone** **zone default-zone-behavior-changes** **zone merge-failure** **zone merge-success** **zone request-reject1** **zone unsupp-mem**

指定した通知をイネーブルにするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
snmp-server enable traps	すべての SNMP 通知をイネーブルにします。

コマンド	目的
snmp-server enable traps aaa[**server-state-change**]	AAA SNMP 通知をイネーブルにします。任意で、次の特定の通知をイネーブルにします。 • **server-state-change**：AAA サーバの状態変化通知をイネーブルにします。
snmp-server enable traps bgp [**cbgp2**]	CISCO-BGP4-MIB SNMP 通知をイネーブルにします。任意で、次の特定の通知をイネーブルにします。 • **bgp cbgp2**—Enables CISCO-BGP4-MIBv2 SNMP notifications.
snmp-server enable traps bridge[**newroot**][**topologychange**]	STP ブリッジ SNMP 通知をイネーブルにします。任意で、次の特定の通知をイネーブルにします。 • **newroot**：STP の新しいルート ブリッジ通知をイネーブルにします。 • **topologychange**：STP ブリッジのトポロジ変更通知をイネーブルにします。
snmp-server enable traps callhome [**event-notify**] [**smtp-send-fail**]	Call Home 通知をイネーブルにします。任意で、次の特定の通知をイネーブルにします。 • **event-notify**：Call Home の外部イベント通知をイネーブルにします。 • **smtp-send-fail**：簡易メール転送プロトコル（SMTP）メッセージの送信失敗通知をイネーブルにします。

コマンド	目的
snmp-server enable traps cfs [**merge-failure**] [**state-change-notif**]	Cisco Fabric Services（CFS）の通知をイネーブルにします。任意で、次の特定の通知をイネーブルにします。 • **merge-failure**：CFS のマージ失敗通知をイネーブルにします。 • **state-change-notif**：CFS の状態変化通知をイネーブルにします。
snmp-server enable traps config [**ccmCLIRunningConfigChanged**]	コンフィギュレーションの変更に対して SNMP 通知をイネーブルにします。 • **ccmCLIRunningConfigChanged**：実行中または起動時のコンフィギュレーションで、コンフィギュレーションの変更に対して SNMP 通知をイネーブルにします。
snmp-server enable traps eigrp [*tag*]	CISCO-EIGRP-MIB SNMP 通知をイネーブルにします。

コマンド	目的
snmp-server enable traps entity [**entity_fan_status_change**] [**entity_mib_change**] [**entity_module_inserted**] [**entity_module_removed**] [**entity_module_status_change**] [**entity_power_out_change**] [**entity_power_status_change**] [**entity_unrecognised_module**]	ENTITY-MIB SNMP 通知をイネーブルにします。任意で、次の特定の通知をイネーブルにします。 • **entity_fan_status_change**：エンティティ ファンの状態変化通知をイネーブルにします。 • **entity_mib_change**：エンティティ MIB 変更通知をイネーブルにします。 • **entity_module_inserted**：エンティティ モジュール挿入通知をイネーブルにします。 • **entity_module_removed**：エンティティ モジュール削除通知をイネーブルにします。 • **entity_module_status_change**：エンティティ モジュールステータス変更通知をイネーブルにします。 • **entity_power_out_change**：エンティティの出力パワー変更通知をイネーブルにします。 • **entity_power_status_change**：エンティティのパワー ステータス変更通知をイネーブルにします。 • **entity_unrecognised_module**：エンティティの未確認モジュール通知をイネーブルにします。

コマンド	目的
snmp-server enable traps feature-control[**FeatureOpStatusChange**]	機能制御 SNMP 通知をイネーブルにします。任意で、次の特定の通知をイネーブルにします。 • **FeatureOpStatusChange**：機能操作の状態変化通知をイネーブルにします。
snmp-server enable traps hsrp[**state-change**]	CISCO-HSRP-MIB SNMP 通知をイネーブルにします。任意で、次の特定の通知をイネーブルにします。 • **state-change**：HSRP の状態変化通知をイネーブルにします。
snmp-server enable traps license [**notify-license-expiry**] [**notify-license-expiry-warning**] [**notify-licensefile-missing**] [**notify-no-license-for-feature**]	ENTITY-MIB SNMP 通知をイネーブルにします。任意で、次の特定の通知をイネーブルにします。 • **notify-license-expiry**：ライセンス失効通知をイネーブルにします。 • **notify-license-expiry-warning**：ライセンス失効の警告通知をイネーブルにします。 • **notify-licensefile-missing**：ライセンス ファイル不明通知をイネーブルにします。 • **notify-no-license-for-feature**：no-license-installed-for-feature 通知をイネーブルにします。

コマンド	目的
snmp-server enable traps link [**IETF-extended-linkDown**] [**IETF-extended-linkUp**] [**cisco-extended-linkDown**] [**cisco-extended-linkUp**] [**linkDown**] [**linkUp**]	IF-MIB リンク通知をイネーブルにします。任意で、次の特定の通知をイネーブルにします。 • **IETF-extended-linkDown**：インターネット技術特別調査委員会（IETF）の拡張リンク ステート ダウン通知をイネーブルにします。 • **IETF-extended-linkUp**：IETF の拡張リンク ステート アップ通知をイネーブルにします。 • **cisco-extended-linkDown**：Cisco 拡張リンク ステート ダウン通知をイネーブルにします。 • **cisco-extended-linkUp**：Cisco 拡張リンク ステート アップ通知をイネーブルにします。 • **linkDown**：IETF リンク ステート ダウン通知をイネーブルにします。 • **linkUp**：IETF リンク ステート アップ通知をイネーブルにします。
snmp-server enable traps ospf[*tag*] [**lsa**]	Open Shortest Path First（OSPF）通知をイネーブルにします。任意で、次の特定の通知をイネーブルにします。 • **lsa**：OSPF リンク ステート アドバタイズメント（LSA）通知をイネーブルにします。

コマンド	目的
snmp-server enable traps port-security [**access-secure-mac-violation**] [**trunk-secure-mac-violation**]	ポート セキュリティ SNMP 通知をイネーブルにします。任意で、次の特定の通知をイネーブルにします。 • **access-secure-mac-violation**：セキュアな Machine Access Control（MAC）違反通知をイネーブルにします。 • **trunk-secure-mac-violation**：仮想 LAN（VLAN）のセキュア MAC 違反通知をイネーブルにします。
snmp-server enable traps rf[**redundancy-framework**]	冗長フレームワーク（RF）SNMP 通知をイネーブルにします。任意で、次の特定の通知をイネーブルにします。 • **redundancy-framework**：RF スーパーバイザ スイッチオーバー MIB 通知をイネーブルにします。

コマンド	目的
snmp-server enable traps rmon [**fallingAlarm**] [**hcFallingAlarm**] [**hcRisingAlarm**] [**risingAlarm**]	リモート モニタリング（RMON）SNMP 通知をイネーブルにします。任意で、次の特定の通知をイネーブルにします。 • **fallingAlarm**：RMON 下限アラーム通知をイネーブルにします。 • **hcFallingAlarm**：RMON high-capacity 下限アラーム通知をイネーブルにします。 • **hcRisingAlarm**：RMON high-capacity 上限アラーム通知をイネーブルにします。 • **risingAlarm**：RMON 上限アラーム通知をイネーブルにします。
snmp-server enable traps snmp [**authentication**]	一般的な SNMP 通知をイネーブルにします。任意で、次の特定の通知をイネーブルにします。 • **authentication**：SNMP 認証通知をイネーブルにします。

コマンド	目的
snmp-server enable traps stpx [**inconsistency**] [**loop-inconsistency**] [**root-inconsistency**]	リモート モニタリング（RMON）SNMP 通知をイネーブルにします。任意で、次の特定の通知をイネーブルにします。 • **inconsistency**：SNMP STPX MIB 不一致アップデート通知をイネーブルにします。 • **loop-inconsistency**：SNMP STPX MIB ループ不一致アップデート通知をイネーブルにします。 • **root-inconsistency**：SNMP STPX MIB ルート不一致アップデート通知をイネーブルにします。
snmp-server enable traps sysmgr [**cseFailSwCoreNotifyExtended**]	ソフトウェア変更通知をイネーブルにします。任意で、次の特定の通知をイネーブルにします。 • **cseFailSwCoreNotifyExtended**：ソフトウェア コア通知をイネーブルにします。
snmp-server enable traps upgrade [**UpgradeJobStatusNotify**] [**UpgradeOpNotifyOnCompletion**]	アップグレード通知をイネーブルにします。任意で、次の特定の通知をイネーブルにします。 • **UpgradeJobStatusNotify**：アップグレード ジョブ ステータス通知をイネーブルにします。 • **UpgradeOpNotifyOnCompletion**：アップグレード グローバル ステータス通知をイネーブルにします。

コマンド	目的
snmp-server enable traps vtp [**notifs**] [**vlancreate**] [**vlandelete**]	VTP 通知をイネーブルにします。任意で、次の特定の通知をイネーブルにします。 • **notifs**：VTP 通知をイネーブルにします。 • **vlancreate**：VLAN 作成の通知をイネーブルにします。 • **vlandelete**：VLAN 削除の通知をイネーブルにします。
snmp-server enable traps zone [**default-zone-behavior-change**] [**merge-failure**] [**merge-success**] [**request-reject1**] [**unsupp-mem**]	デフォルト ゾーン変更通知をイネーブルにします。任意で、次の特定の通知をイネーブルにします。 • **default-zone-behavior-change**：デフォルト ゾーン動作変更通知をイネーブルにします。 • **merge-failure**：マージ失敗通知をイネーブルにします。 • **merge-success**：マージ成功通知をイネーブルにします。 • **request-reject1**：要求拒否通知をイネーブルにします。 • **unsupp-mem**：未サポートメンバ通知をイネーブルにします。

インターフェイスでのリンク通知のディセーブル化

個別のインターフェイスで linkUp および linkDown 通知をディセーブルにできます。フラッピング インターフェイス（Up と Down の間を頻繁に切り替わるインターフェイス）で、この制限通知を使用できます。

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	**interface** *type slot/port* 例： `switch(config)# interface ethernet 2/2`	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。このコマンドは、デフォルトでイネーブルになっています。
ステップ 3	**no snmp trap link-status** 例： `switch(config-if)# no snmp trap link-status`	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。このコマンドは、デフォルトでイネーブルになっています。
ステップ 4	**copy running-config startup-config** 例： `switch(config-if)# 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。

インターフェイスの SNMP ifIndex の表示

SNMP ifIndex は、関連するインターフェイス情報をリンクするために複数の SNMP MIB にわたって使用されます。

手順

	コマンドまたはアクション	目的

ステップ 1	**show interface snmp-ifindex**
	
	例：
	`switch# show interface snmp-ifindex | grep -i Eth12/1`
	`Eth12/1 441974784 (0x1a580000)`
		すべてのインターフェイスについて、IF-MIB から永続的な SNMP ifIndex 値を表示します。任意で、| キーワードと **grep** キーワードを使用すると、出力で特定のインターフェイスを検索できます。

TCP による SNMP のワンタイム認証のイネーブル化

TCP セッション上で SNMP に対するワンタイム認証をイネーブルにできます。

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 tcp-session** [**auth**] 例： `switch(config)# snmp-server tcp-session`	TCP セッション上で SNMP に対するワンタイム認証をイネーブルにします。デフォルトではディセーブルになっています。
ステップ 3	**copy running-config startup-config** 例： `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。

SNMP デバイスの連絡先およびロケーション情報の割り当て

32 文字までの長さで（スペースを含まない）デバイスのコンタクト情報とデバイスのロケーションを指定できます。

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 contact***name* 例： `switch(config)# snmp-server contact Admin`	SNMP コンタクト名として sysContact を設定します。
ステップ 3	**snmp-server location***name* 例： `switch(config)# snmp-server location Lab-7`	SNMP ロケーションとして sysLocation を設定します。
ステップ 4	**show snmp** 例： `switch(config)# show snmp`	（任意） 1 つまたは複数の宛先プロファイルに関する情報を表示します。
ステップ 5	**copy running-config startup-config** 例： `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。

コンテキストとネットワーク エンティティ間のマッピング設定

プロトコル インスタンス、VRF などの論理ネットワーク エンティティに対する SNMP コンテキストのマッピングを設定できます。

はじめる前に

論理ネットワーク エンティティのインスタンスを決定します。VRF およびプロトコル インスタンスの詳細については、『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*』または『*Cisco Nexus 7000 Series NX-OS Multicast Routing Configuration Guide*』を参照してください。

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	[**no**] **snmp-server context***context-name* [**instance***instance-name*] [**vrf***vrf-name*] [**topology***topology-name*] 例： `switch(config)# snmp-server context public1 vrf red`	SNMP コンテキストをプロトコル インスタンス、VRF、またはトポロジにマッピングします。Release 6.2(2) 以前では、名前には最大 32 の英数字を使用できます。Release 6.2(2) 以降では、文字列に英数字以外を含めることができます。ただし、ベスト プラクティスは英数字のみを使用することです。 **no** オプションは、SNMP コンテキストとプロトコル インスタンス、VRF、またはトポロジ間のマッピングを削除します。 （注） コンテキストマッピングを削除する目的で、インスタンス、VRF、またはトポロジを入力しないでください。instance、VRF、または topology キーワードを使用すると、コンテキストとゼロ長ストリング間のマッピングが設定されます。
ステップ 3	**snmp-server mib community-map***community-name***context***context-name* 例： `switch(config)# snmp-server mib community-map public context public1`	（任意） SNMPv2c コミュニティを SNMP コンテキストにマッピングします。名前には最大 32 の英数字を使用できます。
ステップ 4	**show snmp context** 例： `switch(config)# show snmp context`	（任意） 1 つまたは複数の SNMP コンテキストに関する情報を表示します。

	コマンドまたはアクション	目的
ステップ 5	**copy running-config startup-config** 例： `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。

SNMP のディセーブル化

デバイスの SNMP をディセーブルにできます。

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	**no snmp-server protocol enable** 例： `switch(config)# no snmp-server protocol enable`	SNMP をディセーブルにします。SNMP はデフォルトでイネーブルになっています。

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。

	コマンドまたはアクション	目的
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 3600 です。
ステップ 3	**copy running-config startup-config** 例： `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。

SNMP の設定の確認

SNMP 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 interface snmp-ifindex	すべてのインターフェイスについて（IF-MIB から）SNMP の ifIndex 値を表示します。
show running-config snmp [**all**]	SNMP の実行コンフィギュレーションを表示します。
show snmp	SNMP ステータスを表示します。
show snmp community	SNMP コミュニティ ストリングを表示します。
show snmp context	SNMP コンテキスト マッピングを表示します。
show snmp engineID	SNMP engineID を表示します。
show snmp group	SNMP ロールを表示します。
show snmp host	設定した SNMP ホストの情報を表示します。

コマンド	目的
show snmp session	SNMP セッションを表示します。
show snmp source-interface	設定した発信元インターフェイスの情報を表示します。
show snmp trap	イネーブルまたはディセーブルである SNMP 通知を表示します。
show snmp user	SNMPv3 ユーザを表示します。

SNMP の設定例

次に、Blue VRF を使用して、ある通知ホスト レシーバに Cisco linkUp または Down 通知を送信するよう Cisco NX-OS を設定し、Admin と NMS という 2 つの SNMP ユーザを定義する例を示します。

```
configure terminal
snmp-server contact Admin@company.com
snmp-server user Admin auth sha abcd1234 priv abcdefgh
snmp-server user NMS auth sha abcd1234 priv abcdefgh engineID
00:00:00:63:00:01:00:22:32:15:10:03
snmp-server host 192.0.2.1 informs version 3 auth NMS
snmp-server host 192.0.2.1 use-vrf Blue
snmp-server enable traps link cisco
```

次に、ホスト レベルで設定された帯域内ポートを使用してトラップを送信するよう、SNMP を設定する例を示します。

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# snmp-server host 171.71.48.164 version 2c public
switch(config)# snmp-server host 171.71.48.164 source-interface ethernet 1/2
switch(config)# show snmp host
-------------------------------------------------------------------
Host Port Version Level Type SecName
-------------------------------------------------------------------
171.71.48.164 162 v2c noauth trap public
Source interface: Ethernet 1/2
-------------------------------------------------------------------
switch(config)# snmp-server host 171.71.48.164 use-vrf default
switch(config)# show snmp host
-------------------------------------------------------------------
Host Port Version Level Type SecName
-------------------------------------------------------------------
171.71.48.164 162 v2c noauth trap public
Use VRF: default
Source interface: Ethernet 1/2
-------------------------------------------------------------------
```

次に、グローバルに設定した帯域内ポートを使用してトラップを送信するよう SNMP を設定する例を示します。

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# snmp-server source-interface traps ethernet 1/2
switch(config)# show snmp source-interface
-----------------------------------------------------------------------
Notification source-interface
-----------------------------------------------------------------------
trap Ethernet1/2
inform -
-----------------------------------------------------------------------
switch(config)# snmp-server host 171.71.48.164 use_vrf default
switch(config)# show snmp host
-----------------------------------------------------------------------
Host Port Version Level Type SecName
-----------------------------------------------------------------------
171.71.48.164 162 v2c noauth trap public
Use VRF: default
Source interface: Ethernet 1/2
-----------------------------------------------------------------------
```

VRF red を SNMPv2c のパブリック コミュニティ ストリングにマッピングする例を示します。

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# vrf context red
switch(config-vrf)# exit
switch(config)# snmp-server context public1 vrf red
switch(config)# snmp-server mib community-map public context public1
```

OSPF インスタンス Enterprise を同じ SNMPv2c パブリック コミュニティ ストリングにマッピングする例を示します。

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# feature ospf
switch(config)# router ospf Enterprise
switch(config-router)# exit
switch(config)# snmp-server context public1 instance Enterprise
switch(config)# snmp-server mib community-map public context public1
```

次の例は、SNMPv3「newstring」コミュニティで IPv4 と IPv6 の両方の ACL を設定する方法を示しています。

```
switch# configure terminal
switch(config)# snmp-server community newstring use-ipv4acl myacl use-ipv6acl myacl1
switch(config)# show running-config snmp
version 6.2(2)
snmp-server aaa exclusive-behavior enable
snmp-server user admin network-admin auth md5 0x2f2429f3c9b21f1adbae8acc7783e355
priv 0x2f2429f3c9b21f1adbae8acc7783e355 localizedkey
rmon event 1 log trap public description FATAL(1) owner PMON@FATAL
rmon event 2 log trap public description CRITICAL(2) owner PMON@CRITICAL
rmon event 3 log trap public description ERROR(3) owner PMON@ERROR
rmon event 4 log trap public description WARNING(4) owner PMON@WARNING
rmon event 5 log trap public description INFORMATION(5) owner PMON@INFO
snmp-server community newstring group network-operator
snmp-server community newstring use-ipv4acl myacl use-ipv6acl myacl1
switch# show snmp community
Community   Group / Access   context acl_filter
newstring   network-operator         ipv4:myacl ipv6:myacl1
switch#
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
ロールバック CLI コマンド	『*Cisco Nexus 7000 Series NX-OS System Management Command Reference*』
VDC	『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』
IP ACL および AAA	『*Cisco Nexus 7000 Series NX-OS Security Configuration Guide*』
MIB	『*Cisco Nexus 7000 Series and 9000 Series NX-OS MIB Quick Reference*』

RFC

RFC	タイトル
RFC 3414	『*User-based Security Model (USM) for Version 3 of the Simple Network Management Protocol (SNMPv3)*』
RFC 3415	『*View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*』

MIB

MIB	MIB のリンク
SNMP に関連する MIB	サポートされている 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。 ftp://ftp.cisco.com/pub/mibs/supportlists/nexus7000/Nexus7000MIBSupportList.html

SNMP の機能の履歴

次の表に、このマニュアルの新機能および変更された機能を要約し、各機能がサポートされているリリースを示します。ご使用のソフトウェア リリースで、本書で説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。

表 *23* : *SNMP* の機能の履歴

機能名	リリース	機能情報
SNMPv3 ユーザとコミュニティ	6.2(2)	IPv4 および IPv6 ACL の両方を同じ SNMPv3 ユーザまたは SNMPv3 コミュニティに適用する機能が追加されました。
SNMPv3	6.2(2)	場所に基づいてユーザを認証するために SNMPv3 サーバの AAA 排他的動作のサポートが追加されました。
SNMP 通知	5.0(2)	**snmp-server enable traps** コマンドが更新されました。
IPv6 サポート	4.2(1)	IPv6 SNMP ホストの設定がサポートされました。
ACL を使用したコミュニティでの SNMP 要求フィルタ	4.2(1)	ACL を SNMP コミュニティに割り当てて SNMP 要求をフィルタします。
SNMP 通知レシーバ用インターフェイスの使用	4.2(1)	インターフェイスを SNMP 通知用の発信元インターフェイスとして機能するよう指定する機能のサポートが追加されました。
SNMP AAA 同期	4.0(3)	同期したユーザ設定のタイムアウトを変更する機能が追加されました。
SNMP プロトコル	4.0(3)	SNMP プロトコルをディセーブルにする機能が追加されました。

第 13 章

RMON の設定

この章では、Cisco NX-OS デバイスでのリモートモニタリング（RMON）機能を設定する方法について説明します。

この章の内容は、次のとおりです。

- 機能情報の確認，245 ページ
- RMON について，246 ページ
- RMON のライセンス要件，247 ページ
- RMON の前提条件，248 ページ
- RMON の注意事項と制約事項，248 ページ
- RMON のデフォルト設定，248 ページ
- RMON の設定，248 ページ
- RMON 設定の確認，251 ページ
- RMON の設定例，251 ページ
- その他の参考資料，252 ページ
- RMON の機能の履歴，252 ページ

機能情報の確認

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

RMON について

RMON は、各種ネットワーク 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、簡易ネットワーク管理プロトコル（SNMP）インターネット技術特別調査委員会（IETF）の標準モニタリング仕様です。Cisco NX-OS では、Cisco NX-OS デバイスをモニタするための、RMON アラーム、イベント、およびログをサポートします。

RMON アラームは、指定された期間、特定の管理情報ベース（MIB）オブジェクトをモニタリングし、指定されたしきい値でアラームを発生させ、別のしきい値でアラームをリセットします。アラームと RMON イベントを組み合わせて使用し、RMON アラームが発生したときにログ エントリまたは SNMP 通知を生成できます。

Cisco NX-OS では、RMON はデフォルトでイネーブルですが、アラームは設定されていません。RMON アラームを設定するには、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。

RMON アラーム

SNMP INTEGER タイプの解決を行う任意の MIB オブジェクトにアラームを設定できます。指定するオブジェクトは、標準のドット付き表記で表した既存の SNMP MIB オブジェクトでなければなりません（たとえば、1.3.6.1.2.1.2.2.1.14 は ifInOctets.14 を表します）。

アラームを作成する場合、次のパラメータを指定します。

- モニタする MIB オブジェクト。
- サンプリング間隔：MIB オブジェクトのサンプル値を収集するのにデバイスが使用する間隔
- サンプル タイプ：絶対サンプルでは、MIB オブジェクト値の現在のスナップショットを使用します。デルタ サンプルは連続した 2 つのサンプルを使用し、これらの差を計算します。
- 上限しきい値：デバイスが上限アラームを発生させる、または下限アラームをリセットする場合の値
- 下限しきい値：デバイスが下限アラームを発生させる、または上限アラームをリセットする場合の値
- イベント：アラーム（上限または下限）の発生時にデバイスが実行するアクション

（注） hcalarms オプションを使用して、アラームを 64 ビットの整数の MIB オブジェクトに設定します。

たとえば、エラー カウンタ MIB オブジェクトにデルタ タイプ上限アラームを設定できます。エラー カウンタ デルタがこの値を超えた場合、SNMP 通知を送信し、上限アラーム イベントを記録するイベントを発生させることができます。この上限アラームは、エラーカウンタのデルタ サンプルが下限しきい値を下回るまで再度発生しません。

（注） 下限しきい値には、上限しきい値よりも小さな値を指定してください。

RMON イベント

特定のイベントを各 RMON アラームにアソシエートさせることができます。RMON は次のイベント タイプをサポートします。

- SNMP 通知：関連したアラームが発生したときに、SNMP risingAlarm または fallingAlarm 通知を送信します。
- ログ：関連したアラームが発生した場合、RMON ログ テーブルにエントリを追加します。
- 両方：関連したアラームが発生した場合、SNMP 通知を送信し、RMON ログ テーブルにエントリを追加します。

下限アラームおよび上限アラームに異なるイベントを指定できます。

（注） デフォルトの RMON イベント テンプレート設定の使用を選択することも、これらのエントリを削除して新しい RMON イベントを作成することもできます。RMON アラーム設定を作成するまで、これらの設定によってトリガーされるアラームはありません。

RMON のハイ アベイラビリティ

Cisco NX-OS は、RMON 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。

RMON の仮想化サポート

Cisco NX-OS は、RMON のインスタンスを 1 つサポートします。

RMON は Virtual Routing and Forwarding（VRF）を認識します。特定の VRF を使用して RMON SMTP サーバに接続するように RMON を設定できます。

RMON のライセンス要件

製品	ライセンス要件
Cisco NX-OS	RMON 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 nx-os イメージにバンドルされており、無料で提供されます。NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

RMON の前提条件

VDC を設定する場合は、適切なライセンスをインストールし、所定の VDC を開始する必要があります。設定情報については『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』、ライセンス情報については『*Cisco NX-OS Licensing Guide*』を参照してください。

RMON の注意事項と制約事項

RMON には、次の注意事項および制限事項があります。

- SNMP 通知イベント タイプを使用するには、SNMP ユーザおよび通知レシーバを設定する必要があります。
- 整数になる MIB オブジェクトにのみ、RMON アラームを設定できます。
- RMON アラームを設定する場合は、オブジェクト ID がインデックスで 1 オブジェクトだけを示すようになっている必要があります。たとえば、1.3.6.1.2.1.2.2.1.14 は cpmCPUTotal5minRev に対応し、.1 は cpmCPUTotalIndex インデックスに対応し、オブジェクト ID の 1.3.6.1.2.1.2.2.1.14.1 を作成します。

RMON のデフォルト設定

次の表に、RMON パラメータのデフォルト設定を示します。

パラメータ	デフォルト
RMON	イネーブル
アラーム	未設定

RMON の設定

（注） この機能の Cisco NX-OS コマンドは、Cisco IOS のコマンドとは異なる場合があるので注意してください。

RMON アラームの設定

任意の整数の SNMP MIB オブジェクトに RMON アラームを設定できます。

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

SNMP ユーザが設定され、SNMP 通知がイネーブルであることを確認します。

はじめる前に

SNMP ユーザが設定され、SNMP 通知がイネーブルであることを確認します。

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	**rmon alarm***index mib-object sample-interval* {**absolute** | **delta**} **rising-threshold***value* [*event-index*] **falling-threshold***value* [*event-index*] [**owner***name*] 例： `switch(config)# rmon alarm 20 1.3.6.1.2.1.2.2.1.14.1 2900 delta rising-threshold 1500 1 falling-threshold 0 owner test`	RMON アラームを作成します。値の範囲は -2147483647 ～ 2147483647 です。オーナー名は任意の英数字ストリングです。
ステップ 3	**rmon hcalarm***index mib-object sample-interval* {**absolute** | **delta**} **rising-threshold-high***value***rising-threshold-low***value* [*event-index*] **falling-threshold-high***value***falling-threshold-low***value* [*event-index*] [**owner***name*] [**storagetype***type*] 例： `switch(config)# rmon alarm 20 1.3.6.1.2.1.2.2.1.14.16777216 2900 delta rising-threshold-high 15 rising-threshold-low 151 falling-threshold-high 0 falling-threshold-low 0 owner test`	RMON 高容量アラームを作成します。値の範囲は -2147483647 ～ 2147483647 です。オーナー名は任意の英数字ストリングです。 ストレージ タイプの範囲は 1 ～ 5 です。

	コマンドまたはアクション	目的
ステップ 4	**show rmon** {**alarms** | **hcalarms**} 例： `switch(config)# show rmon alarms`	（任意） RMON アラームまたは高容量アラームに関する情報を表示します。
ステップ 5	**copy running-config startup-config** 例： `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。

RMON イベントの設定

RMON アラームとアソシエートするよう RMON イベントを設定できます。複数の RMON アラームで同じイベントを再利用できます。

はじめる前に

SNMP ユーザが設定され、SNMP 通知がイネーブルであることを確認します。

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	**rmon event***index* [**description***string*] [**log**] [**trap** *string*] [**owner***name*] 例： `switch(config)# rmon event 1 trap trap1`	RMON イベントを設定します。説明のストリング、トラップのストリングおよびオーナー名は、任意の英数字ストリングにすることができます。
ステップ 3	**show rmon events** 例： `switch(config)# show rmon events`	（任意） RMON イベントに関する情報を表示します。

	コマンドまたはアクション	目的
ステップ 4	**copy running-config startup-config** 例： `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。

RMON 設定の確認

RMON 設定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	RMON アラームに関する情報を表示します。
show rmon events	RMON イベントに関する情報を表示します。
show rmon hcalarms	RMON 高容量アラームに関する情報を表示します。
show rmon logs	RMON ログに関する情報を表示します。

RMON の設定例

ifInOctets.14 にデルタ上限アラームを作成し、このアラームに通知イベントを関連付ける方法の例を示します。

```
configure terminal
rmon alarm 20 1.3.6.1.2.1.2.2.1.14.1 2900 delta rising-threshold 1500 1 falling-threshold
0 owner test
rmon event 1 trap trap1
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
RMON CLI コマンド	『*Cisco Nexus 7000 Series NX-OS System Management Command Reference*』
VDC および VRF	『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』

MIB

MIB	MIB のリンク
RMON に関連する MIB	サポートされている 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。 ftp://ftp.cisco.com/pub/mibs/supportlists/nexus7000/Nexus7000MIBSupportList.html

RMON の機能の履歴

次の表に、このマニュアルの新機能および変更された機能を要約し、各機能がサポートされているリリースを示します。ご使用のソフトウェア リリースで、本書で説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。

表 *24* : *RMON* の機能の履歴

機能名	リリース	機能情報
RMON	4.0(1)	この機能が導入されました。

第 14 章

オンライン診断の設定

この章では、デバイス上で汎用オンライン診断（GOLD）機能を設定する方法について説明します。

この章の内容は、次のとおりです。

- 機能情報の確認，253 ページ
- オンライン診断について，254 ページ
- オンライン診断機能のライセンス要件，263 ページ
- オンライン診断の注意事項と制約事項，263 ページ
- オンライン診断のデフォルト設定，264 ページ
- オンライン診断の設定，264 ページ
- オンライン診断設定の確認，270 ページ
- オンライン診断のコンフィギュレーション例，272 ページ
- その他の参考資料，272 ページ
- オンライン診断の「機能の履歴」表，272 ページ

機能情報の確認

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

オンライン診断について

オンライン診断機能を使用すると、ハードウェアおよび内部データ パスが設計どおりに動作しているかどうかを確認し、障害を迅速に分離できます。

オンライン診断の概要

オンライン診断機能を使用すると、デバイスをアクティブ ネットワークに接続したまま、デバイスのハードウェア機能をテストして確認できます。

オンライン診断機能には、さまざまなハードウェア コンポーネントを検査し、データ パスと制御信号を確認するテストが組み込まれています。中断を伴うオンライン診断テスト（破壊モードのループバック テストなど）、および中断を伴わないオンライン診断テスト（ASIC レジスタ検査など）は、起動時、ライン モジュールの活性挿抜（OIR）時、およびシステム リセット時に実行されます。中断を伴わないオンライン診断テストは、バックグラウンドヘルスモニタリングの一部として実行され、これらのテストはオンデマンドで実行できます。

オンライン診断は、起動、ランタイムまたはヘルスモニタリング診断、およびオンデマンド診断に分類されます。起動診断は起動時に、ヘルスモニタリング テストはバックグラウンドで、オンデマンド診断はアクティブ ネットワークにデバイスが接続されたときに 1 回だけ、またはユーザが指定した間隔で実行されます。

ブートアップ診断

起動診断は起動中に実行され、Cisco NX-OS 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、デバイスに障害モジュールを搭載した場合、起動診断でモジュールがテストされ、デバイスがそのモジュールをトラフィックの転送に使用しないうちに、モジュールがオフラインにされます。

起動診断では、スーパーバイザとモジュール ハードウェア間、およびすべての ASIC のデータ パスと制御パス間の接続も検査されます。

起動診断テストはエラーを Onboard Failure Logging（OBFL）および syslog に記録し、診断の LED 表示（オン、オフ、合格、失敗）を開始します。

起動診断テストをバイパスするようにデバイスを設定することも、またはすべての起動診断テストを実行するように設定することもできます。

（注） オンデマンド方式で起動テストを使用することはできません。

次の表では、モジュールおよびスーパーバイザの起動診断テストについて説明します。

表 *25* : モジュールの起動診断テスト

テスト名	説明	サポートされているモジュール	サポートされないモジュール
EOBCPortLoopback	中断を伴うテストで、オンデマンド型テストではありません。イーサネット帯域外	すべての F1、M1、M3、F2、F2eおよびF2モジュール	—
OBFL	オンボード障害ロギング（OBFL）フラッシュの整合性を確認します。	すべての F1、M1、M3、F2、F2eおよびF2モジュール	—
FIPS	中断を伴うテストで、FIPSがシステム上でイネーブルの場合にのみ実行されます。モジュール上のセキュリティデバイスを検証するためにモジュール起動時に実行される内部テスト。	N7K-M148GS-11 N7K-M148GS-11L N7K-M108X2-12L N7K-M132XP-12 N7K-M132XP-12L すべての M2 モジュール	N7K-M148GT-11 N7K-M148GT-11L すべてのF1モジュール すべてのF2モジュール N7K-F248XT-25E すべてのF3モジュール すべての M3 モジュール
BootupPortLoopback	中断を伴うテストで、オンデマンド型テストではありません。PortLoopbackテストはモジュールの起動時にだけ実行されます。	N7K-M148GS-11 N7K-M148GS-11L N7K-M108X2-12L N7K-M132XP-12 N7K-M132XP-12L すべての M2 モジュール すべてのF1モジュール すべてのF2モジュール すべて F2e モジュール N77-M348XP-23L N77-M324FQ-25L	N7K-M148GT-11 N7K-M148GT-11L すべてのF3モジュール

表 *26*：スーパーバイザの起動診断テスト

テスト名	説明	サポートされているモジュール	サポートされないモジュール
USB	中断を伴わないテスト。モジュールにおけるUSBコントローラの初期化を検査	Sup1、Sup2、およびSup2E	—
CryptoDevice	中断を伴わないテスト。モジュールにおけるCisco Trusted Security（CTS）デバイスの初期化を検査	Sup1	Sup2およびSup2E
ManagementPortLoopback	中断を伴うテストで、オンデマンド型テストではありません。モジュールの管理ポートでループバックをテストします。	Sup1、Sup2、およびSup2E	—
EOBCPortLoopback	中断を伴うテストで、オンデマンド型テストではありません。イーサネット帯域外。	Sup1、Sup2、およびSup2E	—
OBFL	オンボード障害ロギング（OBFL）フラッシュの整合性を確認します。	Sup1、Sup2、およびSup2E	—

ランタイムまたはヘルス モニタリング診断

ランタイム診断はヘルスモニタリング（HM）診断ともいいます。これらの診断テストによって、アクティブ デバイスの状態に関する情報が得られます。ランタイム ハードウェア エラー、メモリ エラー、ハードウェアモジュールの経時的劣化、ソフトウェア障害、およびリソース不足が検出されます。

アクティブネットワークトラフィックを処理するデバイスの状態を確認するランタイム診断テストは、中断を伴わず、バックグラウンドで実行されます。ランタイム テストをイネーブルまたはディセーブルにできます。ランタイム テストのランタイム間隔を変更できます。

（注） 推奨されるベスト プラクティス：ランタイム間隔は、デフォルト値から変更しないでください。

次の表では、モジュールおよびスーパーバイザのランタイム テストについて説明します。

表 *27*：モジュールのランタイム診断テスト

テスト名	説明	デフォルトのインターバル	サポートされているモジュール	サポートされないモジュール
ASICRegisterCheck	モジュール上の ASIC のレジスタをスクラッチするための読み取りと書き込みアクセス権を確認します。	1 分	すべてのモジュール	—
PrimaryBootROM	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。	30 分	すべてのモジュール	—
SecondaryBootROM	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。	30 分	すべてのモジュール	—
PortLoopback	すべての Admin Down ポートで、ポート単位での診断をチェックします。	15 分	N7K-M148GS-11 RF N7K-M148GS-11L N7K-M108X2-12L N7K-M132XP-12 RF N7K-M132XP-12L N77-F348XP-23 すべての M2、F1、F2、F3、および F2e モジュール N77-M348XP-23L N77-M324FQ-25L	N7K-M148GT-11 N7K-M148GT-11L

テスト名	説明	デフォルトのインターバル	サポートされているモジュール	サポートされないモジュール
RewriteEngineLoopback	中断のないポート単位のループバック テストであり、したがって起動中のポートでも実行できます。ファブリック 接続からLC接続までモニタするよう設計されており、スーパーバイザおよびファブリックの障害を検出できます。	1 分	すべての M1、M2、F2、および F2e モジュール N77-M348XP-23L N77-M324FQ-25L	すべての F1 および F3 モジュール
SnakeLoopback	shut 状態ではないポートも含めたすべてのポート上で中断を伴わないループバックを実行します。ポートは、モジュール起動中にスネークに形成され、スーパーバイザはスネーク接続性を定期的にチェックします。	20 分	すべての F1、F2、および F2e モジュール	すべての M1、M2、M3、および F3 モジュール
InternalPortLoopback	中断のないポート単位のループバック テストであり、したがって起動中のポートでも実行できます。	5 分	すべての M2、F2、および F2e モジュール N77-M348XP-23L N77-M324FQ-25L	すべての M1、F1、および F3 モジュール

表 *28*：スーパーバイザのランタイム診断テスト

テスト名	説明	デフォルトのインターバル	サポートされるスーパーバイザ	サポートされないスーパーバイザ
ASICRegisterCheck	モジュール上のASICのレジスタをスクラッチするための読み取りと書き込みアクセス権を確認します。	20秒	Sup1、Sup2、およびSup2E	—
NVRam	スーパーバイザのNVRAMブロックの健全性を確認します。	5分	Sup1、Sup2、およびSup2E	—
RealTimeClock	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。	5分	Sup1、Sup2、およびSup2E	—
PrimaryBootROM	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。	30分	Sup1、Sup2、およびSup2E	—
SecondaryBootROM	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。	30分	Sup1、Sup2、およびSup2E	—
CompactFlash	内蔵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。	30分	Sup1、Sup2、およびSup2E	—

テスト名	説明	デフォルトのインターバル	サポートされるスーパーバイザ	サポートされないスーパーバイザ
ExternalCompactFlash	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。	30 分	Sup1、Sup2、および Sup2E	—
PwrMgmtBus	スタンバイの電源管理制御バスを確認します。	30 秒	Sup1、Sup2、および Sup2E	—
SpineControlBus	スタンバイ スパイン モジュール制御バスの使用可能性を確認します。	30 秒	Sup1 および Sup2	Sup2E
SystemMgmtBus	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。	30 秒	Sup1、Sup2、および Sup2E	—
StatusBus	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。	30 秒	Sup1、Sup2、および Sup2E	—
StandbyFabricLoopback	スパイン カードのクロスバーに対するスタンバイ スーパーバイザの接続を確認します。	30 秒	Sup1、Sup2、および Sup2E	—

テスト名	説明	デフォルトのインターバル	サポートされるスーパーバイザ	サポートされないスーパーバイザ
PCIeBus	スーパーバイザからファブリック カード上のクロスバー ASIC への PCIe 接続を確認します。	30 秒	Sup2 および Sup2E	—

指定のヘルス モニタリング診断のリカバリ アクション

Cisco NX-OS Release 6.2(8) 以前では、ランタイム テストでハードウェア障害が検出されたときに、修正リカバリアクションが実行されませんでした。EEM を通したデフォルト アクション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。これらのアクションは、情報は提供しますが、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ネットワークから除くものではありませんでした。Cisco NX-OS Release 6.2(8) 以前では、ネットワークを回復するには手動でデバイスをシャットダウンする必要があります。

Cisco NX-OS Release 6.2(8) 以降では、以下のいずれかのランタイムまたはヘルス モニタリング テストで障害が検出された場合、中断アクションを実行するようにシステムを設定できます。

- PortLoopback テスト
- RewriteEngineLoopback テスト
- SnakeLoopback テスト
- StandbyFabricLoopback テスト

リカバリ アクション機能は、デフォルトではディセーブルになっています。この機能を使用すると、ヘルス モニタリングまたはランタイム テストでの繰り返しエラーが起きた場合、中断アクションを実行するようにシステムを設定できます。この機能はすべての 4 つのテスト上の修正および保守アクションをイネーブルまたはディセーブルにします。修正アクションはテストによって異なります。テストに対する連続エラー数の最大値を超えた場合、システムは修正アクションを実行します。

リカバリ アクション機能がイネーブルの場合、各テストでの修正アクションは次のとおりです。

- PortLoopback テスト：システムは、障害を登録しているポートを error-disabled ステートに移動します。
- RewriteEngineLoopback テスト：システムは障害がスーパーバイザ、ファブリック、またはポートのどこで発生しているかに応じて以下のような異なる修正アクションを実行します。

- スタンバイ スーパーバイザを持つシャーシで、システムがスーパーバイザに障害を検出すると、システムはスタンバイ スーパーバイザに切り替えます。シャーシにスタンバイ スーパーバイザがない場合、システムはアクションを実行しません。
- ファブリックに障害が発生すると、システムはファブリックを3回リロードします。失敗が続行する場合、システム電力がファブリックでダウンになっています。
- ポートに障害が発生すると、システムは障害ポートをerror-disabledステートに移動します。

- SnakeLoopbackテスト：テストがモジュール上のいずれかのポートでエラーを10回連続で検出した場合、システムは障害ポートをerror-disabledステートに移動します。
- StandbyFabricLoopbackテスト：このテストでエラーを検出した後、システムはスタンバイ スーパーバイザのリロードを3回試行します。システムがスタンバイ スーパーバイザをリロードできない場合、システムはスーパーバイザの電源をオフにします。

最後に、システムは、各アクションの詳細、テストのタイプ、および重大度を含むリカバリ アクションの履歴を保持します。これらのカウンタは表示可能です。

オンデマンド診断

オンデマンドテストは、障害の場所を特定するのに役立ちます。通常は、次のような状況で必要です。

- 障害の分離など、発生したイベントに対処する場合。
- リソース使用限度の超過などのイベントの発生が予測される場合。

すべてのヘルスモニタリングテストをオンデマンドで実行できます。即時実行するオンデマンド診断テストをスケジューリングできます。

ヘルス モニタリング テストのデフォルト インターバルも変更可能です。

ハイ アベイラビリティ

ハイアベイラビリティの重要な要素は、アクティブネットワークでデバイスが動作しているときに、ハードウェア障害を検出して対策を取ることです。ハイ アベイラビリティのオンライン診断では、ハードウェア障害を検出して、スイッチオーバーを判断するためにハイ アベイラビリティ ソフトウェアにフィードバックします。

Cisco NX-OSは、オンライン診断のステートレス 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。

仮想化のサポート

Cisco NX-OS は、デフォルトの仮想デバイス コンテキスト（VDC）、または Cisco NX-OS Release 6.1 からは管理 VDC でのオンライン診断をサポートします。デフォルトでは、Cisco NX-OS はデフォルト VDC に配置します。

オンライン診断機能は Virtual Routing and Forwarding（VRF）を認識します。特定の VRF を使用してオンライン診断 SMTP サーバに接続するようにオンライン診断機能を設定できます。

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 Cisco NX-OS イメージにバンドルされており、無料で提供されます。NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

オンライン診断の注意事項と制約事項

オンライン診断には、次の注意事項と制限事項があります。

- 中断を伴うオンライン診断テストをオンデマンド方式で実行することはできません。
- F1 シリーズ モジュールは、ASICRegisterCheck、PrimaryBootROM、SecondaryBootROM、EOBCPortLoopback、PortLoopback および BootupPortLoopback のテストをサポートします。
- F1 シリーズ モジュール上の RewriteEngineLoopback および SnakeLoopback テストのサポートは Cisco NX-OS Release 5.2 で非推奨になりました。
- Cisco NX-OS Release 6.1 以降では、F2 シリーズ モジュールが RewriteEngineLoopback および SnakeLoopback テストをサポートします。
- Cisco NX-OS Release 7.3(0)DX(1) 以降では、M3 シリーズ モジュールが汎用オンライン診断をサポートします。

M3 シリーズでは、次の汎用オンライン診断がサポートされます。

表 *29*：*M3* シリーズでサポートされる汎用オンライン診断

ASICRegisterCheck	ヘルス モニタリング/オンデマンド
PrimaryBootROM	ヘルス モニタリング/オンデマンド

SecondaryBootROM	ヘルス モニタリング/オンデマンド
EOBCPortLoopback	ブートアップ テストのみ
OBFL	ブートアップ テストのみ
PortLoopback	port admin がダウンした場合のヘルス モニタリング/オンデマンドのみ
RewriteEngineLoopback	ヘルス モニタリング/オンデマンド
IntPortLoopback	ヘルス モニタリング/オンデマンド
BootupPortLoopback	ブートアップ テストのみ

オンライン診断のデフォルト設定

次の表に、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。

パラメータ	デフォルト
起動時診断レベル	complete
中断を伴わないテスト	active

オンライン診断の設定

（注） この機能の Cisco NX-OS コマンドは、Cisco IOS のコマンドとは異なる場合があるので注意してください。

起動診断レベルの設定

一連のすべてのテストを実行するように起動診断機能を設定することも、またはモジュールが短時間で起動するように、すべての起動診断テストをバイパスするように設定することもできます。

（注） 起動時オンライン診断レベルを complete に設定することを推奨します。起動時オンライン診断をバイパスすることは推奨しません。

はじめる前に

正しい VDC 内にいることを確認します。VDC の変更は **switchto vdc** コマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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	switch(config)# **diagnostic bootup level** {**complete** | **bypass**}	デバイスの起動に続いて診断テストが開始されるように、起動診断レベルを設定します。 • **complete**：すべての起動診断テストを実行します。complete がデフォルトです。 • **bypass**：起動診断テストを実行しません。
ステップ 3	switch(config)# **show diagnostic bootup level**	（任意） 現在、デバイスで実行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	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。

診断テストのアクティブ化

診断テストをアクティブに設定し、任意でテストの実行間隔（時間、分、秒単位）を変更できます。

（注） 推奨されるベスト プラクティス：ランタイム間隔は、デフォルト値から変更しないでください。

はじめる前に

正しい VDC 内にいることを確認します。VDC の変更は **switchto vdc** コマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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	switch(config)# **diagnostic monitor interval module***slot***test** [*test-id* | *name* | **all**] **hour***hour***min***minute***second***second*	（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。 引数の範囲は次のとおりです。 • *slot*：範囲は 1 ～ 10 です。 • *test-id*：範囲は 1 ～ 14 です。 • *name*：最大 32 の英数字を使用できます。大文字と小文字は区別されます。 • *hour*：範囲は 0 ～ 23 時間です。 • *minute*：範囲は 0 ～ 59 分です。 • *second*：範囲は 0 ～ 59 秒です。
ステップ 3	switch(config)# [**no**] **diagnostic monitor module***slot***test** [*test-id* | *name* | **all**]	指定されたテストをアクティブにします。 引数の範囲は次のとおりです。 • *slot*：範囲は 1 ～ 10 です。 • *test-id*：範囲は 1 ～ 14 です。 • *name*：最大 32 の英数字を使用できます。大文字と小文字は区別されます。 このコマンドの [**no**] 形式は、指定されたテストを非アクティブにします。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、スケジュール上のインターバルではテストは実行されません。
ステップ 4	switch(config)# **show diagnostic content module** {*slot* | **all**}	（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。

診断テストを非アクティブとして設定する場合

診断テストを非アクティブとして設定できます。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、スケジュール上のインターバルではテストは実行されません。

グローバルコンフィギュレーションモードで診断テストを非アクティブとして設定するには、次のコマンドを使用します。

コマンド	目的
no diagnostic monitor module slot test [test-id|name | all]	指定されたテストを非アクティブにします。 各キーワードで次の範囲が有効です。 • **slot**：範囲は 1 ～ 10 です。 • **test-id**：範囲は 1 ～ 14 です。 • **name**：最大 32 の英数字を使用できます。大文字と小文字は区別されます。

修正アクションの設定

以下のランタイム診断テストで障害が検出された場合に修正アクションを実行するようにデバイスを設定できます。

- PortLoopback
- RewriteEngineLoopback
- SnakeLoopback
- StandbyFabricLoopback

（注） この機能はすべての4つのテスト上の修正および保守アクションをイネーブルまたはディセーブルにします。修正アクションはテストによって異なります。

はじめる前に

正しい VDC 内にいることを確認します。VDC を変更するには、**switchto vdc** コマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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	switch(config)# [**no**] **diagnostic eem action conservative**	PortLoopback、RewriteEngineLoopback、SnakeLoopback、InternalPortLoopback および StandbyFabricLoopback テストでシステムが障害を検出した場合に、修正アクションをイネーブルまたはディセーブルにします。 （注） これらの修正アクションをディセーブルにするには、コマンドの **no** 形式を使用します。
ステップ 3	switch# **event gold** [**failure-type** {**sup** | **fabric** | **lc** | **port**}] **module** {*module* | **all**} **test** {*test-name* | *test-id*} [**severity** {**major** | **minor** | **moderate**}] **testing-type** {**bootup** | **monitoring** | **ondemand** | **scheduled**} **consecutive-failure***count*	名前で指定されたオンライン診断テストが、設定された回数だけ連続して、設定された重大度で失敗した場合に、イベントを発生させます。 *module* は、モニタする必要があるモジュールの番号を指定します。 *test-name* は設定されたオンライン診断テストの名前です。*test-id* は、イベント条件のテスト ID を指定します。値の範囲は 1 ～ 30 です。 *count* の範囲は 1 ～ 1000 です。 （注） この CLI コマンドを使用して、GOLD システムのデフォルト ポリシーの連続エラー数も変更できます。

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を開始または中止できます。任意で、このテストを繰り返す回数の変更や、テストが失敗した場合のアクションの変更を行えます。

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、破壊モードの診断テストを開始する場合は、手動での開始に限定することを推奨します。

はじめる前に

正しい VDC 内にいることを確認します。VDC を変更するには、**switchto vdc** コマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **diagnostic ondemand iteration***number*	（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	switch# **diagnostic ondemand action-on-failure** {**continue failure-count***num-fails* | **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。*num-fails* の範囲は 1 ～ 999 です。デフォルトは 1 です。
ステップ 3	switch# **diagnostic start module***slot***test** [*test-id* | *name* | **all** | **non-disruptive**] [**port***port-number* | **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。モジュール スロットの範囲は 1 ～ 10 です。*test-id* の範囲は 1 ～ 14 です。テスト名は大文字と小文字を区別し、最大 32 の英数字を使用できます。ポート範囲は 1 ～ 48 です。
ステップ 4	switch# **diagnostic stop module***slot***test** [*test-id* | *name* | **all**]	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。モジュール スロットの範囲は 1 ～ 10 です。*test-id* の範囲は 1 ～ 14 です。テスト名は大文字と小文字を区別し、最大 32 の英数字を使用できます。
ステップ 5	switch# **show diagnostic status module***slot*	（任意） 診断テストがスケジューリングされていることを確認します。

診断結果の消去

診断テスト結果を消去できます。

診断テストの結果を消去するには、任意のモードで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**}	指定されたテストのテスト結果を消去します。 有効な範囲は次のとおりです。 • *slot*：範囲は 1 ～ 10 です。 • *test-id*：範囲は 1 ～ 14 です。

診断結果のシミュレーション

診断テスト結果をシミュレートできます。

次のコマンドをいずれかのモードで使用して、診断テスト結果をシミュレートするか、またはシミュレーション テスト結果をクリアします。

コマンド	目的
diagnostic test simulation module*slot***test***test-id* {**fail** | **random-fail** | **success**} [**port***number* | **all**]	指定されたテストのテスト結果をシミュレートします。 有効な範囲は次のとおりです。 • *slot*：範囲は 1 ～ 10 です。 • *test-id*：範囲は 1 ～ 14 です。 • **port***number*：範囲は 1 ～ 48 です。
diagnostic test simulation module*slot***test***test-id***clear**	指定されたテストのシミュレーション結果を消去します。 有効な範囲は次のとおりです。 • *slot*：範囲は 1 ～ 10 です。 • *test-id*：範囲は 1 ～ 14 です。

オンライン診断設定の確認

オンライン診断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 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。

コマンド	目的
show diagnostic eem [**action** [**description**] | **policy module** {*module number* | **all**}]	レベルに設定されている Embedded Event Manager（EEM）アクション レベルと EEM ポリシーを表示します。
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。
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 event manager events action-log event-type [**gold** | **gold_sup_failure** | **gold_fabric_failure** | **gold_module_failure** | **gold_port_failure**]	スイッチオーバー、リロード、電源切断の数、およびタイムスタンプ、障害理由、モジュール ID、ポートリスト、テスト名、テスト タイプ、および重大度を含む、指定の障害のリカバリ アクション履歴を表示します。このデータは異常リロード時も保持されます。
show hardware capacity [**eobc** | **forwarding** | **interface** | **module** | **power**]	ハードウェアの機能、およびシステムによる現在のハードウェア使用率の情報を表示します。
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。

オンライン診断のコンフィギュレーション例

この例は、モジュール 6 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、モジュール 6 でテストテスト 2 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

内容	マニュアル タイトル
オンライン診断 CLI コマンド	『*Cisco Nexus 7000 Series NX-OS System Management Command Reference*』
VDC および VRF	『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』

オンライン診断の「機能の履歴」表

次の表に、この機能のリリース履歴を示します。

機能名	リリース	機能情報
オンライン診断（GOLD）	7.3(0)DX(1)	M3 シリーズ モジュールでの次の診断テストのサポートが追加されました。ASICRegisterCheck、PrimaryBootROM、SecondaryBootROM、EOBCPortLoopback、OBFL、PortLoopback、RewriteEngineLoopback、IntPortLoopback、および IntPortLoopback。
オンライン診断（GOLD）	7.2(0)D1(1)	この機能が導入されました。

機能名	リリース	機能情報
オンライン診断（GOLD）	6.2(10)	• PortLoopbackテストに、N77-F348XP-23モジュールのサポートが追加されました。 • すべてのM2、F2、およびF2eモジュールでのInternalPortLoopbackテストのサポートが追加されました。
指定のヘルス モニタリング診断でのリカバリ アクション。	6.2(8)	次のランタイム診断テストでリカバリアクションを設定できます。PortLoopback、RewriteEngineLoopback、SnakeLoopback、およびStandbyFabricLoopback。
オンライン診断（GOLD）	6.2(6)	N77-F348XP-23を除くすべてのF3モジュールのサポートが追加されました。
オンライン診断（GOLD）	6.1(1)	• スーパーバイザ2およびM2シリーズモジュールのサポートが追加されました。 • F2シリーズモジュールでのRewriteEngineLoopbackおよびSnakeLoopbackテストのサポートが追加されました。 • 管理VDCでオンライン診断設定に対するサポートを追加しました。
オンライン診断（GOLD）	5.2(1)	• スタンバイ スーパーバイザのSpineControlBusテストがイネーブルになりました。 • F1シリーズモジュールのSnakeLoopbackテストが非推奨になりました。
オンライン診断（GOLD）	5.1(2)	F1シリーズモジュールでのSnakeLoopbackテストのサポートが追加されました。
オンライン診断（GOLD）	5.1(1)	FIPSおよびBootupPortLoopbackテストのサポートが追加されました。
オンライン診断（GOLD）	4.2(1)	PortLoopback、StatusBus、およびStandbyFabricLoopbackテストのサポートが追加されました。
オンライン診断（GOLD）	4.0(1)	この機能が導入されました。

第 15 章

Embedded Event Manager の設定

この章では、Embedded Event Manager（EEM）を設定して Cisco NX-OS デバイス上のクリティカル イベントを検出し、対処する方法について説明します。

この章は、次の項で構成されています。

- 機能情報の確認，275 ページ
- EEM について，276 ページ
- EEM のライセンス要件，280 ページ
- EEM の前提条件，280 ページ
- EEM の注意事項と制約事項，281 ページ
- EEM のデフォルト設定，281 ページ
- EEM の設定，282 ページ
- EEM 設定の確認，307 ページ
- EEM のコンフィギュレーション例，308 ページ
- 関連資料，309 ページ
- EEM の機能の履歴，309 ページ

機能情報の確認

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

EEM について

EEM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 は次の 3 種類の主要コンポーネントからなります。

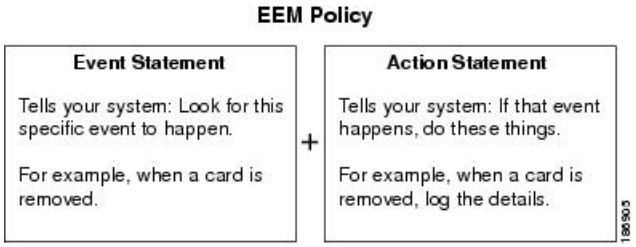
- イベント文：別の Cisco NX-OS コンポーネントからモニタし、アクション、回避策、または通知が必要になる可能性のあるイベント。
- アクション文：電子メールの送信、インターフェイスのディセーブル化など、イベントから回復するために EEM が実行できるアクション。
- ポリシー：イベントのトラブルシューティングまたはイベントからの回復を目的とした 1 つまたは複数のアクションとペアになったイベント。

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。

この図は、EEM ポリシーの基本的な 2 種類の文を示します。

図 *2*：*EEM* ポリシー文



コマンドライン インターフェイス（CLI）または VSH スクリプトを使用して EEM ポリシーを設定できます。

EEM からデバイス全体のポリシー管理ビューが得られます。スーパーバイザ上で EEM ポリシーを設定すると、EEMがイベントタイプに基づいて、正しいモジュールにポリシーをプッシュします。EEMはモジュール上でローカルに、またはスーパーバイザ上で（デフォルトのオプション）、発生したイベントに対応するアクションを実行します。

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。

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 ポリシーを作成すると、そのポリシーと同じイベントに関連するシステム ポリシー アクションが EEM によって発生したあと、ユーザ ポリシーで指定したアクションが行われます。

一部のシステムポリシーは上書きすることもできます。設定した上書き変更がシステムポリシーの代わりになります。イベントまたはアクションの上書きが可能です。

設定済みのシステム ポリシーを表示して、上書き可能なポリシーを判断するには、**show event manager system-policy** コマンドを使用します。

（注） **show running-config eem** コマンドを使用して、各ポリシーのコンフィギュレーション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。

（注） 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。

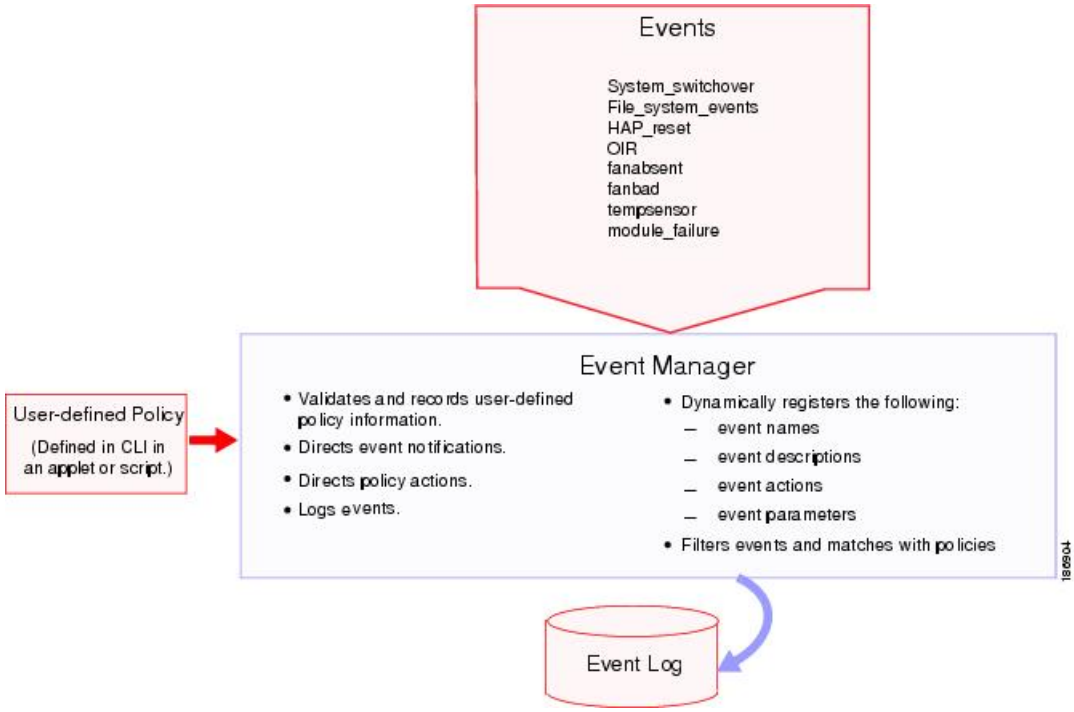
イベント文

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。

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。

この図は、EEM によって処理されたイベントを示します。

図 *3*：*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。複数イベント トリガーを設定できます。

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。

（注） 発生したイベントでデフォルトのアクションを処理できるようにする場合は、event-default アクション文を許可して EEM ポリシーを設定する必要があります。

アクション ステートメント

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
- デバイスのリロード。
- 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。

（注） 発生したイベントでデフォルトのアクションを処理できるようにする場合は、デフォルトのアクションを許可する EEM ポリシーを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。

（注） 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。VSHスクリプト ポリシーを書き込んだ後、デバイスにコピーしてアクティブにします。

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。

この例では、「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.”
```

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 foreshut 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。

EEM イベント相関

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**、**ANDNOT**）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。

ハイ アベイラビリティ

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。

仮想化のサポート

ログインした仮想デバイス コンテキスト（VDC）で、EEM を設定します。デフォルトでは、Cisco NX-OS はデフォルト VDC に配置します。モジュールベースのイベントに対応するポリシーを設定する場合は、この VDC を使用する必要があります。

すべての VDC ですべてのアクションまたはイベントを確認できるわけではありません。ポリシーを設定するには、network-admin または vdc-admin の権限が必要です。

VDC の詳細については、『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』を参照してください。

EEM のライセンス要件

製品	ライセンス要件
Cisco 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 nx-os イメージにバンドルされており、無料で提供されます。NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

EEM の前提条件

EEM の前提条件は、次のとおりです。

- 非デフォルト VDC で EEM を設定するには、admin のユーザ名（network-admin または vdc admin ユーザ権限を所有）が必要です。

EEM の注意事項と制約事項

EEM に関する設定時の注意事項および制約事項は、次のとおりです。

- 設定可能な EEM ポリシーの最大数は 500 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。
- 発生したイベントでデフォルトのアクションを処理できるようにする場合は、デフォルトのアクションを許可する EEM ポリシーを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。
- 通常のコマンド式に適用できるルールは、すべてのキーワードを拡張する必要があること、そして * 記号のみが引数の置換に使用できることです。
- EEM イベント相関はスーパーバイザ モジュールだけでサポートされます。
- EEM イベント相関は、単一ポリシー内の別のモジュール間ではサポートされません。
- EEM イベント相関は 1 つのポリシーに最大 4 つのイベント文をサポートします。イベント タイプは同じでも別でもかまいませんが、サポートされるイベント タイプは、cli、カウンタ、モジュール、モジュール障害、oir、snmp、syslog だけです。
- 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。
- EEM イベント相関はシステムのデフォルト ポリシーを上書きしません。
- デフォルト アクション実行は、タグ付きのイベントで設定されているポリシーではサポートされません。
- Python から EEM を呼び出すことができます。Python の詳細については、『*Cisco Nexus 7000 Series NX-OS Programmability Guide*』を参照してください。

EEM のデフォルト設定

次の表に、EEM パラメータのデフォルト設定を示します。

パラメータ	デフォルト
システム ポリシー	Active

EEM の設定

システムポリシーに基づいて実行されるアクションを含むポリシーを作成できます。システムポリシーに関する情報を表示するには、**show event manager system-policy** コマンドを使用します。

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	**event manager environment***variable-name variable-value* 例： `switch(config)# event manager environment emailto “admin@anyplace.com”`	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** {*variable-name* | **all**} 例： `switch(config)# show event manager environment all`	（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** 例： `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。

CLI によるユーザ ポリシーの定義

CLI を使用して、デバイスにユーザ ポリシーを定義できます。

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	**event manager applet***applet-name*
	
	例：
	`switch(config)# event manager applet monitorShutdown`
	`switch(config-applet)#`
		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* 例： `switch(config-applet)# description "Monitors interface shutdown."`	（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* 例： `switch(config-applet)# event cli match "shutdown"`	ポリシーのイベント文を設定します。イベント文が複数ある場合、このステップを繰り返します。イベント文の設定，（284 ページ）を参照してください。
ステップ 5	**tag***tag* {**and** | **andnot** | **or**} *tag* [**and** | **andnot** | **or** {*tag*}] {**happens***occurs in seconds*} 例： `switch(config-applet)# tag one or two happens 1 in 10000`	（任意） ポリシー内の複数のイベントを相互に関連付けます。 *occurs* 引数の範囲は 1 ～ 4294967295 です。*seconds* 引数の範囲は 0～4294967295 秒です。
ステップ 6	**action***label* **action-statement*** 例： `switch(config-applet)# action 1.0 cli show interface e 3/1`	ポリシーのアクション文を設定します。アクション文が複数ある場合、このステップを繰り返します。アクション文の設定，（291 ページ）を参照してください。
ステップ 7	**show event manager policy-state***name* [**module***module-id*] 例： `switch(config-applet)# show event manager policy-state monitorShutdown`	（任意） 設定したポリシーの状態に関する情報を表示します。

	コマンドまたはアクション	目的
ステップ 8	**copy running-config startup-config** 例： `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。

イベント文の設定

イベント文を設定するには、アプレット 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
event application [**tag***tag*] **sub-system***sub-system-id***type***event-type* 例： `switch(config-applet)# event application sub-system 798 type 1`	イベントの指定がサブシステム ID およびアプリケーション イベント タイプに一致する場合に、イベントを発生させます。 *sub-system-id* と *event-type* の範囲は 1 ～ 4294967295 です。 **tag***tag* 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。 （注） このコマンドを使用するには、まず **feature evmed** コマンドをイネーブルにすることで一般的なイベント ディテクタをイネーブルにする必要があります。
event cli [**tag***tag*] **match***expression* [**count***repeats* | **time***seconds*] 例： `switch(config-applet)# event cli match "shutdown"`	正規表現と一致するコマンドが入力された場合に、イベントを発生させます。 **tag***tag* 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。

コマンド	目的
event counter [**tag***tag*] **name***counter***entry-val***entry***entry-op** {**eq** | **ge** | **gt** | **le** | **lt** | **ne**} [**exit-val***exit***exit-op** {**eq** | **ge** | **gt** | **le** | **lt** | **ne**}] 例： `switch(config-applet)# event counter name mycounter entry-val 20 gt`	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。 **tag***tag* 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。 *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* 例： `switch(config-applet)# event fanabsent time 300`	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。*number* の範囲はモジュールに依存します。*repeats* の範囲は 10 ～ 64000 です。
event fanbad [**fan***number*] **time***seconds* 例： `switch(config-applet)# event fanbad time 3000`	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。*number* の範囲はモジュールに依存します。*repeats* の範囲は 10 ～ 64000 です。
event fib {**adjacency extra** | **resource tcam usage** | **route** {**extra** | **inconsistent** | **missing**}} 例： `switch(config-applet)# event fib adjacency extra`	次のいずれかに対するイベントを発生させます。 • **adjacency extra**：ユニキャスト FIB に追加のルートがある場合。 • **resource tcam usage**：TCAM 使用率がいずれかの方向で 5 の倍数になるごとに。 • **route** {**extra** | **inconsistent** | **missing**}：ユニキャスト FIB でルートが追加、変更、または削除される場合。

コマンド	目的
event gold [**failure-type** {**sup** | **fabric** | **lc** | **port**}] **module** {*module* | **all**} **test** {*test-name* | *test-id*} [**severity** {**major** | **minor** | **moderate**}] **testing-type** {**bootup** | **monitoring** | **ondemand** | **scheduled**} **consecutive-failure***count* 例： `switch(config-applet)# event gold failure-type module 2 test 7 ASICRegisterCheck testing-type ondemand consecutive-failure 2`	名前で指定されたオンライン診断テストが、設定された回数だけ連続して、設定された重大度で失敗した場合に、イベントを発生させます。 *module* は、モニタする必要があるモジュールの番号を指定します。 *test-name* は設定されたオンライン診断テストの名前です。*test-id* は、イベント条件のテスト ID を指定します。値の範囲は 1 ～ 30 です。 *count* の範囲は 1 ～ 1000 です。
event interface [**tag***tag*] {**name***interface slot*/*port***parameter**} 例： `switch(config-applet)# event interface ethernet 2/2 parameter`	カウンタが指定のインターフェイスに対して超えた場合に、イベントを発生させます。 **tag***tag* 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。 （注） このコマンドを使用するには、まず **feature evmed** コマンドをイネーブルにすることで一般的なイベント ディテクタをイネーブルにする必要があります。
event memory {**critical** | **minor** | **severe**} 例： `switch(config-applet)# event memory critical`	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。メモリのしきい値の設定，（304 ページ）も参照してください。
event module [**tag***tag*] **status** {**online** | **offline** | **any**} **module** {**all** | *module-num*} 例： `switch(config-applet)# event module status offline module all`	指定したモジュールが選択された状態になったときにイベントを発生させます。 **tag***tag* 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。

コマンド	目的
event module-failure [**tag***tag*] **type***failure-type***module** {*slot* | **all**} **count***repeats* [**time***seconds*] 例： `switch(config-applet)# event module-failure type lc-failed module 3 count 1`	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。 **tag***tag* 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 0 ～ 4294967295 です。*seconds* の範囲は 0 ～ 4294967295 秒です。0 は無制限を示します。
event none 例： `switch(config-applet)# event none`	手動で指定されたイベントがないポリシー イベントを実行します。 （注） このコマンドを使用するには、まず **feature evmed** コマンドをイネーブルにすることで一般的なイベント ディテクタをイネーブルにする必要があります。
event oir [**tag***tag*] {**fan** | **module** | **powersupply**} {**anyoir** | **insert** | **remove**} [*number*] 例： `switch(config-applet)# event oir fan remove 4`	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。 **tag***tag* 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。 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：モジュール依存 • モジュール番号：デバイス依存 • 電源モジュール番号：範囲は 1 ～ 3 です。

コマンド	目的
event policy-default count*repeats* [**time***seconds*] 例： `switch(config-applet)# event policy-default count 3`	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。*seconds* の範囲は 0 ～ 4294967295 秒です。0 は無制限を示します。
event poweroverbudget 例： `switch(config-applet)# 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。
event snmp [**tag***tag*] **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* 例： `switch(config-applet)# event snmp oid 1.3.6.1.2.1.31.1.1.1.6 get-type next entry-op lt 300 entry-val 0 exit-op eq 400 exit-time 30 polling-interval 300`	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。 **tag***tag* 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。 *entry* および *exit* の値の範囲は 0 ～ 18446744073709551615 です。time の範囲は 0 ～ 2147483647 秒です。interval の範囲は 1 ～ 2147483647 秒です。
event storm-control 例： `switch(config-applet)# event storm-control`	ポート上のトラフィックが設定されたストーム制御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 syslog [**occurs***count*] {**pattern***string* | **period***time* | **priority***level* | **tag***tag*} 例： `switch(config-applet)# event syslog period 500`	指定した syslog のしきい値を超えた場合にイベントを発生させます。カウントの範囲は 1 ～ 65000 で、時間の範囲は 1 ～ 4294967295 です。プライオリティの範囲は 0 ～ 7 です。 **tag***tag* 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。
event sysmgr memory [**module***module-num*] **major***major-percent***minor***minor-percent***clear***clear-percent* 例： `switch(config-applet)# event sysmgr memory minor 80`	指定したシステム マネージャの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。パーセンテージの範囲は 1 ～ 99 です。
event sysmgr switchover count*count***time***interval* 例： `switch(config-applet)# event sysmgr switchover count 10 time 1000`	指定した switchover count が、指定した time interval を超えた場合にイベントを発生させます。switchover count の範囲は 1 ～ 65000 です。time interval の範囲は 0 ～ 2147483647 です。
event temperature [**module***slot*] [*sensor-number*] **threshold** {**any** | **major** | **minor**} 例： `switch(config-applet)# event temperature module 2 threshold any`	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。sensor の範囲は 1 ～ 18 です。

コマンド	目的
event timer {**absolute time***time***name***name* | **countdown time***time***name***name* | **cron cronentry***string* | **tag***tag* | **watchdog time***time***name***name*} 例： `switch(config-applet)# event timer absolute time 100 name abtimer`	指定した時間に到達した場合に、イベントを発生させます。時間の範囲は 1 ～ 4294967295 です。 • **absolute time**：指定された絶対時刻が発生した場合に、イベントを発生させます。 • **countdown time**：指定された時間がゼロにカウントダウンされたときに、イベントを発生させます。タイマーはリセットされません。 • **cron cronentry**：CRON 文字列の指定が現在時刻に一致する場合に、イベントを発生させます。 • **watchdog time**：指定された時間がゼロにカウントダウンされたときに、イベントを発生させます。タイマーは、初期値に自動的にリセットされ、カウント ダウンが続行されます。 **tag***tag* 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。 （注） このコマンドを使用するには、まず **feature evmed** コマンドをイネーブルにすることで一般的なイベント ディテクタをイネーブルにする必要があります。

コマンド	目的
event track [**tag***tag*] *object-number***state** {**any** | **down** | **up**} 例： `switch(config-applet)# event track 1 state down`	トラッキング対象オブジェクトが設定された状態になった場合に、イベントを発生させます。 **tag***tag* 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。 指定できる *object-number* の範囲は 1 ～ 500 です。

アクション文の設定

アクション文を設定するには、アプレット コンフィギュレーション（config-applet）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*label***cli***command1* [*command2...*][**local**] 例： `switch(config-applet)# action 1.0 cli "show interface e 3/1"`	設定された CLI コマンドを実行します。任意で、イベントが発生したモジュール上でコマンドを実行できます。 アクション ラベルのフォーマットは number1.number2 です。*number1* 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*label***counter name***counter***value***val***op** {**dec** | **inc** | **nop** | **set**} 例： `switch(config-applet)# action 2.0 counter name mycounter value 20 op inc`	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。*number1* 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 28 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。

コマンド	目的
action*label***event-default** 例： `switch(config-applet)# action 1.0 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。*number1* 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*label***forceshut** [**module***slot* | **xbar***xbar-number*] **reset-reason***seconds* 例： `switch(config-applet)# action 1.0 forceshut module 2 reset-reason "flapping links"`	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。*number1* 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。 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*label***overbudgetshut** [**module***slot*[*-slot*]] 例： `switch(config-applet)# action 1.0 overbudgetshut module 3-5`	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。 アクション ラベルのフォーマットは number1.number2 です。*number1* 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*label***policy-default** 例： `switch(config-applet)# action 1.0 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。*number1* 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*label***publish-event** 例： `switch(config-applet)# action 1.0 publish-event`	アプリケーション固有のイベントの発行を強制します。 アクション ラベルのフォーマットは number1.number2 です。*number1* 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。

コマンド	目的
action*label***reload** [**module***slot*[-*slot*]] 例： `switch(config-applet)# action 1.0 reload module 3-5`	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。 アクション ラベルのフォーマットは number1.number2 です。*number1* 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*label***snmp-trap** {[**intdata1***data* [**intdata2***data*]] [**strdata***string*]} 例： `switch(config-applet)# action 1.0 snmp-trap strdata "temperature problem"`	設定されたデータを使用して SNMP トラップを送信します。 アクション ラベルのフォーマットは number1.number2 で、*number1* 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。 *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*label***syslog** [**priority***prio-val*] **msg***error-message* 例： `switch(config-applet)# action 1.0 syslog priority notifications msg "cpu high"`	設定されたプライオリティで、カスタマイズした syslog メッセージを送信します。 アクション ラベルのフォーマットは number1.number2 です。*number1* 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 80 文字の英数字を引用符で囲んで使用できます。
action*label***end** 例： `switch(config-applet)# action 1.0 end`	if/else および while などの条件付きアクションブロックの終了を識別します。 アクション ラベルのフォーマットは number1.number2 です。*number1* 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*label***exit** [*result*] 例： `switch(config-applet)# action 1.0 exit 25`	現在実行中のアプレット コンフィギュレーション モードを終了します。 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。

コマンド	目的
action*label***else** 例： `switch(config-applet)# action 1.0 else`	*if/else* 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識別します。 アクション ラベルのフォーマットは number1.number2 です。*number1* 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*label***elseif***string-1* {**eq** | **gt** | **ge** | **lt** | **le** | **ne**} *string-2* `switch(config-applet)# action 1.0 elseif $x ge 10`	*else/if* 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識別します。 アクション ラベルのフォーマットは number1.number2 です。*number1* 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*label***if***string-1* {**eq** | **gt** | **ge** | **lt** | **le** | **ne**} *string-2* `switch(config-applet)# action 1.0 if $x lt 10`	*if* 条件付きアクション ブロックの開始を識別します。 アクション ラベルのフォーマットは number1.number2 です。*number1* 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*label***if***string-1* {**eq** | **gt** | **ge** | **lt** | **le** | **ne**} *string-2***goto***label* `switch(config-applet)# action 2.0 if $x lt 10 goto 1.0`	指定された条件が True であればアプレットが与えられたラベルにジャンプするよう指示します。 アクション ラベルのフォーマットは number1.number2 です。*number1* 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*label***puts***string* 例： `switch(config-applet)# action 2.0 puts "Hello world"`	データを直接端末に印刷するアクションを有効にします。 アクション ラベルのフォーマットは number1.number2 です。*number1* 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。

コマンド	目的
action*label***add** {*long-integer* | *variable-name*} {*long-integer* | *variable-name*} 例： `switch(config-applet)# action 2.0 add $var1 10`	2 つの変数を追加するアクションを指定します。 アクション ラベルのフォーマットは number1.number2 です。*number1* 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*label***decrement***variable-name**long-integer* 例： `switch(config-applet)# action 1.0 decrement $varname 12`	変数の値をデクリメントするアクションを指定します。 アクション ラベルのフォーマットは number1.number2 です。*number1* 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*label***increment***variable-name**long-integer* 例： `switch(config-applet)# action 2.0 increment $varname 12`	変数の値を増分するアクションを指定します。 アクション ラベルのフォーマットは number1.number2 です。*number1* 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*label***multiply** {*long-integer1* | *variable-name1*} {*long-integer2* | *variable-name2*} `switch(config-applet)# action 2.0 multiply 12 35`	変数の値に長整数値を掛けるアクションを指定します。 アクション ラベルのフォーマットは number1.number2 です。*number1* 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*label***subtract** {*long-integer1* | *variable-name1*} {*long-integer2* | *variable-name2*} 例： `switch(config-applet)# action 2.0 subtract $var1 $var2`	変数の値を別の変数から引くアクションを指定します。 アクション ラベルのフォーマットは number1.number2 です。*number1* 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*label***comment***string* 例： `switch(config-applet)# action 2.0 comment keyvalue`	アプレットにコメントを追加します。 アクション ラベルのフォーマットは number1.number2 です。*number1* 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。

コマンド	目的
action*label***break** 例： `switch(config-applet)# action 2.0 break`	アクションがアクションのループを終了するよう指定します。 アクション ラベルのフォーマットは number1.number2 です。*number1* 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*label***continue** 例： `switch(config-applet)# action 2.0 continue`	アクションがアクションのループを継続するよう指定します。 アクション ラベルのフォーマットは number1.number2 です。*number1* 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*label***foreach***string-iteratorstring-input* [*string-delimiter*] 例： `switch(config-applet)# action 3.1 foreach _iterator "orange blue green"`	デリミタをトークン化パターンとして使用し、入力文字列の反復を指定します。 アクション ラベルのフォーマットは number1.number2 です。*number1* 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*label***while***string-op-1operatorstring-op-2* 例： `switch(config-applet)# action 3.2 while $i lt 10`	ループ アクション ブロックの開始を識別します。 アクション ラベルのフォーマットは number1.number2 です。*number1* 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。 *operator* の有効な値は、ge、gt、eq、ne、lt、le です。

文字列操作をイネーブルにするには、アプレット コンフィギュレーション（config-applet）モードで次のいずれかのアクション コマンドを使用します。

コマンド	目的
action*label***append***var-name* [*var-value*] `switch(config-applet)# action 4.2 append $var 12`	文字列の値を現在の変数の値に追加するアクションを指定します。 アクション ラベルのフォーマットは number1.number2 です。*number1* は 16 桁までの任意の数値にできます。*number2* の範囲は 0 ～ 9 です。変数が存在しない場合、作成されて特定の値に設定されます。
action*label***regexp***string-patternstring-input* [*string-match* [*string-submatch1*] [*string-submatch2*] [*string-submatch3*]] `switch(config-applet)# action 4.3 regexp "(.*) (.*) (.*)" "one two three" _match _sub1`	*string-input* の *string-pattern* に正規表現を一致させます。*string-match* および *string-submatch* は、一致する結果を格納します。 アクション ラベルのフォーマットは number1.number2 です。 *number1* は 16 桁までの任意の数値にできます。*number2* の範囲は 0 ～ 9 です。
action*label***string compare** [**nocase**] [**length***integer*] *string1string2* `switch(config-applet)# action 4.5 string compare nocase length 3`	2 つの等しくない文字列を比較します。結果は、組み込み変数 *$_string_result* に格納されます。 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*label***string equal** [**nocase**] [**length***integer*] *string1string2* `switch(config-applet)# action 4.5 string equal "contains" "data"`	2 つの文字列を比較し、2 つの文字列が等しければ 1 を返します。結果は、組み込み変数 *$_string_result* に格納されます。 アクション ラベルのフォーマットは number1.number2 です。*number1* 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*label***string first***string1string2* [*index-value*] `switch(config-applet)# action 4.6 string first "contains" $str`	*string2* 内に *string1* が最初に出現したインデックスを返します。*index-value* はオプションで、最初のテストを開始する位置を示します。 アクション ラベルのフォーマットは number1.number2 です。*number1* 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。

コマンド	目的
action*label***string index***string* [*value* | *end*] `switch(config-applet)# action 4.7 string index "this is a test" 6`	特定のインデックス値で指定された文字を返します。*end* は、文字列の最後の文字を示します。文字は、組み込み変数 *$_string_result* に格納されます。 アクション ラベルのフォーマットは number1.number2 です。*number1* 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*label***string last***string1string2* [*index-value*] `switch(config-applet)# action 4.9 string last "contains" $str`	*string2* 内に *string1* が最後に出現したインデックスを返します。 アクション ラベルのフォーマットは number1.number2 です。*number1* は 16 桁までの任意の数値にできます。*number2* の範囲は 0 ～ 9 です。
action*label***string length***string* `switch(config-applet)# action 5.0 string length "contains"`	文字列の文字数を返します。結果は、組み込み変数 *$_string_result* に格納されます。 アクション ラベルのフォーマットは number1.number2 です。*number1* 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*label***string match** [**nocase**] *string-patternstring* `switch(config-applet)# action 5.2 string match "*Bl*"  $str`	指定されたパターン、*string-pattern* に *string* を一致させます。両者が一致すると、結果 1 が組み込み変数 *$_string_result* に格納されます。 アクション ラベルのフォーマットは number1.number2 です。*number1* 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*label***string range***stringstart-indexend-index* `switch(config-applet)# action 5.2 string range "$data" 4 9`	*start-index* で開始し、*end-index* で終了する文字列の文字の範囲を格納します。結果の文字は、組み込み変数 *$_string_result* に格納されます。 アクション ラベルのフォーマットは number1.number2 です。*number1* 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。

コマンド	目的
action*label***string replace***stringstart-indexend-index* [*new-string*] `switch(config-applet)# action 5.4 string replace $str 1 4 "test"`	指定した文字列の文字を置き換えることにより、新しい文字列を作成します。*new-string* を指定しない場合、文字は空白に置き換えられます。新しく作成された文字列は、組み込み変数 *$_string_result* に格納されます。 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*label***string tolower***string* [*start-index*] [*end-index*] `switch(config-applet)# action 5.5 string tolower "$string" 11 16`	文字列の指定の範囲の文字を小文字で保存します。文字は、組み込み変数 *$_string_result* に格納されます。 アクション ラベルのフォーマットは number1.number2 です。*number1* 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*label***string toupper***string* [*start-index*] [*end-index*] `switch(config-applet)# action 5.6 string toupper "$string" 0 7`	文字列の指定の範囲の文字を大文字で保存します。文字は、組み込み変数 *$_string_result* に格納されます。 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*label***string trim***string1* [*string2*] `switch(config-applet)# action 5.7 string trim "$string"`	*string2* の文字を、*string1* の両端からトリムします。デフォルトで、*string2* は空白に相当します。 アクション ラベルのフォーマットは number1.number2 です。*number1* は 16 桁までの任意の数値にできます。*number2* の範囲は 0 ～ 9 です。
action*label***string trimleft***string1* [*string2*] `switch(config-applet)# action 5.7 string trimleft "$string" "Hello"`	*string2* の文字を、*string1* の左端からトリムします。デフォルトで、*string2* は空白に相当します。 アクション ラベルのフォーマットは number1.number2 です。*number1* 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。

コマンド	目的
action*label***string trimright***string1* [*string2*] `switch(config-applet)# action 5.7 string trimright "this is a testtest" "test"`	*string2* の文字を、*string1* の右端からトリムします。デフォルトで、*string2* は空白に相当します。 アクション ラベルのフォーマットは number1.number2 です。*number1* 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*label***set***variable-name variable-value* `switch(config-applet)# action 6.0 set $string "Container"`	変数の値を設定します。 アクション ラベルのフォーマットは number1.number2 です。*number1* 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。

（注） 発生したイベントでデフォルトのアクションを処理できるようにする場合は、デフォルトのアクションを許可する EEM ポリシーを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** コマンドを使用すると、CLI が一致するすべての EEM ポリシーで、CLI コマンドを実行できます。

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できます。

はじめる前に

管理者の権限でログインしていることを確認します。

スクリプト名がスクリプト ファイル名と同じ名前であることを確認します。

手順

ステップ 1 テキスト エディタで、ポリシーを定義するコマンド 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 次のシステム ディレクトリにファイルをコピーします。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	**event manager policy***policy-script* 例： `switch(config)# event manager policy moduleScript`	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 policy internal***name* 例： `switch(config)# show event manager policy internal moduleScript`	（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** 例： `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。

EEM ポリシーのスケジューリング

登録済みの EEM ポリシーをスケジューリングし、ポリシーのスケジューリング オプションを設定できます。

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。

	コマンドまたはアクション	目的
ステップ 2	**event manager scheduler applet thread class***class-options***number***thread-number* 例： `switch(config)# event manager scheduler applet thread class default number 2`	EEM ポリシーをスケジューリングし、ポリシーのスケジューリングオプション（class など）および実行のスレッド番号を設定します。
ステップ 3	**event manager scheduler script thread class***class-options***range***class-range***number***thread-number* 例： `switch(config)# event manager scheduler script thread class A B range D-E number 1`	EEM ポリシーをスケジューリングし、スクリプトのスケジュールオプションを設定します。
ステップ 4	**event manager scheduler clear** {**all** | **policy***job-id* | **queue-type applet** [**class***class-options*]} [**processor** {**rp_primary** | **rp_standby**}] 例： `switch# event manager scheduler clear policy 2`	現在実行中または実行保留中の EEM ポリシーをクリアします。
ステップ 5	**event manager scheduler hold** {**all** | **policy***job-id* | **queue-type applet** [**class***class-options*]} 例： `switch# event manager scheduler hold policy 2`	EEM スケジューラで、スケジュールされた EEM ポリシーイベントまたはイベントキューをホールドします。
ステップ 6	**event manager scheduler modify** {**all** | **policy***job-id* | **queue-type applet**} {**class***class-options* [**queue-priority** {**high** | **last** | **low** | **normal**}] | **queue-priority** {**high** | **last** | **low** | **normal**} [**class***class-options*]} 例： `switch# event manager scheduler modify all class A`	EEM ポリシーのスケジューリングパラメータを変更します。
ステップ 7	**event manager scheduler release** {**all** | **policy***policy-id* | **queue-type applet** [**class***class-options*]} 例： `switch# event manager scheduler release all`	event manger scheduler hold コマンドによってホールドされていた EEM ポリシーを解放します。

ポリシーの上書き

システム ポリシーは上書き可能です。

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	**show event manager policy-state***system-policy*
	
	例：
	`switch(config-applet)# show event manager policy-state __ethpm_link_flap`
	`Policy __ethpm_link_flap`
	`Cfg count : 5`
	`Cfg time interval : 10.000000 (seconds)`
	`Hash default, Count 0`
		（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。システム ポリシー名を突き止めるには、**show event manager system-policy** コマンドを使用します。システム ポリシーについては、Embedded Event Manager システム イベントおよびコンフィギュレーション例, （531 ページ）を参照してください。

ステップ 3	**event manager applet***applet-name***override***system-policy*
	
	例：
	`switch(config)# event manager applet ethport override __ethpm_link_flap`
	`switch(config-applet)#`
		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 の英数字を使用できます。*system-policy* は、既存のシステム 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* 例： `description “Overrides link flap policy.”`	（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	**event***event-statement* 例： `switch(config-applet)# event policy-default count 2 time 1000`	ポリシーのイベント文を設定します。
ステップ 6	**action***number action-statement* 例： `switch(config-applet)# action 1.0 syslog priority warnings msg “Link is flapping.”`	ポリシーのアクション文を設定します。 アクション文が複数ある場合、このステップを繰り返します。
ステップ 7	**show event manager policy-state***name* 例： `switch(config-applet)# show event manager policy-state ethport`	（任意） 設定したポリシーに関する情報を表示します。

	コマンドまたはアクション	目的
ステップ 8	**copy running-config startup-config** 例： `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。

メモリのしきい値の設定

イベントを発生させるメモリしきい値を設定し、オペレーティング システムがメモリを割り当てられない場合にプロセスを終了させるかどうかを設定できます。

はじめる前に

管理者の権限でログインしていることを確認します。

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	**system memory-thresholds minor***minor***severe***severe***critical***critical* 例： `switch(config)# system memory-thresholds minor 60 severe 70 critical 80`	EEM メモリ イベントを生成するシステム メモリしきい値を設定します。デフォルト値は次のとおりです。 • Minor-85 • Severe-90 • Critical-95 これらのメモリのしきい値を超えた場合、システムは次の syslog を生成します。 • 2013 May 7 17:06:30 switch %$ %PLATFORM-2-MEMORY_ALERT: Memory Status Alert : MINOR • 2013 May 7 17:06:30 switch %$ %PLATFORM-2-MEMORY_ALERT: Memory Status Alert : SEVERE

	コマンドまたはアクション	目的
		• 2013 May 7 17:06:30 switch %$ %PLATFORM-2-MEMORY_ALERT: Memory Status Alert : CRITICAL • 2013 May 7 17:06:35 switch %$ %PLATFORM-2-MEMORY_ALERT: Memory Status Alert : MINOR ALERT RECOVERED • 2013 May 7 17:06:35 switch %$ %PLATFORM-2-MEMORY_ALERT: Memory Status Alert : SEVERE ALERT RECOVERED • 2013 May 7 17:06:35 switch %$ %PLATFORM-2-MEMORY_ALERT: Memory Status Alert : CRITICAL ALERT RECOVERED
ステップ 3	**system memory-thresholds threshold critical no-process-kill** 例： `switch(config)# system memory-thresholds threshold critical no-process-kill`	（任意） メモリを割り当てることができない場合にプロセスを停止しないようにシステムを設定します。デフォルト値では、最もメモリを消費するプロセスから終了できます。
ステップ 4	**show running-config | include "system memory"** 例： `switch(config-applet)# show running-config | include "system memory"`	（任意） システムメモリ設定に関する情報を表示します。
ステップ 5	**copy running-config startup-config** 例： `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。

EEM パブリッシャとしての syslog の設定

スイッチからの syslog メッセージをモニタできます。

（注） syslog メッセージをモニタする検索文字列の最大数は 10 です。

はじめる前に

EEM は、Syslog による登録に使用可能である必要があります。

Syslog デーモンが設定され、実行される必要があります。

手順

	コマンドまたはアクション	目的

ステップ 1	**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	**event manager applet***applet-name*
	
	例：
	`switch(config)# event manager applet abc`
	`switch(config-applet)#`
		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。

ステップ 3	**event syslog** [**tag***tag*] {**occurs***number* | **period***seconds* | **pattern***msg-text* | **priority***priority*} 例： `switch(config-applet)# event syslog occurs 10`	syslog メッセージを監視し、ポリシーの検索文字列に基づいてポリシーを呼び出します。 • **tag***tag* 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。 • **occurs***number* のキーワードと引数のペアは、発生回数を指定します。指定できる範囲は 1 ～ 65000 です。 • **period***seconds* のキーワードと引数のペアは、イベントの発生間隔を指定します。範囲は 1 ～ 4294967295 です。 • **pattern***msg-text* のキーワードと引数のペアは、一致する正規表現を指定します。パターンには、文字テキスト、環境変数、またはこの 2 つの組み合わせを含めることができます。文字列に空白が含まれる場合は引用符で囲みます。 • **priority***priority* のキーワードと引数のペアは、syslog メッセージのプライオリティを指定します。このキーワードを指定しないと、すべての Syslog メッセージのプライオリティ レベルが「情報レベル」に設定されます。

	コマンドまたはアクション	目的
ステップ 4	**copy running-config startup-config** 例： `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。

EEM 設定の確認

EEM の設定情報を表示するには、次のコマンドのいずれかを入力します。

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。
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。

コマンド	目的
show event manager policy active [**class***class-options* | [**detailed**] [**queue-type** [**applet**]]]	実行されている EEM ポリシーを表示します。
show event manager policy pending [**class***class-options* | [**detailed**] [**queue-typeapplet** [**detailed**]]	実行保留中ののポリシーを表示します。
show event manager scheduler thread detailed	EEM ポリシーのスケジューリングされたアクティビティを表示します。

EEM のコンフィギュレーション例

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方法の例を示します。この例では、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
```

__ethpm_link_flap システム ポリシーを上書きし、インターフェイスをシャットダウンする方法の例を示します。

```
event manager applet ethport override __ethpm_link_flap
event policy-default count 2 time 1000
action 1 cli conf t
action 2 cli int et1/1
action 3 cli no shut
```

CLI コマンドの実行を許可し、ユーザがデバイスでコンフィギュレーション 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
```

（注） 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 ポリシーの複数イベントを関連付け、イベント トリガーの組み合わせに基づいてポリシーを実行する例を示します。この例では、EEM ポリシーは、指定された syslog パターンのいずれかが 120 秒以内に発生したときにトリガーされます。

```
event manager applet eem-correlate
event syslog tag one pattern "copy bootflash:.* running-config.*”
event syslog tag two pattern “copy run start”
```

```
event syslog tag three pattern "hello"
tag one or two or three happens 1 in 120
action 1.0 reload module 1
```

（注） 追加の EEM の設定例については、Embedded Event Manager システム イベントおよびコンフィギュレーション例, （531 ページ）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
EEM コマンド	『*Cisco Nexus 7000 Series NX-OS System Management Command Reference*』
VDC	『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』

EEM の機能の履歴

次の表に、このマニュアルの新機能および変更された機能を要約し、各機能がサポートされているリリースを示します。ご使用のソフトウェア リリースで、本書で説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。

表 *30* : *EEM* の機能の履歴

機能名	リリース	機能情報
EEM イベント相関	5.2(1)	単一の EEM ポリシーで複数のイベント トリガーのサポートが追加されました。
EEM パブリッシャとしての syslog	5.1(1)	スイッチからの syslog メッセージのモニタのサポートが追加されました。
メモリしきい値の設定	4.1(3)	メモリしきい値に関して設定の項を追加

第 16 章

オンボード障害ロギングの設定

この章では、Cisco NX-OS デバイスで Onboard Failure Logging（OBFL）機能を設定する方法について説明します。

この章は、次の項で構成されています。

- 機能情報の確認，311 ページ
- OBFL の概要，312 ページ
- 仮想化のサポート，312 ページ
- OBFL のライセンス要件，312 ページ
- OBFL の前提条件，313 ページ
- OBFL の注意事項と制約事項，313 ページ
- OBFL のデフォルト設定，313 ページ
- OBFL の設定，313 ページ
- OBFL コンフィギュレーションの確認，315 ページ
- OBFL のコンフィギュレーション例，317 ページ
- その他の参考資料，317 ページ
- OBFL の機能の履歴，317 ページ

機能情報の確認

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

OBFL の概要

Cisco NX-OS には永続ストレージに障害データを記録する機能があるので、あとから記録されたデータを取得して表示し、分析できます。この OBFL 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、障害モジュールの分析に役立ちます。

OBFL は次のタイプのデータを保存します。

- 最初の電源投入時刻
- モジュールのシャーシ スロット番号
- モジュールの初期温度
- ファームウェア、BIOS、FPGA、および ASIC のバージョン
- モジュールのシリアル番号
- 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

仮想化のサポート

OBFL 情報を設定して表示するには、デフォルト仮想デバイス コンテキスト（VDC）を使用する必要があります。VDC の詳細については、『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』を参照してください。

OBFL のライセンス要件

製品	ライセンス要件
Cisco NX-OS	OBFL 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 nx-os イメージにバンドルされており、無料で提供されます。NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

OBFL の前提条件

VDC を設定する場合は、適切なライセンスをインストールし、所定の VDC を開始する必要があります。設定情報については『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』、ライセンス情報については『*Cisco NX-OS Licensing Guide*』を参照してください。

network-admin ユーザ権限で、デフォルト VDC にログインする必要があります。

OBFL の注意事項と制約事項

OBFL に関する注意事項および制約事項は、次のとおりです。

- OBFL はデフォルトでイネーブルになっています。
- OBFL フラッシュがサポートする書き込みおよび消去の回数には制限があります。イネーブルにするロギング数が多いほど、この書き込みおよび消去回数に早く達してしまいます。

（注） この機能の Cisco NX-OS コマンドは、Cisco IOS のコマンドとは異なる場合があるので注意してください。

OBFL のデフォルト設定

次の表に、OBFL パラメータのデフォルト設定を示します。

パラメータ	デフォルト
OBFL	すべての機能がイネーブル

OBFL の設定

Cisco NX-OS デバイス上で OBFL 機能を設定できます。

はじめる前に

グローバル コンフィギュレーション モードになっていることを確認します。

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	**hw-module logging onboard**
	
	例：
	`switch(config)# hw-module logging onboard`
	`Module: 7 Enabling ... was successful.`
	`Module: 10 Enabling ... was successful.`
	`Module: 12 Enabling ... was successful.`
		すべてのOBFL機能をイネーブルにします。

ステップ 3	**hw-module logging onboard counter-stats**
	
	例：
	`switch(config)# hw-module logging onboard counter-stats`
	`Module: 7 Enabling counter-stats ... was successful.`
	`Module: 10 Enabling counter-stats ... was successful.`
	`Module: 12 Enabling counter-stats ... was successful.`
		OBFL カウンタ統計情報をイネーブルにします。

ステップ 4	**hw-module logging onboard cpuhog**
	
	例：
	`switch(config)# hw-module logging onboard cpuhog`
	`Module: 7 Enabling cpu-hog ... was successful.`
	`Module: 10 Enabling cpu-hog ... was successful.`
	`Module: 12 Enabling cpu-hog ... was successful.`
		OBFL CPU hog イベントをイネーブルにします。

ステップ 5	**hw-module logging onboard environmental-history**
	
	例：
	`switch(config)# hw-module logging onboard environmental-history`
	`Module: 7 Enabling environmental-history ... was successful.`
	`Module: 10 Enabling environmental-history ... was successful.`
	`Module: 12 Enabling environmental-history ... was successful.`
		OBFL 環境履歴をイネーブルにします。

ステップ 6	**hw-module logging onboard error-stats**
	
	例：
	`switch(config)# hw-module logging onboard error-stats`
	`Module: 7 Enabling error-stats ... was successful.`
	`Module: 10 Enabling error-stats ... was successful.`
		OBFL エラー統計をイネーブルにします。

	コマンドまたはアクション	目的
	`Module: 12 Enabling error-stats ... was successful.`	

ステップ 7	**hw-module logging onboard interrupt-stats**
	
	例：
	`switch(config)# hw-module logging onboard interrupt-stats`
	`Module: 7 Enabling interrupt-stats ... was successful.`
	`Module: 10 Enabling interrupt-stats ... was successful.`
	`Module: 12 Enabling interrupt-stats ... was successful.`
		OBFL 割り込み統計をイネーブルにします。

ステップ 8	**hw-module logging onboard module***slot*
	
	例：
	`switch(config)# hw-module logging onboard module 7`
	`Module: 7 Enabling ... was successful.`
		モジュールの OBFL 情報をイネーブルにします。

ステップ 9	**hw-module logging onboard obfl-logs**
	
	例：
	`switch(config)# hw-module logging onboard obfl-logs`
	`Module: 7 Enabling obfl-log ... was successful.`
	`Module: 10 Enabling obfl-log ... was successful.`
	`Module: 12 Enabling obfl-log ... was successful.`
		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	**show logging onboard** 例： `switch(config)# show logging onboard`	（任意） OBFL に関する情報を表示します。
ステップ 11	**copy running-config startup-config** 例： `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。

OBFL コンフィギュレーションの確認

モジュールのフラッシュに保存されている OBFL 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 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 counter-stats	すべての ASIC カウンタについて、統計情報を表示します。
show logging onboard credit-loss	OBFL クレジット損失のログを表示します。
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	指定した終了時刻までの 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 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 obfl-logs	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 status	OBFL ステータス情報を表示します。

OBFL の設定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
----------------------------
OBFL Status
----------------------------
Switch OBFL Log: Enabled

Module: 4 OBFL Log: Enabled
cpu-hog Enabled
credit-loss Enabled
environmental-history Enabled
error-stats Enabled
exception-log Enabled
interrupt-stats Enabled
mem-leak Enabled
miscellaneous-error Enabled
obfl-log (boot-uptime/device-version/obfl-history) Enabled
register-log Enabled
request-timeout Enabled
stack-trace Enabled
system-health Enabled
timeout-drops Enabled
stack-trace Enabled
```

```
Module: 22 OBFL Log: Enabled
cpu-hog Enabled
credit-loss Enabled
environmental-history Enabled
error-stats Enabled
exception-log Enabled
interrupt-stats Enabled
mem-leak Enabled
miscellaneous-error Enabled
obfl-log (boot-uptime/device-version/obfl-history) Enabled
register-log Enabled
request-timeout Enabled
stack-trace Enabled
system-health Enabled
timeout-drops Enabled
stack-trace Enabled
```

上記の各 **show** コマンド オプションの OBFL 情報を消去するには、**clear logging onboard** コマンドを使用します。

OBFL のコンフィギュレーション例

モジュール 2 で環境情報について OBFL をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# hw-module logging onboard module 2 environmental-history
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
OBFL CLI コマンド	『*Cisco Nexus 7000 Series NX-OS System Management Command Reference*』
コンフィギュレーション ファイル	『*Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide*』
VDC	『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』

OBFL の機能の履歴

次の表に、このマニュアルの新機能および変更された機能を要約し、各機能がサポートされているリリースを示します。ご使用のソフトウェア リリースで、本書で説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/

bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。

表 *31* : *OBFL* の機能の履歴

機能名	リリース	機能情報
OBFL	4.0(1)	この機能が導入されました。

第 17 章

SPAN の設定

この章では、Cisco NX-OS デバイス上のポート間のトラフィックを分析するようにイーサネット スイッチド ポート アナライザ（SPAN）を設定する方法について説明します。

- 機能情報の確認，319 ページ
- SPAN の概要，320 ページ
- SPAN のライセンス要件，326 ページ
- SPAN の前提条件，326 ページ
- SPAN の注意事項および制約事項，326 ページ
- SPAN のデフォルト設定，335 ページ
- SPAN の設定，335 ページ
- SPAN の設定確認，368 ページ
- SPAN のコンフィギュレーション例，368 ページ
- 関連資料，373 ページ
- SPAN の機能の履歴，373 ページ

機能情報の確認

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

SPAN の概要

SPAN は、外付けアナライザが接続された宛先ポートに SPAN セッション トラフィックを送ることで、送信元ポート間のすべてのトラフィックを分析します。

ローカル デバイス上で、SPAN セッションでモニタする送信元と宛先を定義できます。

SPAN ソース

トラフィックを監視できる監視元インターフェイスのことを SPAN 送信元と呼びます。送信元では、監視するトラフィックを指定し、さらに入力、出力、または両方向のトラフィックをコピーするかどうかを指定します。SPAN 送信元には次のものが含まれます。

- イーサネット ポート
- ポート チャネル
- コントロール プレーン CPU への帯域内インターフェイス。
- VLAN（入力のみ）：VLAN が SPAN 送信元として指定されている場合は、VLAN 内でサポートされているすべてのインターフェイスが SPAN 送信元になります。
- リモート SPAN（RSPAN）VLAN
- Cisco Nexus 2000 Series Fabric Extender（FEX）に接続されたファブリック ポート チャネル
- Cisco Nexus 2000 Series Fabric Extender 上のサテライト ポートおよびホスト インターフェイス ポート チャネル：これらのインターフェイスは、レイヤ 2 アクセス モード、レイヤ 2 トランク モード、およびレイヤ 3 モードでサポートされます。

（注） レイヤ 3 サブインターフェイスはサポートされません。

（注） 1 つの SPAN セッションに、上述の送信元を組み合わせて使用できます。

送信元ポートの特性

SPAN 送信元ポートには、次の特性があります。

- 送信元ポートとして設定されたポートを宛先ポートとしても設定することはできません。
- RSPAN VLAN は、SPAN 送信元として使用できません。
- スーパーバイザ帯域内インターフェイスを SPAN 送信元として使用する場合、次のパケットがモニタされます。

- スーパーバイザ ハードウェアに着信するすべてのパケット（入力）
- スーパーバイザ ハードウェアによって生成されるすべてのパケット（出力）

SPAN 宛先

SPAN 宛先とは、送信元ポートを監視するインターフェイスを指します。宛先ポートは SPAN 送信元からコピーされたトラフィックを受信します。

宛先ポートの特性

SPAN 宛先元ポートには、次の特性があります。

- SPAN セッションの宛先には、アクセス モードまたはトランク モードのイーサネット ポートまたはポートチャネル インターフェイスが含まれます。
- 宛先ポートとして設定されたポートを送信元ポートとしても設定することはできません。
- 宛先ポートは、一度に 1 つの SPAN セッションだけで設定できます。
- 宛先ポートはスパニングツリー インスタンスに関与しません。SPAN 出力にはブリッジ プロトコル データ ユニット（BPDU）スパニングツリー プロトコル hello パケットが含まれます。
- 指定のセッション用に設定されたすべての SPAN 宛先は、すべてのスパンされたトラフィックを受信します。
- RSPAN VLAN は、SPAN 宛先として使用できません。
- 侵入検知システム（IDS）のサポートとして、パケットを挿入して特定の TCP パケット ストリームを中断するように SPAN 宛先を設定できます。
- 転送エンジンが IDS の MAC アドレスを学習できるように SPAN 宛先を設定できます。
- F シリーズ モジュールの FabricPath コア ポート、Fabric Extender ホスト インターフェイス（HIF）ポート、HIF ポート チャネル、およびファブリック ポート チャネル ポートは SPAN 宛先ポートとしてサポートされていません。
- 共有インターフェイスを SPAN 宛先として使用することはできません。
- SPAN 宛先ポートへの VLAN ACL リダイレクトはサポートされません。
- 指定のセッション用に設定されたすべての SPAN 宛先は、すべてのスパンされたトラフィックを受信します。

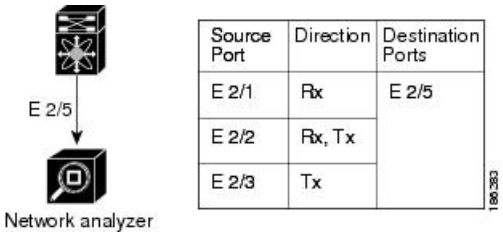
SPAN セッション

モニタする送信元と宛先を指定する SPAN セッションを作成できます。

サポートされる SPAN セッション数に関する情報については、『*Cisco Nexus 7000 Series NX-OS Verified Scalability Guide*』を参照してください。

この図では、SPAN の設定を示します。3 つのイーサネット ポート上のパケットが宛先ポートのイーサネット 2/5 にコピーされます。コピーされるのは、指定した方向のトラフィックだけです。

図 *4*：*SPAN* の設定



拡張 SPAN セッション

Cisco NX-OS Release 6.2(2) 以降のリリースでは、前のリリースでサポートされた 2 つの従来の SPAN セッションに加えて拡張 SPAN セッションもサポートされます。拡張 SPAN セッションは、従来の方式または単方向が可能です。セッションの方向はセッション作成時に指定されます。12 の独立したセッション リソースのプールを使用できます。単方向セッションは 1 つのリソースを使用し、従来のセッションは 2 つのリソースを使用します。これら 12 のリソースがすべての VDC にわたってローカルおよび SPAN 送信元セッションで共有されます。

Cisco Nexus 7710 スイッチまたは Cisco Nexus 7718 スイッチで拡張 SPAN セッションを設定している場合、以下が適用されます。

- **mode extended** コマンドは、3 つ目のコンフィギュレーション セッションとともに使用する必要があります。
- 必要に応じて 16 のセッションを単方向または双方向として設定できます。
- 2 つの従来のセッションを維持する必要はありません。
- リソース マネージャを使用して 2 つの従来のセッションを予約する必要はありません。

SPAN セッションあたり 4K の VLAN

Cisco NX-OS Release 7.3(0)D1(1) 以降では、SPAN セッションあたり 4K の VLAN がサポートされます。**source interface all** コマンドを使用してスイッチでのモニタ セッションをイネーブルにすると、物理ポート、ポート チャネル、FEX ポート、および FEX ポート チャネルなど、VDC 内のすべての VLAN とポートをモニタできます。さらに、SPAN セッションあたり 4K の VLAN 機能では、**filter vlan** コマンドと **source interface all** コマンドを使用して無関係の VLAN をフィルタすることにより、モニタ セッションで現在サポートされている VLAN 送信元制限よりも多くの、指定の VLAN 送信元をモニタできます。

SPAN セッションあたり 4K の VLAN 機能には、次の特性があります。

- M3 シリーズ モジュールではサポートされません。
- M3 シリーズ モジュールでは、**source interface all** コマンドを設定しても、トラフィックをキャプチャできません。
- **source interface all** コマンドは、同じ VDC 内の複数のセッションに使用できます。
- MTU 切り捨て、サンプリング、レート制限など、すべてのセッション パラメータをサポートします。
- **source interface all** コマンドは、単純および複雑ルール ベースの SPAN をサポートします。これにより、VDC 全体で一連のフィルタ ルールを使用してトラフィック フロー ベースのモニタリングをすることができます。
- スーパーバイザが生成するトラフィックはスパンされません。
- Cisco Nexus 7000 シリーズ スイッチのイーサネット VDC においてのみサポートされます。
- 拡張 SPAN セッションでのみサポートされます。

ルール ベース SPAN

ルール ベースの SPAN は、一連のルールに基づいて入力または出力 SPAN トラフィックをフィルタします。6.2(2) より前の Cisco NX-OS リリースでは、VLAN、宛先インデックス、および送信元インデックスをフィルタできました。Cisco NX-OS Release 6.2(2) 以降では、レイヤ 2、レイヤ 3、またはレイヤ 4 ヘッダー パケットのフィールドの組み合わせに基づいて SPAN トラフィックをフィルタできます。

すべての SPAN セッション（従来および拡張）には関連するフィルタがあります。すべての SPAN セッションには 1 つのフィルタ リソースがあります。単純なフィルタには 1 つのみのルールがあり、このルールに複数のフィールドまたは組み合わせを追加できます。パケットは、すべての条件が満たされた場合にのみ複製されます。

表 *32*：サポートされるフィルタ フィールド

イーサネット	IPv4	IPv6	ARP/RARP	FCoE

フレーム タイプ	フレームタイプ	フレーム タイプ	フレーム タイプ	フレーム タイプ
VLAN	VLAN	VLAN	VLAN	VLAN
TR	TR	TR	TR	TR
BPDU	BPDU	BPDU	BPDU	BPDU
ポート チャネル レーン	ポートチャネル レーン	ポート チャネル レーン	ポート チャネル レーン	ポート チャネル レーン
フロー ハッシュ	フローハッシュ	フロー ハッシュ	フロー ハッシュ	フロー ハッシュ
L2 MAC DA	L2 MAC DA	L2 MAC DA	L2 MAC DA	L2 MAC DA
L2 MAC SA	L2 MAC SA	L2 MAC SA	L2 MAC SA	L2 MAC SA
EtherType	EtherType	EtherType	EtherType	EtherType
CoS/VL	CoS/VL	CoS/VL	CoS/VL	CoS/VL
	ToS	ToS	ARP	FCD_ID
	L4 Protocol	L4 Protocol	Request	FCS_ID
	IPv4 SA	IPv6 SA	Sender IP	SOF
	IPv4 DA	IPv6 DA	Target IP	R_CTL
				TYPE
				Cmd_Code

例外 SPAN

例外 SPAN を使用して、例外パケットをスパンできます。侵入検知システム（IDS）、レイヤ 3 IP 識別、および FabricPath で失敗したパケットは例外パケットとして扱われます。

（注） Cisco NX-OS Release 6.2(10) 以降では、SPAN パケットから FabricPath および VLAN タグ ヘッダーを削除できます。**system default switchport monitor exclude header** および **switchport monitor exclude header** コマンドを使用します。これらのコマンドの詳細については、『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』を参照してください。

例外 SPAN セッションは、2 つの従来の双方向性 SPAN セッションのいずれかまたは拡張 SPAN セッションのいずれかでサポートされます。レート リミッタ、MTU トランケーション、およびサンプリングは例外 SPAN セッションでサポートされます。ドロップ宛先インターフェイスに送信された例外パケットのみが SPAN 送信元としてサポートされます。スーパーバイザ、ACLQoS、またはレイヤ 2 にプッシュされた例外パケットはスパンされません。各 VDC は、1 つの例外 SPAN セッションのみサポートします。

拡張 SPAN は出力方向でのみサポートされます。拡張 SPAN Rx セッションの場合、例外送信元設定は拒否されます。

仮想 SPAN セッション

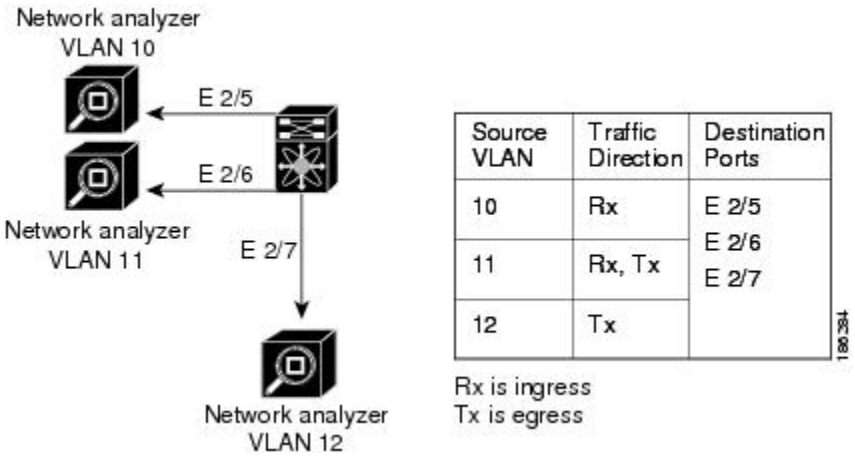
仮想 SPAN セッションを作成して、複数の VLAN 送信元をモニタし、対象の VLAN のみを選択して

複数の宛先ポートに送信することができます。たとえば、トランク ポート上で SPAN を設定して、異なる複数の VLAN からのトラフィックを異なる複数の宛先ポート上でモニタしたりできます。

次の図に、仮想 SPAN の設定を示します。仮想 SPAN セッションでは、3 つの VLAN から指定した 3 つの宛先ポートへトラフィックがコピーされます。各宛先ポートで許可する VLAN を選択することによって、そのポートでデバイスが送信するトラフィックを制限できます。次の図では、デバイスは各宛先ポートの 1 つの VLAN からパケットを送信します。

（注） 仮想 SPAN セッションでは、パケットが宛先で必要かどうかに関係なく、すべての送信元パケットがすべての宛先にコピーされます。VLAN トラフィックのフィルタリングは、出力側の宛先ポート レベルで行われます。

図 *5*：仮想 *SPAN* の設定



仮想 SPAN セッションの設定については、「仮想 *SPAN* セッションの設定」の項を参照してください。

Network Analysis Module; ネットワーク解析モジュール

Cisco Network Analysis Module（NAM）を使用して、アプリケーション パフォーマンス、トラフィック分析、およびパケット ヘッダー分析に関して SPAN データ ソースをモニタできます。

Cisco Nexus 7000 SPAN データ ソースのモニタリングに NAM を使用する詳細については、『*Cisco Nexus 7000 Series Network analysis Module (NAM-NX1) Quick Start Guide*』を参照してください。

ハイ アベイラビリティ

SPAN 機能はステートレス リスタートおよびステートフル 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 スイッチオーバー後に、実行コンフィギュレーションを適用します。ハイ アベイラビリティの詳細については、『*Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide*』を参照してください。

仮想化のサポート

仮想デバイス コンテキスト（VDC）は、一連のシステム リソースを論理的に表現する用語です。SPAN が適用されるのは、コマンドが入力された VDC だけです。

VDC の設定方法については、『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』を参照してください。

SPAN のライセンス要件

製品	ライセンス要件
Cisco NX-OS	SPAN 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 nx-os イメージにバンドルされており、無料で提供されます。NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

SPAN の前提条件

SPAN の前提条件は、次のとおりです。

- 各デバイス上で、まず所定の SPAN 設定をサポートするポートを設定する必要があります。詳細については、『*Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide*』を参照してください。

SPAN の注意事項および制約事項

SPAN の一般的な注意事項と制限事項

- SPAN セッションの制限については、『*Cisco Nexus 7000 Series NX-OS Verified Scalability Guide*』を参照してください。

- SPAN は、管理ポートではサポートされません。
- すべてのスパンのレプリケーションはハードウェアで行われます。スーパーバイザ CPU は関与しません。
- 宛先ポートは、一度に 1 つの SPAN セッションだけで設定できます。
- ポートをソース ポートと宛先ポートの両方として設定することはできません。
- 帯域内インターフェイスの送信元となっている VDC 内にモジュールがない場合、スーパーバイザに送信予定のパケットはキャプチャできません。
- 6.1 より前の Cisco NX-OS リリースでは、帯域内インターフェイスはデフォルトの VDC からのみモニタできます。すべての VDC からの帯域内トラフィックがモニタされます。Cisco NX-OS Release 6.1 以降、帯域内インターフェイスのモニタリングはデフォルトの VDC にのみ制限されなくなりました。
  - ネットワーク管理者権限を持つユーザのみが帯域内インターフェイスを SPAN ソースとして追加できます。
  - 帯域内インターフェイスは、管理 VDC 以外の任意の VDC から送信元として追加できますが、帯域内インターフェイスを送信元として持つことができる VDC は常に 1 つだけです。
- 帯域内スパンは、共有リソースとして扱われます。特定の VDC に割り当てられたリソースがない場合はインバンド ポート ソースは拒否されます。同様に、帯域内スーパーバイザ リソースが割り当てられた VDC が帯域内ポートをすべてのモニタ セッションのソース リストから削除した場合、帯域内リソースはその VDC からリリースされます。
- スーパーバイザ帯域内インターフェイスの場合、SPAN は帯域内インターフェイスの送信元となっている VDC でだけサポートされます。モジュールが帯域内インターフェイスの送信元でない VDC の一部である場合、このモジュールからスーパーバイザ帯域内パケットをキャプチャするには、モジュールの少なくとも 1 つのインターフェイスが帯域内インターフェイスの送信元である VDC 内に存在する必要があります。
- 1 つの SPAN セッションに、次の送信元を組み合わせて使用できます。
  - サブインターフェイスではないイーサネット ポート。
  - VLAN。ポート チャネル サブインターフェイスに割り当て可能です。
  - コントロール プレーン CPU への帯域内インターフェイス。
- SPAN セッションに送信元インターフェイスと送信元 VLAN 句の両方が含まれている場合、他の VLAN がもスパンされる可能性があります。
- 宛先ポートはスパニングツリー インスタンスに関与しません。SPAN 出力にはブリッジ プロトコル データ ユニット（BPDU）スパニングツリー プロトコル hello パケットが含まれます。
- SPAN セッションに、送信方向または送信および受信方向でモニタされている送信元ポートまたは VLAN 送信元が含まれている場合、パケットが実際にはその送信元ポートで送信され

なくても、これらのポートが受け取るパケットが SPAN の宛先ポートに複製される可能性があります。ソース ポート上でのこの動作の例を、次に示します。

- フラッディングから発生するトラフィック
- ブロードキャストおよびマルチキャスト トラフィック

- 送信元ポートで SPAN をイネーブルにしてから、動作上アクティブになることができます。したがって、レイヤ2ポートに対して、これらのポートを含むVLANに入ってくるトラフィックはリンクがポートに接続されていなくてもキャプチャされます。
- 入力と出力の両方が設定されている VLAN SPAN セッションでは、パケットが同じ VLAN 上でスイッチングされる場合に、宛先ポートから 2 つのパケット（入力側から 1 つ、出力側から 1 つ）が転送されます。
- Cisco NX-OS Release 6.2(2) 以降では、帯域内インターフェイスのスパニングは次のとおりです。
  - スーパーバイザ 1 システムでは、2 つの双方向性の従来のセッションは帯域内 SPAN ソースをサポートできます。
  - スーパーバイザ 2 およびスーパーバイザ 2e のシステムでは、すべての SPAN セッションが帯域内 SPAN 送信元をサポートできます。
  - 1 度に帯域内 SPAN をサポートできる VDC は 1 つだけです。
- RSPAN VLAN を設定できるのは、SPAN セッションの送信元として使用する場合に限られます。
- SPAN セッションを設定できるのはローカル デバイス上だけです。
- インター VLAN ルーティングがレイヤ 2 マルチパス（L2MP）を通してイネーブルになっている場合に FabricPath コア インターフェイスをスパンすると、コア インターフェイスから出力されるトラフィックをキャプチャすることはできません。
- SPAN はレイヤ2アクセス モード、レイヤ2トランク モード、およびレイヤ3モードの Fabric Extender インターフェイスでサポートされます。レイヤ 3 サブインターフェイスはサポートされません。
- Cisco NX-OS は、ソース インターフェイスが Fabric Extender HIF（ダウンリンク）ポートまたは HIF ポート チャネルである場合、Link Layer Discovery Protocol（LLDP）または Link Aggregation Control Protocol（LACP）パケットはスパンしません。
- SPAN セッションは、セッションの送信元がスーパーバイザのイーサネット インバンド インターフェイスの場合、ARP 要求および Open Shortest Path First（OSPF）プロトコル hello パケットのようなスーパーバイザに到達するブロードキャストまたはマルチキャスト MAC アドレスを持つパケットをキャプチャできません。これらのパケットをキャプチャするには、SPAN セッションの送信元として物理インターフェイスを使用する必要があります。
- SPAN セッションのレート制限の割合は、それぞれのモジュールに対して 10G、40G、および100Gに基づいており（つまり、1パーセントはそれぞれ0.1G、0.4Gまたは1Gに対応）、各転送エンジン インスタンスに値が適用されます。

- Cisco NX-OS Release 6.1 以降では、スーパーバイザ 2 で SPAN がサポートされます。
- 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。
- スーパーバイザ 1 およびスーパーバイザ 2 の両方で、FCoE 帯域内トラフィックをモニタすることはできません。
- 共有インターフェイス、または VLAN を含むイーサネット インターフェイスを通したローカル SPAN セッションで入力および出力の両方の FCoE トラフィックをモニタできます。共有インターフェイスでは、ストレージ VDC でのみ FCoE トラフィックを監視できます。
- SPAN コピー内の MAC-in-MAC（MiM）ヘッダーは、次の SPAN 宛先では保持されます。
  - Release 6.2 以降のリリースでの F2e モジュール。
  - 任意の Cisco NX-OS Release での F3 シリーズ モジュール。
  - Release 6.2.(6a)、6.2.(6b)、または 6.2(8) での F3 シリーズ モジュールでは、FabricPath（FP）ヘッダーは無条件で保持されます。Release 6.2.10 では、FP ヘッダーはデフォルトで保持されますが、**switchport monitor exclude header** コマンドを使用して VDC 内の指定の SPAN 宛先に対する FP または VLAN タグ ヘッダーを削除するか、または **system default switchport monitor exclude header** コマンドを使用して VDC 内のすべての宛先ポートに対する FP または VLAN タグ ヘッダーを削除することにより、この動作を変更できます。Release 6.2.12 では、SPAN 宛先で **switchport monitor exclude header** コマンドを使用して、FabricPath および VLAN タグ ヘッダーを削除できます。
- SPAN コピー内の MiM ヘッダーは、次の SPAN 宛先では保持されません。
  - 任意の Cisco NX-OS Release での F1 および F2 シリーズ モジュール。
  - Release 6.1(x) での F2e モジュール。
  - Release 6.2.6 での F3 シリーズ モジュールでは、FabricPath（FP）ヘッダーは保持されません。

F1 シリーズ モジュールの注意事項と制約事項

- 複数の SPAN 宛先は、F シリーズモジュールが VDC 内に存在する場合はサポートされません。複数の SPAN 宛先が SPAN セッション内で設定されている場合、セッションは F シリーズ モジュールの電源が切断されるか、別の VDC に移動されるか、または複数の SPAN 宛先が単一の宛先に削減されるまでディセーブルになります。
- FabricPath コア ポートは、F シリーズ モジュールが VDC 内に存在する場合は SPAN 宛先としてサポートされません。ただし、FabricPath コア ポートは、SPAN 送信元インターフェイスとして設定できます。

- F1 シリーズ モジュールは、レイヤ 2 ドメイン モジュールです。レイヤ 3 送信元のパケットは、F1 シリーズ モジュール SPAN 宛先にスパンおよび送信できます。F1 シリーズ モジュール インターフェイスはレイヤ 3 として設定することはできませんが、SPAN 宛先モードでレイヤ 3 トラフィックを受信することができます。
- F1 シリーズまたは F2 シリーズ モジュールで SPAN セッションを使用する場合、特定のセッション内の送信元トラフィックの合計量が SPAN 宛先インターフェイスまたはそのセッションのポート チャネルの容量以下であることを確認してください。SPAN 送信元トラフィックが SPAN 宛先の容量を超えると、SPAN 送信元インターフェイスでパケット ドロップが発生する場合があります。このガイドラインは、F2e シリーズ銅線およびファイバー モジュールには適用されません。
- MTU 切り捨ておよび SPAN レート制限は、F シリーズおよび M2 シリーズ モジュールおよびスーパーバイザ 2 でサポートされます。

（注） F1 シリーズ モジュール上の同じ SPAN セッションに対して MTU 切り捨ておよび SPAN レート制限をイネーブルにすることはできません。1 セッションで両方を設定した場合、レート制限の設定をディセーブルにするまで、レート制限だけが F1 シリーズ モジュールで許可され、MTU 切り捨てがディセーブルになります。この制限は、F2 および M2 シリーズ モジュールまたはスーパーバイザ 2 には適用されません。

- F1 シリーズ モジュールでは、SPAN 宛先がコア ヘッダーを削除するため、出力スパン FabricPath（コア）パケット上の MTU 切り捨ては設定値より 16 バイト少なくなります。また、トランク ポートが SPAN 宛先として使用される場合、スパンされる入力パケットは、設定された MTU 切り捨てサイズよりも 4 バイト多くなります。
- F シリーズ モジュール、M2 シリーズ モジュール、およびスーパーバイザ 2 の特定のレート制限およびパケット サイズ値では、パケット サイズの内部アカウンティングおよび内部ヘッダーのため、SPAN パケット レートは設定された値より少なくなります。
- SPAN サンプリングは F シリーズ モジュールでのみサポートされます。
- 従来の SPAN セッションは、F シリーズおよび M シリーズ モジュールからのトラフィックをサポートします。拡張 SPAN セッションは、F シリーズおよび M2 シリーズ モジュールからのみのトラフィックをサポートします。
- F1 シリーズ モジュールはルール ベースの SPAN を制限付きでサポートします。IPv6 送信元 IP および IPv6 宛先 IP フィルタをサポートしません。これらは 0 ～ 3.までの値で IPv4 および IPv6 ToS フィルタのみサポートします。ポート チャネル メンバー レーン、FCoE 送信元 ID、および FCoE 宛先 ID はサポートされていません。

F2/F2e シリーズ モジュールの注意事項と制約事項

- F シリーズ モジュール、M2 シリーズ モジュール、およびスーパーバイザ 2 の特定のレート制限およびパケット サイズ値では、パケット サイズの内部アカウンティングおよび内部ヘッダーのため、SPAN パケット レートは設定された値より少なくなります。
- SPAN サンプリングは F シリーズ モジュールでのみサポートされます。
- 従来の SPAN セッションは、F シリーズおよび M シリーズ モジュールからのトラフィックをサポートします。拡張 SPAN セッションは、F シリーズおよび M2 シリーズ モジュールからのみのトラフィックをサポートします。
- スーパーバイザ帯域内インターフェイスが F2 シリーズ モジュールの送信方向でモニタされる場合、12 バイトの SHIM ヘッダーが SPAN パケットの SMAC の後に追加されます。
- 複数の SPAN 宛先は、F シリーズモジュールが VDC 内に存在する場合はサポートされません。複数の SPAN 宛先が SPAN セッション内で設定されている場合、セッションは F シリーズ モジュールの電源が切断されるか、別の VDC に移動されるか、または複数の SPAN 宛先が単一の宛先に削減されるまでディセーブルになります。
- FabricPath コア ポートは、F シリーズ モジュールが VDC 内に存在する場合は SPAN 宛先としてサポートされません。ただし、FabricPath コア ポートは、SPAN 送信元インターフェイスとして設定できます。
- サテライト ポートおよびホスト インターフェイス ポート チャネル上の SPAN 送信元機能は FEX が F2 または F2e シリーズ モジュールに接続されている場合はサポートされません。
- F1 シリーズまたは F2 シリーズ モジュールで SPAN セッションを使用する場合、特定のセッション内の送信元トラフィックの合計量が SPAN 宛先インターフェイスまたはそのセッションのポート チャネルの容量以下であることを確認してください。SPAN 送信元トラフィックが SPAN 宛先の容量を超えると、SPAN 送信元インターフェイスでパケット ドロップが発生する場合があります。このガイドラインは、F2e シリーズ銅線およびファイバー モジュールには適用されません。
- FEX インターフェイスを含む VLAN を SPAN 送信元にすることができますが、F2 シリーズのモジュール ベースの FEX ポートからの入力トラフィックはキャプチャできません。
- F2 シリーズ モジュールは、FEX をサポートしますが、FEX SPAN はサポートしません。したがって、F2 シリーズを通して接続された FEX インターフェイスは SPAN 送信元にすることはできません。
- F2 シリーズ モジュール上で Fabric ポート チャネルをスパンすることができます。
- レイヤ 3 マルチキャスト出力パケットは F2 シリーズ モジュール上でスパンすることはできません。
- MTU 切り捨ておよび SPAN レート制限は、F シリーズおよび M2 シリーズ モジュールおよびスーパーバイザ 2 でサポートされます。これらの機能は M1 シリーズ モジュールではサポートされていません。

- F2 シリーズ モジュールでは、VNTag ヘッダーが SPAN 宛先で削除されるため、Fabric ポート チャネルでスパンされた入力 FEX パケットは設定された MTU サイズよりも 6 バイト少なくなります。
- F2 シリーズ モジュールでは、MAC-in-MAC ヘッダーが内部的に追加され、SPAN 宛先で削除されるため、レイヤ 2 ポートに入ってくるすべてのトラフィック（エッジツーエッジ トラフィックを含む）の出力 SPAN パケットは設定された MTU サイズよりも 16 バイト少なくなります。
- SPAN の宛先ポート チャネルを使用した F2 シリーズ モジュールでは、SPAN トラフィックはメンバー ポートで分散されます。ただし、分散パターンは正規（SPAN でない宛先）のポート チャネルのものとは異なる場合があります。たとえば、正規のポート チャネルでは均等な負荷分散でも SPAN 宛先ポート チャネルでは不均等な負荷分散（または負荷均衡なし）となる場合があります。
- F シリーズ モジュール、M2 シリーズ モジュール、およびスーパーバイザ 2 の特定のレート制限およびパケット サイズ値では、パケット サイズの内部アカウンティングおよび内部ヘッダーのため、SPAN パケット レートは設定された値より少なくなります。
- SPAN サンプリングは F シリーズ モジュールでのみサポートされます。M シリーズ モジュールではサポートされません。
- Cisco NX-OS Release 6.1 以降では、F2 シリーズ モジュールの FCoE スパンがストレージ VDC でサポートされます。
- ハードウェア セッション 15 は F2 および F2e シリーズ モジュールの NetFlow で使用されます。このハードウェア ID を使用する拡張セッションは F2 および F2e ポートの着信トラフィックをスパンしません。
- F2 および F2e シリーズ モジュールはルール ベースの SPAN を制限付きでサポートします。これらのモジュールは IPv6 送信元 IP フィルタと IPv6 宛先 IP フィルタでワイルドカードはサポートしません。これらのモジュールは宛先 MAC アドレスおよび送信元 MAC アドレスに対する出力 SPAN フィルタリングをサポートしません。

F3 シリーズ モジュールの注意事項と制約事項

- F シリーズ モジュール、M2 シリーズ モジュール、およびスーパーバイザ 2 の特定のレート制限およびパケット サイズ値では、パケット サイズの内部アカウンティングおよび内部ヘッダーのため、SPAN パケット レートは設定された値より少なくなります。
- SPAN サンプリングは F シリーズ モジュールでのみサポートされます。
- 従来の SPAN セッションは、F シリーズおよび M シリーズ モジュールからのトラフィックをサポートします。拡張 SPAN セッションは、F シリーズおよび M2 シリーズ モジュールからのみのトラフィックをサポートします。
- レイヤ 3 マルチキャスト出力パケットは F3 シリーズ モジュール上でスパンすることはできません。

- 複数の SPAN 宛先は、F シリーズモジュールが VDC 内に存在する場合はサポートされません。複数の SPAN 宛先が SPAN セッション内で設定されている場合、セッションは F シリーズ モジュールの電源が切断されるか、別の VDC に移動されるか、または複数の SPAN 宛先が単一の宛先に削減されるまでディセーブルになります。
- MTU 切り捨ておよび SPAN レート制限は、F シリーズおよび M2 シリーズ モジュールおよびスーパーバイザ 2 でサポートされます。
- FabricPath コア ポートは、F シリーズ モジュールが VDC 内に存在する場合は SPAN 宛先としてサポートされません。ただし、FabricPath コア ポートは、SPAN 送信元インターフェイスとして設定できます。
- F3 シリーズ モジュールは IPv6 送信元 IP フィルタと IPv6 宛先 IP フィルタでワイルドカードはサポートしません。

M1/M1XL シリーズ モジュールの注意事項と制約事項

- SPAN サンプリングは M シリーズ モジュールではサポートされません。
- 従来の SPAN セッションは、F シリーズおよび M シリーズ モジュールからのトラフィックをサポートします。拡張 SPAN セッションは、F シリーズおよび M2 シリーズ モジュールからのみのトラフィックをサポートします。
- Cisco NX-OS Release 5.2 以降では、Cisco Nexus 2000 シリーズ Fabric Extender に接続されている Cisco Nexus 2000 シリーズ Fabric Extender（FEX）インターフェイスおよびファブリック ポート チャネルを SPAN 送信元として設定できます。ただし、SPAN 宛先としては設定できません。

（注） Fabric Extender インターフェイスおよびファブリック ポート チャネル上の SPAN は M1 シリーズおよび M2 シリーズ モジュールでサポートされます。SPAN は、Fabric Extender 上ではなく、Cisco Nexus 7000 シリーズ デバイス上で動作します。

- ポート チャネルが Cisco Nexus 7000 M1 シリーズ モジュールが送信元となっている SPAN トラフィックの宛先インターフェイスの場合、インターフェイスの 1 つのメンバーだけがソース パケットのコピーを受信します。この制限は、Cisco Nexus 7000 M1-XL シリーズ モジュールを含むその他すべての Cisco Nexus シリーズ モジュールからの SPAN トラフィックには適用されません。
- MTU 切り捨ておよび SPAN レート制限は、M1 シリーズ モジュールではサポートされません。
- SPAN サンプリングは M シリーズ モジュールではサポートされません。
- マルチキャストのベストエフォート モードは M1 シリーズ モジュールだけに適用されます。

- 拡張 SPAN セッションは入力または出力のいずれの方向でも M1 シリーズ モジュールの着信トラフィックの送信元となることはできません。
- 従来の SPAN セッションは、F シリーズおよび M シリーズ モジュールからのトラフィックをサポートします。拡張 SPAN セッションは、F シリーズおよび M2 シリーズ モジュールからのみのトラフィックをサポートします。
- M1 シリーズ モジュールおよびスーパーバイザ 1 はルール ベースの SPAN をサポートしません。VLAN のフィルタリングだけをサポートします。
- M1 および M2 シリーズのモジュールは、非管理 VDC でのみ例外 SPAN をサポートし、モジュールの少なくとも 1 つのインターフェイスが VDC に存在する必要があります。

M2/M2XL シリーズ モジュールの注意事項と制約事項

- Cisco NX-OS Release 5.2 以降では、Cisco Nexus 2000 シリーズ Fabric Extender に接続されている Cisco Nexus 2000 シリーズ Fabric Extender（FEX）インターフェイスおよびファブリック ポート チャネルを SPAN 送信元として設定できます。ただし、SPAN 宛先としては設定できません。

（注） Fabric Extender インターフェイスおよびファブリック ポート チャネル上の SPAN は M1 シリーズおよび M2 シリーズ モジュールでサポートされます。SPAN は、Fabric Extender 上ではなく、Cisco Nexus 7000 シリーズ デバイス上で動作します。

- F シリーズ モジュール、M2 シリーズ モジュール、およびスーパーバイザ 2 の特定のレート制限およびパケット サイズ値では、パケット サイズの内部アカウンティングおよび内部ヘッダーのため、SPAN パケット レートは設定された値より少なくなります。
- SPAN サンプリングは M シリーズ モジュールではサポートされません。
- 従来の SPAN セッションは、F シリーズおよび M シリーズ モジュールからのトラフィックをサポートします。拡張 SPAN セッションは、F シリーズおよび M2 シリーズ モジュールからのみのトラフィックをサポートします。
- M1 および M2 シリーズのモジュールは、非管理 VDC でのみ例外 SPAN をサポートし、モジュールの少なくとも 1 つのインターフェイスが VDC に存在する必要があります。
- M2 シリーズ モジュールの MTU 切り捨てでは、切り捨てられた SPAN パケットの長さは最も近い 16 バイトの乗数に丸められます。たとえば、65 から 79 の MTU の設定値では、パケットは 64 バイトに丸められます。
- M2 シリーズ モジュールでレート制限をサポートするのは 8 つのセッションだけです。追加のハードウェア セッションは、M2 シリーズ モジュールで設定されたレート リミッタを適用しません。

- M1 および M2 シリーズのモジュールは、非管理 VDC でのみ例外 SPAN をサポートし、モジュールの少なくとも 1 つのインターフェイスが VDC に存在する必要があります。

M3 シリーズ モジュールの注意事項と制約事項

- Cisco NX-OS Release 7.3(1)DX(1) 以降では、SPAN は、M3 シリーズ モジュールでサポートされます。
- SPAN サンプリングは M シリーズ モジュールおよびスーパーバイザ 2 でサポートされます。
- 拡張 SPAN セッションは M3 シリーズ モジュールからのトラフィックをサポートします。F シリーズモジュールが VDC 内に存在する場合、複数の SPAN 宛先がサポートされます。Fx モジュールからの SPAN パケットを送信するには、プライマリ宛先が使用されます。

SPAN のデフォルト設定

次の表に、SPAN パラメータのデフォルト設定を示します。

パラメータ	デフォルト
SPAN セッション	シャット ステートで作成されます。
MTU 切り捨て	ディセーブル
マルチキャスト ベスト エフォート モード	ディセーブル
従来の SPAN セッションの SPAN レート制限	ディセーブル
拡張 SPAN セッションの SPAN レート制限	イネーブル
SPAN サンプリング	ディセーブル

SPAN の設定

（注） この機能の Cisco NX-OS コマンドは、Cisco IOS のコマンドと異なる場合があります。

SPAN セッションの設定

SPAN セッションを設定できるのはローカル デバイス上だけです。デフォルトでは、SPAN セッションはシャット ステートで作成されます。

送信元にはイーサネット ポート、ポート チャネル、スーパーバイザ帯域内インターフェイス、および VLAN（入力のみ）を指定できます。

1 つの SPAN セッションに、イーサネット ポート、VLAN、コントロール プレーン CPU への帯域内インターフェイスを組み合わせた送信元を使用できます。イーサネット ポートのサブインターフェイスを、SPAN セッションの送信元として指定することはできません。

（注）

- モニタ セッションで、レイヤ 3 ポートチャネル サブインターフェイスを SPAN 送信元として使用するには、フィルタ VLAN としてサブインターフェイスに IEEE 802.1Q VLAN カプセル化を設定するときに入力した VLAN ID を指定する必要があります。メイン インターフェイスと SPAN VLAN フィルタを使用して、サブインターフェイス上の 802.1Q VLAN をフィルタする場合、SPAN には、SPAN の宛先ポート上のすべてのサブインターフェイスに対するトラフィックが示されます。
- トランクのメンバを含む VLAN が SPAN 送信元 として設定され、他の一連の VLAN が SPAN VLAN フィルタとして設定されている場合、これらのフィルタ VLAN による不要なトラフィックをキャプチャすることができます。

SPAN 送信元としてスーパーバイザ インバンド インターフェイスを指定すると、デバイスはスーパーバイザ ハードウェアに到達したすべてのパケット（入力）をモニタします。

宛先ポートには、アクセス モードまたはトランク モードのイーサネット ポートまたはポート チャネルを指定できます。すべての宛先ポートでモニタ モードをイネーブルにする必要があります。

双方向性の従来のセッションでは、トラフィックの方向を指定せずにセッションを設定できます。

拡張 SPAN セッションの場合、以下のいずれかの方法でセッションを設定できます。

- セッション作成時に方向を指定せず、**mode extended** コマンドを入力してモードを extended に変更することで双方向セッションを設定します。
- セッション作成時にトラフィック方向を指定することで単方向セッションを設定します。

はじめる前に

正しい VDC 内にいることを確認します。VDC を切り替えるには、switchto vdc コマンドを使用します。

アクセス モードまたはトランク モードで宛先ポートが設定されている必要があります。詳細については、『*Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide*』を参照してください。

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	**interface ethernet***interface slot*/*port*]
	
	例：
	`switch(config)# interface ethernet 2/5`
	`switch(config-if)#`
		選択したスロットおよびポート上でインターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**switchport**
	
	例：
	`switch(config-if)# switchport`
	`switch(config-if)#`
		選択したスロットおよびポートまたはポート範囲でスイッチポート パラメータを設定します。

ステップ 4	**switchport mode** [**access**|**trunk**|**private-vlan**]
	
	例：
	`switch(config-if)# switchport mode trunk`
	`switch(config-if)#`
		選択したスロットおよびポートまたはポート範囲でスイッチポート パラメータを設定します。
		• アクセス
		• トランク
		• private-vlan

ステップ 5	**switchport monitor** [**ingress** [**learning**]] 例： `switch(config-if)# switchport monitor`	SPAN 宛先としてスイッチポート インターフェイスを設定します。 • **ingress**： （任意）SPAN 宛先ポートが、特定の TCP パケット ストリームを中断するパケットを注入できるようにします。たとえば、ネットワークでは IDS を使用します。 • **ingress learning**： SPAN 宛先ポートがパケットを注入できるようにし、MAC アドレス学習を可能にします。たとえば、IDS MAC アドレスです。
ステップ 6	ステップ 2 および 3 を繰り返して、追加の SPAN 宛先でモニタリングを設定します。	（任意） —

	コマンドまたはアクション	目的
ステップ 7	**no monitor session***session-number* 例： `switch(config)# no monitor session 3`	指定した SPAN セッションのコンフィギュレーションを消去します。新しいセッション コンフィギュレーションは、既存のセッション コンフィギュレーションに追加されます。

ステップ 8	**monitor session***session-number* [**shut**]
	
	例：
	`switch(config)# monitor session 3 rx`
	`switch(config-monitor)#`
	
	例：
	`switch(config)# monitor session 3 tx`
	`switch(config-monitor)#`
	
	例：
	`switch(config)# monitor session 3 shut`
	`switch(config-monitor)#`
		指定した SPAN セッションのコンフィギュレーションを消去します。新しいセッション コンフィギュレーションは、既存のセッション コンフィギュレーションに追加されます。
		
		モニタ コンフィギュレーション モードを開始します。新しいセッション コンフィギュレーションは、既存のセッション コンフィギュレーションに追加されます。デフォルトでは、セッションが shut ステートで作成されます。このセッションは、ローカル SPAN セッションです。オプションのキーワードは次のとおりです。
		• rx：入力拡張 SPAN セッションを指定します。
		• tx：出力拡張 SPAN セッションを指定します。
		• shut：選択したセッションに対して shut 状態を指定します。

ステップ 9	**mode extended** 例： `switch(config-monitor)# mode extended`	（任意）SPAN セッションを拡張双方向セッションとして設定します。 （注） 単方向の SPAN セッションではこのコマンドは使用できません。
ステップ 10	**description***description* 例： `switch(config-monitor)# description my_span_session_3`	セッションの説明を設定します。デフォルトでは、説明は定義されません。説明には最大 32 の英数字を使用できます。

ステップ 11	**source** {**interface** {**all** | *type*} | **vlan** {*number* | *range*}} [**rx** | **tx** | **both**]
	
	例：
	`switch(config-monitor)# source interface ethernet 2/1-3, ethernet 3/1 rx`
	
	例：
	`switch(config-monitor)# source interface port-channel 2`
		送信元およびパケットをコピーするトラフィックの方向を設定します。イーサネット ポートの範囲、ポート チャネル、帯域内インターフェイス、VLAN の範囲、Cisco Nexus 2000 Series Fabric Extender インターフェイス、または Cisco Nexus 2000 Series Fabric Extender に接続されたファブリック ポート チャネルを入力できます。
		
		送信元は 1 つ設定することも、またはカンマで区切った一連のエントリとして、または番号の範囲として、複数設定することもできます。最大 128 のインター

	コマンドまたはアクション	目的

	例：
	`switch(config-monitor)# source interface sup-eth 0 both`
	
	例：
	`switch(config-monitor)# source vlan 3, 6-8 rx`
	
	例：
	`switch(config-monitor)# source interface ethernet 101/1/1-3`
	
	例：
	`switch(config-monitor)# source interface all rx`
		フェイスを指定できます。VLAN の範囲は 1 ～ 3967 です。4048 ～ 4093 の VLAN の範囲は、6.1 以前の Cisco NX-OS リリースでもサポートされます。
		コピーするトラフィック方向を、入力（rx）、出力（tx）、または両方向（both）として指定できます。デフォルトは both です。単一方向のセッションには、送信元の方向はセッションで指定された方向に一致する必要があります。Cisco NX-OS Release 7.3(0)D1(1) 以降では、**all** キーワードを使用してモニタリング セッションをイネーブルにし、物理ポート、ポートチャネル、FEX ポート、および FEX ポート チャネルなど、VDC 内のすべての VLAN とポートをモニタできます。**all** キーワードは、拡張 SPAN セッションでのみサポートされます。

ステップ 12	ステップ 11 を繰り返して、すべての SPAN 送信元を設定します。	（任意） —
ステップ 13	**filter vlan** {*number* | *range*} [**include-untagged**] 例： `switch(config-monitor)# filter vlan 3-5, 7`	（任意） （任意）設定された送信元から選択する VLAN を設定します。VLAN は 1 つ設定することも、またはカンマで区切った一連のエントリとして、または番号の範囲として、複数設定することもできます。VLAN の範囲は 1 ～ 3967 です。4048 ～ 4093 の VLAN の範囲は、6.1 以前の Cisco NX-OS リリースでもサポートされます。 include-untagged キーワードは、VLAN アクセス マップを 1 つ以上の VLAN に適用し、さらに、レイヤ 3 サブインターフェイスのポート上にタグなしフレームを含めます。 **filter vlan** コマンドと **source interface all** コマンドを使用して無関係の VLAN をフィルタすることにより、拡張 SPAN モニタ セッションで現在サポートされている VLAN 送信元制限よりも多くの、指定の VLAN 送信元をモニタできます。
ステップ 14	ステップ 13 を繰り返して、すべての送信元 VLAN のフィルタリングを設定します。	（任意） —

	コマンドまたはアクション	目的
ステップ 15	**destination interface***type* {*number* | *range*} 例： `switch(config-monitor)# destination interface ethernet 2/5, ethernet 3/7`	コピーする送信元パケットの宛先を設定します。宛先は 1 つ設定することも、またはカンマで区切った一連のエントリとして、または番号の範囲として、複数設定することもできます。最大 128 のインターフェイスを指定できます。 （注） SPAN宛先ポートは、アクセス ポートまたはトランク ポートのどちらかにする必要があります。 （注） Cisco Nexus 2000 シリーズ Fabric Extender インターフェイスおよび Cisco Nexus 2000 シリーズ Fabric Extender に接続されたファブリック ポート チャネルは、SPAN 宛先として設定できません。
ステップ 16	ステップ 15 を繰り返して、すべてのSPAN宛先ポートを設定します。	（任意） —
ステップ 17	**no shut** 例： `switch(config-monitor)# no shut`	SPAN セッションをイネーブルにします。デフォルトでは、セッションはシャット ステートで作成されます。
ステップ 18	**show monitor session** {**all** | *session-number* | **range***session-range*} [**brief**] 例： `switch(config-monitor)# show monitor session 3`	（任意） SPAN 設定を表示します。
ステップ 19	**copy running-config startup-config** 例： `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。

F2 シリーズ モジュールでの複数宛先 SPAN の設定

Cisco Nexus 7000 スイッチで SPAN セッションの複数宛先ポートを設定する手順は次のとおりです。

- 複数の SPAN 宛先ポートを設定する際に,モジュール タイプ制限を削除して、SPAN セッションを許可します。
- Fx モジュールのいずれか、またはスーパーバイザを含む VDC でプライマリ宛先ポートを指定し、SPAN セッションをアクティブ化します。

（注） プライマリ宛先の設定は、M シリーズ モジュールから発信される SPAN パケットの転送には影響しません。SPAN セッションをアクティブ化するにはプライマリ宛先をアクティブ化する必要があります。

送信元には、ポート、VLAN または RSPAN VLAN を指定できます。

はじめる前に

F シリーズ モジュール（F1/F2/F2E/F3）を含む VDC では、複数宛先 SPAN セッションはサポートされていませんでした。そのため、そのようなセッションは、設定されていても、VDC で有効になりませんでした。Cisco NX-OS Release 7.2 以降では、複数宛先 SPAN セッションがサポートされます。Fx モジュールからの SPAN パケットを送信するには、プライマリ宛先が使用されます。

はじめる前に

正しい VDC を使用していることを確認します（または **switch to vdc** コマンドを使用します）。

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	**no monitor session***session-number* 例： `switch(config)# no monitor session 3`	指定した SPAN セッションのコンフィギュレーションを消去します。新しいセッション コンフィギュレーションは、既存のセッション コンフィギュレーションに追加されます。

ステップ 3	**monitor session***session-number*
	
	例：
	`switch(config)# monitor session 4 rx`
	`switch(config-monitor)#`
	
	例：
	`switch(config)# monitor session 3 tx`
	`switch(config-monitor)#`
		モニタ コンフィギュレーション モードを開始します。既存のセッション設定に新しいセッション設定が追加され、これにより、送信元レート制限が設定される SPAN セッションが指定されます。デフォルトでは、セッションが shut ステートで作成されます。このセッションは、ローカル SPAN セッションです。

	コマンドまたはアクション	目的
ステップ 4	**source** {**interface***type* | **vlan** {*number* | *range*}} [**rx** | **tx** | **both**] 例： `switch(config-monitor)# source interface ethernet 2/1-3, ethernet 3/1 rx`	送信元およびパケットをコピーするトラフィックの方向を設定します。イーサネット ポート範囲、ポート チャネル、帯域内インターフェイス、または VLAN 範囲を入力できます。 送信元は 1 つ設定することも、またはカンマで区切った一連のエントリとして、または番号の範囲として、複数設定することもできます。最大 128 のインターフェイスを指定できます。 コピーするトラフィック方向を、入力（rx）、出力（tx）、または両方向（both）として指定できます。デフォルトは both です。 （注） 送信元 VLAN は、入力（rx）方向に限りサポートされます。
ステップ 5	ステップ 4 を繰り返して、すべての仮想 SPAN VLAN 送信元を設定します。	（任意） —
ステップ 6	**destination interface***type* {*number* | *range*} [primary] 例： `switch(config-monitor)# destination interface ethernet 2/5, ethernet 3/7 primary`	コピーする送信元パケットの宛先を設定します。宛先は 1 つ設定することも、またはカンマで区切った一連のエントリとして、または番号の範囲として、複数設定することもできます。ただし、このようなプライマリ ポートは、1 つのセッションに 1 つしか設定できません。最大 128 のインターフェイスを指定できます。 （注） SPAN 宛先ポートは、アクセス ポートまたはトランク ポートのどちらかにする必要があります。
ステップ 7	**no rate-limit** 例： `switch(config-monitor)# no rate limit`	SPAN トラフィックのレート制限を設定します。
ステップ 8	**no destination interface***type* {*number* | *range*} [primary] 例： `switch(config-monitor)# destination interface ethernet 2/5, ethernet 3/7 primary`	宛先ポートにプライマリ属性が設定されていないことを確認します。複数のポートが設定されている場合、エラー メッセージを表示します。 （注） ERROR：1 つのセッションに複数の「プライマリ」宛先ポートは設定できません。
ステップ 9	ステップ 12 を繰り返して、すべての送信元 VLAN のフィルタリングを設定します。	（任意） —

	コマンドまたはアクション	目的
ステップ 10	**no shut** 例： `switch(config-monitor)# no shut`	SPAN セッションをイネーブルにします。デフォルトでは、セッションはシャットステートで作成されます。
ステップ 11	**show monitor session** {**all** | *session-number* | **range***session-range*} [**brief**] 例： `switch(config-monitor)# show monitor session 3`	（任意） SPAN 設定を表示します。
ステップ 12	**copy running-config startup-config** 例： `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。

SPAN 宛先ポートでの複数 SPAN セッションの設定

はじめる前に

正しい VDC を使用していることを確認します（または **switch to vdc** コマンドを使用します）。

はじめる前に

複数の SPAN セッションを導入する場合、複数の SPAN セッションで宛先インターフェイスを共有することが重要です。これにより、SPAN セッションとトラフィックをモニタする N7K のハードウェア コストを削減できるだけでなく、全体的なネットワーク接続を簡素化できます。

- SPAN 宛先ポートを共有している SPAN セッションでは、レート リミッタの auto モードは使用できません。
- 個々の SPAN セッションにレート制限が必要な場合、manual モードが推奨されます。

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。

	コマンドまたはアクション	目的

ステップ 2	**monitor session***session-number*[*session-type*]
	
	例：
	`switch(config)# monitor session 3 span`
	`switch(config-monitor)#`
		モニタ コンフィギュレーション モードを開始し、SPAN セッションを指定します。

ステップ 3	**destination interface** {**ethernet x/y** | **port-channel z**} 例： `switch(config-monitor)# destination interface ethernet1/2`	（任意）宛先ポートを追加するオプションを指定します。 （注） レート制限の auto は、複数のセッションでSPAN宛先ポートを共有するため、ディセーブルにする必要があります。ただし、レート制限の auto が宛先ポートでイネーブルの場合に、宛先ポートがすでに他のいずれかの SPAN セッションで使用されている場合、auto モードをディセーブルにするよう要求されます。
ステップ 4	**no rate-limit** {**auto** | **rate-value**} 例： `switch(config-monitor-local)# no rate-limit auto`	（任意）レート制限をイネーブルにします。 （注） レート制限の autoは、複数のセッションで SPAN 宛先ポートを共有するため、ディセーブルにする必要があります。SPAN セッションで共有宛先ポートを設定すると、共有宛先ポートを削除するまで、CLI は拒否されるようになります。

仮想 SPAN セッションの設定

仮想 SPAN セッションを設定すると、送信元ポート、VLAN、および RSPAN VLAN からローカル デバイス上の宛先ポートへのパケットをコピーできます。デフォルトでは、SPAN セッションはシャット ステートで作成されます。

送信元には、ポート、VLAN または RSPAN VLAN を指定できます。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

トランク モードで宛先ポートが設定されています。詳細については、『Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide』を参照してください。

switchport monitor コマンドを使用して、SPAN セッションをモニタする宛先ポートが設定されています。

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	**no monitor session***session-number* 例： `switch(config)# no monitor session 3`	指定した SPAN セッションのコンフィギュレーションを消去します。新しいセッション コンフィギュレーションは、既存のセッション コンフィギュレーションに追加されます。

ステップ 3	**monitor session***session-number*
	
	例：
	`switch(config)# monitor session 3 rx`
	`switch(config-monitor)#`
	
	例：
	`switch(config)# monitor session 3 tx`
	`switch(config-monitor)#`
	
	例：
	`switch(config)# monitor session 3 shut`
	`switch(config-monitor)#`
		モニタ コンフィギュレーション モードを開始します。新しいセッション コンフィギュレーションは、既存のセッション コンフィギュレーションに追加されます。デフォルトでは、セッションが shut ステートで作成されます。このセッションは、ローカル SPAN セッションです。オプションの shut キーワードは、選択したセッションに対して shut ステートを指定します。

ステップ 4	**source** {**interface***type* | **vlan** {*number* | *range*}} [**rx** | **tx** | **both**]
	
	例：
	`switch(config-monitor)# source interface ethernet 2/1-3, ethernet 3/1 rx`
	
	例：
	`switch(config-monitor)# source interface port-channel 2`
	
	例：
	`switch(config-monitor)# source interface sup-eth 0 both`
	
	例：
	`switch(config-monitor)# source vlan 3, 6-8 rx`
	
	例：
	`switch(config-monitor)# source interface ethernet 101/1/1-3`
		送信元およびパケットをコピーするトラフィックの方向を設定します。イーサネット ポート範囲、ポート チャネル、帯域内インターフェイス、または VLAN 範囲を入力できます。
		
		送信元は 1 つ設定することも、またはカンマで区切った一連のエントリとして、または番号の範囲として、複数設定することもできます。最大 128 のインターフェイスを指定できます。
		
		コピーするトラフィック方向を、入力（rx）、出力（tx）、または両方向（both）として指定できます。デフォルトは both です。
		
		（注） 送信元 VLAN は、入力（rx）方向に限りサポートされます。
		
		単一方向のセッションには、送信元の方向はセッションで指定された方向に一致する必要があります。

	コマンドまたはアクション	目的
ステップ 5	ステップ 4 を繰り返して、すべての仮想 SPAN VLAN 送信元を設定します。	（任意） —
ステップ 6	**destination interface***type* {*number* | *range*} 例： `switch(config-monitor)# destination interface ethernet 2/5, ethernet 3/7`	コピーする送信元パケットの宛先を設定します。宛先は 1 つ設定することも、またはカンマで区切った一連のエントリとして、または番号の範囲として、複数設定することもできます。最大128のインターフェイスを指定できます。 （注） SPAN 宛先ポートは、アクセス ポートまたはトランク ポートのどちらかにする必要があります。
ステップ 7	ステップ12を繰り返して、すべての送信元 VLAN のフィルタリングを設定します。	（任意） —
ステップ 8	**no shut** 例： `switch(config-monitor)# no shut`	SPANセッションをイネーブルにします。デフォルトでは、セッションはシャット ステートで作成されます。
ステップ 9	**show monitor session** {**all** | *session-number* | **range***session-range*} [**brief**] 例： `switch(config-monitor)# show monitor session 3`	（任意） SPAN 設定を表示します。
ステップ 10	**interface ethernet***slot/port [port]* 例： `switch(config)# interface ethernet 2/5 switch(config-if)#`	選択したスロットおよびポートまたはポート範囲で、インターフェイス コンフィギュレーション モードを開始します。
ステップ 11	**switchport trunk allowed vlan** {**all** | *session-number* | **range***session-range*} [**brief**] 例： `switch(config-monitor)# show monitor session 3`	（任意） インターフェイスで許可する VLAN の範囲を設定します。既存の VLAN に対して追加または削除する、指定した以外のすべての VLAN を選択する、すべての VLAN を選択する、またはすべての VLAN を選択しないでおくことができます。デフォルトでは、インターフェイス上ですべての VLAN が許可されます。 VLANは1つ設定することも、またはカンマで区切った一連のエントリとして、または番号の範囲として、複数設定することもできます。VLANの範囲は 1 ～ 3967 です。

	コマンドまたはアクション	目的
		4048 ～ 4093 の VLAN の範囲は、6.1 以前の Cisco NX-OS リリースでもサポートされます。
ステップ 12	（任意）ステップ 10 および 11 を繰り返して、各宛先ポートで許可する VLAN を設定します。	
ステップ 13	（任意）**show interface ethernet** 例： `switch(config)# interface ethernet 2/5 switch(config-if)#`	（任意）選択したスロットおよびポートまたはポート範囲に対応するインターフェイス トランキング設定を表示します。
ステップ 14	**copy running-config startup-config** 例： `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。

RSPAN VLAN の設定

リモート SPAN（RSPAN）VLAN を SPAN セッション送信元として指定できます。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

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	**vlan***vlan* 例： `switch(config)# vlan 901 switch(config-vlan)#`	指定した VLAN の VLAN コンフィギュレーション モードを開始します。
ステップ 3	**remote-span** 例： `switch(config-vlan)# remote-span`	VLAN を RSPAN VLAN として設定します。

	コマンドまたはアクション	目的

ステップ 4	**exit**
	
	例：
	`switch(config-vlan)# exit`
	`switch(config)#`
		VLAN コンフィギュレーション モードを終了します。

ステップ 5	（任意）**show vlan** 例： `switch(config)# show vlan`	（任意）VLAN コンフィギュレーションを表示します。RSPAN VLAN が一覧表示されます。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） （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。

SPAN セッションのシャットダウンまたは再開

SPAN セッションをシャットダウンすると、送信元から宛先へのパケットのコピーを切断することができます。1 セッションをシャット ダウンしてハードウェア リソースを解放し、別のセッションをイネーブルにできます。デフォルトでは、SPAN セッションはシャット ステートで作成されます。

SPAN セッションを再開（イネーブルに）すると、送信元から宛先へのパケットのコピーを再開できます。すでにイネーブルになっていて、動作状況がダウンの SPAN セッションをイネーブルにするには、そのセッションをいったんシャットダウンしてから、改めてイネーブルにする必要があります。

SPAN セッションのシャット ステートおよびイネーブル ステートは、グローバルまたはモニタ コンフィギュレーション モードのどちらのコマンドでも設定できます。

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。

	コマンドまたはアクション	目的
ステップ 2	[no] **monitor session** {*session-range* | **all**} **shut** 例： `switch(config)# monitor session 3 shut`	指定の SPAN セッションをシャットダウンします。デフォルトでは、セッションはシャット ステートで作成されます。 コマンドの **no** 形式は、指定された SPAN セッションを再開（イネーブルに）します。デフォルトでは、セッションはシャット ステートで作成されます。 （注） モニタ セッションがイネーブルで動作状況がダウンの場合、セッションをイネーブルにするには、最初に **monitor session shut** コマンドを指定してから、**no monitor session shut** コマンドを続ける必要があります。

ステップ 3	**monitor session***session-number*
	
	例：
	`switch(config)# monitor session 3`
	`switch(config-monitor)#`
		モニタ コンフィギュレーション モードを開始します。新しいセッション コンフィギュレーションは、既存のセッション コンフィギュレーションに追加されます。

ステップ 4	[no] **shut** 例： `switch(config-monitor)# shut`	SPANセッションをシャットダウンします。デフォルトでは、セッションはシャット ステートで作成されます。 コマンドの **no** 形式は SPAN セッションをイネーブルにします。デフォルトでは、セッションはシャット ステートで作成されます。
ステップ 5	**show monitor** 例： `switch(config-monitor)# show monitor`	（任意） SPAN セッションのステータスを表示します。
ステップ 6	**copy running-config startup-config** 例： `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。

SPAN セッションごとの MTU の切り捨ての設定

SPANトラフィック帯域幅を減らすには、SPANセッションの各複製パケットで許可される最大バイト数を設定できます。この値は、最大伝送単位（MTU）の切り捨てサイズと呼ばれます。設定されたサイズよりも大きい SPAN パケットはすべて、設定されたサイズに切り捨てられます。

（注） F1 シリーズ モジュール上の同じ SPAN セッションに対して MTU 切り捨ておよび SPAN レート制限をイネーブルにすることはできません。1 セッションで両方を設定した場合、レート制限の設定をディセーブルにするまで、レート制限だけが F1 シリーズ モジュールで許可され、MTU 切り捨てがディセーブルになります。この制限は、F2 および M2 シリーズ モジュールまたはスーパーバイザ 2 には適用されません。

（注） MTU の切り捨てと SPAN サンプリングは同時にイネーブルにでき、互いに優先順位はありません。これは、送信元パケットのさまざまな側面（サイズ対パケット数）に適用されるためです。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

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	**monitor session***session-number*
	
	例：
	`switch(config)# monitor session 3`
	`switch(config-monitor)#`
		モニタ コンフィギュレーション モードを開始し、MTU 切り捨てサイズが設定された SPAN セッションを指定します。

ステップ 3	**[no] mtu***mtu* 例： `switch(config-monitor)# mtu 64`	指定した SPAN セッションのパケットの MTU 切り捨てサイズを設定します。指定できる範囲は 64 ～ 1500 バイトです。

ステップ 4	**show monitor session***session-number*
	
	例：
	`switch(config)# monitor session 3`
	`switch(config-monitor)#`
		（オプション）MTU 切り捨ての設定ステータス、セッションごとに各パケットで許可される最大バイト数、MTU 切り捨てがサポートされるモジュールとサポートされないモジュールを含む、SPAN セッションのステータスを表示します。

ステップ 5	**copy running-config startup-config** 例： `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。

各 SPAN セッションのソース レート制限の設定

SPAN セッションが高トラフィック環境の送信元として複数のインターフェイスまたは VLAN に設定されている場合、宛先ポートが過負荷状態になり、送信元ポートの通常のデータ トラフィックの障害となる可能性があります。この問題、また送信元転送インスタンスでのトラフィック過負荷は、各 SPAN セッションに送信元レート制限を設定することで軽減できます。

（注） F1 シリーズ モジュール上の同じ SPAN セッションに対して MTU 切り捨ておよび SPAN レート制限をイネーブルにすることはできません。1 セッションで両方を設定した場合、レート制限の設定をディセーブルにするまで、レート制限だけが F1 シリーズ モジュールで許可され、MTU 切り捨てがディセーブルになります。この制限は、F2 および M2 シリーズ モジュールまたはスーパーバイザ 2 には適用されません。

（注） SPAN サンプリングは SPAN 送信元レート制限に優先されます。レート制限は、サンプリングが SPAN ソース パケットで完了した後に発生します。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

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	**monitor session***session-number*
	
	例：
	`switch(config)# monitor session 3`
	`switch(config-monitor)#`
		モニタ コンフィギュレーション モードを開始し、送信元レート制限が設定された SPAN セッションを指定します。

	コマンドまたはアクション	目的
ステップ 3	**[no] rate-limit {auto | *rate-limit*}** 例： `switch(config-monitor)# rate-limit auto`	自動または手動での指定された SPAN セッションの SPAN パケットの送信元レート制限を設定します。 • 自動モード：次のように、自動的にギガバイト単位でレート制限を計算します：宛先帯域幅/合計送信元帯域幅。たとえば、ギガバイトごとのレート制限が 0.5 の場合、各送信元トラフィックについて、パケットの 0.5 G のみスパンされます。 入力トラフィックの場合、送信元が可能な最大帯域幅でスパンされるように、ギガバイトごとの制限が、SPAN 送信元として使用されるポートの数に基づいて F シリーズ モジュールの各転送エンジンに適用されます。出力トラフィックの場合、ギガバイトごとの制限が、SPAN 送信元として使用されるポートの数に関係なく F シリーズ モジュールの各転送エンジンに適用されます。 • 手動モード：モジュールの各転送エンジンから送信できる SPAN パケットの最大レートのパーセンテージを指定します。範囲は 1 ～ 100 です。たとえば、レート制限が 10 パーセントの場合、F シリーズ モジュールの各転送エンジンから送信できる SPAN パケットの最大レートは 1G（10G ライン レートの 10 パーセント）です。

ステップ 4	**show monitor session***session-number*
	
	例：
	`switch(config)# monitor session 3`
	`switch(config-monitor)#`
		（任意）レート制限の設定ステータスを含む SPAN セッションのステータス、セッションごとに許可される最大 SPAN レートの割合、およびレート制限がサポートされるまたはサポートされないモジュールを表示します。

ステップ 5	**copy running-config startup-config** 例： `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。

各 SPAN セッションのサンプリングの設定

Cisco NX-OS Release 6.1 以降では、SPAN トラフィック帯域幅を削減し、ピアツーピア トラフィックをモニタするために、スパンされたトラフィックに対してサンプリング範囲を設定できます。パケット範囲ベースのサンプリングが SPAN 送信元パケットの正確な値を提供するために使用されます。

（注） サンプリングと MTU の切り捨ては同時にイネーブルにでき、互いに優先順位はありません。これは、送信元パケットのさまざまな側面（パケット数対サイズ）に適用されるためです。ただし、サンプリングはSPAN送信元レート制限に優先されます。レート制限は、サンプリングが SPAN ソース パケットで完了した後に発生します。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

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	**monitor session***session-number*
	
	例：
	`switch(config)# monitor session 3`
	`switch(config-monitor)#`	

ステップ 3	**monitor session***session-number* [*rt*|*tx*] [*shut*] 例： `switch(config-monitor)# sampling 100`	SPAN 送信元パケットのサンプリングの範囲を設定します。サンプリング値は、x パケットから 1 つのパケットがスパンされる範囲です。x は 2 から 1023 です。この例では、100 パケットごとに 1 つのパケットがスパンされます。
ステップ 4	**show monitor session** {**all** | *session-number* | **range***session-range*} [**brief**] 例： `switch(config-monitor)# show monitor session 3`	（任意） SPAN サンプリングのステータス、サンプリング値、およびサンプリングがサポートされるまたはサポートされないモジュールを含む、SPAN セッションのステータスを表示します。

	コマンドまたはアクション	目的
ステップ 5	**copy running-config startup-config** 例： `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。

複雑ルール ベース SPAN

はじめる前に

複数のフィルタおよび製品テーブル リソースによって複雑なフィルタ ルールを作成できます。本リリースでは、いくつかのキーワード、**Match**、**Permit**、**Deny** および **Filter-list** が導入されました。Match キーワードにより、ユーザは、フィールドや値セットで照合を行うことができます。フィルタ名の前に Permit キーワードを入れると、すべてのフィルタが一致した場合に、SPAN コピーが生成されます。フィルタ名の前に Deny キーワードを入れると、すべてのフィルタが一致しなかった場合に、SPAN コピーが生成されます。Filter-list は、permit および deny キーワードにより定義されるルールをすべて指定するキーワードです。

（注） 各フィルタ リストに複数の permit-deny ルールを含めることができます。

フィルタの作成

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

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	**monitorfilter***filter-name*
	
	例：
	`switch(config)# monitor filter test-filter`
	`switch(config-monitor-filter)#`
		モニタ フィルタ コンフィギュレーション モードを開始します。
		（注） 文字列の長さが 32 文字を超えることはできません。

	コマンドまたはアクション	目的

ステップ 3	**match**[**eth-type***eth-type* | **src-mac***mac-addressmac-mask* | **dest-mac***mac-addressmac-mask* | **frame-type** *[arp| eth | fcoe |ipv4 |ipv6*]
	
	例：
	`switch(config-monitor-filter)# match eth-type 0x0800`
	`switch(config-monitor-filter)# match src-mac 40:55:39:0c:98:c1 ff:ff:ff:ff:ff:00 dest-mac 40:55:39:0c:98:c1 ff:ff:ff:ff:ff:00`
		モニタ フィルタ コンフィギュレーション モードでパケット内の特定のフィールドを照合します。
		（注） 同じ行、複数の行で指定した一致基準による結果は同じです。

フィルタ リストの作成

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

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	**monitorfilter-list***filter-list-name*
	
	例：
	`switch(config)# monitor filter-list sample-filter-list`
	`switch(config-monitor-filter-list)#`
		モニタ フィルタ コンフィギュレーション モードを開始します。
		（注） 文字列の長さが 32 文字を超えることはできません。

ステップ 3	**permitfilter***filter-names* **denyfilter***filter-names* 例： `switch(config-monitor-filter-list)# permit filter test-filter deny`	フィルタ リストでフィルタを許可および/または拒否するには、このコマンドを使用します。

	コマンドまたはアクション	目的

	`filter test-filter1`
	`switch(config-monitor-filter-list)#`
	
	`switch(config-monitor-filter-list)#`
	`permit filter test-filter2`
	`switch(config-monitor-filter-list)#`
	
	`switch(config-monitor-filter-list)#`
	`deny filter test-filter3`
	`switch(config-monitor-filter-list)#`
		（注）
		• コマンド **permit filter***filter-names* **denyfilter***filter-names* が同じ行で指定されている場合、ルールはすべての permit および deny 基準を照合し、その場合、permit フィルタ X と deny フィルタ Y にあるフィルタ x およびフィルタ y に一致するパケットが SPAN-の対象となります（AND 条件）。
		• コマンド **permit filter***filter-names* **denyfilter***filter-names* が別々の行で指定されている場合、ルールは permit または deny 基準のいずれかを照合し、その場合、permit フィルタ X と deny フィルタ Y にあるフィルタ x またはフィルタ y に一致するパケットが SPAN-の対象となります（OR 条件）。

モニタリング セッションへのフィルタ リストの関連付け

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

（注） SPAN セッションに複雑なフィルタをアタッチする必要がある場合は、SPAN セッションにすでにアタッチされたフィルタがないことを確認します。

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。

	コマンドまたはアクション	目的

ステップ 2	**monitor session***session-number* [*rt*|*tx*]
	
	例：
	`switch(config)# monitor session 3 rx`
	`switch(config-monitor)# filter filter-list sample-filter-list`
		モニタ コンフィギュレーション モードを開始し、SPAN セッションを指定します。オプションのキーワードは次のとおりです。
		• rx：入力拡張 SPAN セッションを指定します。
		• tx：出力拡張 SPAN セッションを指定します。
		（注） • Nexus 7000 シリーズ スイッチの SPAN セッションにフィルタ リストをアタッチする場合、SPAN セッション内で **mode extended** コマンドを指定する必要があります。
		• フィルタの方向は、SPAN セッション方向から取得されます。

ステップ 3	**exit** 例： `switch(config-monitor)# exit`	グローバル コンフィギュレーション モードに戻ります。

ルールがイネーブルなセッションの設定

ローカル/単一方向 ERSPAN 送信元/双方向セッションを作成するには、次を設定します。

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	**monitor session***session-number* [*rt*|*tx*] [*shut*]
	
	例：
	`switch(config)# monitor session 3 rx`
	`switch(config-monitor)#`
		ローカル SPAN/ERSPAN セッションを設定するためのモニタ コンフィギュレーション モードを開始します。オプションのキーワードは次のとおりです。
		• rx：入力拡張 SPAN セッションを指定します。
		• tx：出力拡張 SPAN セッションを指定します。

	コマンドまたはアクション	目的
		• shut：選択したセッションに対して shut 状態を指定します。
ステップ 3	**mode extended** 例： `switch(config-monitor)# mode extended`	（任意）モードを、双方向セッションの拡張モードに変更します。
ステップ 4	**filter frame-typesource-ip src-ip** 例： `switch(config-monitor)# filter frame-type ipv4 src-ip 10.1.1.3/32 cos 3`	セッションにルール ベースのフィルタを関連付けます。

ステップ 5	**source interface ethernet x/y**
	
	例：
	`switch(conf-monitor)# source interface Ethernet 4/7`
	`switch(conf-monitor)# destination interface Ethernet 4/7`
		送信元ポートと宛先ポートを関連付けます。

ステップ 6	**no shut** 例： `switch(config-monitor)# no shut`	セッションを表示します。 （注） フィルタ コマンドを個別の行に分割して、セッション モードで設定することができます。セッションで指定されたすべてのフィルタは、AND ルールで制御されます。

SPAN セッションのマルチキャスト ベスト エフォート モードの設定

任意の SPAN セッションのマルチキャスト ベスト エフォート モードを設定できます。デフォルトでは、SPAN レプリケーションが入力および出力モジュールの両方で実行されます。マルチキャストのベスト エフォート モードをイネーブルにすると、SPAN レプリケーションは、マルチキャスト トラフィックの入力モジュールか、レイヤ 3 インターフェイスから出て行くパケットの出力モジュールのみで行われます（つまり、出力モジュールでは、レイヤ 2 インターフェイスから出て行くパケットは、SPAN 用にレプリケートされません）。

（注） レイヤ 3 マルチキャスト トラフィックでは、SPAN レプリケーションが出力モジュールで発生します。トラフィックが複数の出力モジュールにマルチキャストされる場合、各パケットに対して複数の SPAN コピーをキャプチャできます（つまり、各出力モジュールから 1 つのコピー）。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

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	**monitor session***session-number*
	
	例：
	`switch(config)# monitor session 3`
	`switch(config-monitor)#`
		モニタ コンフィギュレーション モードを開始し、送信元レート制限が設定された SPAN セッションを指定します。

ステップ 3	**[no] multicast best-effort** 例： `switch(config-monitor)# multicast best-effort`	指定された SPAN セッションのマルチキャスト ベスト エフォート モードを設定します。

ステップ 4	**show monitor session***session-number*
	
	例：
	`switch(config)# monitor session 3`
	`switch(config-monitor)#`
		（任意）レート制限の設定ステータスを含む SPAN セッションのステータス、セッションごとに許可される最大 SPAN レートの割合、およびレート制限がサポートされるまたはサポートされないモジュールを表示します。

ステップ 5	**copy running-config startup-config** 例： `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。

ルール ベース SPAN の設定

一連のルールに基づいて入力または出力 SPAN トラフィックにフィルタを設定できます。単純なフィルタには 1 つのみのルールがあり、このルールに複数のフィールドまたは組み合わせを追加できます。パケットは、すべての条件が満たされた場合にのみスパンされます。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

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	**monitor session***session-number* [**shut**]
	
	例：
	`switch(config)# monitor session 3`
	`switch(config-monitor)#`
		モニタ コンフィギュレーション モードを開始します。新しいセッション コンフィギュレーションは、既存のセッション コンフィギュレーションに追加されます。デフォルトでは、セッションが shut ステートで作成されます。このセッションは、ローカル SPAN セッションです。オプションのキーワードは次のとおりです。
		• **rx**：入力拡張 SPAN セッションを指定します。
		• **tx**：出力拡張 SPAN セッションを指定します。
		• **shut**：選択したセッションに対して shut 状態を指定します。

ステップ 3	**mode extended** 例： `switch(config-monitor)# mode extended`	（任意）SPAN セッションを拡張双方向セッションとして設定します。
ステップ 4	[**no**] **filter**[*vlan-range*] [**bpdu** [**true** | **false**]] [**cos***cos-value*] [**dest-mac***dest-mac*] [**eth-type** *eth-value*] [**flow-hash***flow-value*] [**frame-type** [**eth** | **arp** | **fcoe** | **ipv4** | **ipv6**]] [**pc-lane***port-number*] [**src_mac***mac-address*] [**trace-route** [**true** | **false**]]	SPAN セッションのフィルタを設定します。セッションからフィルタを削除するには、このコマンドの **no 形式** を入力します。オプションのキーワードは次のとおりです。 • **vlan**：VLAN の範囲に基づいてフィルタを指定します。

	コマンドまたはアクション	目的

	例：
	`switch(config-monitor)# filter vlan 10,20`
	`switch(config-monitor)# filter frame-type arp trace-route true`
	`switch(config-monitor)# filter bpdu false`
		• **bpdu**：パケットのブリッジ プロトコル データ ユニット（BPDU）クラスに基づいてフィルタを指定します。
		• **cos**：サービス クラス（CoS）に基づいて dotlq ヘッダーにフィルタを指定します。
		• **dest-mac**：宛先 MAC アドレスに基づいてフィルタを指定します。
		• **eth-type**：イーサネット タイプに基づいてフィルタを指定します。
		• **flow-hash**：Result Bundle Hash（RBH）値に基づいてフィルタを指定します。
		• **frame-type**：フレーム タイプに基づいてフィルタを指定します。
		• **pc-lane**：ポート チャネル メンバーに基づいてフィルタを指定します。
		• **src-mac**：送信元 MAC アドレスに基づいてフィルタを指定します。
		• **trace-route**：ヘッダーのルート ビットに基づいてフィルタを指定します。

ステップ 5	[**no**]**filter frame-type eth** 例： `switch(config-monitor)# filter frame-type eth`	（任意） （任意）SPAN セッションのイーサネット フレーム タイプのフィルタを設定します。セッションからフィルタを削除するには、このコマンドの **no** 形式を入力します。
ステップ 6	[**no**]**filter frame-type arp** [[**arp-rarp** [**arp** | **rarp**]] [**req-resp** [**req** |**rsp**]] [**sender-ip** *ip-address*] [**target-ip***ip-address*]] 例： `switch(config-monitor)# filter frame-type arp arp-rarp arp`	（任意） （任意）SPAN セッションの ARP フレーム タイプのフィルタを設定します。セッションからフィルタを削除するには、このコマンドの **no** 形式を入力します。オプションのキーワードは次のとおりです。 • **arp-rarp**：ARP または RARP フレーム タイプのフィルタを指定します。 • **req-resp**：要求または応答に基づいてフィルタを指定します。 • **sender-ip**：送信者の IP アドレスに基づいてフィルタを指定します。

	コマンドまたはアクション	目的
		• **target-ip**：受信者の IP アドレスに基づいてフィルタを指定します。
ステップ 7	[**no**]**filter frame-type fcoe fcoe** [[**fc-sid***FC-source-ID*] [**fc-did***FC-dest-ID*] [**fcoe-type***fcoe-value*] [**r-ctl***r-ctl-value*] [**sof***sof-value*] [**cmd-code***cmd-value*]] 例： `switch(config-monitor)# filter frame-type fcoe`	（任意） （任意）SPAN セッションの FCoE フレーム タイプのフィルタを設定します。セッションからフィルタを削除するには、このコマンドの **no 形式**を入力します。オプションのキーワードは次のとおりです。 • **fc-sid**：FC 送信元 ID に基づいてフィルタを指定します。 • **fc-did**：FC 宛先 ID に基づいてフィルタを指定します。 • **fcoe-type**：FCoE タイプに基づいてフィルタを指定します。 • **r-ctl**：ルーティング制御フラグ（R CTL）値に基づいてフィルタを指定します。 • **sof**：フレーム開始（SOF）パケットに基づいてフィルタを指定します。 • **cmd-code**：コマンド コードに基づいてフィルタを指定します。
ステップ 8	[**no**]**filter frame-type ipv4** [[**src-ip***src-ip*] [**dest-ip***dest-ip*] [**tos** tos-value] [**l4-protocol***l4-value*]] 例： `switch(config-monitor)# filter frame-type ipv4 l4-protocol 3`	（任意） （任意）SPAN セッションの IPv4 フレーム タイプのフィルタを設定します。セッションからフィルタを削除するには、このコマンドの no 形式を入力します。オプションのキーワードは次のとおりです。 • **src-ip**：IPv4 送信元 IP アドレスに基づいてフィルタを指定します。 • **dest-ip**：IPv4 宛先 IP アドレスに基づいてフィルタを指定します。 • **tos**：IP ヘッダーのタイプ オブ サービス（TOS）に基づいてフィルタを指定します。 • **l4-protocol**：IP ヘッダーのプロトコル フィールドに設定されたレイヤ 4 プロトコル数に基づいてフィルタを指定します。

	コマンドまたはアクション	目的
ステップ 9	[**no**]**filter frame-type ipv6** [[**src-ip***src-ip*] [**dest-ip***dest-ip*] [**tos** tos-value] [**l4-protocol***l4-value*]] 例： `switch(config-monitor)# filter frame-type ipv6 src-ip 10.0.0.1`	（任意） （任意）SPAN セッションの IPv6 フレーム タイプのフィルタを設定します。セッションからフィルタを削除するには、このコマンドの no 形式を入力します。オプションのキーワードは次のとおりです。 • **src-ip**：IPv6 送信元 IP アドレスに基づいてフィルタを指定します。 • **dest-ip**：IPv4 宛先 IP アドレスに基づいてフィルタを指定します。 • **tos**：IP ヘッダーのタイプ オブ サービス（TOS）に基づいてフィルタを指定します。 • **l4-protocol**：IP ヘッダーのプロトコル フィールドに設定されたレイヤ 4 プロトコル数に基づいてフィルタを指定します。
ステップ 10	（任意）ステップ 4 から 9 をセッションのすべてのフィルタに対して繰り返します。	
ステップ 11	**source** {**interface** *type* | **vlan** {*number* | *range*}} [**rx** | **tx** | **both**] 例： `switch# configure terminal switch(config)#`	（任意）送信元およびパケットをコピーするトラフィックの方向を設定します。イーサネット ポートの範囲、ポート チャネル、帯域内インターフェイス、VLAN の範囲、Cisco Nexus 2000 Series Fabric Extender インターフェイス、または Cisco Nexus 2000 Series Fabric Extender に接続されたファブリック ポート チャネルを入力できます。送信元は 1 つ設定することも、またはカンマで区切った一連のエントリとして、または番号の範囲として、複数設定することもできます。 最大 128 のインターフェイスを指定できます。VLAN の範囲は 1 ～ 3967 です。4048 ～ 4093 の VLAN の範囲は、6.1 以前の Cisco NX-OS リリースでもサポートされます。 コピーするトラフィック方向を、入力（rx）、出力（tx）、または両方向（both）として指定できます。デフォルトは both です。 単一方向のセッションには、送信元の方向はセッションで指定された方向に一致する必要があります。

	コマンドまたはアクション	目的
ステップ 12	**destination interface***type* {*number* | *range*} 例： `switch(config-monitor)# destination interface ethernet 2/5, ethernet 3/7`	コピーする送信元パケットの宛先を設定します。宛先は 1 つ設定することも、またはカンマで区切った一連のエントリとして、または番号の範囲として、複数設定することもできます。最大 128 のインターフェイスを指定できます。 （注） SPAN 宛先ポートは、アクセス ポートまたはトランク ポートのどちらかにする必要があります。 （注） Cisco Nexus 2000 シリーズ Fabric Extender インターフェイスおよび FEX に接続されたファブリック ポート チャネルは、SPAN 宛先として設定できません。
ステップ 13	**no shut** 例： `switch(config-monitor)# no shut`	SPAN セッションをイネーブルにします。デフォルトでは、セッションはシャット ステートで作成されます。
ステップ 14	**show monitor session** {**all** | *session-number* | **range***session-range*} [**brief**] 例： `switch(config-monitor)# show monitor session 3`	（任意） SPAN 設定を表示します。
ステップ 15	**copy running-config startup-config** 例： `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。

例外 SPAN の設定

例外パケットをスパンするようにデバイスを設定できます。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

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	**monitor session***session-number* [**rx**|**tx**| **both**]
	
	例：
	`switch(config)# monitor session 3`
	`switch(config-monitor)#`
		モニタ コンフィギュレーション モードを開始し、SPAN セッションを指定します。オプションのキーワードは次のとおりです。
		• **rx**：入力拡張 SPAN セッションを指定します。
		• **tx**：出力拡張 SPAN セッションを指定します。
		• **shut**：選択したセッションに対して shut 状態を指定します。

ステップ 3	**mode extended** 例： `switch(config-monitor)# mode extended`	（任意） （任意）SPAN セッションを、コマンドの拡張双方向セッション形式で設定します。
ステップ 4	[**source exception**{**layer3**|**fabricpath**|**other** | **all**} 例： `switch(config-monitor)# filter frame-type eth`	（任意） 送信元を例外の SPAN セッションとして設定します。以下の例外タイプがサポートされます。 • **layer3**：レイヤ 3 例外タイプを指定します。 • **fabricpath**：FabricPath 例外タイプを指定します。 • **other**：ドロップ宛先インターフェイスが組み込まれているリダイレクト登録を通してドロップされたその他の例外を指定します。 • **all**：レイヤ 3、FabricPath およびその他のすべての例外が含まれます。
ステップ 5	**destination interface***type [number* |*range*} 例： `switch(config-monitor)# destination interface ethernet 2/5, ethernet 3/7`	コピーする送信元パケットの宛先を設定します。宛先は 1 つ設定することも、またはカンマで区切った一連のエントリとして、または番号の範囲として、複数設定することもできます。最大 128 のインターフェイスを指定できます。 （注） SPAN 宛先ポートは、アクセス ポートまたはトランク ポートのどちらかにする必要があります。

	コマンドまたはアクション	目的
		（注） Cisco Nexus 2000 シリーズ Fabric Extender インターフェイスおよび FEX に接続されたファブリック ポート チャネルは、SPAN 宛先として設定できません。
ステップ 6	**no shut** 例： `switch(config)# no shut`	SPAN セッションをイネーブルにします。デフォルトでは、セッションはシャット ステートで作成されます。
ステップ 7	**show monitor session***session-number* 例： `switch(config)# show monitor session 3`	（任意）レート制限の設定ステータスを含む SPAN セッションのステータス、セッションごとに許可される最大 SPAN レートの割合、およびレート制限がサポートされるまたはサポートされないモジュールを表示します。
ステップ 8	**copy running-config startup-config** 例： `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。

FabricPath および VNTAG ヘッダーの削除

FabricPath や VNTAG ヘッダーを認識しない SPAN 宛先ポートに接続されたデバイスを使用している場合には、これらのヘッダーをパケットから除去したい場合があります。

グローバルまたはポート レベルで、これを行うことができます。VDC 内のすべての SPAN 宛先ポートへのヘッダーを削除するには、グローバル コマンドを適用します。特定のポートにのみコマンドを適用するには、ポート レベルのコマンドを使用します。ポートが SPAN 宛先ポートでない場合、コマンドは拒否されます。

この機能のグローバル設定とポート レベル設定の両方を入力した場合、ポート レベル設定がグローバル設定を上書きします。

（注） ポート レベル コマンドはグローバル コマンドを上書きします。したがって、グローバル設定でヘッダーを除去するようデバイスを設定し、その後、ポート レベル コマンドの no 形式を発行して、指定したポートでヘッダーを除去しないよう設定できます。

グローバルなヘッダーの削除

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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	switch(config)# **system default switchport monitor exclude header**	VDC 内のすべての SPAN 宛先ポートの FabricPath および VNTAG ヘッダーを削除します。 SPAN宛先ポートでパケットのヘッダーを保持するには、このコマンドの **no** 形式を使用します。
ステップ 3	switch(config)# **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。

ポートごとのヘッダーの削除

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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	switch(config)# **interface***type* {*module* | *port*}	インターフェイス モードを開始して、FabricPath および VNTAG ヘッダーを削除する 1 つまたは複数のポートを指定します。
ステップ 3	switch(config)# [**no**]**switchport monitor exclude header**	（任意） VDC 内の指定の SPAN 宛先ポートの FabricPath および VNTAG ヘッダーを削除します。 SPAN 宛先ポートでパケットのヘッダーを保持するには、このコマンドの **no** 形式を使用します。

	コマンドまたはアクション	目的
ステップ 4	switch(config)# **exit**	（任意） グローバル コンフィギュレーション モードに戻ります。
ステップ 5	switch# **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。

SPAN の設定確認

SPAN の設定を表示するには、次のいずれかの作業を行います。

コマンド	目的
show monitor session {**all** | *session-number* | **range***session-range*} [**brief**]	SPAN セッションの設定を表示します。
show resource monitor-session	従来のセッションで使用可能なリソースを表示します。
show resource monitor-session-extended	拡張セッションで使用可能なリソースを表示します。
show running-config	SPAN の FabricPath および VNTAG ヘッダーを削除するコマンドの設定を表示します。

SPAN のコンフィギュレーション例

SPAN セッションのコンフィギュレーション例

SPAN セッションを設定する手順は、次のとおりです。

手順

ステップ 1 アクセス モードで宛先ポートを設定し、SPAN モニタリングをイネーブルにします。

例：

```
switch# configure terminal
switch(config)# interface ethernet 2/5
switch(config-if)# switchport
switch(config-if)# switchport monitor
switch(config-if)# no shut
switch(config-if)# exit
switch(config)#
```

ステップ 2 SPAN セッションを設定します。

例：

```
switch(config)# no monitor session 3
switch(config)# monitor session 3
switch(config-monitor)# source interface ethernet 2/1-3, ethernet 3/1 rx
switch(config-monitor)# source interface port-channel 2
switch(config-monitor)# source interface sup-eth 0 both
switch(config-monitor)# source vlan 3, 6-8 rx
switch(config-monitor)# source interface ethernet 101/1/1-3
switch(config-monitor)# filter vlan 3-5, 7
switch(config-monitor)# destination interface ethernet 2/5
switch(config-monitor)# no shut
switch(config-monitor)# exit
switch(config)# show monitor session 3
switch(config)# copy running-config startup-config
```

拡張 SPAN モニタ セッション内のすべての VLAN とポートをモニタする設定例

次に、拡張 SPAN モニタ セッションですべての VLAN とポートをモニタする例を示します。

```
switch# configure terminal
switch(config)# monitor session 3
switch(config-monitor)# mode extended
switch(config-monitor)# source interface all
switch(config-monitor)# destination interface ethernet 2/5
switch(config-monitor)# no shut
switch(config-monitor)# exit
switch(config)# show monitor session 3
switch(config)# copy running-config startup-config
```

次に、拡張 SPAN モニタ セッションで現在サポートされている VLAN 送信元制限よりも多くの、指定の VLAN 送信元をモニタする例を示します。

```
switch# configure terminal
switch(config)# monitor session 2
switch(config-monitor)# mode extended
switch(config-monitor)# source interface all
switch(config-monitor)# filter vlan 1-1000
switch(config-monitor)# destination interface ethernet 4/1
switch(config-monitor)# no shut
switch(config-monitor)# exit
switch(config)# show monitor session 2
switch(config)# copy running-config startup-config
```

単一方向 SPAN セッションの設定例

単一方向 SPAN セッションを設定するには、次の手順を実行します。

手順

ステップ 1 アクセス モードで宛先ポートを設定し、SPAN モニタリングをイネーブルにします。

例：

```
switch# configure terminal
switch(config)# interface ethernet 2/5
switch(config-if)# switchport
switch(config-if)# switchport monitor
switch(config-if)# no shut
switch(config-if)# exit
switch(config)#
```

ステップ 2 SPAN セッションを設定します。

例：

```
switch(config)# no monitor session 3
switch(config)# monitor session 3 rx
switch(config-monitor)# source interface ethernet 2/1-3, ethernet 3/1 rx
switch(config-monitor)# filter vlan 3-5, 7
switch(config-monitor)# destination interface ethernet 2/5
switch(config-monitor)# no shut
switch(config-monitor)# exit
switch(config)# show monitor session 3
switch(config)# copy running-config startup-config
```

仮想 SPAN セッションの設定例

手順

ステップ 1 アクセス モードまたはトランク モードで宛先ポートを設定し、SPAN モニタリングをイネーブルにします。

例：

```
switch# configure terminal
 switch(config)# interface ethernet 3/1
  switch(config-if)# switchport
  switch(config-if)# switchport mode trunk
  switch(config-if)# switchport trunk allowed vlan add 100-200
  switch(config-if)# switchport monitor
  switch(config-if)# no shut
  switch(config-if)# exit
switch(config)# interface ethernet 3/2
  switch(config-if)# switchport
```

```
  switch(config-if)# switchport mode trunk
  switch(config-if)# switchport trunk allowed vlan add 201-300
  switch(config-if)# switchport monitor
  switch(config-if)# no shut
 switch(config-if)# exit
switch(config)#
```

ステップ 2 SPAN セッションを設定します。

例：

```
switch(config)# no monitor session 4
switch(config)# monitor session 4tx
  switch(config-monitor)# source vlan 100-300
  switch(config-monitor)# destination interface ethernet 3/1-2
  switch(config-monitor)# no shut
  switch(config-monitor)# exit
switch(config)# show monitor session 4
switch(config)# copy running-config startup-config
```

プライベート VLAN 送信元の SPAN セッションの設定例

プライベート VLAN 送信元が含まれる SPAN セッションを設定する手順は、次のとおりです。

手順

ステップ 1 送信元 VLAN を設定します。

例：

```
switch# configure terminal
  switch(config)# vlan 100
    switch(config-vlan)# private-vlan primary
    switch(config-vlan)# exit
    switch(config)# interface ethernet 3/1
  switch(config-if)# switchport
    switch(config-if)# switchport access vlan 100
    switch(config-if)# no shut
    switch(config-if)# exit
  switch(config)# interface ethernet 3/2
    switch(config-if)# switchport
    switch(config-if)# switchport mode trunk
    switch(config-if)# switchport trunk native vlan 100
    switch(config-if)# no shut
    switch(config-if)# exit
  switch(config)#
```

ステップ 2 アクセス モードまたはトランク モードで宛先ポートを設定し、SPAN モニタリングをイネーブルにします。

例：

```
switch# configure terminal
  switch(config)# interface ethernet 3/3
    switch(config-if)# switchport
    switch(config-if)# switchport mode trunk
    switch(config-if)# switchport trunk allowed vlan add 100-200
```

```
  switch(config-if)# switchport monitor
    switch(config-if)# switchport access vlan 100
    switch(config-if)# no shut
    switch(config-if)# exit
  switch(config)#
```

ステップ 3 SPAN セッションを設定します。

例：

```
switch# no monitor session 3
switch(config)# monitor session 3
  switch(config-if)# source vlan 100
  switch(config-if)# destination interface ethernet 3/3
  switch(config-if)# no shut
  switch(config-if)# exit
switch(config-if)# show monitor session 3
switch(config-if)# copy running-config startup-config
```

SPAN の MTU 切り捨ておよび SPAN サンプリングの設定例

次に、SPAN セッションの MTU 切り捨ておよび SPAN サンプリングを設定する例を示します。

```
switch# configure terminal
switch(config)# monitor session 3
switch(config-monitor)# mtu 100
switch(config-monitor)# sampling 10
switch(config-monitor)# show monitor session 3
```

ルール ベース SPAN の設定例

次に、ルール ベースの SPAN セッションを設定する例を示します。

```
switch# configure terminal
switch(config)# monitor session 3
switch(config-monitor)# mode extended
switch(config-monitor)# filter frame-type ipv4 src-ip 10.1.1.1/24
switch(config-monitor)# source interface ethernet 2/1-3, ethernet 3/1 rx
switch(config-monitor)# destination interface ethernet 2/5, ethernet 3/7
switch(config-monitor)# no shut
switch(config)# show monitor session 3
```

例外 SPAN の設定例

次に、例外パケットをスパンするように SPAN セッションを設定する例を示します。

```
switch# configure terminal
switch(config)# monitor session 3
switch(config-monitor)# source exception all
switch(config-monitor)# destination interface ethernet 2/5, ethernet 3/7
switch(config-monitor)# no shut
switch(config)# show monitor session 3
```

関連資料

表 *33* : 関連資料

関連項目	マニュアル タイトル
『Cisco Network Analysis Module (NAM)』	『*Cisco Network Analysis Module (NAM) for Nexus 7000 Quick Start Guide*』
VDC	『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』
ファブリック エクステンダ	『*Cisco Nexus 2000 Series Fabric Extender Software Configuration Guide*』
SPAN コマンド：コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト、使用上の注意事項、および例	『*Cisco Nexus 7000 Series NX-OS System Management Command Reference*』

SPAN の機能の履歴

次の表に、このマニュアルの新機能および変更された機能を要約し、各機能がサポートされているリリースを示します。ご使用のソフトウェア リリースで、本書で説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。

表 *34* : *SPAN* の機能の履歴

機能名	リリース	機能情報
SPAN	7.3(0)DX(1)	M3 シリーズ モジュールのサポートが追加されました。
SPAN	7.3(0)D1(1)	SPAN セッションあたり 4K の VLAN のサポートが追加されました。
SPAN	6.2(10)	SPAN パケットから FabricPath および VLAN タグ ヘッダーを削除するサポートが追加されました。

SPAN	6.2(2)	SPAN データソースに対する NAM サポートが追加されました。
SPAN	6.2(2)	F2e シリーズ モジュールでのみ、Tx 方向の SPAN 送信元としての FEX ポートのサポートが追加されました。
SPAN	6.2(2)	拡張 SPAN のサポートが追加されました。
SPAN	6.2(2)	ルール ベースの SPAN のサポートが追加されました。
SPAN	6.2(2)	例外 SPAN のサポートが追加されました。
SPAN	6.1(1)	SPAN サンプリングのサポートが追加されました。
SPAN	6.1(1)	帯域内インターフェイスが管理 VDC 以外の任意の VDC から送信元として追加可能になりました。
SPAN	6.1(1)	スーパーバイザ 2 のサポートが追加されました。
SPAN	6.1(1)	M2 シリーズ モジュールのサポートが追加されました。
SPAN	6.1(1)	ストレージ VDC に対して F2 シリーズ モジュール上で FCoE SPAN サポートが追加されました。
SPAN	6.0(1)	F2 シリーズ モジュールのサポートが追加されました。
SPAN	5.2(1)	Cisco Nexus 2000 Series Fabric Extender インターフェイスに対する SPAN 送信元サポートが追加されました。

SPAN	5.2(1)	各 SPAN セッションに対する MTU 切り捨て、送信元レート制限、およびマルチキャスト ベスト エフォートを設定する機能が追加されました。
SPAN	5.1(1)	F1 シリーズ モジュールのサポートが追加され、サポートされる SPAN セッションが 18 から 48 に増加されました。
SPAN	4.1(3)	SPAN セッションの上限の表が追加されました。

第 18 章

ERSPAN の設定

この章は、カプセル化リモート スイッチド ポート アナライザ（ERSPAN）を Cisco NX-OS デバイスの IP ネットワークでミラーリングされたトラフィックを転送するように設定する方法について説明します。

この章の内容は、次のとおりです。

- 機能情報の確認，377 ページ
- ERSPAN について，378 ページ
- ERSPAN のライセンス要件，383 ページ
- ERSPAN の前提条件，383 ページ
- ERSPAN の注意事項および制約事項，384 ページ
- デフォルト設定，389 ページ
- ERSPAN の設定，389 ページ
- ERSPAN 設定の確認，410 ページ
- ERSPAN の設定例，410 ページ
- 関連資料，413 ページ
- ERSPAN の機能の履歴，414 ページ

機能情報の確認

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

ERSPAN について

ERSPAN は、IP ネットワークでミラーリングされたトラフィックを転送して、ネットワーク内で複数のスイッチのリモート モニタリングを提供します。トラフィックは、送信元ルータでカプセル化され、ネットワーク間を転送されます。パケットは宛先ルータでカプセル化解除され、宛先インターフェイスに送信されます。

ERSPAN タイプ

Cisco NX-OS Release 6.1 以降のリリースは、ERSPAN タイプ II および タイプ III をサポートします。以前のすべての Cisco NX-OS リリースでは ERSPAN タイプ II のみがサポートされました。

ERSPAN タイプ III は ERSPAN タイプ II のすべての特徴と機能をサポートし、以下の拡張機能が追加されています。

- ERSPAN タイプ III ヘッダーに、エッジ、集約、およびコア スイッチ間でパケット遅延を計算するために使用できるタイムスタンプ情報を表示。
- ERSPAN タイプ III ヘッダー フィールドを使用して潜在的なトラフィック ソースを識別。
- クロック マネージャが ERSPAN タイマーを同期する方法を指定するためにすべての VDC にわたってタイムスタンプ詳細を設定する機能を提供。

ERSPAN 送信元

トラフィックをモニタできるモニタ元インターフェイスのことを ERSPAN 送信元と呼びます。送信元では、監視するトラフィックを指定し、さらに入力、出力、または両方向のトラフィックをコピーするかどうかを指定します。ERSPAN 送信元には次のものが含まれます。

- イーサネット ポートおよびポート チャネル。
- コントロール プレーン CPU の帯域内インターフェイス：帯域内インターフェイスをモニタできるのは、デフォルト仮想デバイス コンテキスト（VDC）からに限定されます。すべての VDC からの帯域内トラフィックがモニタされます。
- VLAN（入力のみ）：VLAN が ERSPAN 送信元として指定されている場合は、VLAN 内でサポートされているすべてのインターフェイスが ERSPAN 送信元になります。
- Cisco Nexus 2000 Series Fabric Extender（FEX）に接続されたファブリック ポート チャネル。
- Cisco Nexus 2000 Series Fabric Extender 上のサテライト ポートおよびホスト インターフェイス ポート チャネル：これらのインターフェイスは、レイヤ 2 アクセス モード、レイヤ 2 トランク モード、およびレイヤ 3 モードでサポートされます。

（注） レイヤ 3 サブインターフェイスはサポートされません。

（注） 1 つの ERSPAN セッションに、上述の送信元を組み合わせて使用できます。

サポートされる ERSPAN セッション数に関する情報については、『*Cisco Nexus 7000 Series NX-OS Verified Scalability Guide*』を参照してください。

ERSPAN 送信元ポートには、次の特性があります。

- 送信元ポートとして設定されたポートを宛先ポートとしても設定することはできません。
- ERSPAN は送信元に関係なく、スーパーバイザ 1 によって生成されるパケットをモニタしません。この制限はスーパーバイザ 2 には適用されません。

ERSPAN 宛先

宛先ポートは ERSPAN 送信元からコピーされたトラフィックを受信します。

ERSPAN 宛先元ポートには、次の特性があります。

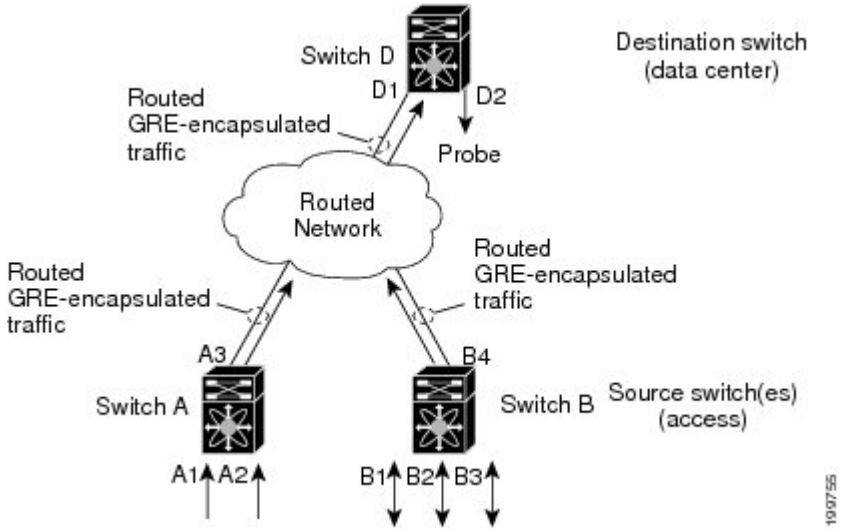
- ERSPANセッションの宛先には、アクセス モードまたはトランク モードのイーサネット ポートまたはポートチャネル インターフェイスが含まれます。
- 宛先ポートとして設定されたポートを送信元ポートとしても設定することはできません。
- 宛先ポートは、一度に 1 つの ERSPAN セッションだけで設定できます。
- 宛先ポートはスパニングツリー インスタンスまたはレイヤ 3 プロトコルに参加しません。
- 入力および入力学習オプションは、モニタ宛先ポートではサポートされていません。
- F シリーズ モジュールのコア ポート、Fabric Extender ホスト インターフェイス（HIF）ポート、HIF ポート チャネル、およびファブリック ポート チャネル ポートは ERSPAN 宛先ポートとしてサポートされていません。

ERSPAN セッション

モニタする送信元と宛先を指定する ERSPAN セッションを作成できます。

次の図に、ERSPAN の設定を示します。

図 *6*：*ERSPAN* の設定



拡張 ERSPAN セッション

Cisco NX-OS Release 6.2(2) 以降のリリースでは、前のリリースでサポートされた 2 つの従来の ERSPAN セッションに加えて拡張 ERSPAN セッションもサポートされます。拡張 ERSPAN セッションは双方向および単方向の両方が可能です。セッションの方向はセッション作成時に指定されます。12 の独立したセッション リソースのプールを使用できます。単方向セッションは 1 つのリソースを使用し、双方向セッションは 2 つのリソースを使用します。これら 12 のリソースがすべての VDC にわたってローカルおよび ERSPAN 送信元セッションで共有されます。

Cisco Nexus 7710 スイッチまたは Cisco Nexus 7718 スイッチで拡張 SPAN セッションを設定している場合、以下が適用されます。

- **mode extended** コマンドを使用する必要はありません。すべてのセッションがデフォルトで拡張されます。
- 必要に応じて 16 のセッションを単方向または双方向として設定できます。
- 2 つの従来のセッションを維持する必要はありません。
- リソース マネージャを使用して 2 つの従来のセッションを予約する必要はありません。
- ERSPAN ACL ベースのフィルタリングはサポートされていません。

ERSPAN セッションあたり 4K の VLAN

Cisco NX-OS Release 7.3(0)D1(1) 以降では、ERSPAN セッションあたり 4K の VLAN がサポートされます。**source interface all** コマンドを使用してスイッチでのモニタ セッションをイネーブルにす

ると、物理ポート、ポート チャネル、FEX ポート、および FEX ポート チャネルなど、VDC 内のすべての VLAN とポートをモニタできます。さらに、ERSPAN セッションあたり 4K の VLAN 機能では、**filter vlan** コマンドと **source interface all** コマンドを使用して無関係の VLAN をフィルタすることにより、モニタ セッションで現在サポートされている VLAN 送信元制限よりも多くの、指定の VLAN 送信元をモニタできます。

ERSPAN セッションあたり 4K の VLAN 機能には、次の特性があります。

- **source interface all** コマンドは、同じ VDC 内の複数のセッションに使用できます。
- MTU 切り捨て、サンプリング、レート制限など、すべてのセッション パラメータをサポートします。
- **source interface all** コマンドは、単純および複雑ルール ベースの SPAN をサポートします。これにより、VDC 全体で一連のフィルタ ルールを使用してトラフィック フロー ベースのモニタリングをすることができます。
- スーパーバイザが生成するトラフィックはスパンされません。
- Cisco Nexus 7000 シリーズ スイッチのイーサネット VDC においてのみサポートされます。
- 拡張 SPAN セッションでのみサポートされます。

ルール ベースの ERSPAN

ルール ベースの ERSPAN は、一連のルールに基づいて入力または出力 ERSPAN トラフィックをフィルタします。6.2(2) より前の Cisco NX-OS リリースでは、VLAN、宛先インデックス、および送信元インデックスをフィルタできました。Cisco NX-OS Release 6.2(2) 以降では、レイヤ 2、レイヤ 3、またはレイヤ 4 ヘッダー パケットのフィールドの組み合わせに基づいて ERSPAN トラフィックをフィルタできます。

すべての ERSPAN セッション（従来および拡張）には関連するフィルタがあります。すべての ERSPAN セッションには 1 つのフィルタ リソースがあります。単純なフィルタには 1 つのみのルールがあり、このルールに複数のフィールドまたは組み合わせを追加できます。パケットは、すべての条件が満たされた場合にのみスパンされます。

イーサネット	IPv4	IPv6	ARP/RARP	FCoE
フレーム タイプ VLAN TR BPDU ポート チャネル レーン フロー ハッシュ L2 MAC DA L2 MAC SA EtherType CoS/VL	フレーム タイプ VLAN TR BPDU ポート チャネル レーン フロー ハッシュ L2 MAC DA L2 MAC SA EtherType CoS/VL ToS L4 Protocol IPv4 SA IPv4 DA	フレーム タイプ VLAN TR BPDU ポート チャネル レーン フロー ハッシュ L2 MAC DA L2 MAC SA EtherType CoS/VL ToS L4 Protocol IPv6 SA IPv6 DA	フレーム タイプ VLAN TR BPDU ポート チャネル レーン フロー ハッシュ L2 MAC DA L2 MAC SA EtherType CoS/VL 『ARP』 Request 送信者 IP Target IP	フレーム タイプ VLAN TR BPDU ポート チャネル レーン フロー ハッシュ L2 MAC DA L2 MAC SA EtherType CoS/VL FCD_ID FCS_ID SOF R_CTL TYPE Cmd_Code Sec_Hdr Exists

例外 ERSPAN

例外 ERSPAN を使用して、例外パケットをスパンできます。侵入検知システム（IDS）、レイヤ 3 IP 識別、および FabricPath で失敗したパケットは例外パケットとして扱われます。

例外 ERSPAN セッションは、2 つの従来の ERSPAN セッションのいずれかまたは拡張 ERSPAN セッションのいずれかでサポートされます。レート リミッタ、MTU トランケーション、およびサンプリングは例外 ERSPAN セッションでサポートされます。ドロップ宛先インターフェイスに送信された例外パケットのみが ERSPAN 送信元としてサポートされます。スーパーバイザ、ACLQoS、またはレイヤ 2 にプッシュされた例外パケットはスパンされません。各 VDC は、1 つの例外 ERSPAN セッションのみサポートします。

例外 ERSPAN は出力方向でのみサポートされます。拡張 ERSPAN Rx セッションの場合、例外送信元設定は拒否されます。

Network Analysis Module; ネットワーク解析モジュール

Cisco Network Analysis Module（NAM）を使用して ERSPAN データ ソースをモニタし、アプリケーション パフォーマンス、トラフィック、およびパケット ヘッダーを分析することもできます。

Cisco Nexus 7000 NetFlow データ ソースのモニタリングに NAM を使用する詳細については、『*Cisco Nexus 7000 Series Network Analysis Module (NAM-NX1) Quick Start Guide*』を参照してください。

ハイ アベイラビリティ

ERSPAN 機能はステートレスおよびステートフル 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 スイッチオーバー後に、実行コンフィギュレーションを適用します。

ハイ アベイラビリティの詳細については、『*Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide*』を参照してください。

仮想化のサポート

仮想デバイス コンテキスト（VDC）は、一連のシステム リソースを論理的に表現する用語です。ERSPAN が適用されるのは、コマンドが入力された VDC だけです。

（注） 帯域内インターフェイスをモニタできるのは、デフォルトの VDC からだけです。すべての VDC からの帯域内トラフィックがモニタされます。

VDC の設定方法については、『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』を参照してください。

ERSPAN 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
Cisco NX-OS	ERSPAN 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 nx-os イメージにバンドルされており、無料で提供されます。NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

ERSPAN の前提条件

ERSPAN には、次の前提条件があります。

- 各デバイス上で、まず所定の ERSPAN 設定をサポートするポートを設定する必要があります。詳細については、『*Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide*』を参照してください。

ERSPAN の注意事項および制約事項

ERSPAN 設定時の注意事項と制約事項は次のとおりです。

- ERSPAN セッションの制限については、『*Cisco Nexus 7000 Series NX-OS Verified Scalability Guide*』を参照してください。
- すべての ERSPAN レプリケーションはハードウェアで行われます。スーパーバイザ CPU は関与しません。
- Supervisor 2 によって生成されるコントロール プレーン トラフィックは ERSPAN によるカプセル化が可能ですが、ERSPAN ACL によるフィルタはできません。
- Supervisor 1 によって生成されるコントロール プレーン パケットは ERSPAN によってカプセル化することも ERSPAN ACL によってフィルタリングすることもできません。
- ERSPAN および ERSPAN ACL は、F1 シリーズ モジュールではサポートされていません。F1 シリーズ モジュールを持つ VDC のみに対して、ERSPAN 送信元セッションと宛先セッションおよびERSPAN ACL 送信元セッションを設定できますが、表示されることはありません。
- ERSPAN 送信元セッションは、F2 シリーズおよび F2e（拡張）シリーズ モジュール上でサポートされます。Cisco NX-OS Release 6.2(2) 以降では、ERPSPAN の宛先セッションは、以下のモジュールでもサポートされます。ただし、ERSPAN ACL セッションは F2 シリーズおよび F2e シリーズ モジュールではサポートされません。
- ERSPAN 送信元、宛先、および ACL セッションは M シリーズ モジュールでサポートされます。
- 総称ルーティング カプセル化（GRE）または F1 シリーズ モジュールで受信される ERSPAN パケットのカプセル化解除はサポートされません。
- ERSPAN と ERSPAN ACL セッションは、宛先ルータで同様に終了します。
- ERSPAN は、管理ポートではサポートされません。
- 宛先ポートは、一度に 1 つの ERSPAN セッションだけで設定できます。
- ポートをソース ポートと宛先ポートの両方として設定することはできません。
- 1 つの ERSPAN セッションに、次の送信元を組み合わせて使用できます。
  - イーサネット ポートまたはポート チャネル（サブ インターフェイスを除く）。
  - VLAN（入力のみ）
  - コントロール プレーン CPU へのインバンド インターフェイスまたはポート チャネル。

（注） ERSPAN は送信元に関係なく、スーパーバイザによって生成されるパケットをモニタしません。

- 宛先ポートはスパニングツリー インスタンスまたはレイヤ 3 プロトコルに参加しません。
- ERSPAN セッションに、送信方向または送信および受信方向でモニタされている送信元ポートまたはVLAN送信元が含まれている場合、パケットが実際にはその送信元ポートで送信されなくても、これらのポートが受け取るパケットがERSPANの宛先ポートに複製される可能性があります。ソース ポート上でのこの動作の例を、次に示します。
  - フラッディングから発生するトラフィック
  - ブロードキャストおよびマルチキャスト トラフィック
- 送信元ポートで ERSPAN をイネーブルにしてから、動作上アクティブになることができます。レイヤ 2 ポートの場合、これらのポートが含まれる VLAN にフラッディングされるトラフィックは、リンクがポートに接続されていない場合でもキャプチャされます。
- 入力と出力の両方が設定されている VLAN ERSPAN セッションでは、パケットが同じ VLAN 上でスイッチングされる場合に、宛先ポートから 2 つのパケット（入力側から 1 つ、出力側から 1 つ）が転送されます。
- 帯域内インターフェイスをモニタできるのは、デフォルトの VDC からだけです。すべての VDC からの帯域内トラフィックがモニタされます。
- FabricPath コア ポートは、F2 シリーズまたは F2e シリーズ モジュールが VDC に存在する場合は ERSPAN 宛先としてサポートされません。ただし、FabricPath コア ポートは、ERSPAN 送信元インターフェイスとして設定できます。
- F2 シリーズまたは F2e シリーズ モジュールで ERSPAN セッションを使用する場合、特定のセッション内の送信元トラフィックの合計量が SPAN 宛先インターフェイスまたはそのセッションのポート チャネルの容量以下であることを確認してください。ERSPAN 送信元トラフィックが ERSPAN 宛先の容量を超えると、ERSPAN 送信元インターフェイスでパケットドロップが発生する場合があります。
- Cisco NX-OS Release 5.2 以降では、Cisco Nexus 2000 Series Fabric Extender に接続されている Cisco Nexus 2000 Series Fabric Extender（FEX）インターフェイスおよびファブリック ポート チャネルを ERSPAN 送信元として設定できます。ただし、ERSPAN 宛先としては設定できません。

（注） Fabric Extender インターフェイスおよびファブリック ポート チャネル上の ERSPAN は M1 シリーズおよび M2 シリーズ モジュールでサポートされます。ERSPAN は、Fabric Extender 上ではなく、Cisco Nexus 7000 シリーズ デバイス上で動作します。F2 シリーズおよび F2e シリーズ モジュールは FEX をサポートしますが、FEX ERSPAN をサポートしません。したがって、F2 シリーズおよび F2e シリーズ モジュールに接続される FEX インターフェイスは ERSPAN 送信元にすることはできません。

- F2 シリーズおよび F2e シリーズ モジュールのファブリック ポート チャネルをスパンすることができます。
- FEX インターフェイスを含む VLAN を ERSPAN 送信元にすることができますが、F2 シリーズまたは F2e シリーズ モジュール ベースの FEX ポートを介した入力トラフィックはキャプチャできません。
- レイヤ 3 マルチキャスト出力パケットは F2 シリーズまたは F2e シリーズ モジュール上でスパンすることはできません。
- ERSPAN はレイヤ 2 アクセス モード、レイヤ 2 トランク モード、およびレイヤ 3 モードの Fabric Extender インターフェイスでサポートされます。レイヤ 3 サブインターフェイスはサポートされません。
- ERSPAN セッションの場合、パケットがカプセル化された後に MTU 切り捨てが発生するため、推奨 MTU サイズは 144 バイト以上です。
- ERSPAN セッションのレート制限の割合は、それぞれのモジュールに対して 10G、40G、および 100G に基づいており（つまり、1 パーセントはそれぞれ 0.1G、0.4G または 1G に対応）、各転送エンジン インスタンスに値が適用されます。
- MTU の切り捨ておよび ERSPAN の送信元レート制限は、F2 シリーズ、F2e シリーズ、および M2 シリーズ モジュールおよびスーパーバイザ 2 のみでサポートされます。M1 シリーズ モジュールではサポートされていません。
- F2 シリーズおよび F2e シリーズ モジュールの場合、スパンされた FabricPath（コア）パケットは ERSPAN 宛先に 16 バイトのコア ヘッダーを持ち、ファブリック ポート チャネルを通してスパンされる入力 FEX パケットには ERSPAN 宛先に 6 バイトの Vntag ヘッダーがあります。また、トランク ポートが ERSPAN 宛先として使用される場合、スパンされるパケットに 4 バイトの VLAN タグがあります。
- F2 シリーズおよび F2e シリーズ モジュールの場合、レイヤ 2 ポート（エッジツーエッジ トラフィックを含む）上に送信されるすべてのトラフィックの出力 ERSPAN パケットには ERSPAN 宛先で 16 バイトの MAC-in-MAC ヘッダーが含まれます。
- ERSPAN ヘッダーで IP TTL を設定する際、
  - M シリーズ LC では、ERSPAN のカプセル化/カプセル化解除の後、パケットは EARL に送信されて再循環し、したがって、TTL は EARL によってデクリメントされます。

- F2/F2e には再循環のオーバーヘッドがなく、そのため、TTL デクリメントの実際の動作との間にずれが生じます。
- F1 シリーズは、ERSPAN をサポートしません。

- M2 シリーズ モジュールの MTU 切り捨てでは、切り捨てられた ERSPAN パケットの長さは最も近い 16 バイトの乗数に丸められます。たとえば、65 から 79 の MTU の設定値では、パケットは 64 バイトに丸められます。
- F2 シリーズ モジュール、F2e シリーズ モジュール、M2 シリーズ モジュール、およびスーパーバイザ 2 の特定のレート制限およびパケット サイズ値では、パケット サイズの内部アカウンティングおよび内部ヘッダーのため、ERSPAN パケット レートは設定された値より少なくなります。
- ERSPAN サンプリングは、F2 シリーズ モジュールおよび F2e シリーズ モジュールでのみサポートされています。M シリーズ モジュールではサポートされません。
- マルチキャストのベストエフォート モードは M1 シリーズ モジュールだけに適用されます。
- Cisco NX-OS Release 6.1 以降では、ERSPAN 送信元セッションは、スーパーバイザ 2 でサポートされますが、ERSPAN ACL セッションはサポートされません。
- ERSPAN タイプ III の送信元は F2 シリーズ、F2e シリーズおよび M2 シリーズ モジュールのみでサポートされます。
- ERSPAN タイプ III 終端は M2 シリーズ モジュールでのみサポートされます。つまり、タイプ III ERSPAN パケットは M2 シリーズ モジュールを介して宛先に到達する場合にのみカプセル化解除されます。
- Cisco NX-OS Release 6.2(2) 以降では、F2 シリーズまたは F2e シリーズ モジュールで宛先スイッチに着信する ERSPAN パケットを終了できます。IPv4 終端はサポートされますが、IPv6 終端はサポートされません。VDC 仮想ルーティングおよび転送（VRF）インスタンスの F2 シリーズ モジュールの終端はサポートされません。
- スーパーバイザ 2 は、帯域内ポートに対して ERSPAN タイプ II および ERSPAN タイプ III をサポートしますが、タイム スタンプは高精度時間プロトコル（PTP）はマスター タイマーと同期化されません。
- 1588 粒度モードは、Cisco NX-OS Release 6.1 でサポートされず、選択した場合は拒否されます。
- M2 シリーズ モジュールは、100 マイクロ秒（ms）、100 ナノ秒（ns）、および ns 粒度をサポートします。F2 シリーズおよび F2e シリーズ モジュールは 100 ms と 100 ns の粒度だけをサポートします。
- ERSPAN トラフィックが M2 シリーズ モジュールで終了する場合、1 つのセッションのすべての ERSPAN トラフィックが 1 つの転送インスタンスに収束されるため、高いレートでドロップが発生することがあります。
- グローバル粒度設定が特定のモジュールに対してサポートされていない場合、そのモジュールは 100-ms 粒度に戻ります。たとえば、粒度が ns に設定されている場合、すべての M2 シリーズ モジュールで ns 粒度がイネーブルにされ、すべての F2 シリーズおよび F2e シリーズ

はパケットを 100-ms タイムスタンプで内部でイネーブルにして送信します。各モジュールでサポートされるまたはサポートされない粒度を表示するには **show monitor session** コマンドを使用します。

- F2 シリーズおよび F2e シリーズ モジュールは ERSPAN タイプ III ACL のアクセス コントロール リスト（ACL）コンプレックスを使用しないため、ACL フィルタは F2 シリーズおよび F2e シリーズ モジュールのトラフィックに適用できません。ただし、M2 シリーズ モジュールに対して、ACL の適用後に Type III ヘッダーを使用してパケットをカプセル化することができます。
- F2 シリーズおよび F2e シリーズ モジュールは ERSPAN タイプ III ヘッダーの 32 ビット タイムスタンプをサポートする一方、M2 シリーズ モジュールは 64 ビットのタイムスタンプをサポートします。
- vPC で ERSPAN をイネーブルにし、ERSPAN パケットが vPC を介して宛先にルーティングする必要がある場合、vPC ピア リンクを通過するパケットはキャプチャできません。
- 拡張 ERSPAN セッションは入力または出力のいずれの方向でも M1 シリーズ モジュールの着信トラフィックの送信元となることはできません。
- 従来の SPAN セッションは、F シリーズおよび M シリーズ モジュールからのトラフィックをサポートします。拡張 SPAN セッションは、F シリーズおよび M2 シリーズ モジュールからのみのトラフィックをサポートします。
- ハードウェア セッション 15 は F2 および F2e シリーズ モジュールの NetFlow で使用されます。このハードウェア ID を使用する拡張セッションは F2 および F2e ポートの着信トラフィックをスパンしません。
- M2 シリーズ モジュールでレート制限をサポートするのは 8 つのセッションだけです。追加のハードウェア セッションは、M2 シリーズ モジュールで設定されたレート リミッタを適用しません。
- M1 シリーズ モジュールおよびスーパーバイザ 1 はルール ベースの ERSPAN をサポートしません。VLAN のフィルタリングだけをサポートします。
- M1 および M2 シリーズのモジュールは、非管理 VDC でのみ例外 ERSPAN をサポートし、モジュールの少なくとも 1 つのインターフェイスが VDC に存在する必要があります。
- F1 シリーズ モジュールはルール ベースの ERSPAN を制限付きでサポートします。これらのモジュールは IPv6 送信元 IP フィルタと IPv6 宛先 IP フィルタをサポートしません。これらは 0 ～ 3.までの値で IPv4 および IPv6 ToS フィルタのみサポートします。ポート チャネル メンバー レーン、FCoE 送信元 ID、および FCoE 宛先 ID はサポートされていません。
- F2 および F2e シリーズ モジュールはルール ベースの ERSPAN を制限付きでサポートします。IPv6 送信元 IP フィルタおよび IPv6 宛先 IP フィルタでワイルドカードをサポートせず、宛先 MAC アドレスおよび送信元 MAC アドレスで出力 ERSPAN フィルタリングをサポートしません。
- ERSPAN ACL は、OTV との併用はサポートされていません。
- ERSPAN 送信元セッションは、F3 シリーズ モジュールでサポートされます。Cisco NX-OS Release 7.2 以降では、ERPSPAN 宛先セッションは、以下のモジュールでもサポートされて

います。ただし、ERSPAN ACL セッションは F3 シリーズ モジュールではサポートされていません。

- Cisco NX-OS Release 7.3(0)DX(1) 以降では、ERSPAN 送信元および宛先セッションは、M3 シリーズ モジュールでサポートされます。

デフォルト設定

次の表に、ERSPAN パラメータのデフォルト設定を示します。

表 *35*：デフォルトの *ERSPAN* パラメータ

パラメータ	デフォルト
ERSPAN サンプリング	ディセーブル
ERSPAN セッション	シャット ステートで作成されます
従来の ERSPAN セッションに対する ERSPAN ソース レート制限	ディセーブル
拡張 ERSPAN セッションに対する ERSPAN ソース レート制限	イネーブル
ERSPAN タイプ III セッションのグローバル粒度	100 マイクロ秒
MTU 切り捨て	ディセーブル
マルチキャスト ベスト エフォート モード	ディセーブル

ERSPAN の設定

（注） この機能の Cisco NX-OS コマンドは、Cisco IOS のコマンドとは異なる場合があるので注意してください。

ERSPAN 送信元セッションの設定

ERSPAN セッションを設定できるのはローカル デバイス上だけです。デフォルトでは、ERSPAN セッションはシャット ステートで作成されます。

送信元にはイーサネットポート、ポートチャネル、スーパーバイザ帯域内インターフェイス、および VLAN（入力のみ）を指定できます。1 つの ERSPAN セッションに、イーサネット ポート、VLAN、コントロールプレーン CPU への帯域内インターフェイスを組み合わせた送信元を使用できます。

従来のセッションでは、トラフィックの方向を指定せずにセッションを設定できます。

（注） ERSPAN は送信元に関係なく、スーパーバイザによって生成されるパケットをモニタしません。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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	switch(config)# **monitor erspan origin ip-address***ip-address***global**	ERSPAN のグローバルな送信元 IP アドレスを設定します。
ステップ 3	switch(config)# **no monitor session** {*session-number* | **all**}	指定した ERSPAN セッションの設定を消去します。新しいセッション コンフィギュレーションは、既存のセッション コンフィギュレーションに追加されます。
ステップ 4	switch(config)# **monitor session** {*session-number* | **all**} **type erspan-source** [**shut**]	ERSPAN タイプ II 送信元セッションを設定します。デフォルトでは、セッションは双方向です。オプションの shut キーワードは、選択したセッションに対して shut ステートを指定します。
ステップ 5	switch(config-erspan-src)# **description***description*	セッションの説明を設定します。デフォルトでは、説明は定義されません。説明には最大 32 の英数字を使用できます。
ステップ 6	switch(config-erspan-src)# **source** {[**interface** [**all**] [*type slot/port*[*-port*][, *type slot/port*[*-port*]]] [**port-channel***channel-number*]] [**vlan** {*number* | *range*}]} [**rx** | **tx** | **both**]	送信元およびパケットをコピーするトラフィックの方向を設定します。イーサネット ポート範囲、ポートチャネル、帯域内インターフェイス、または VLAN 範囲を入力できます。 送信元は 1 つ設定することも、またはカンマで区切った一連のエントリとして、または番号の範囲として、複数設定することもできます。 コピーするトラフィックの方向には、入力、出力、または両方を指定できます。デフォルトは双方向です。

	コマンドまたはアクション	目的
		（注） 送信元 VLAN は、入力（rx）方向に限りサポートされます。 単一方向のセッションには、送信元の方向はセッションで指定された方向に一致する必要があります。 Cisco NX-OS Release 7.3(0)D1(1) 以降では、**all** キーワードを使用してモニタリング セッションをイネーブルにし、物理ポート、ポート チャネル、FEX ポート、および FEX ポート チャネルなど、VDC 内のすべての VLAN とポートをモニタできます。**all** キーワードは、拡張 ERSPAN セッションでのみサポートされます。
ステップ 7	ステップ 6 を繰り返して、すべての ERSPAN 送信元を設定します。	（任意） —
ステップ 8	switch(config-erspan-src)# **filter vlan** {*number* | *range*}	（任意） 設定された送信元から選択する VLAN を設定します。VLAN は 1 つ設定することも、またはカンマで区切った一連のエントリとして、または番号の範囲として、複数設定することもできます。VLAN の範囲については、『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide*』を参照してください。 **filter vlan** コマンドと **source interface all** コマンドを使用して無関係の VLAN をフィルタすることにより、拡張 ERSPAN モニタ セッションで現在サポートされている VLAN 送信元制限よりも多くの、指定の VLAN 送信元をモニタできます。
ステップ 9	ステップ 8 を繰り返して、すべての送信元 VLAN のフィルタリングを設定します。	（任意） —
ステップ 10	switch(config-erspan-src)# **filter access-group***acl-filter*	（任意） ACL を ERSPAN セッションにアソシエートします。 （注） 標準の ACL 設定プロセスを使用して ACL を作成できます。詳細については、『*Cisco Nexus 7000 Series NX-OS Security Configuration Guide*』を参照してください。

	コマンドまたはアクション	目的
ステップ 11	switch(config-erspan-src)# **destination ip***ip-address*	ERSPAN セッションの宛先 IP アドレスを設定します。ERSPAN 送信元セッションごとに 1 つの宛先 IP アドレスのみがサポートされます。
ステップ 12	switch(config-erspan-src)# **erspan-id***erspan-id*	ERSPAN 送信元セッションの ERSPAN ID を設定します。ERSPAN の範囲は 1 ～ 1023 です。
ステップ 13	switch(config-erspan-src)# **vrf***vrf-name*	ERSPAN 送信元セッションがトラフィックの転送に使用する仮想ルーティングおよびフォワーディング（VRF）インスタンスを設定します。VRF 名には最大 32 文字の英数字を使用できます。大文字と小文字は区別されます。
ステップ 14	switch(config-erspan-src)# **ip ttl***ttl-number*	（任意） ERSPAN トラフィックの IP 存続可能時間（TTL）値を設定します。範囲は 1 ～ 255 です。
ステップ 15	switch(config-erspan-src)# **ip dscp***dscp-number*	（任意） ERSPAN トラフィックのパケットの DiffServ コードポイント（DSCP）値を設定します。範囲は 0 ～ 63 です。
ステップ 16	switch(config-erspan-src)# **no shut**	ERSPAN 送信元セッションをイネーブルにします。デフォルトでは、セッションはシャット ステートで作成されます。
ステップ 17	switch(config-erspan-src)# **exit**	モニタ コンフィギュレーション モードを終了します。
ステップ 18	switch(config)# **show monitor session** {**all** | *session-number* | **range***session-range*} [**brief**]	（任意） ERSPAN セッション設定を表示します。
ステップ 19	switch(config)# **show running-config monitor**	（任意） ERSPAN の実行コンフィギュレーションを表示します。
ステップ 20	switch(config)# **show startup-config monitor**	（任意） ERSPAN のスタートアップ コンフィギュレーションを表示します。
ステップ 21	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。

ERSPAN 宛先セッションの設定

送信元 IP アドレスからローカルデバイス上の宛先ポートにパケットをコピーするように ERSPAN 宛先セッションを設定できます。デフォルトでは、ERSPAN 宛先セッションはシャット ステートで作成されます。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

すでにモニタ モードで宛先ポートが設定されていることを確認します。詳細については、『*Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide*』を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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	switch(config)# **interface ethernet***slot/port*[*-port*]	選択したスロットおよびポートまたはポート範囲で、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# **switchport**	選択したスロットおよびポートまたはポート範囲でスイッチポート パラメータを設定します。
ステップ 4	switch(config-if)# **switchport mode** [**access** | **trunk**]	選択したスロットおよびポートまたはポート範囲で次のスイッチポート モードを設定します。 • アクセス • トランク
ステップ 5	switch(config-if)# **switchport monitor**	ERSPAN 宛先としてスイッチポート インターフェイスを設定します。
ステップ 6	ステップ 2 ～ 5 を繰り返して、追加の ERSPAN 宛先でモニタリングを設定します。	（任意） —
ステップ 7	switch(config-if)# **no monitor session** {*session-number* | **all**}	指定した ERSPAN セッションの設定を消去します。新しいセッション コンフィギュレーションは、既存のセッション コンフィギュレーションに追加されます。
ステップ 8	switch(config-if)# **monitor session** {*session-number* | **all**} **type erspan-destination**	ERSPAN 宛先セッションを設定します。

	コマンドまたはアクション	目的
ステップ 9	switch(config-erspan-dst)# **description***description*	セッションの説明を設定します。デフォルトでは、説明は定義されません。説明には最大32の英数字を使用できます。
ステップ 10	switch(config-erspan-dst)# **source ip***ip-address*	ERSPAN セッションの送信元 IP アドレスを設定します。ERSPAN 宛先セッションごとに 1 つの送信元 IP アドレスのみがサポートされます。 （注） 送信元 IP アドレスは、ERSPAN 送信元で宛先IPアドレスとして設定されたローカル デバイスの IP アドレスである必要があります。これは、Cisco Nexus 7000 デバイスがパケットを受信してカプセル化を解除すると期待されるローカルデバイスのインターフェイスです。
ステップ 11	switch(config-erspan-dst)# **destination** {[**interface** [*type slot/port*[*-port*][*, type slot/port*[*-port*]]] | [**port-channel***channel-number*]]}	コピーされたソース パケットの宛先を設定します。1 つ以上のインターフェイスを、カンマで区切った一連のエントリとして設定できます。 （注） 宛先ポートをトランク ポートとして設定できます。詳細については、『*Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide*』を参照してください。
ステップ 12	ステップ 11 を繰り返して、すべての ERSPAN 宛先ポートを設定します。	（任意） —
ステップ 13	switch(config-erspan-dst)# **erspan-id***erspan-id*	ERSPAN セッションの ERSPAN ID を設定します。指定できる範囲は 1 ～ 1023 です。
ステップ 14	switch(config-erspan-dst)# **vrf***vrf-name*	ERSPAN 宛先セッションがトラフィックの転送に使用する VRF を設定します。
ステップ 15	switch(config-erspan-dst)# **no shut**	ERSPAN宛先セッションをイネーブルにします。デフォルトでは、セッションはシャット ステートで作成されます。
ステップ 16	switch(config-erspan-dst)# **exit**	モニタ コンフィギュレーション モードを終了します。
ステップ 17	switch(config)# **exit**	グローバル コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 18	switch# **show monitor session** {**all** | *session-number* | **range***session-range*} [**brief**]	（任意） ERSPAN セッション設定を表示します。
ステップ 19	switch# **show running-config monitor**	（任意） ERSPAN の実行コンフィギュレーションを表示します。
ステップ 20	switch# **show startup-config monitor**	（任意） ERSPAN のスタートアップ コンフィギュレーションを表示します。
ステップ 21	switch# **copy running-config startup-config** [**vdc-all**]	（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。

ERSPAN セッションのシャットダウンまたはアクティブ化

ERSPAN セッションをシャットダウンすると、送信元から宛先へのパケットのコピーを切断できます。1 セッションをシャット ダウンしてハードウェア リソースを解放し、別のセッションをイネーブルにできます。デフォルトでは、ERSPAN セッションはシャット ステートで作成されます。

ERSPAN セッションをイネーブルにすると、送信元から宛先へのパケットのコピーをアクティブ化できます。すでにイネーブルになっていて、動作状況がダウンの ERSPAN セッションをイネーブルにするには、そのセッションをいったんシャットダウンしてから、改めてイネーブルにする必要があります。ERSPAN セッション ステートをシャットダウンおよびイネーブルにするには、グローバルまたはモニタ コンフィギュレーション モードのいずれかのコマンドを使用できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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	switch(config)# **monitor session** {*session-range* | **all**} **shut**	指定の ERSPAN セッションをシャットダウンします。デフォルトでは、セッションはシャット ステートで作成されます。
ステップ 3	switch(config)# **no monitor session** {*session-range* | **all**} **shut**	指定の ERSPAN セッションを再開（イネーブルに）します。デフォルトでは、セッションはシャット ステートで作成されます。

	コマンドまたはアクション	目的
		モニタ セッションがイネーブルで動作状況がダウンの場合、セッションをイネーブルにするには、最初に **monitor session shut** コマンドを指定してから、**no monitor session shut** コマンドを続ける必要があります。
ステップ 4	switch(config)# **monitor session***session-number***type erspan-source**	ERSPAN送信元タイプのモニタ コンフィギュレーション モードを開始します。新しいセッション コンフィギュレーションは、既存のセッション コンフィギュレーションに追加されます。
ステップ 5	switch(config-erspan-src)# **monitor session***session-number***type erspan-destination**	ERSPAN 宛先タイプのモニタ コンフィギュレーション モードを開始します。
ステップ 6	switch(config-erspan-src)# **shut**	ERSPAN セッションをシャットダウンします。デフォルトでは、セッションはシャット ステートで作成されます。
ステップ 7	switch(config-erspan-src)# **no shut**	ERSPAN セッションをイネーブルにします。デフォルトでは、セッションはシャット ステートで作成されます。
ステップ 8	switch(config-erspan-src)# **exit**	モニタ コンフィギュレーション モードを終了します。
ステップ 9	switch(config)# **show monitor session all**	（任意） ERSPAN セッションのステータスを表示します。
ステップ 10	switch(config)# **show running-config monitor**	（任意） ERSPAN の実行コンフィギュレーションを表示します。
ステップ 11	switch(config)# **show startup-config monitor**	（任意） ERSPANのスタートアップ コンフィギュレーションを表示します。
ステップ 12	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。

ERSPAN セッションごとの MTU の切り捨ての設定

Cisco NX-OS Release 6.1 以降では、ERSPAN トラフィックの帯域幅を減らすために、ERSPAN セッション内の各複製パケットに割り当てられた最大バイト数を設定できます。この値は、最大伝送単位（MTU）の切り捨てサイズと呼ばれます。設定されたサイズよりも大きいERSPANパケットはすべて、設定されたサイズに切り捨てられます。

（注） MTU の切り捨てと ERSPAN サンプリングは同時にイネーブルにでき、互いに優先順位はありません。これは、送信元パケットのさまざまな側面（サイズ対パケット数）に適用されるためです。

（注） Cisco Catalyst 6000 シリーズ スイッチは、これらの切り捨てが適用されたパケットをドロップするため、宛先 ERSPAN ルータが Cisco Catalyst 6000 シリーズ スイッチの場合、MTU 切り捨てをイネーブルにしないでください。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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	switch(config)# **monitor session***session-number***type erspan-source**	ERSPAN 送信元タイプでモニタ コンフィギュレーション モードを開始し、MTU サイズの切り詰めが設定される ERSPAN セッションを指定します。
ステップ 3	switch(config-erspan-src)# **header-type***version*	（任意） ERSPAN 送信元セッションをタイプ II からタイプ III に変更します。
ステップ 4	switch(config-erspan-src)# [**no**] **mtu***mtu*	指定した ERSPAN セッションのパケットの MTU 切り捨てサイズを設定します。指定できる範囲は 176 ～ 1500 バイトです。
ステップ 5	switch(config-erspan-src)# **exit**	モニタ コンフィギュレーション モードを終了します。
ステップ 6	switch(config)# **exit**	グローバル コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 7	switch# **show monitor session***session-number*	（任意） MTU切り捨ての設定ステータス、セッションごとに各パケットで許可される最大バイト数、MTU切り捨てがサポートされるモジュールとサポートされないモジュールを含む、ERSPAN セッションのステータスを表示します。
ステップ 8	switch# **copy running-config startup-config** [**vdc-all**]	（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。

各 ERSPAN セッションのソース レート制限の設定

ERSPAN セッションが高トラフィック環境の送信元として複数のインターフェイスに設定されている場合、宛先ポートが過負荷状態になり、送信元ポートの通常のデータ トラフィックの障害となる可能性があります。Cisco NX-OS Release 6.1 以降では、各 ERSPAN セッションに送信元レート制限を設定することで、送信元の転送インスタンスのこの問題および送信元転送インスタンスのトラフィックの負荷を軽減できます。

（注） ERSPAN サンプリングは ERSPAN 送信元レート制限に優先されます。レート制限は、サンプリングが ERSPAN ソース パケットで完了した後に発生します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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	switch(config)# **monitor session***session-number***type erspan-source**	ERSPAN 送信元タイプでモニタ コンフィギュレーション モードを開始し、送信元レート制限が設定される ERSPAN セッションを指定します。
ステップ 3	switch(config-erspan-src)# **header-type***version*	（任意） ERSPAN 送信元セッションをタイプ II からタイプ III に変更します。
ステップ 4	switch(config-erspan-src)# [**no**] **rate-limit** {**auto** | *rate-limit*}	自動または手動モードの指定された ERSPAN セッションの ERSPAN パケットの送信元レート制限を設定します。

	コマンドまたはアクション	目的
		• 自動モード：次のように、自動的にギガバイト単位でレート制限を計算します：宛先帯域幅/合計送信元帯域幅。たとえば、ギガバイトごとのレート制限が 0.5 の場合、各送信元トラフィックについて、パケットの 0.5 G のみスパンされます。 入力トラフィックの場合、送信元が可能な最大帯域幅でスパンされるように、ギガバイトごとの制限が、ERSPAN 送信元として使用されるポートの数に基づいて F2 シリーズまたは F2e シリーズ モジュールの各転送エンジンに適用されます。出力トラフィックの場合、ギガバイトごとの制限が、ERSPAN 送信元として使用されるポートの数に関係なく F2 シリーズまたは F2e シリーズ モジュールの各転送エンジンに適用されます。 • 手動モード：モジュールの各転送エンジンから送信できる ERSPAN パケットの最大レートのパーセンテージを指定します。範囲は 1 ～ 100 です。たとえば、レート制限が 10 パーセントの場合、F2 シリーズまたは F2e シリーズ モジュールの各転送エンジンから送信できる ERSPAN パケットの最大レートは 1G（10G ライン レートの 10 パーセント）です。
ステップ 5	switch(config-erspan-src)# **exit**	モニタ コンフィギュレーション モードを終了します。
ステップ 6	switch(config)# **exit**	グローバル コンフィギュレーション モードを終了します。
ステップ 7	switch# **show monitor session***session-number*	（任意） レート制限の設定ステータスを含む ERSPAN セッションのステータス、セッションごとに許可される最大 ERSPAN レートの割合、およびレート制限がサポートされるまたはサポートされないモジュールを表示します。
ステップ 8	switch# **copy running-config startup-config** [**vdc-all**]	（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。

各 ERSPAN セッションのサンプリングの設定

Cisco NX-OS Release 6.1 以降では、ERSPAN トラフィック帯域幅を削減し、ピアツーピア トラフィックをモニタするために、スパンされたトラフィックに対してサンプリング範囲を設定できます。パケット範囲ベースのサンプリングが ERSPAN 送信元パケットの正確な値を提供するために使用されます。

（注） サンプリングと MTU の切り捨ては同時にイネーブルにでき、互いに優先順位はありません。これは、送信元パケットのさまざまな側面（パケット数対サイズ）に適用されるためです。ただし、サンプリングは ERSPAN 送信元レート制限に優先されます。レート制限は、サンプリングが ERSPAN ソース パケットで完了した後に発生します。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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	switch(config)# **monitor session***session-number***type erspan-source**	ERSPAN 送信元タイプでモニタ コンフィギュレーション モードを開始し、ERSPAN サンプリングが設定される ERSPAN セッションを指定します。
ステップ 3	switch(config-erspan-src)# **header-type***version*	（任意） ERSPAN 送信元セッションをタイプ II からタイプ III に変更します。
ステップ 4	switch(config-erspan-src)# [**no**] **sampling***range*	ERSPAN 送信元パケットのサンプリング範囲を設定します。サンプリング値は、x パケットから 1 つのパケットがスパンされる範囲です。x は 2 から 1023 です。この例では、100 パケットごとに 1 つのパケットがスパンされます。
ステップ 5	switch(config-erspan-src)# **exit**	モニタ コンフィギュレーション モードを終了します。
ステップ 6	switch(config)# **exit**	グローバル コンフィギュレーション モードを終了します。
ステップ 7	switch# **show monitor session***session-number*	（任意） ERSPAN サンプリングのステータス、サンプリング値、およびサンプリングがサポートされるまた

	コマンドまたはアクション	目的
		はサポートされないモジュールを含む、ERSPAN セッションのステータスを表示します。
ステップ 8	switch# **copy running-config startup-config** [**vdc-all**]	（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。

ERSPAN セッションのマルチキャスト ベスト エフォート モードの設定

任意の ERSPAN セッションのマルチキャスト ベスト エフォート モードを設定できます。デフォルトでは、ERSPAN の複製が、入力および出力モジュールの両方で実行されます。マルチキャストのベスト エフォート モードをイネーブルにすると、ERSPAN の複製は、マルチキャスト トラフィックの入力モジュールか、レイヤ 3 インターフェイスから出て行くパケットの出力モジュールのみで行われます（つまり、出力モジュールでは、レイヤ 2 インターフェイスから出て行くパケットは、ERSPAN 用に複製されません）。

（注） レイヤ 3 マルチキャスト トラフィックでは、ERSPAN 複製が出力モジュールで発生します。トラフィックが複数の出力モジュールにマルチキャストされる場合、各パケットに対して複数の ERSPAN コピーをキャプチャできます（つまり、各出力モジュールから 1 つのコピー）。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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	switch(config)# **monitor session***session-number***type erspan-source**	ERSPAN 送信元タイプでモニタ コンフィギュレーション モードを開始し、マルチキャスト ベスト エフォート モードが設定される ERSPAN セッションを指定します。
ステップ 3	switch(config-erspan-src)# **header-type***version*	（任意） ERSPAN 送信元セッションをタイプ II からタイプ III に変更します。

	コマンドまたはアクション	目的
ステップ 4	switch(config-erspan-src)# [**no**] **multicast best-effort**	指定された ERSPAN セッションのマルチキャスト ベスト エフォート モードを設定します。

ルール ベース ERSPAN の設定

一連のルールに基づいて入力または出力 ERSPAN トラフィックにフィルタを設定できます。単純なフィルタには 1 つのみのルールがあり、このルールに複数のフィールドまたは組み合わせを追加できます。パケットは、すべての条件が満たされた場合にのみスパンされます。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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	switch(config)# **monitor erspan origin ip-address***ip-address***global**	ERSPAN のグローバルな送信元 IP アドレスを設定します。 グローバルな送信元 IP アドレスはデフォルト VDC または管理 VDC で設定できます。この VDC で設定した値は、すべての VDC で有効です。デフォルトまたは管理 VDC で加えられる変更はすべてのデフォルト以外の VDC に適用されます。
ステップ 3	switch(config)# **monitor erspan granularity** {**100_ms** | **100_ns** | **1588** | **ns**}	（任意） すべての VDC にわたるすべての ERSPAN タイプ III セッションの粒度を指定します。粒度のオプションは 100 ミリ秒（ms）、100 ナノ秒（ns）、IEEE 1588（秒またはナノ秒）、およびナノ秒です。 （注） クロック マネージャは粒度の設定に基づいて ERSPAN タイマーを調整します。IEEE 1588 を設定すると、クロック マネージャは、複数のスイッチで ERSPAN タイマーを同期化します。設定しないと、クロック マネージャはスイッチのマスター タイマーに ERSPAN タイマーを同期化します。

	コマンドまたはアクション	目的
		（注） 1588 粒度モードは、Cisco NX-OS Release 6.1 でサポートされず、選択した場合は拒否されます。 （注） M2 シリーズ モジュールは、100 ms、100 ns、および ns の粒度をサポートします。F2 シリーズおよび F2e シリーズ モジュールは 100 ms と 100 ns の粒度だけをサポートします。 （注） このコマンドは、デフォルトの VDC でのみ適用できます。
ステップ 4	switch(config)# **no monitor session** {*session-number* | **all**}	指定した ERSPAN セッションの設定を消去します。新しいセッション コンフィギュレーションは、既存のセッション コンフィギュレーションに追加されます。
ステップ 5	switch(config)# **monitor session** {*session-number* | **all**} **type erspan-source** [**rx** | **tx**] [**shut**]	ERSPAN タイプ II 送信元セッションを設定します。デフォルトでは、セッションは双方向です。オプションのキーワードは次のとおりです。 • **rx**：入力拡張 ERSPAN 送信元セッションを指定します。 • **tx**：出力拡張 ERSPAN 送信元セッションを指定します。 • **shut**：選択したセッションに対して shut 状態を指定します。
ステップ 6	switch(config-erspan-src)# **mode extended**	（任意） ERSPAN 送信元セッションを拡張双方向セッションとして設定します。 （注） 単方向の ERSPAN 送信元セッションではこのコマンドは使用できません。
ステップ 7	switch(config-erspan-src)# **header-type***version*	（任意） ERSPAN 送信元セッションをタイプ II からタイプ III に変更します。 （注） ERSPAN 送信元セッションをタイプ III からタイプ II に変更するには、このコマンドの no 形式を使用します。
ステップ 8	switch(config-erspan-src)# **description***description*	（任意） セッションの説明を設定します。デフォルトでは、説明は定義されません。説明には最大 32 の英数字を使用できます。

	コマンドまたはアクション	目的
ステップ 9	switch(config-erspan-src)# [**no**] **filter** [**access-group***acl-filter*] [**vlan***vlan-range*] [**bpdu** [**true** | **false**]] [**cos***cos-value*] [**dest-mac***dest-mac*] [**eth-type***eth-value*] [**flow-hash***flow-value*] [**frame-type** [**eth** | **arp** | **fcoe** | **ipv4** | **ipv6**]] [**pc-lane***port-number*] [**src_mac***mac-address*] [**trace-route** [**true** | **false**]]	ERSPANセッションのフィルタを設定します。セッションからフィルタを削除するには、このコマンドの **no 形式**を入力します。オプションのキーワードは次のとおりです。 • **access-group**：アクセス制御グループに基づいてフィルタを指定します。 • **vlan**：VLAN の範囲に基づいてフィルタを指定します。 • **bpdu**：パケットのブリッジ プロトコル データ ユニット（BPDU）クラスに基づいてフィルタを指定します。 • **cos**：サービス クラス（CoS）に基づいて dotlq ヘッダーにフィルタを指定します。 • **dest-mac**：宛先 MAC アドレスに基づいてフィルタを指定します。 • **eth-type**：イーサネット タイプに基づいてフィルタを指定します。 • **flow-hash**：Result Bundle Hash（RBH）値に基づいてフィルタを指定します。 • **frame-type**：フレーム タイプに基づいてフィルタを指定します。 • **pc-lane**：ポート チャネル メンバーに基づいてフィルタを指定します。 • **src-mac**：送信元 MAC アドレスに基づいてフィルタを指定します。 • **trace-route**：ヘッダーのルート ビットに基づいてフィルタを指定します。
ステップ 10	switch(config-erspan-src)# [**no**] **filter frame-type eth**	（任意） ERSPAN セッションのイーサネット フレーム タイプのフィルタを設定します。セッションからフィルタを削除するには、このコマンドの **no 形式**を入力します。

	コマンドまたはアクション	目的
ステップ 11	switch(config-erspan-src)# [**no**] **filter frame-type arp** [[**arp-rarp** [**arp** | **rarp**]] [**req-resp** [**req** | **rsp**]] [**sender-ip***ip-address*] [**target-ip***ip-address*]]	（任意） ERSPAN セッションの ARP フレーム タイプのフィルタを設定します。セッションからフィルタを削除するには、このコマンドの no 形式を入力します。 • **arp-rarp**：ARP または RARP フレーム タイプのフィルタを指定します。 • **req-resp**：要求または応答に基づいてフィルタを指定します。 • **sender-ip**：送信者の IP アドレスに基づいてフィルタを指定します。 • **target-ip**：受信者の IP アドレスに基づいてフィルタを指定します。
ステップ 12	switch(config-erspan-src)# [**no**] **filter frame-type fcoe** [[**fc-sid***FC-source-ID*] [**fc-did***FC-dest-ID*] [**fcoe-type***fcoe-value*] [**r-ctl***r-ctl-value*] [**sof***sof-value*] [**cmd-code***cmd-value*]]	（任意） ERSPAN セッションの FCoE フレーム タイプのフィルタを設定します。セッションからフィルタを削除するには、このコマンドの **no 形式**を入力します。オプションのキーワードは次のとおりです。 • **fc-sid**：FC 送信元 ID に基づいてフィルタを指定します。 • **fc-did**：FC 宛先 ID に基づいてフィルタを指定します。 • **fcoe-type**：FCoE タイプに基づいてフィルタを指定します。 • **r-ctl**：ルーティング制御フラグ（R CTL）値に基づいてフィルタを指定します。 • **sof**：フレーム開始（SOF）パケットに基づいてフィルタを指定します。 • **cmd-code**：コマンド コードに基づいてフィルタを指定します。
ステップ 13	switch(config-erspan-src)# [**no**] **filter frame-type ipv4** [[**src-ip***src-ip*] [**dest-ip***dest-ip*] [**tos***tos-value*] [**l4-protocol***l4-value*]]	（任意） ERSPAN セッションの IPv4 フレーム タイプのフィルタを設定します。セッションからフィルタを削除するには、このコマンドの **no 形式**を入力します。オプションのキーワードは次のとおりです。

	コマンドまたはアクション	目的
		• **src-ip**：IPv4 送信元 IP アドレスに基づいてフィルタを指定します。 • **dest-ip**：IPv4 宛先 IP アドレスに基づいてフィルタを指定します。 • **tos**：IP ヘッダーのタイプ オブ サービス（ToS）に基づいてフィルタを指定します。 • **l4-protocol**：IP ヘッダーのプロトコル フィールドに設定されたレイヤ4プロトコル数に基づいてフィルタを指定します。
ステップ 14	switch(config-erspan-src)# [**no**] **filter frame-type ipv6** [[**src-ip***src-ip*] [**dest-ip***dest-ip*] [**tos***tos-value*] [**l4-protocol***l4-value*]]	（任意） ERSPAN セッションの IPv6 フレーム タイプのフィルタを設定します。セッションからフィルタを削除するには、このコマンドの **no 形式**を入力します。オプションのキーワードは次のとおりです。 • **src-ip**：IPv6 送信元 IP アドレスに基づいてフィルタを指定します。 • **dest-ip**：IPv6 宛先 IP アドレスに基づいてフィルタを指定します。 • **tos**：IP ヘッダーのタイプ オブ サービス（ToS）に基づいてフィルタを指定します。 • **l4-protocol**：IP ヘッダーのプロトコル フィールドに設定されたレイヤ4プロトコル数に基づいてフィルタを指定します。
ステップ 15	ステップ 9 から 14 をセッションのすべてのフィルタに対して繰り返します。	（任意） —
ステップ 16	switch(config-erspan-src)# **source** {[**interface** [*type slot/port* [*-port*] [*,type slot/port*[*-port*]]] [**port-channel***channel-number*]]	[**vlan** {*number*	*range*}]} [**rx**	**tx**	**both**]	送信元およびパケットをコピーするトラフィックの方向を設定します。イーサネット ポートの範囲、ポート チャネル、帯域内インターフェイス、VLAN の範囲、Cisco Nexus 2000 Series Fabric Extender インターフェイス、または Cisco Nexus 2000 Series Fabric Extender に接続されたファブリック ポート チャネルを入力できます。 送信元は 1 つ設定することも、またはカンマで区切った一連のエントリとして、または番号の範囲として、複数設定することもできます。最大128のインターフェ

	コマンドまたはアクション	目的
		イスを指定できます。VLAN の範囲は 1 ～ 3967 です。4048 ～ 4093 の VLAN の範囲は、6.1 以前の Cisco NX-OS リリースでもサポートされます。 コピーするトラフィック方向を、入力（rx）、出力（tx）、または両方向（both）として指定できます。デフォルトは both です。 単一方向のセッションには、送信元の方向はセッションで指定された方向に一致する必要があります。
ステップ 17	ステップ 16 を繰り返して、すべての ERSPAN 送信元を設定します。	（任意） —
ステップ 18	switch(config-erspan-src)# **destination ip***ip-address*	ERSPAN セッションの宛先 IP アドレスを設定します。ERSPAN 送信元セッションごとに 1 つの宛先 IP アドレスのみがサポートされます。 （注） Cisco Nexus 2000 Series Fabric Extender インターフェイスおよび FEX に接続されたファブリック ポート チャネルは、ERSPAN 宛先として設定できません。
ステップ 19	switch(config-erspan-src)# **erspan-id***erspan-id*	ERSPAN セッションの ERSPAN ID を設定します。ERSPAN の範囲は 1 ～ 1023 です。
ステップ 20	switch(config-erspan-src)# **vrf***vrf-name*	ERSPAN 送信元セッションがトラフィックの転送に使用する VRF インスタンスを設定します。VRF 名には最大 32 文字の英数字を使用できます。大文字と小文字は区別されます。
ステップ 21	switch(config-erspan-src)# **ip ttl***ttl-number*	（任意） ERSPAN トラフィックの IP 存続可能時間（TTL）値を設定します。範囲は 1 ～ 255 です。
ステップ 22	switch(config-erspan-src)#**ip dscp***dscp-number*	（任意） ERSPAN トラフィックのパケットの DiffServ コード ポイント（DSCP）値を設定します。範囲は 0 ～ 63 です。
ステップ 23	switch(config-erspan-src)# **no shut**	ERSPAN セッションをイネーブルにします。デフォルトでは、セッションはシャット ステートで作成されます。
ステップ 24	switch(config-erspan-src)# **exit**	モニタ コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 25	switch(config)# **exit**	グローバル コンフィギュレーション モードを終了します。
ステップ 26	switch# **show monitor session** {**all** | *session-number* | **range***session-range*} [**brief**]	（任意） マルチキャスト ベスト エフォート モードの設定ステータス、およびベスト エフォート モードがサポートされているモジュールとサポートされていないモジュールを含む、ERSPAN セッションのステータスを表示します。
ステップ 27	switch# **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。

例外 ERSPAN の設定

例外パケットをスパンするようにデバイスを設定できます。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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	switch(config)# **monitor session***session-number***type erspan-source** [**rx** | **tx**] [**shut**]	モニタ コンフィギュレーション モードを開始し、ERSPAN セッションを指定します。例外 ERSPAN は出力方向でのみサポートされます。拡張 ERSPAN Rx セッションの場合、例外送信元設定は拒否されます。オプションのキーワードは次のとおりです。 • **rx**：入力拡張 ERSPAN 送信元セッションを指定します。 • **tx**：出力拡張 ERSPAN 送信元セッションを指定します。 • **shut**：選択したセッションに対して shut 状態を指定します。

	コマンドまたはアクション	目的
ステップ 3	switch(config-erspan-src)# **mode extended**	（任意） ERSPANセッションを拡張双方向セッションとして設定します。
ステップ 4	switch(config-erspan-src)# **source exception** {**layer3** | **fabricpath** | **other** | **all**}	送信元を例外のERSPANセッションとして設定します。以下の例外タイプがサポートされます。 • **layer3**：F2 シリーズおよび M シリーズ モジュールに対するレイヤ 3 例外タイプを指定します。 • **fabricpath**：F シリーズ モジュールに対する FabricPath 例外タイプを指定します。 • **other**：ドロップ宛先インターフェイスにプログラムされているリダイレクト登録によってドロップされた M シリーズ モジュールに対する例外を指定します。 • **all**：レイヤ 3、FabricPath およびその他のすべての例外が含まれます。
ステップ 5	switch(config-erspan-src)# **destination ip***ip-address*	ERSPAN セッションの宛先 IP アドレスを設定します。ERSPAN 送信元セッションごとに 1 つの宛先 IP アドレスのみがサポートされます。 （注） Cisco Nexus 2000 Series Fabric Extender インターフェイスおよび FEX に接続されたファブリック ポート チャネルは、ERSPAN 宛先として設定できません。
ステップ 6	switch(config-erspan-src)# **no shut**	ERSPANセッションをイネーブルにします。デフォルトでは、セッションはシャット ステートで作成されます。
ステップ 7	switch(config-erspan-src)# **exit**	モジュール コンフィギュレーション モードを終了します。
ステップ 8	switch(config)# **exit**	グローバル コンフィギュレーション モードを終了します。
ステップ 9	switch# **show monitor session***session-number*	（任意） マルチキャスト ベスト エフォート モードの設定ステータス、およびベスト エフォート モードがサポートされているモジュールとサポートされていないモジュールを含む、ERSPANセッションのステータスを表示します。

	コマンドまたはアクション	目的
ステップ 10	switch# **copy running-config startup-config** [**vdc-all**]	（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。

ERSPAN 設定の確認

ERSPAN の設定を表示するには、次のいずれかの作業を行います。

コマンド	目的
show monitor session {**all** | *session-number* | **range***session-range*} [**brief**]	ERSPAN セッション設定を表示します。
show running-config monitor	ERSPANの実行コンフィギュレーションを表示します。
show startup-config monitor	ERSPAN のスタートアップ コンフィギュレーションを表示します。
show resource monitor-session-extended	拡張セッションで使用可能なリソースを表示します。
show resource monitor-session-mx-exception-src	例外セッションで使用可能なリソースを表示します。

これらのコマンド出力のフィールドの詳細については、『*Cisco Nexus 7000 Series NX-OS System Management Command Reference*』を参照してください。

ERSPAN の設定例

ERSPAN タイプ III 送信元セッションの設定例

次に、ERSPAN タイプ III 送信元セッションを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 14/30
switch(config-if)# no shut
switch(config-if)# exit
```

```
switch(config)# monitor erspan origin ip-address 3.3.3.3 global
switch(config)# monitor erspan granularity 100_ns
switch(config)# monitor session 1 type erspan-source
switch(config-erspan-src)# mode extended
switch(config-erspan-src)# header-type 3
switch(config-erspan-src)# source interface ethernet 14/30
switch(config-erspan-src)# erspan-id 1
switch(config-erspan-src)# ip ttl 16
switch(config-erspan-src)# ip dscp 5
switch(config-erspan-src)# vrf default
switch(config-erspan-src)# destination ip 9.1.1.2
switch(config-erspan-src)# no shut
switch(config-erspan-src)# exit
switch(config)# show monitor session 1
```

拡張 ERSPAN モニタ セッション内のすべての VLAN とポートをモニタする設定例

次に、拡張 ERSPAN モニタ セッションですべての VLAN とポートをモニタする例を示します。

```
switch# configure terminal
switch(config)# monitor session 1 type erspan-source
switch(config-monitor)# mode extended
switch(config-monitor)# source interface all
switch(config-monitor)# destination interface ethernet 14/29
switch(config-monitor)# vrf default
switch(config-monitor)# erspan-id 200
switch(config-monitor)# no shut
switch(config-monitor)# exit
switch(config)# show monitor session 1
switch(config)# copy running-config startup-config
```

次に、拡張 ERSPAN モニタ セッションで現在サポートされている VLAN 送信元制限よりも多くの、指定の VLAN 送信元をモニタする例を示します。

```
switch# configure terminal
switch(config)# monitor session 2 type erspan-source
switch(config-monitor)# mode extended
switch(config-monitor)# source interface all tx
switch(config-monitor)# destination ip 192.0.2.1
switch(config-monitor)# vrf default
switch(config-monitor)# erspan-id 200
switch(config-monitor)# filter vlan 1-1000
switch(config-monitor)# no shut
switch(config-monitor)# exit
switch(config)# show monitor session 2
switch(config)# copy running-config startup-config
```

単一方向 ERSPAN セッションの設定例

次に、単一方向 ERSPAN セッションを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 14/30
switch(config-if)# no shut
switch(config-if)# exit
switch(config)# no monitor session 3
switch(config)# monitor session 3 rx
switch(config-erspan-src)# source interface ethernet 2/1-3 rx
switch(config-erspan-src)# erspan-id 1
switch(config-erspan-src)# ip ttl 16
switch(config-erspan-src)# ip dscp 5
switch(config-erspan-src)# vrf default
```

```
switch(config-erspan-src)# destination ip 9.1.1.2
switch(config-erspan-src)# no shut
switch(config-erspan-src)# exit
switch(config)# show monitor session 1
```

ERSPAN 宛先セッションの設定例

次に、ERSPAN 宛先セッションを設定する例を示します。

```
switch# configure terminal
switch(config)# interface e14/29
switch(config-if)# no shut
switch(config-if)# switchport
switch(config-if)# switchport monitor
switch(config-if)# exit
switch(config)# monitor session 2 type erspan-destination
switch(config-erspan-dst)# source ip 9.1.1.2
switch(config-erspan-dst)# destination interface e14/29
switch(config-erspan-dst)# erspan-id 1
switch(config-erspan-dst)# vrf default
switch(config-erspan-dst)# no shut
switch(config-erspan-dst)# exit
switch(config)# show monitor session 2
```

ERSPAN ACL の設定例

次に、ERSPAN ACL を設定する例を示します。

```
switch# configure terminal
switch(config)# ip access-list match_11_pkts
switch(config-acl)# permit ip 11.0.0.0 0.255.255.255 any
switch(config-acl)# exit
switch(config)# ip access-list match_12_pkts
switch(config-acl)# permit ip 12.0.0.0 0.255.255.255 any
switch(config-acl)# exit
switch(config)# vlan access-map erspan_filter 5
switch(config-access-map)# match ip address match_11_pkts
switch(config-access-map)# action forward
switch(config-access-map)# exit
switch(config)# vlan access-map erspan_filter 10
switch(config-access-map)# match ip address match_12_pkts
switch(config-access-map)# action forward
switch(config-access-map)# exit
switch(config)# monitor session 1 type erspan-source
switch(config-erspan-src)# header-type 3
switch(config-erspan-src)# filter access_group erspan_filter
```

ERSPAN の MTU 切り捨ておよび ERSPAN サンプリングの設定例

次に、ERSPAN セッションの MTU 切り捨ておよび ERSPAN サンプリングを設定する例を示します。

```
switch# configure terminal
switch(config)# monitor session 1 type erspan-source
switch(config-erspan-src)# mtu 100
switch(config-erspan-src)# sampling 10
switch(config-erspan-src)# show monitor session 1
```

マルチキャスト ベスト エフォート モードを使用した ERSPAN の設定例

次に、ERSPAN セッションのマルチキャストのベスト エフォート モードを設定する例を示します。

```
switch# configure terminal
switch(config)# monitor session 1 type erspan-source
switch(config-erspan-src)# multicast best-effort
switch(config-erspan-src)# show monitor session 1
```

ルール ベースの ERSPAN の設定例

次に、ルール ベースの ERSPAN セッションを設定する例を示します。

```
switch# configure terminal
switch(config)# monitor erspan origin ip-address 10.0.0.1 global
switch(config)# monitor erspan granularity 100_ns
switch(config)# no monitor session 3
switch(config)# monitor session 3 type erspan-source
switch(config-erspan-src)# mode extended
switch(config-erspan-src)# header-type 3
switch(config-erspan-src)# description erspan_src_session_3
switch(config-erspan-src)# filter frame-type ipv4 src-ip 10.1.1.1/24
switch(config-erspan-src)# filter vlan 10,20
switch(config-erspan-src)# source interface ethernet 2/1-3, ethernet 3/1 rx
switch(config-erspan-src)# destination ip 10.1.1.1
switch(config-erspan-src)# erspan-id 5
switch(config-erspan-src)# vrf default
switch(config-erspan-src)# ip ttl 25
switch(config-erspan-src)# ip dscp 42
switch(config-erspan-src)# no shut
switch# show monitor session 3
```

例外 ERSPAN の設定例

次に、ERSPAN 例外セッションを設定する例を示します。

```
switch# configure terminal
switch(config)# monitor session 3 type erspan-source
switch(config-erspan-src)# mode extended
switch(config-erspan-src)# source exception all
switch(config-erspan-src)# destination ip 10.1.1.1
switch(config-erspan-src)# no shut
switch# show monitor session 3
```

関連資料

関連項目	マニュアル タイトル

ERSPAN コマンド：コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト、使用上の注意事項、および例	『*Cisco Nexus 7000 Series NX-OS System Management Command Reference*』
VDC	『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』
『Cisco Network Analysis Module (NAM)』	『*Cisco Network Analysis Module (NAM) for Nexus 7000 Quick Start Guide*』
ファブリック エクステンダ	『*Cisco Nexus 2000 Series Fabric Extender Software Configuration Guide*』

ERSPAN の機能の履歴

次の表に、このマニュアルの新機能および変更された機能を要約し、各機能がサポートされているリリースを示します。ご使用のソフトウェア リリースで、本書で説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。

表 *36*：*ERSPAN* の機能の履歴

機能名	リリース	機能情報
ERSPAN	7.3(0)DX(1)	M3 シリーズ モジュールでの ERSPAN 送信元および宛先セッションのサポートが追加されました。
ERSPAN	7.3(0)D1(1)	ERSPAN セッションあたり 4K の VLAN のサポートが追加されました。
ERSPAN	6.2(2)	F2 および F2e シリーズ モジュールの ERSPAN 宛先セッションのサポートが追加されました。
ERSPAN	6.2(2)	ERSPAN データ ソースに対する NAM サポートが追加されました。
ERSPAN	6.2(2)	拡張 ERSPAN のサポートが追加されました。

ERSPAN	6.2(2)	ルールベースの ERSPAN のサポートが追加されました。
ERSPAN	6.2(2)	例外 ERSPAN のサポートが追加されました。
ERSPAN	6.2(2)	F2 または F2e シリーズモジュールで ERSPAN の終端のサポートが追加されました。
ERSPAN	6.1(2)	F2e シリーズ モジュールのサポートが追加されました。
ERSPAN	6.1(1)	ERSPAN タイプ III のサポートが追加されました。
ERSPAN	6.1(1)	スーパーバイザ 2 のサポートが追加されました。
ERSPAN	6.1(1)	F2 および M2 シリーズモジュールのサポートが追加されました。
ERSPAN	6.1(1)	ERSPAN サンプリングのサポートが追加されました。
ERSPAN	6.1(1)	MTU 切り捨てと各 ERSPAN セッションの送信元レート制限を設定する機能が追加されました。
ERSPAN	6.0(1)	ERSPAN および ERSPAN ACL は、F2 シリーズモジュールではサポートされていません。
ERSPAN	5.2(1)	Cisco Nexus 2000 Series Fabric Extender インターフェイスに対する ERSPAN 送信元サポートが追加されました。
ERSPAN	5.2(1)	ERSPAN セッションのマルチキャスト ベスト エフォート モードを設定する機能が追加されました。
ERSPAN および ERSPAN ACL	5.1(1)	この機能が導入されました。

ERSPAN	7.2	ERSPAN 送信元セッションは、F3 シリーズモジュールでサポートされます。ただし、ERSPAN ACL セッションはF3 シリーズモジュールではサポートされていません。

第 19 章

LLDP の設定

この章では、ローカル ネットワーク上の他のデバイスを検出するために、Link Layer Discovery Protocol（LLDP）を設定する方法について説明します。

この章は、次の項で構成されています。

- 機能情報の確認，417 ページ
- LLDP について，418 ページ
- LLDP のライセンス要件，420 ページ
- LLDP に関する注意事項および制約事項，420 ページ
- LLDP のデフォルト設定，420 ページ
- LLDP の設定，421 ページ
- LLDP コンフィギュレーションの確認，424 ページ
- LLDP のコンフィギュレーション例，425 ページ
- 関連資料，425 ページ
- LLDP の機能の履歴，426 ページ

機能情報の確認

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

LLDP について

Cisco Discovery Protocol（CDP）は、ネットワークに接続された他のシスコ デバイスを自動的に検出し学習することをネットワーク管理アプリケーションによって可能にするデバイス検出プロトコルです。

他社製デバイスのディスカバリを許可するために、スイッチは、IEEE 802.1ab 規格で定義されているベンダー ニュートラルなデバイス ディスカバリ プロトコルであるリンク層検出プロトコル（LLDP）もサポートしています。LLDP を使用すると、ネットワーク デバイスはネットワーク デバイスに関する情報を、ネットワーク上の他のデバイスにアドバタイズできます。このプロトコルはデータリンク層で動作するため、異なるネットワーク層プロトコルが稼働する 2 つのシステムで互いの情報を学習できます。

LLDP は、デバイスおよびそのインターフェイスの機能と現在のステータスに関する情報を送信する単一方向のプロトコルです。LLDP デバイスはこのプロトコルを使用して、他の LLDP デバイスからだけ情報を要求します。

LLDP は一連の属性をサポートしており、これを使用して他のデバイスを検出します。これらの属性には、タイプ、長さ、および値（TLV）の説明が含まれています。LLDP デバイスは TLV を使用して、ネットワーク上の他のデバイスと情報を送受信できます。設定情報、デバイスの機能、デバイス ID などの詳細情報は、このプロトコルを使用してアドバタイズできます。

LLDP は、デフォルトで次の TLV を通知します。

- DCBXP
- 管理アドレス
- ポート記述
- ポート VLAN
- システム機能
- システム記述
- システム名

DCBXP について

Data Center Bridging Exchange Protocol（DCBXP）は、LLDP を拡張したプロトコルです。これは、ピア間のノード パラメータのアナウンス、交換、およびネゴシエートに使用されます。DCBXP パラメータは、特定の DCBXP TLV にパッケージ化されます。この TLV は、受信した LLDP パケットに応答するように設計されています。このように、DCBXP は負荷の軽い確認応答メカニズムを LLDP の上位に追加し、このためリンク レベル プロトコルからの要求応答セマンティックを必要とするすべてのアプリケーションが DCBXP を利用できるようになります。

DCBXP を使用してパラメータとピア ノードの交換およびネゴシエーションが必要な他のアプリケーションは次のとおりです。

- 優先度ベース フロー制御（PFC）：PFC は、イーサネットの既存のポーズ メカニズムを拡張するものです。これは、ユーザ プライオリティまたはサービス クラスに基づいてポーズをイネーブルにします。PFC を使用して 8 つの仮想リンクに分割された物理リンクは、他の仮想リンクのトラフィックに影響を与えることなく、単一の仮想リンクでポーズを使用できる機能を提供します。ユーザごとのプライオリティ単位でポーズをイネーブルにすることで、IP トラフィック用のパケット ドロップの輻輳管理を維持しながら、ドロップの無いサービスが必要なトラフィックに対し管理者がロスレス リンクを作成できます。
- イネーブル化転送選択（ETS）：ETS は、仮想リンクの最適帯域幅管理を可能にします。また、ETS は、優先度のグループ化とも呼ばれます。PFC の同じ優先度クラス内の処理の区別をイネーブルにします。ETS は帯域割り当て、低遅延、またはベストエフォートに基づいた順位付け処理を提供し、結果としてグループ単位のトラフィック クラスの割り当てを提供します。たとえば、同一クラス内では、トラフィックのイーサネット クラスが高いプライオリティの指定とベストエフォートがある可能性があります。ETS によって、同じ優先度クラスの中でトラフィックを区別でき、優先度グループを作成できます。
- アプリケーション プライオリティ設定 TLV：特定のプロトコルで使用される VLAN に関する情報を伝送します。

（注） Quality of Service（QoS）機能の詳細については、『*Cisco Nexus 7000 Series NX-OS Quality of Service Configuration Guide*』を参照してください。

DCBXP はデフォルトでイネーブルであり、提供された LLDP はイネーブルです。LLDP がイネーブルである場合、**[no] lldp tlv-select dcbxp** コマンドを使用して DCBXP をイネーブルまたはディセーブルにすることができます。LLDP の送信または受信がディセーブルになっているポートでは、DCBXP はディセーブルです。

ハイ アベイラビリティ

LLDP 機能はステートレス リスタートおよびステートフル 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 スイッチオーバー後に、実行コンフィギュレーションを適用します。

ハイ アベイラビリティの詳細については、『*Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide*』を参照してください。

仮想化のサポート

サポートされる LLDP のインスタンスは 1 個です。

LLDP のライセンス要件

製品	ライセンス要件
Cisco NX-OS	LLDP 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 nx-os イメージにバンドルされており、無料で提供されます。NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

LLDP に関する注意事項および制約事項

LLDP に関する設定時の注意事項および制約事項は、次のとおりです。

- インターフェイス上で LLDP をイネーブルまたはディセーブルにするには、事前にデバイス上で LLDP をイネーブルにしておく必要があります。
- LLDP は物理インターフェイスだけでサポートされています。
- LLDP は 1 つのポートにつき 1 つのデバイスを検出できます。
- Converged Network Adapter（CNA）を使用していない場合、LLDP は Linux サーバを検出できます。LLDP は他のタイプのサーバを検出できません。
- DCBXP の非互換性のメッセージは、物理ループバック接続がデバイスにある場合に network QoS ポリシーを変更するときに表示されることがあります。非互換性があるのは短時間で、すぐに解消されます。
- DCBXP は Cisco Nexus 2000 シリーズ Fabric Extender ではサポートされません。
- Cisco NX-OS Release 5.2 以降では、LLDP が Cisco Nexus 2000 シリーズ Fabric Extender でサポートされます。LLDP パケットはネイバー探索用の Fabric Extender ポート経由で送受信できます。
  - Fabric Extender ポート上のすべての LLDP 設定はスーパーバイザ上で発生します。LLDP 設定および **show** コマンドは Fabric Extender コンソールでは表示されません。
  - LLDP は Fabric Extender-virtual port channel（vPC）接続でサポートされません。

LLDP のデフォルト設定

この表は、LLDP のデフォルト設定を示します。

パラメータ	デフォルト
グローバル LLDP	ディセーブル

パラメータ	デフォルト
インターフェイス上の LLDP	イネーブル（LLDP がグローバルにイネーブルになった後）
LLDP 保持時間（ディセーブルになる前）	120 秒
LLDP 再初期化遅延	2 秒
LLDP タイマー（パケット更新頻度）	30 秒
LLDP TLV	イネーブル
LLDP 受信	イネーブル（LLDP がグローバルにイネーブルになった後）
LLDP 転送	イネーブル（LLDP がグローバルにイネーブルになった後）
DCBXP	イネーブル（提供された LLDP がイネーブルになります）

LLDP の設定

（注） この機能の Cisco NX-OS コマンドは、類似した機能の Cisco IOS コマンドと異なる場合があります。

LLDP のグローバルなイネーブルまたはディセーブル

デバイスで LLDP をグローバルにイネーブルまたはディセーブルにできます。デバイスで LLDP パケットの送信および受信を可能にするには、LLDP をグローバルにイネーブルにする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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	switch(config)# [**no**] **feature lldp**	デバイス上で LLDP をイネーブルまたはディセーブルにします。LLDP はデフォルトでディセーブルです。

	コマンドまたはアクション	目的
ステップ 3	switch(config)# **show running-config lldp**	（任意） LLDP のグローバル コンフィギュレーションを表示します。LLDP が有効の場合、「feature lldp」を表示します。LLDP が有効の場合、「Invalid command」エラーを表示します。
ステップ 4	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。

インターフェイス上での LLDP のイネーブルまたはディセーブル

LLDPをグローバルにイネーブルにすると、LLDPは、デフォルトでサポートされているすべてのインターフェイス上でイネーブルになります。ただし、LLDP パケットの送信だけ、または受信だけを実行するために、個々のインターフェイスでの LLDP のイネーブルまたはディセーブル、あるいはインターフェイスの選択的な設定を実行できます。

はじめる前に

デバイスで LLDP をグローバルにイネーブルにしていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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	switch(config)# **interface***interface slot*/*port*	LLDP をイネーブルにするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# [**no**] **lldp transmit**	インターフェイス上でLLDPパケットの送信をイネーブルまたはディセーブルにします。LLDP をグローバルにイネーブルにすると、LLDP は、デフォルトでサポートされているすべてのインターフェイス上でイネーブルになります。
ステップ 4	switch(config-if)# [**no**] **lldp receive**	インターフェイス上でLLDPパケットの受信をイネーブルまたはディセーブルにします。LLDP をグローバルにイネーブルにすると、LLDP は、デフォルトでサポートされているすべてのインターフェイス上でイネーブルになります。

	コマンドまたはアクション	目的
ステップ 5	switch(config-if)# **show lldp interface***interface slot/port*	（任意） インターフェイス上の LLDP 設定を表示します。
ステップ 6	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。

LLDP オプション パラメータの設定

LLDP の更新頻度、受信デバイスが情報を破棄するまでに保持している時間、および初期化の遅延時間を設定できます。TLV を選択して、LLDP パケットに含まれるようにすることもできます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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	switch(config)# [**no**] **lldp holdtime***seconds*	（任意） ユーザのデバイスから送信された情報が、受信側デバイスで廃棄されるまでに保持される時間を秒単位で指定します。 値の範囲は 10 ～ 255 秒で、デフォルト値は 120 秒です。
ステップ 3	switch(config)# [**no**] **lldp reinit***seconds*	（任意） 任意のインターフェイス上で LLDP を初期化する際の遅延時間を秒単位で指定します。 指定できる範囲は 1 ～ 10 秒です。デフォルトは 2 秒です。
ステップ 4	switch(config)# [**no**] **lldp timer***seconds*	（任意） LLDP アップデートの送信頻度を秒単位で設定します。 値の範囲は 5 ～ 254 秒で、デフォルト値は 30 秒です。

	コマンドまたはアクション	目的
ステップ 5	switch(config)# **show lldp timers**	（任意） LLDP の保持時間、遅延時間、更新頻度の設定を表示します。
ステップ 6	switch(config)# [**no**] **lldp tlv-select***tlv*	（任意） LLDP パケットで送受信する TLV を指定します。使用できる TLV は、dcbxp、management-address、port-description、port-vlan、system-capabilities、system-description、および system-name です。使用できるすべての TLV はデフォルトでイネーブルになっています。
ステップ 7	switch(config)# **show lldp tlv-select**	（任意） LLDP TVL コンフィギュレーションを表示します。
ステップ 8	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。

LLDP コンフィギュレーションの確認

LLDP の設定を表示するには、次のいずれかの作業を行います。

コマンド	目的
show running-config lldp	LLDP のグローバル コンフィギュレーションを表示します。
show lldp interface*interfaceslot*/*port*	LLDP のインターフェイス コンフィギュレーションを表示します。
show lldp timers	LLDP の保持時間、遅延時間、更新頻度の設定を表示します。
show lldp tlv-select	LLDP TVL コンフィギュレーションを表示します。
show lldp dcbx interface*interfaceslot*/*port*	ローカルな DCBX 制御ステータスを表示します。
show lldp neighbors {**detail** | **interface***interfaceslot*/*port*}	LLDP ネイバーのデバイス ステータスを表示します。

コマンド	目的
show lldp traffic	LLDP カウンタ（デバイスによって送信および受信された LLDP パケットの数、破棄されたパケットの数、未確認 TLV の数など）を表示します。
show lldp traffic interface*interfaceslot*/*port*	インターフェイス上で送信および受信された LLDP パケットの数を表示します。

LLDP の統計を消去するには、**clear lldp counters** コマンドを使用します。

LLDP のコンフィギュレーション例

次に、1 つのデバイス上での LLDP のイネーブル化、一部のインターフェイス上での LLDP のディセーブル化、オプション パラメータ（保持時間、遅延時間、更新頻度など）の設定、およびいくつかの LLDP TLV のディセーブル化の例を示します。

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# feature lldp
switch(config)# interface ethernet 7/9
switch(config-if)# no lldp transmit
switch(config-if)# no lldp receive
switch(config-if)# exit
switch(config)# interface ethernet 7/10
switch(config-if)# no lldp transmit
switch(config-if)# no lldp receive
switch(config-if)# exit
switch(config)# lldp holdtime 200
switch(config)# lldp reinit 5
switch(config)# lldp timer 50
switch(config)# no lldp tlv-select port-vlan
switch(config)# no lldp tlv-select system-name
```

関連資料

関連項目	関連項目
LLDP コマンド：コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト、使用上の注意事項、および例	『*Cisco Nexus 7000 Series NX-OS System Management Command Reference*』
VDC	『*Cisco Nexus 2000 Series Fabric Extender Software Configuration Guide*』
ファブリック エクステンダ	『*Cisco Network Analysis Module (NAM) for Nexus 7000 Quick Start Guide*』

LLDP の機能の履歴

次の表に、このマニュアルの新機能および変更された機能を要約し、各機能がサポートされているリリースを示します。ご使用のソフトウェア リリースで、本書で説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。

表 *37* : *LLDP* の機能の履歴

機能名	リリース	機能情報
LLDP	5.2(1)	Cisco Nexus 2000 シリーズ Fabric Extender に LLDP サポートが追加されました。
DCBXP	5.1(1)	この機能が導入されました。
LLDP	5.0(2)	この機能が導入されました。

第 20 章

NetFlow の設定

この章では、Cisco NX-OS デバイス上で NetFlow 機能を設定する方法について説明します。

- 機能情報の確認，427 ページ
- NetFlow，428 ページ
- NetFlow のライセンス要件，433 ページ
- NetFlow の前提条件，434 ページ
- NetFlow に関する注意事項および制約事項，434 ページ
- NetFlow のデフォルト設定，437 ページ
- NetFlow の設定，438 ページ
- NetFlow 設定の確認，451 ページ
- NetFlow のモニタリング，452 ページ
- NetFlow の設定例，452 ページ
- NetFlow CoPP インターフェイス サポートの確認例，453 ページ
- 関連資料，454 ページ
- NetFlow 機能の履歴，454 ページ

機能情報の確認

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

NetFlow

NetFlow は入力 IP パケットと出力 IP パケットの両方について、パケット フローを識別し、各パケット フローに基づいて統計情報を提供します。NetFlow のためにパケットやネットワーキング デバイスを変更する必要はありません。

NetFlow の概要

NetFlow ではフローを使用して、アカウンティング、ネットワーク モニタリング、およびネットワーク プランニングに関連する統計情報を提供します。フローは送信元インターフェイス（または VLAN）に届く単方向のパケット ストリームで、キーの値は同じです。キーは、パケット内のフィールドを識別する値です。フローを作成するには、フロー レコードを使用して、フロー固有のキーを定義します。

Cisco NX-OS は、ネットワーク異常とセキュリティ問題の高度な検出をイネーブルにする Flexible NetFlow 機能をサポートします。フレクシブル NetFlow 機能を使用すると、大量の定義済みフィールドの集合からキーを選択することで、そのアプリケーションに最適なフロー レコードを定義できます。

1 つのフローと見なされるパケットでは、すべてのキー値が一致している必要があります。フローは、設定したエクスポート レコード バージョンに基づいて、関係のある他のフィールドを集めることもあります。フローは NetFlow キャッシュに格納されます。

フロー用に NetFlow が収集したデータをエクスポートするには、フロー エクスポータを使用し、このデータをリモート NetFlow コレクタにエクスポートします。Cisco NX-OS は次の状況で、NetFlow エクスポート用のユーザ データグラム プロトコル（UDP）データグラムの一部としてフローをエクスポートします。

- あまりにも長期間にわたってフローが非アクティブまたはアクティブである。
- フロー キャッシュが満杯になった。
- カウンタの 1 つ（パケットまたはバイト）が最大値を超えた。
- ユーザがフローの強制的エクスポートを行った。

フロー レコードによってフロー用に収集するデータのサイズが決まります。フロー モニタはフロー レコードおよびフロー エクスポータを NetFlow キャッシュ情報と結合します。

Cisco NX-OS は、フル モードまたはサンプル モードのどちらでも、NetFlow 統計情報を収集できます。フル NetFlow モードの場合、Cisco NX-OS はインターフェイスまたはサブインターフェイス上のすべてのパケットを分析します。サンプル モードに対して、Cisco NX-OS がパケットを分析するレートを設定します。

フロー レコード

フロー レコードでは、フロー内のパケットを識別するために NetFlow で使用するキーとともに、NetFlow がフローについて収集する関連フィールドを定義します。キーと関連フィールドを任意の組み合わせで指定して、フロー レコードを定義できます。Cisco NX-OS は、様々なキー セットをサポートしています。フロー レコードでは、フロー単位で収集するカウンタのタイプも定義します。32 ビットまたは 64 ビットのパケット カウンタまたはバイト カウンタを設定できます。

キー フィールドは、match キーワードで指定されます。対象フィールドとカウンタは match キーワードで指定されます。

Cisco NX-OS では、フロー レコードの作成時に次の match フィールドをデフォルトとして使用できます。

- match interface input
- match interface output
- match flow direction

フロー エクスポータ

フロー エクスポータでは、NetFlow エクスポート パケットに関して、ネットワーク層およびトランスポート層の詳細を指定します。フロー エクスポータで設定できる情報は次のとおりです。

- エクスポート宛先 IP アドレス
- 送信元インターフェイス
- UDP ポート番号（コレクタが NetFlow パケットをリスニングするところ）

（注） NetFlow エクスポート パケットでは、送信元インターフェイスに割り当てられた IP アドレスを使用します。送信元インターフェイスに IP アドレスが割り当てられていない場合、フロー エクスポータはアクティブになりません。

Cisco NX-OS は、タイムアウトが発生するたびに、またはフローが終了したときに（TCP FIN または RST を受信した場合など）、コレクタにデータをエクスポートします。次のタイマーを設定すると、フローを強制的にエクスポートできます。

- アクティブ タイムアウト：キャッシュからキャッシュ エントリを削除します。長期間のフローが長時間コレクタに不可視になることを防止します。アクティブ タイムアウト値は常に非アクティブなタイムアウトより大きい必要があります。アクティブ タイムアウトは、M1、M2、F3、および M3 シリーズ モジュールでサポートされます。
- 非アクティブ タイムアウト：キャッシュからキャッシュ エントリを削除します。非アクティブ タイムアウトは、M1、M2、F3、および M3 シリーズ モジュールでサポートされます。

- 高速タイムアウト：M1 および M2 シリーズ モジュールで、ヒットが低いフローをフラッシュします。
- アグレッシブ タイムアウト：M1 および M2 シリーズ モジュールで、キャッシュが満杯になるとフローをアグレッシブにタイムアウトします。
- セッション タイムアウト：TCP クローズ接続ハンドシェイクが検出されたらフローをエージングします（FIN/FIN_ACK パケット）。セッション タイムアウトは、M1 および M2 シリーズ モジュールでサポートされます。
- フラッシュ キャッシュ タイムアウト：F2、F2e、および F3 シリーズ モジュールで、キャッシュをフラッシュします。

（注） 最初の 5 つのタイムアウトは、M シリーズ モジュール上の NetFlow キャッシュにのみ適用されます。フロー タイムアウトは、F2、F2e、および F3 および シリーズ モジュールでのみサポートされます。

アクティブおよび非アクティブ タイムアウトはデフォルトで存在し、設定は解除できません。時間の値だけを設定できます。

エクスポート フォーマット

Cisco NX-OS は、Version 5 と Version 9 のエクスポート フォーマットをサポートします。次の理由から、Version 9 エクスポート フォーマットを使用することを推奨します。

- ネットワークをより効率的に利用可能
- IPv6 フィールドとレイヤ 2 フィールドのサポート

Version 5 エクスポート フォーマットを設定する場合、次の 3 つの制約があります。

- 固定フィールド仕様
- IPv6 フィールドとレイヤ 2 フィールドのサポートなし
- Netflow.InputInterface および Netflow.OutputInterface は、インターフェイスの 16 ビット I/O 記述子（IOD）を表します。

（注） インターフェイスの IOD 情報は、show system internal im info global コマンドを使用して取得できます。

（注） Cisco NX-OS は、最大 2 つのコレクタにエクスポートする場合のトランスポート プロトコルとして、UDP をサポートします。

（注） M1 シリーズ モジュールは、バージョン 5 からバージョン 9 エクスポート フォーマットの設定変更をサポートしますが、F2、F2e、および F3 シリーズ モジュールはサポートしません。

フロー モニタ

フロー モニタは、フロー レコードおよびフロー エクスポータを参照します。フロー モニタはインターフェイスに適用します。

サンプラー

Cisco NX-OS はサンプル化された NetFlow をサポートします。この機能は、インターフェイスの着信および発信パケットをサンプリングします。パケットはサンプリングされ、その後フローを作成するために適性確認されます。

サンプリングされた NetFlow は、フローを作成するパケット数およびフロー数を制限することで、コレクタに送信されるエクスポート データの量を削減します。これは、フローが、転送エンジン上ではなく、ライン カードまたは外部デバイス上で作成された場合に重要です。F2、F2e、F3、および M3 シリーズ モジュールは、サンプリングされた NetFlow のみをサポートします。

F2 および F2e シリーズ モジュールで NetFlow を実装すると、ソフトウェアでフローが作成されます。フローの作成または更新を試みるパケットが多すぎる場合、CPU の負荷が増加し、保護レート リミッタの必要が増加します。レート リミッタは、CPU に到達するパケット数を約 1000 パケット/秒に制限します。F3 および M3 シリーズ モジュールでは、NetFlow プロセッサとして使用される FSA と呼ばれる特別なハードウェアを使用してフローが作成されます。

F2、F2e、F3、M3、M1、および M2 モジュールでサポートされるサンプリング モードは、M out of N です。このモードでは、各 N パケットごとに M パケットがサンプル用にランダムに選択され、これらのパケットのみがフローを作成できます。

（注） F2 および F2e シリーズ モジュールでは、スケーリング因数を設定する必要があることに注意してください。これは、設定されたサンプリングで乗算される 1:1000 の追加サンプリングです。この因数を見落とした場合、レポートされるレートに実際の値は反映されません。

レート リミッタは、F2 および F2e シリーズ モジュール上で、CPU に到達するパケット数を 約 1000 パケット/秒に制限します。F3 シリーズ モジュールでは、ASIC（SoC）あたり 500 PPS のレート制限が実装されます。したがって、Cisco NX-OS 7000 では、F3 シリーズ モジュールに 6 つの SoC が搭載されている場合、F3 シリーズ モジュールあたりの CPU に対するレート制限は、500*6=3000 PPS になります。Cisco NX-OS 7700 では、F3 シリーズ モジュールに 12 個 の SoC が搭載されている場合、F3 シリーズ モジュールあたりの CPU に対するレート制限は、500*12=6000 PPS になります。

他のシリーズモジュール F2 および F2e で 1:8191 であるのに対し、F3 および M3 シリーズモジュールは、より高いサンプリング レート、1:131071 をサポートします。

（注） F3 シリーズ モジュールは、バージョン 9 でさらに多くのサンプリング レートをサポートします。7.2(0)D1(1) リリースでの F3 シリーズ モジュールのパフォーマンスは、6.2.x リリースの場合と比較して、パケット処理機能が 20 ～ 50 倍向上しています。つまり、50000 pps まで強化されています。速度の改善により、このリリースでの F3 シリーズ モジュールでは、低いサンプリング レートを使用できます。たとえば、1:4000 のサンプリングを 1:80 のサンプリングに置き換えることができます。

M3 シリーズ モジュールでは、デフォルトのレート制限値は ASIC（SoC）あたり 8000 PPS です。このようなシナリオでは、Cisco Nexus 7700 の M3 シリーズ、48 ポート 1/10G イーサネット モジュール（2 つの SoC を搭載）の M3 シリーズ モジュールあたりの CPU に対するレート制限は、8000*2=16000 PPS のみとなります。特定の M3 シリーズ モジュールでレート制限値を 24000 PPS に設定するには、**hardware rate-limiter layer-2 netflow** *rate* **module** *m3module* コマンドを使用します。この設定により、M3 リーズ モジュールの、M3 リーズ モジュールあたりの CPU に対するレート制限を 24000*2=48000 PPS にすることができます。

同様に、Cisco Nexus 7700 の M3 シリーズ、24 ポート 40G イーサネット モジュール（4 つの SoC を搭載）の M3 シリーズ モジュールあたりの CPU に対するレート制限は、8000*4=32000 PPS のみとなります。特定の M3 シリーズ モジュールでレート制限値を 12000 PPS に設定するには、**hardware rate-limiter layer-2 netflow** *rate* **module** *m3module* コマンドを使用します。この設定により、M3 リーズ モジュールの、M3 リーズ モジュールあたりの CPU に対するレート制限を 12000*4=48000 PPS にすることができます。

次の制限は、サンプルされた NetFlow および F2 シリーズおよび F2e シリーズ モジュールに適用されます。

- 1:100 の追加サンプリングが、F2 シリーズおよび F2e シリーズ モジュールの設定値に適用されます。たとえば、設定されたサンプリングが 1/200 の場合、実際に適用されるサンプリングは 1/20000 です。サンプラ値を 1:4956 に設定すると、システムはレート リミッタを開始しません。この値は、モジュールを通過する最大トラフィックに基づいて計算されます。
- 従来の NetFlow と比較したサンプル NetFlow の精度は、設定したサンプリング レートに依存します。サンプリング レートが 1:1 の場合、サンプリングされた NetFlow は、従来の NetFlow と同様に精密です。サンプリング レートが 1:100 の場合、サンプリングされた NetFlow は従来ほどは正確ではありませんが、デバイスのモニタに充分な統計パターンを生成します。

CoPP インターフェイスでの NetFlow サポート

CoPP インターフェイスでの NetFlow サポート機能により、スーパーバイザ モジュール（つまりコントロール プレーン）を宛先とするパケットに NetFlow を適用できます。

CoPP インターフェイスでの NetFlow サポート機能により、コントロール プレーンに出力されるパケットをモニタできます。このモニタリング機能は、NX-OS release 7.3(0)D1(1) で追加されました。

コントロール プレーン ポリシングの詳細については、『*Cisco Nexus 7000 Series NX-OS Security Configuration Guide*』を参照してください。

Network Analysis Module; ネットワーク解析モジュール

Cisco Network Analysis Module（NAM）を使用して、NetFlow データソースをモニタすることもできます。NAM を使用すると、ホスト、アプリケーション、対話、VLAN、QoS などのトラフィック分析の表示およびレポート作成が可能になります。「NetFlow の設定例」の NAM の設定例を参照してください。

Cisco Nexus 7000 NetFlow データ ソースのモニタリングに NAM を使用する詳細については、『*Cisco Nexus 7000 Series Network Analysis Module (NAM-NX1) Quick Start Guide*』を参照してください。

ハイ アベイラビリティ

Cisco NX-OS は、NetFlow のステートフル 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。

フロー キャッシュはプロセスの再起動で保持されず、再起動中にソフトウェアに送信されるパケットは処理されないため、スイッチオーバ中のフローはすべて失われ、復元することはできません。

仮想化のサポート

仮想デバイス コンテキスト（VDC）は、一連のシステム リソースを論理的に表現する用語です。各 VDC 内で、NetFlow を設定できます。デフォルトでは、Cisco NX-OS はデフォルトの VDC が使用されるようにします。また、このモードで定義したフローを使用できるのは、デフォルト VDC のインターフェイスに限られます。

VDC の設定方法については、『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』を参照してください。

NetFlow のライセンス要件

表 *38*：*NetFlow* のライセンス要件

製品	ライセンス要件

Cisco NX-OS	NetFlow 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。NX-OS ライセンス方式の詳細については、『Cisco NX-OS Licensing Guide』を参照してください。

NetFlow の前提条件

NetFlow の前提条件は、次のとおりです。

- NetFlow はメモリおよび CPU リソースを大量に消費するので、デバイス上で必要なリソースについて理解しておく必要があります。
- VDC を設定する場合は、適切なライセンスをインストールし、所定の VDC を開始する必要があります。設定情報については『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』、ライセンス情報については『Cisco NX-OS Licensing Guide』を参照してください。

NetFlow に関する注意事項および制約事項

NetFlow に関する設定時の注意事項および制約事項は、次のとおりです。

- NDE エクスポートでは、送信元インターフェイスを設定する必要があります。送信元インターフェイスを設定しなかった場合、フロー エクスポータはディセーブル ステートのままです。
- フロー モニタごとに、有効なレコード名を設定する必要があります。
- NetFlow タイムアウトはすべて、フロー タイムアウトを除き、M1 および M2 シリーズ モジュールだけに適用されます。フロー タイムアウトは、F2、F2e、および F3 および シリーズ モジュールでのみサポートされます。アクティブおよび非アクティブ タイムアウトのみ、M3 シリーズ モジュールに適用されます。
- ロールバック中、ハードウェアでプログラムされているレコードを変更しようとすると、ロールバックは失敗します。
- レイヤ 2 インターフェイスではレイヤ 2 NetFlow だけが適用され、レイヤ 3 インターフェイスではレイヤ 3 NetFlow だけが適用されます。
- レイヤ 2 NetFlow に対してすでに設定されているポート チャネルにメンバを追加すると、NetFlow の設定が削除され、ポート チャネルのレイヤ 2 設定が追加されます。
- レイヤ 2 インターフェイスをレイヤ 3 インターフェイスへ変更すると、ソフトウェアで、インターフェイスからレイヤ 2 の NetFlow 設定が削除されます。

- NetFlow コネクタで完全な 32 ビットの SNMP ifIndex 値を表示するには、NetFlow v9 エクスポートを使用してください。
- NetFlow でサポートされているエントリの最大数は 512,000 です。
- トンネル インターフェイスでは、NetFlow は設定はできますがサポートされません。
- Cisco Nexus 2000 シリーズ Fabric Extender（FEX）は、FEX ポートのレイヤ 3 NetFlow 設定をサポートします。
- Cisco Nexus 2000 シリーズ FEX はブリッジされた NetFlow をサポートします（VLAN 内のフロー対象）。
- M1 シリーズ モジュールは、バージョン 5 からバージョン 9 エクスポート フォーマットの設定変更をサポートしますが、F2、F2e、および F3 シリーズ モジュールはサポートしません。
- F2、F2e、F3、および M3 シリーズ モジュールは、次の変更はサポートしません。
  - アクティブ モニタに適用されるレコード内のフィールドの変更。
  - アクティブ モニタに適用されるサンプラ上のサンプリング モード値の変更。
- Cisco NX-OS Release 5.2 以降では、少なくとも 1 つの M1 シリーズ モジュールがある場合、NetFlow は F1 シリーズ ポートのスイッチ仮想インターフェイス（SVI）でサポートされます。SVI NetFlow は、VLAN 間でルーティングされたトラフィックを対象としています。
- M シリーズ モジュールで、SVI にレイヤ 3 NetFlow 入力フロー モニタを適用し、レイヤ 2 インターフェイスにレイヤ 2 NetFlow 入力フロー モニタをたとえば同じ基盤 VLAN が可能なトランクとして適用した場合、両方のインターフェイスへのすべての入力フローはレイヤ 2 NetFlow フロー モニタのみによってレポートされます。
- F2、F2e、F3、および M3 シリーズ モジュールは、サンプリングされた NetFlow のみをサポートします。
- Cisco NX-OS Release 6.1(2) 以降では、サンプリングされた NetFlow は、F2 および F2e シリーズ モジュールでサポートされます。
- Cisco NX-OS Release 6.2(6) 以降では、サンプリングされた NetFlow は、F3 シリーズ モジュールでサポートされます。
- 出力 NetFlow は、F2、F2e モジュールではサポートされず、これらのモジュールが存在するいずれの混合 VDC でもサポートされません。
- Cisco NX-OS Release 7.2(0)D1(1) 以降では、出力 NetFlow は、F3 モジュールでサポートされます。
- Cisco NX-OS Release 7.2(1)D1(1) 以降では、サブインターフェイスは、F2、F2e、および F3 シリーズ モジュールでサポートされます。
- Cisco NX-OS Release 7.3(0)DX(1) 以降では、入力および出力 NetFlow は、M3 シリーズ モジュールでサポートされます。
- デフォルトでは、入力 NetFlow サンプリングを使用することはできず、DHCP は同じインターフェイス上で一緒にリレーします。ただし、Cisco NX-OS Release 6.2(2) 以降では、デフォル

トを上書きして、同じインターフェイス上でこれら 2 つの機能を **hardware access-list resource feature bank-mapping** コマンドを、各機能それぞれをイネーブルにするのに必要なコマンドを入力した後で使用することで設定できます。このコマンドの詳細については、『*Cisco Nexus 7000 Series NX-OS Security Configuration Guide*』の「**Configuring IP ACLs**」の章を参照してください。

- Cisco NX-OS Release 6.2(2) 以降では、NetFlow 全体が SPAN を通して Cisco NetFlow Generation Appliance（NGA）でサポートされます。サンプルされた NetFlow がサンプルされた SPAN を通して NGA でサポートされます。

NetFlow には、M1、M2 シリーズと F2、F2e、F3、および M3 シリーズ モジュールの両方において混合 VDC に対する以下の制限があります。

- VDC は、少なくとも 1 つの F2e シリーズ ポートまたは少なくとも 1 つの F3 シリーズ ポートを含む場合、混合 VDC のみとして分類されます。
- レイヤ 2 NetFlow：M1 および M2 シリーズ モジュール ポートではサンプリングされた NetFlow と NetFlow 全体がサポートされ、F2e、F3、および M3 シリーズ モジュール ポートではサンプリングされた NetFlow のみがサポートされます。
- レイヤ 3 NetFlow：M1 および M2 シリーズ モジュール ポートではサンプリングされた NetFlow と NetFlow 全体がサポートされます。F2 および F2e シリーズ モジュール ポートはプロキシ モードで開始するため、レイヤ 3 ポートとして設定することはできません。したがって、レイヤ 3 NetFlow およびサブインターフェイス NetFlow はこれらのポートで機能しません。F3 および M3 シリーズ モジュール ポートでは、サンプリングされた NetFlow がサポートされます。
- VLAN、SVI、およびポート チャネル：M1、M2 シリーズと F2e、F3、および M3 シリーズ モジュールの両方において、サンプリングされた NetFlow のみが VLAN、SVI、およびポート チャネルでサポートされます。
- サブインターフェイス（物理/ポート チャネル）：NetFlow 設定は F2、F2e、F3、および M3 シリーズ モジュール インターフェイスでサポートされます。
- 動的な構成変更は、M1 および M2 シリーズと F2e、F3、および M3 モジュールで適用されたポリシーに対して混合 VDC で使用できません。
- フロータイムアウトは F2e および F3 シリーズ モジュールだけに適用されます。他の NetFlow タイマーは M1 および M2 シリーズ モジュールに適用されます。アクティブおよび非アクティブ タイムアウトのみ、M3 シリーズ モジュールに適用されます。
- 出力 NetFlow は M シリーズおよび F2e および F3 シリーズ モジュールの両方を含む VDC で完全にブロックされます。

CoPP インターフェイスでの NetFlow サポート機能固有の注意事項と制約事項：

- この機能は、デフォルトの VDC でのみ設定できます。
- ユニキャスト パケットがサポートされます。

- この機能は、レイヤ 3 NetFlow フィールドのキャプチャのみをサポートします。レイヤ 2 フィールドのキャプチャはサポートされません。
- この機能には、サンプラの必須設定が必要です。
- この機能はイネーブル化されると、システム内のすべてのライン カードに次のように適用されます。
  - M1/M2 ラインカードは、ハードウェア テーブル内にサンプリングされたフローを作成します。512,000 のエントリを含むグローバル ルーティング テーブルが通常の NetFlow と共有されます。
  - F2/F2e ラインカードは、ソフトウェア テーブル内にサンプリングされたフローを作成します。テーブルあたりのパケット/秒（PPS）のサイズ制限が通常の NetFlow と共有されます。追加の 1:100 のサンプラも通常どおりに適用されます。
  - F3 ラインカードは、ソフトウェアでフローを作成します。テーブルあたりの PPS のサイズ制限が通常の NetFlow と共有されます。
  - パケットはスーパーバイザ モジュールに出力されるため、この機能は出力方向にのみ適用されます。

NetFlow のデフォルト設定

次の表に、NetFlow パラメータのデフォルト設定を示します。

表 *39*：デフォルトの *NetFlow* パラメータ

パラメータ	デフォルト
出力および入力キャッシュ サイズ	512,000
フロー アクティブ タイムアウト	1800 秒
フロータイムアウト（F2、F2e および F3 シリーズ モジュールのみ対象）	15 秒
フロー タイムアウト アグレッシブしきい値	ディセーブル
フロー タイムアウト高速しきい値	ディセーブル
フロー タイムアウトの非アクティブ化	15 秒
フロー タイムアウト セッション エージング	ディセーブル

NetFlow の設定

NetFlow を設定する手順は、次のとおりです。

手順

ステップ 1 NetFlow 機能をイネーブルにします。

ステップ 2 フローにキーおよびフィールドを指定することによって、フロー レコードを定義します。

ステップ 3 エクスポート フォーマット、プロトコル、宛先、およびその他のパラメータを指定することによって、任意でフロー エクスポータを定義します。

ステップ 4 フロー レコードおよびフロー エクスポータに基づいて、フロー モニタを定義します。

ステップ 5 送信元インターフェイス、サブインターフェイス、VLAN インターフェイスにフロー モニタを適用します。

NetFlow 機能のイネーブル

フローを設定するには、先に NetFlow をグローバルでイネーブルにしておく必要があります。

NetFlow をイネーブルにするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
feature netflow 例： `switch(config)# feature netflow`	NetFlow 機能をイネーブルにします。

コマンド	目的
no feature netflow 例： `switch(config)# no feature netflow`	NetFlow 機能をディセーブルにします。デフォルトではディセーブルになっています。

フロー レコードの作成

フロー レコードを作成し、照合するためのキー、および収集するための非キー フィールドをフロー内に追加します。

はじめる前に

正しい VDC 内にいることを確認します。VDC の変更は **switchto vdc** コマンドを使用します。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure t**
	
	例：
	`switch# config t`
	`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	**flow record***name*
	
	例：
	`switch(config)# flow record Test`
	`switch(config-flow-record)#`
		フロー レコードを作成し、フロー レコード コンフィギュレーション モードを開始します。フロー レコード名を最大 63 文字の英数字で入力できます。

ステップ 3	**description***string*
	
	例：
	`switch(config-flow-record)#`
	`description Ipv4Flow`
		（任意）
		（任意）最大 63 文字で、このフローの説明を指定します。

ステップ 4	**match***type* 例： `switch(config-flow-record)# match transport destination-port`	（任意） 一致キーを指定します。 （注） レイヤ 4 ポートのデータをエクスポートするには、**match transport destination-port** および **match ip protocol** コマンドが必要です。
ステップ 5	**collect***type* 例： `switch(config-flow-record)# collect counter packets`	（任意）コレクション フィールドを指定します。
ステップ 6	**show flow record** [**name**] [*record-name*] |**netflow-original** | **netflow protocol-port** | **netflow** {**ipv4** | **ipv6**} {**original-input** | **original-output**}}	（任意）NetFlow のフロー レコード情報を表示します。フロー レコード名を最大 63 文字の英数字で入力できます。

	コマンドまたはアクション	目的
	例： `switch(config-flow-exporter)# show flow record netflow protocol-port`	
ステップ 7	**copy running-config startup-config** 例： `switch(config-flow-exporter)# copy running-config startup-config`	（任意）この設定の変更を保存します。

match パラメータの指定

フロー レコードごとに、次の match パラメータを 1 つ以上設定する必要があります。

コマンド	目的
match ip {**protocol** | **tos**} 例： `switch(config-flow-record)# match ip protocol`	IP プロトコルまたは ToS フィールドをキーとして指定します。 （注） レイヤ 4 ポートのデータをエクスポートするには、**match transport destination-port** および **match ip protocol** コマンドが必要です。**show hardware flow ip** コマンドでもデータは収集され出力に表示されますが、上記の両方のコマンドを設定しないと、収集とエクスポートはされません。
match ipv4 {**destination address** | **source address**} 例： `switch(config-flow-record)# match ipv4 destination address`	IPv4 送信元または宛先アドレスをキーとして指定します。
match ipv6 {**destination address** | **source address** | **flow-label** | **opitons** } 例： `switch(config-flow-record)# match ipv6 flow label`	IPv6 キーを指定します。

コマンド	目的
match transport {**destination-port** | **source-port**} 例： `switch(config-flow-record)# match transport destination-port`	トランスポート送信元または宛先ポートをキーとして指定します。 （注） レイヤ4ポートのデータをエクスポートするには、**match transport destination-port** および **match ip protocol** コマンドが必要です。**show hardware flow ip** コマンドでもデータは収集され出力に表示されますが、上記の両方のコマンドを設定しないと、収集とエクスポートはされません。
match datalink {**mac source-address** | **mac destination-address** | **ethertype** | **vlan**} 例： `switch(config-flow-record)# match datalink ethertype`	レイヤ 2 属性をキーとして指定します。

collect パラメータの指定

フロー レコードごとに、次の collect パラメータを 1 つ以上設定する必要があります。

コマンド	目的
collect counter {**bytes** | **packets**} [**long**] 例： `switch(config-flow-record)# switch(config-flow-record)# collect counter packets`	フローからパケットベースまたはバイト カウンタを収集します。任意で、64 ビット カウンタを使用することを指定できます。
collect flow sampler id 例： `switch(config-flow-record)# collect flow sampler`	フローに使用するサンプラの ID を収集します。
collect timestampsys-uptime {**first** | **last**} 例： `switch(config-flow-record)# collect timestamp sys-uptime last`	フローの先頭または最終パケットに関するシステム稼働時間を収集します。
collect transporttcpflags 例： `switch(config-flow-record)# collect transport tcp flags`	フローのパケットに対応する TCP トランスポート層フラグを収集します。

コマンド	目的
collect ip version 例： `switch(config-flow-record)# collect ip version`	フローの IP バージョンを収集します。

フロー エクスポータの作成

フロー エクスポータの設定では、フローに対するエクスポート パラメータを定義し、リモート NetFlow コレクタへの到達可能性情報を指定します。

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	**flow exporter***name* 例： `switch(config)# flow exporter flow-exporter-one`	フローエクスポータを作成し、フローエクスポータ コンフィギュレーション モードを開始します。フローエクスポータ名を最大 63 文字の英数字で入力できます。
ステップ 3	**destination** { **ipv4-address** | **ipv6-address**} [**use-vrf***name*] 例： `switch(config-flow-exporter)# destination 192.0.2.1`	このフロー エクスポータの宛先 IPv4 または IPv6 アドレスを設定します。任意で、NetFlow コレクタに到達するために使用する VRF を設定できます。VRF 名には最大 32 文字の英数字を入力できます。
ステップ 4	**sourceinterface-type***name/port* 例： `switch(config-flow-exporter)# source ethernet 2/1`	設定された宛先で NetFlow コネクタに到達するために使用するインターフェイスを指定します。
ステップ 5	**description***string* 例： `switch(config-flow-exporter)# description exportversion9`	（任意） （任意）このフローエクスポータについて説明します。説明には最大 63 文字の英数字を入力できます。

	コマンドまたはアクション	目的
ステップ 6	**dscp***value* 例： `switch(config-flow-exporter)# dscp 0`	（任意） （任意）DSCP（DiffServ コードポイント）値を指定します。範囲は 0 ～ 63 です。
ステップ 7	**transport udp***port* 例： `switch(config-flow-exporter)# transport udp 200`	（任意） （任意）NetFlow コレクタに到達するために使用する UDP ポートを指定します。範囲は 0 ～ 65535 です。 （注） UDP ポートを指定しない場合は、9995 がデフォルトとして選択されます。
ステップ 8	**version** {**5** | **9**} 例： `switch(config-flow-exporter)# version 9`	NetFlow エクスポート バージョンを指定します。フローエクスポータのバージョン 9 コンフィギュレーション サブモードを開始するには、バージョン 9 を選択します。
ステップ 9	**option** {**exporter-stats** | **interface-table** | **sampler-table**} **timeout***seconds* 例： `switch(config-flow-exporter-version-9)# option exporter-stats timeout 1200`	（任意） フローエクスポータの統計情報再送信タイマーを設定します。値の範囲は 1 ～ 86400 秒です。
ステップ 10	**templatedatatimeout***seconds* 例： `switch(config-flow-exporter-version-9)# template data timeout 1200`	（任意） テンプレートデータ再送信タイマーを設定します。値の範囲は 1 ～ 86400 秒です。
ステップ 11	**exit** 例： `switch(config-flow-exporter-version-9)# exit`	フロー エクスポータ コンフィギュレーション モードに戻ります。
ステップ 12	**exit** 例： `switch(config-flow-exporter)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 13	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

フロー モニタの作成

フロー モニタを作成して、フロー レコードおよびフロー エクスポータと関連付けることができます。1 つのモニタに属しているすべてのフローは、様々なフィールド上で照合するために関連するフロー レコードを使用します。データは指定されたフローエクスポータにエクスポートされます。

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	**flow monitor***name* 例： `switch(config)# flow monitor flow-monitor-one`	フロー モニタを作成し、フロー モニタ コンフィギュレーション モードを開始します。フロー モニタ名を最大 63 文字の英数字で入力できます。
ステップ 3	**description***string* 例： `switch(config-flow-monitor)# description IPv4Monitor`	（任意） このフローモニタについて説明します。説明には最大 63 文字の英数字を入力できます。
ステップ 4	**exporter***name* 例： `switch(config-flow-monitor)# export v9`	（任意） フローエクスポータとこのフローモニタを関連付けます。エクスポータ名には最大63 文字の英数字を入力できます。
ステップ 5	**record** {*name***netflow-original** | **netflow protocol-port** | **netflow** {**ipv4** | **ipv6**} {**original-input** | **original-output**}} 例： `switch(config-flow-monitor)# record IPv4Flow`	フロー レコードを指定したフローモニタと関連付けます。レコード名には最大63 文字の英数字を入力できます。
ステップ 6	**exit** 例： `switch(config-flow-monitor)# exit`	グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 7	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

サンプラーの作成

フロー サンプラーを作成し、フローに対して NetFlow サンプリング レートを定義することができます。

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	**sampler***name* 例： `switch(config)# sampler testsampler`	サンプラーを作成し、サンプラー コンフィギュレーション モードを開始します。フロー サンプラー名を最大 63 文字の英数字で入力できます。
ステップ 3	**description***string* 例： `switch(config-flow-sampler)# description samples`	（任意） （任意）このサンプラーについて説明します。説明には最大 63 文字の英数字を入力できます。
ステップ 4	**mode***sample-number***out-of***packet-number* 例： `switch(config-flow-sampler)# mode 1 out-of 128`	受信パケット数あたりの取得サンプル数を定義します。sample-number の範囲は 1 ～ 64 で、packet-number の範囲は 1 ～ 65536 です。
ステップ 5	**exit** 例： `switch(config-flow-sampler)# exit`	グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

インターフェイスへのフロー モニタの適用

（注） 出力インターフェイスにはフロー モニタを適用できません。入力 NetFlow のみサポートされています。

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	**interface***interface-typeslot/port* 例： `switch(config)# interface ethernet 2/1`	インターフェイス コンフィギュレーション モードを開始します。インターフェイス タイプには、イーサネット（サブインターフェイスを含む）、ポート チャネル、またはVLANインターフェイスを使用できます。
ステップ 3	**ip flow monitor***name***inputsampler***name* 例： `switch(config-if)# ip flow monitor testmonitor input sampler testsampler`	入力パケットのインターフェイスに、IPv4 フローモニタおよびサンプラを関連付けます。フロー モニタ名およびサンプラ名を最大 63 文字の英数字で入力できます。
ステップ 4	**ipv6 flow monitor***name***inputsampler***name* 例： `switch(config-if)# ipv6 flow monitor testmonitorv6 input sampler testsamplerv6`	入力パケットのインターフェイスに、IPv6 フローモニタおよびサンプラを関連付けます。フロー モニタ名およびサンプラ名を最大 63 文字の英数字で入力できます。

	コマンドまたはアクション	目的
ステップ 5	**layer2-switched flow monitor***name***inputsampler***name* 例： `switch(config-if)# layer2-switched flow monitor testmonitorl2 input sampler testsamplerl2`	入力パケットのインターフェイスに、レイヤ 2 スイッチ フローモニタとサンプラを関連付けます。フローモニタ名およびサンプラ名を最大 63 文字の英数字で入力できます。
ステップ 6	**exit** 例： `switch(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

CoPP インターフェイスでの NetFlow サポートの設定

フロー レコードを作成し、照合するためのキー、および収集するための非キー フィールドをフロー内に追加します。

はじめる前に

デフォルトの VDC で次の設定を行います。

手順

ステップ 1 グローバル コンフィギュレーション モードを開始します。
switch# **configure terminal**

ステップ 2 コントロール プレーン コンフィギュレーション モードを開始します。ユーザが、デバイスのコントロール プレーンに関連付けられている属性を関連付けることができるようにします。
switch(config)# **control-plane**

ステップ 3 出力パケットのコントロールプレーンに、IPv4 フローモニタおよびサンプラを関連付けます。フロー モニタ名およびサンプラ名を最大 63 文字の英数字で入力できます。
switch(config-cp)# **ip flow monitor***name***output sampler***name*

次の作業

CoPP インターフェイスでの NetFlow サポート機能の設定を完了するには、次の作業を実行する必要があります。

フロー レコードの作成, （439 ページ）

フロー モニタの作成

サンプラーの作成, （445 ページ）

VLAN 上でのブリッジ型 NetFlow の設定

VLAN にフロー モニタおよびサンプラを適用できます。

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	**vlan configuration***vlan-id* 例： `switch(config)# vlan configuration 30`	VLAN コンフィギュレーション モードを開始します。vlan-id の範囲は 1 ～ 3967、または 4048 ～ 4093 です。 （注） VLAN コンフィギュレーション モードでは、作成とは無関係に VLAN を設定できます。これは、VTP クライアントのサポートに必要です。
ステップ 3	{**ipipv6**} **flow monitor***name***inputsampler***name* 例： `switch(config-vlan-config)# ip flow monitor testmonitor input sampler testsampler`	入力パケットの VLAN にフロー モニタおよびサンプラを関連付けます。フロー モニタ名およびサンプラ名を最大 63 文字の英数字で入力できます。
ステップ 4	**exit** 例： `switch(config-vlan-config)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

	コマンドまたはアクション	目的

レイヤ 2 NetFlow の設定

フレクシブル NetFlow レコード内でレイヤ 2 キーを定義できます。このレコードを使用して、レイヤ 2 インターフェイスのフローをキャプチャできます。レイヤ 2 のキーは次のとおりです。

- 送信元および宛先 MAC アドレス
- 送信元 VLAN ID
- イーサネット フレームのイーサネット タイプ

受信方向については、次のインターフェイスに対してレイヤ 2 NetFlow を適用できます。

- アクセス モードのスイッチ ポート
- トランク モードのスイッチ ポート
- レイヤ 2 のポート チャネル

（注） Layer 2 NetFlow を VLAN、送信インターフェイス、またはレイヤ 3 インターフェイス（VLAN インターフェイスなど）に適用できます。

はじめる前に

正しい VDC 内にいることを確認します。VDC を変更するには、**switchto vdc** コマンドを使用します。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure t**
	
	例：
	`switch# configure terminal`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
		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	**flow record***name* 例： `switch(config)# flow record L2_record`	フロー レコード コンフィギュレーション モードを開始します。フロー レコードの設定方法については、「フロー レコードの作成」の項を参照してください。

	コマンドまたはアクション	目的
ステップ 3	**match datalink** {**mac source-address** | **mac destination-address** | **ethertype** | **vlan**} 例： `switch(config-flow-record)# match datalink ethertype`	レイヤ 2 属性をキーとして指定します。
ステップ 4	**interface** {**ethernet***slotport*} | {**port-channel***number*} 例： `switch(config-flow-record)# interface Ethernet 6/3`	インターフェイス コンフィギュレーション モードを開始します。インターフェイス タイプは、物理的なイーサネット ポートまたはポート チャネルを指定できます。
ステップ 5	**switchport** 例： `switch(config-if)# switchport`	インターフェイスをレイヤ 2 の物理インターフェイスに変更します。スイッチ ポートの設定方法については、『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide*』を参照してください。
ステップ 6	**mac packet-classify** 例： `switch(config-if)# mac packet-classify`	パケットの MAC 分類を強制します。 mac packet-classify コマンドの使用については、『*Cisco Nexus 7000 Series NX-OS Security Configuration Guide.*』を参照してください。 （注） フローを検出するためにこのコマンドを使用する必要があります。
ステップ 7	**layer2-switched flow monitor***flow-name***input**[**sampler***sampler-name*] 例： `switch(config-vlan)# layer2-switched flow monitor L2_monitor input sampler L2_sampler`	フロー モニタおよびオプションのサンプラーをスイッチ ポートの入力パケットに関連付けます。 • フロー モニタ名およびサンプラ名を最大 63 文字の英数字で入力できます。
ステップ 8	**show flow record netflow layer2-switched input** 例： `switch(config-if# show flow record netflow layer2-switched input`	（任意）レイヤ 2 NetFlow のデフォルト レコードの情報を表示します。

	コマンドまたはアクション	目的
ステップ 9	**copy running-config startup-config** 例： `switch(config-vlan)# copy running-config startup-config`	（任意）この設定の変更を保存します。

NetFlow タイムアウトの設定

任意で、システム内のすべてのフローに適用されるグローバルな NetFlow タイムアウトを設定できます。

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	**flow timeout***seconds* 例： `switch(config)# flow timeout 30`	フラッシュ タイムアウト値を秒単位で設定します。範囲は 5 ～ 60 秒です。
ステップ 3	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

NetFlow 設定の確認

NetFlow の設定を表示するには、次のいずれかの作業を行います。

コマンド	目的
show flow exporter [*name*]	NetFlow のフロー エクスポータ情報と統計情報を表示します。フロー エクスポータ名を最大 63 文字の英数字で入力できます。

コマンド	目的
show flow interface [*interface-type slot/port*]	NetFlow インターフェイスに関する情報を表示します。
show flow record [*name*]	NetFlow のフロー レコード情報を表示します。フロー レコード名を最大 63 文字の英数字で入力できます。
show flow record netflow layer2-switched input	レイヤ 2 NetFlow コンフィギュレーションの情報を表示します。
show flow timeout	NetFlow タイムアウト情報を表示します。
show sampler [*name*]	NetFlow サンプラに関する情報を表示します。 サンプラ名には最大 63 文字の英数字を入力できます。
show hardware ip flow	NetFlow ハードウェア IP フローに関する情報を表示します。
show running-config netflow	デバイスの現在の NetFlow 設定を表示します。

NetFlow のモニタリング

NetFlow の統計情報を表示するには、**show flow exporter** コマンドを使用します。NetFlow フロー エクスポータの統計情報を消去するには、**clear flow exporter** コマンドを使用します。

NetFlow の設定例

次に、IPv4 に対して NetFlow エクスポータを設定する例を示します。

```
feature netflow
flow exporter ee
 version 9
flow record rr
 match ipv4 source address
 match ipv4 destination address
 collect counter bytes
 collect counter packets
flow monitor foo
 record rr
 exporter ee
interface Ethernet2/45
 ip flow monitor foo input
 ip address 10.20.1.1/24
 no shutdown
```

この例は、Cisco Nexus 7000 シリーズ スイッチから NAM への IPv4 に対する NetFlow エクスポータ設定を示しています。

```
flow exporter pw
  destination 172.20.101.87 use-vrf management
  transport udp 3000
  source mgmt0
  version 9

flow record pw
  match ipv4 source address
  match ipv4 destination address
  match ip protocol
  match ip tos
  match transport source-port
  match transport destination-port
  collect counter bytes long
  collect counter packets long
  collect timestamp sys-uptime first
  collect timestamp sys-uptime last
  collect ip version

flow monitor pw
  record pw
  exporter pw

interface Ethernet2/9
  ip flow monitor pw input
  ip flow monitor pw output
```

NetFlow CoPP インターフェイス サポートの確認例

show hardware flow ip コマンドの出力例

```
 switch(config-if)# show hardware flow ip

D - Direction; L4 Info - Protocol:Source Port:Destination Port
IF - Interface: (Eth)ernet, (S)vi, (V)lan, (P)ortchannel, (T)unnel
TCP Flags: Ack, Flush, Push, Reset, Syn, Urgent

D  IF          SrcAddr          DstAddr          L4 Info          PktCnt     TCP Fl
--+-----------+---------------+---------------+---------------+----------+------
CP sup-eth1    010.014.014.002 010.014.014.001 001:00000:00000 0000000021 ......
```

show running-configuration netflow コマンドの出力例

```
 switch# show running-configuration netflow

version 7.3(0)D1(1)

feature netflow

flow timeout active 60
flow exporter exp1
  destination 10.76.80.132 use-vrf management
  transport udp 9995
  source mgmt0
  version 9
    template data timeout 5
    option sampler-table timeout 8
sampler s3
  mode 2 out-of 3
flow monitor M2
  record netflow ipv4 original-input
  exporter exp1
```

```
control-plane
  ip flow monitor M2 output sampler s3
```

関連資料

関連項目	関連項目
NetFlow CLI コマンド	『*Cisco Nexus 7000 Series NX-OS System Management Command Reference*』
VDC および VRF	『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』
『Cisco Network Analysis Module (NAM)』	『*Cisco Network Analysis Module (NAM) for Nexus 7000 Quick Start Guide*』
『Cisco NetFlow Generation Appliance (NGA)』	『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』

NetFlow 機能の履歴

次の表に、このマニュアルの新機能および変更された機能を要約し、各機能がサポートされているリリースを示します。ご使用のソフトウェア リリースで、本書で説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。

表 *40*：*NetFlow* 機能の履歴

機能名	リリース	機能情報
NetFlow	7.3(0)DX(1)	M3 シリーズ モジュールで NetFlow のサポートが追加されました。
NetFlow	7.3(0)D1(1)	CoPP インターフェイスでの NetFlow サポートの追加されました。
NetFlow	7.2(0)D1(1)	F3 シリーズ モジュールのパケット処理率を 50000 pps に強化しました。

NetFlow	6.2(6)	F3 シリーズモジュールのサポートが追加されました。
NetFlow	6.2(2)	同じインターフェイスで設定される入力 NetFlow サンプリングおよび DHCP リレーのサポートが追加されました。
NetFlow	6.2(2)	NetFlow データソースに対する NAM サポートが追加されました。
NetFlow	6.2(2)	Cisco NetFlow Generation Appliance（NGA）で NetFlow 全体およびサンプリングされた NetFlow のサポートが追加されました。
NetFlow	6.1(2)	F2 シリーズおよび F2e シリーズモジュールでサンプリングされた NetFlow のサポートが追加されました。
NetFlow	6.1(2)	F2 シリーズおよび F2e シリーズモジュールで flow timeout seconds コマンドが追加されました。
NetFlow	6.0(1)	NetFlow は、F2 シリーズモジュールではサポートされません。
NetFlow	6.0(1)	ACL エントリによって拒否されたフローのコレクションをトリガするために collect routing forwarding-status コマンドのサポートが追加されました。
NetFlow	5.2(1)	NetFlow は F1 シリーズポートのスイッチ仮想インターフェイス（SVI）でサポートされます。
ブリッジ NetFlow	5.1(1)	VLAN 上でブリッジ NetFlow を設定する場合に、作成とは独立して VLAN を設定できる VLAN 設定モードがサポートされます。

NetFlow の確認	5.0(2)	NetFlow の IPv4 フローおよび NetFlow のテーブル使用率を表示する NetFlow インスタンスを指定できます。
レイヤ 2 NetFlow	4.2(1)	フレクシブル NetFlow レコード内でレイヤ 2 キーを定義できます。このレコードを使用して、レイヤ 2インターフェイスのフローをキャプチャできます。
NetFlow 中のロールバック	4.1(3)	ロールバック中、ハードウェアでプログラムされているレコードを変更しようとすると、NetFlow のロールバックは失敗します。

第 21 章

EEE の設定

この章は、Cisco NX-OS デバイス上で Energy Efficient Ethernet（EEE）を設定する方法について説明します。

- 機能情報の確認，457 ページ
- EEE について，458 ページ
- 仮想化のサポート，458 ページ
- EEE のライセンス要件，458 ページ
- EEE の前提条件，459 ページ
- 注意事項と制約事項，459 ページ
- デフォルト設定，459 ページ
- EEE の設定，460 ページ
- EEE 設定の確認，461 ページ
- EEE の設定例，463 ページ
- 関連資料，463 ページ
- EEE の機能の履歴，463 ページ

機能情報の確認

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

EEE について

EEE

Energy Efficient Ethernet (EEE) は、アイドル時間にイーサネット ネットワークの消費電力を減らすように設計された IEEE 802.3az の標準です。低電力アイドル（LPI）モードをサポートするデバイスで EEE をイネーブルにできます。このようなデバイスは、低い使用率のときに LPI モードを開始して、電力を節約できます。LPI モードでは、リンクの両端にあるシステムは、特定のサービスをシャット ダウンして、電力を節約できます。EEE は上位層プロトコルおよびアプリケーションに対して透過的であるように、LPIモードに移行したり、LPIモードから移行する必要があるプロトコルを提供します。

EEE LPI のスリープしきい値

EEE LPI スリープしきい値は、アイドル状態を検出した後、インターフェイスがスリープ状態になる前の待ち時間を指定します。アグレッシブまたは非アグレッシブにしきい値を設定できます。

EEE 遅延

EEE Latency はトラフィックに加えられる EEE の遅延を指定します。デフォルト値は 6 マイクロ秒の一定の遅延です。

仮想化のサポート

デフォルトでは、仮想デバイス コンテキスト（VDC）を特別に設定しない限り Cisco NX-OS のデフォルトの VDC が使用されます。VDC の詳細については、『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』を参照してください。

EEE のライセンス要件

製品	ライセンス要件
Cisco NX-OS	EEE にはライセンスは必要ありません。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。NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

EEE の前提条件

EEE には、次の前提条件があります。

- VDC を設定するには、適切なライセンスをインストールする必要があります。設定情報については『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』、ライセンス情報については『*Cisco NX-OS Licensing Guide*』を参照してください。

注意事項と制約事項

注意事項と制約事項：

- F2e（拡張）銅線ポート モジュールのみが EEE をサポートします。F2e ファイバ ポート モジュールは EEE をサポートしません。
- EEE は 10 ギガビット リンク速度でのみサポートされます。1 ギガビット リンク速度ではサポートされません。
- EEE の設定を変更すると、デバイスがレイヤ 1 の自動ネゴシエーションを再起動しなければならないため、インターフェイスがリセットされます。
- 受信パスでデータを受け入れる前により長いウェイク アップ時間を必要とするデバイスのリンク層検出プロトコル（LLDP）をイネーブルにする必要がある場合があります。これにより、デバイスは送信リンク パートナーから拡張システムのウェイク アップ時間についてネゴシエーションできます。

デフォルト設定

EEE パラメータのデフォルト設定を示します。

表 *41*： デフォルトの *EEE* パラメータ

パラメータ	デフォルト
EEE	ディセーブル
EEE LPI のスリープしきい値	非アグレッシブ
EEE Latency	6 マイクロ秒

EEE の設定

この項では、次のトピックについて取り上げます。

- EEE のイネーブル化またはディセーブル化
- EEE LPI スリープしきい値の設定

EEE のイネーブル化またはディセーブル化

EEE 対応リンク パートナーに接続されているインターフェイスの EEE をイネーブルまたはディセーブルにできます。

はじめる前に

正しい VDC 内にいることを確認します。VDC の変更は **switchto vdc** コマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードに切り替えます。
ステップ 2	switch(config)# **interface ethernet** *slot/port*	グローバル コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# [**no**] **power efficient-ethernet auto**	指定されたインターフェイスの EEE をイネーブルまたはディセーブルにします。EEEがイネーブルの場合、デバイスはリンク パートナーに EEE をアドバタイズし、自動ネゴシエートします。
ステップ 4	switch(config-if)# **show interface ethernet***slot/port*	（任意） インターフェイスの EEE の状態を表示します。
ステップ 5	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

EEE LPI スリープしきい値の設定

インターフェイスで EEE LPI スリープしきい値を設定してどの程度アグレッシブにスリープさせるかを指定できます。

はじめる前に

正しい VDC 内にいることを確認します。VDC を変更するには、**switchto vdc** コマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードに切り替えます。
ステップ 2	switch(config)# **interface ethernet** *slot/port*	グローバル コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# [**no**] **power efficient-ethernet sleep threshold aggressive**	インターフェイスの EEE LPI のスリープしきい値をアグレッシブまたは非アグレッシブに設定します。このコマンドの no 形式は非アグレッシブしきい値をイネーブルにします。 • アグレッシブ：アイドル状態が検出されてから 20 マイクロ秒後に LPI モードになるようにデバイスを設定します。 • 非アグレッシブ：アイドル状態が検出されてから 600 マイクロ秒後に LPI モードになるようにデバイスを設定します。
ステップ 4	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

EEE 設定の確認

EEE の設定を表示するには、次のいずれかの作業を行います。

表 *42*：イーサネット インターフェイス上の *EEE*

コマンド	目的
show environment power detail	現在の電力使用状況を表示します。
show interface ethernet*slot/port*	インターフェイスの EEE の状態を表示します。オプションは次のとおりです。 • N/A：インターフェイスは EEE に対応できません。 • Disabled：EEE はこのインターフェイスでディセーブルです。 • Disagreed：リンク パートナーとの EEE 自動ネゴシエートが失敗しました。 • Operational：EEE がこのインターフェイスでイネーブルになっており、稼動しています。
show interface ethernet*slot/port***capabilities**	インターフェイスが EEE に対応しているかどうかを表示します。
show interface ethernet*slot/port***counters detailed**	インターフェイスで次の EEE の統計情報を表示します。 • Tx LPI usecs：転送リンク パートナーが LPI モードを終了した後にデータの転送を開始するまでに待つ期間（マイクロ秒単位）。 • Rx LPI usecs：受信リンク パートナーが LPI モード終了後にデータ転送までに転送リンク パートナーが待つことを受信リンク パートナーが要求する期間（マイクロ秒単位）。 • Tx LPI requests：転送リンク パートナーが LPI モードを開始するリクエストを作成する回数。 • Rx LPI indications： 転送リンク パートナーが LPI モードを開始したことを受信リンク パートナーが検出した回数。

EEE の設定例

次に、イーサネット インターフェイス上で EEE をイネーブルにする例を示します。

```
switch# config t
switch(config)# interface ethernet 7/1
switch(config-if)# power efficient-ethernet auto
switch(config-if)# power efficient-ethernet sleep threshold aggressive
switch(config-if)# show interface ethernet 7/1
Ethernet7/1 is up
   EEE(efficient-ethernet): Operational
```

関連資料

関連項目	マニュアル タイトル
EEE CLI コマンド	『*Cisco Nexus 7000 Series NX-OS System Management Command Reference*』
VDC	『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』

EEE の機能の履歴

次の表に、このマニュアルの新機能および変更された機能を要約し、各機能がサポートされているリリースを示します。ご使用のソフトウェア リリースで、本書で説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。

表 *43* : *EEE* の機能の履歴

機能名	リリース	機能情報
EEE	6.1(2)	この機能が導入されました。

第 22 章

GIRの設定（Cisco NX-OS Release 7.3(0)D1(1)）

この章は、次の項で構成されています。

- GIR について，465 ページ
- GIR の注意事項と制約事項，471 ページ
- カスタム メンテナンス モードプロファイルおよびカスタム通常モードプロファイルの設定，472 ページ
- スナップショットの作成，473 ページ
- スナップショットへの show コマンドの追加，474 ページ
- スナップショット セクションのダンプ，476 ページ
- メンテナンス モードの開始，477 ページ
- 通常モードへの復帰，481 ページ
- メンテナンス プロファイルの削除，482 ページ
- GIR の設定例，482 ページ
- GIR の確認，488 ページ
- GIR の機能の履歴，491 ページ

GIR について

グレースフル挿入と削除（GIR）を使用して、スイッチをメンテナンス モードにしてデバッグやアップグレードを実行することができます。スイッチのメンテナンスが完了したら、スイッチを通常モードに戻すことができます。

スイッチをメンテナンス モードにすると、すべてのプロトコルがネットワークから分離されます。通常モードに戻すと、すべてのプロトコルが起動状態に戻ります。

Cisco NX-OS 7.2(0)D1(1) リリースでは、GIR のデフォルト モードは **shutdown** です。スイッチをメンテナンス モードにすると、すべてのプロトコルはグレースフルに（正常に）ダウン状態になり、すべての物理ポートがシャットダウンします。通常モードに戻すと、すべてのプロトコルおよびポートが起動状態に戻ります。次のプロトコルがサポートされています。

- Border Gateway Protocol（BGP）
- BGPv6
- Enhanced Interior Gateway Routing Protocol（EIGRP）
- EIGRPv6
- Intermediate System-to-Intermediate System（ISIS）
- ISISv6
- Open Shortest Path First（OSPF）
- OSPFv3
- RIP

以下もサポートされます。

- 仮想ポート チャネル（vPC）および vPC+
- インターフェイス
- FabricPath

Cisco NX-OS Release 7.3(0)D1(1) 以降では、GIR のデフォルト モードは **isolate** です。すべてのイネーブルのプロトコルをメンテナンス モードにするには、**system mode maintenance** コマンドを使用します。スイッチでは、プロトコルをネットワークから分離するために、**isolate** コマンドを使用します。これにより、スイッチはネットワークから分離されますが、シャットダウンはされません。スイッチがネットワークから分離されると、スイッチではルーティング プロトコルが実行されて、ピア スイッチとのネイバーシップが維持されます。**isolate** コマンドはプロトコル インスタンスに適用され、次のプロトコルに適用できます。

- Border Gateway Protocol（BGP）
- BGPv6
- Enhanced Interior Gateway Routing Protocol（EIGRP）
- EIGRPv6
- Intermediate System-to-Intermediate System（ISIS）
- ISISv6
- Open Shortest Path First（OSPF）
- OSPFv3
- FabricPath（スパイン スイッチにのみ適用可能）

（注）

- Cisco NX-OS Release 7.2(0)D1(1) と同様に、**system mode maintenance shutdown** を使用して GIR の **shutdown** モードを使用することができます。
- カスタム プロファイルが設定され、メンテナンス モードをサポートしない他の Cisco NX-OS リリースに対する Cisco NX-OS Release 7.3(1)D1(1) イメージを実行しているスイッチをコールドブートする場合、write-erase リロード後に同じコンフィギュレーション ファイルを使用することはできません。
- 通常モードでは、プロトコルの処理は、プロトコルがメンテナンス モードで処理される順序と逆の順序で行われます。同様に、メンテナンス モードでは、プロトコルの処理は、プロトコルが通常モードで処理される順序と逆の順序で行われます。

メンテナンス プロファイル

メンテナンス プロファイルには、グレースフル削除またはグレースフル挿入時に順次適用される一連のコマンドが含まれています。

デフォルトでは、すべての有効なプロトコルは、グレースフル削除中に分離され、グレースフル挿入時に復元されます。プロトコルは、定義済みの順序で分離および復元されます。

スイッチは、次のプロファイルをサポートしています。

- メンテナンス モード プロファイル：スイッチがメンテナンス モードになったときに、グレースフル削除中に実行されるすべてのコマンドが含まれます。
- 通常モード プロファイル：スイッチが通常モードに戻ったときに、グレースフル挿入中に実行されるすべてのコマンドが含まれます。

システム生成プロファイル

特定の設定コマンドを使用して、システムによりメンテナンス モードまたは通常モードのプロファイルが生成されるようにできます。**system mode maintenance** コマンドによりメンテナンス モード プロファイル、**no system mode maintenance** コマンドにより通常モード プロファイルがシステムにより生成されます。

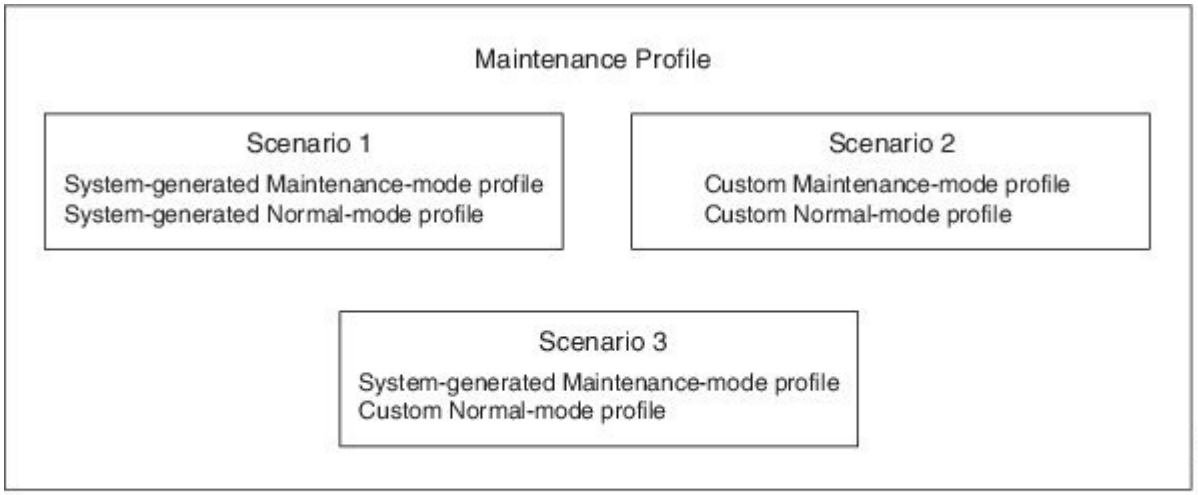
カスタム プロファイル

グレースフル削除またはグレースフル挿入時に適用できる設定コマンドを使用して、カスタム メンテナンス モード プロファイルまたは通常モード プロファイルを作成し、プロトコルを個々に分離、シャットダウン、または復元する（または追加の設定を実行する）ことができます。システム生成プロファイルが必要な設定を提供しない場合や、既存のシステム生成プロファイルまたはカスタム プロファイルに実装固有の追加の機能を含めるよう強化する必要がある場合、カスタム プロファイルを使用できます。**configure maintenance profile maintenance-mode** コマンドを使用して必要なコマンドを含むカスタム メンテナンス モード プロファイルを設定するか、または

configure maintenance profile normal-mode コマンドを使用して必要なコマンドを含むカスタム通常モード プロファイルを設定します。

システム生成プロファイルはカスタム プロファイルを上書きしますが、逆もまた起こります。システムに同時に設定できるのは、システム生成メンテナンス モード プロファイルかカスタム メンテナンスモードプロファイルのいずれかになります。同様に、システムに同時に設定できるのは、システム生成通常モードプロファイルかカスタム通常モードプロファイルのいずれかになります。シナリオは次の図に示すとおりです。

図 7: メンテナンス プロファイルのシナリオ



（注） シナリオ 1 または 2 の使用を推奨します。

計画外メンテナンス

重大な障害が原因でスイッチがリロードしたら、スイッチを計画外メンテナンス モードにすることができます。単一のスーパーバイザ搭載のスイッチでは、**system mode maintenance on-reload reset-reason** コマンドを使用してリセット理由 CLI を設定し、スイッチが重大な障害が原因でリロードした後にメンテナンスモードに入ることができるようにします。デュアル スーパーバイザ搭載のスイッチでは、スイッチに重大な障害が発生すると SUP スイッチオーバーが生じ、スイッチはメンテナンスモードに入りません。スイッチが計画外メンテナンスモードに入ると、スタートアップ コンフィギュレーションに存在するメンテナンスモードプロファイルが適用されます。スイッチが計画外メンテナンスモードに入る際にスタートアップコンフィギュレーションにメンテナンス モード プロファイルが存在しない場合、システム生成メンテナンス モード プロファイルが作成されます。

メンテナンス モード タイマー

スイッチを指定した期間（分）メンテナンスモードに維持するには、メンテナンスモードに入る前に **system mode maintenance timeout** コマンドを使用します。このコマンドは、スイッチがメンテナンスモードのときに、スイッチがメンテナンスモードである期間（分）を変更するのにも使用できます。その場合、タイマーは新しいタイマー値によるインスタントから再開されます。設定された時間が経過すると、**no system mode maintenance mode** を使用しなくてもスイッチは自動的に通常モードに戻ります。タイマーを無効にするには、**no system mode maintenance timeout** コマンドを使用します。

Snapshot

snapshot コマンドを使用して、選択した機能の実行状態をキャプチャし、永続ストレージ メディアに実行状態を保存します。

スナップショットを使用して、メンテナンス モードになる前と通常モードに戻った後に、スイッチの状態を比較することができます。スナップショット プロセスは、次の 3 つの部分で構成されます。

- 事前に選択したスイッチの一部機能の状態のスナップショットを作成し、永続ストレージ メディアに保存する。
- さまざまな時間間隔で取得したスナップショットを一覧にして、管理する。
- スナップショットを比較し、各機能の概要と詳細を表示する。

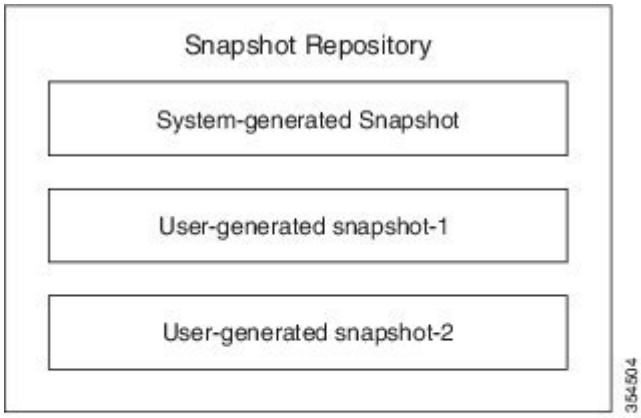
スナップショットには、次の 2 つのタイプがあります。

- システム生成スナップショット：**[no] system mode maintenance** コマンドを使用すると、システムにより生成されます。システムは、システムがメンテナンス モードに入る直前に before_maintenance スナップショットを作成します。システムは、システムが通常モードに入る直前に after_maintenance スナップショットを作成します。**[no] system mode maintenance** コマンドを使用すると、システムは古いスナップショットを上書きします。システム生成スナップショットを削除するには、**snapshot delete** {**all** | *snapshot-name}* コマンドを使用します。
- ユーザ生成スナップショット：ユーザ生成スナップショットを作成するには、**snapshot create** *name description* コマンドを使用します。ユーザ生成スナップショットを削除するには、**snapshot delete** {**all** | *snapshot-name}* コマンドを使用します。

特定のシナリオでは、ハードウェア プログラミングが実行されている場合に、システム生成の after_maintenance スナップショットが作成される場合があります。このような場合は、システムがハードウェア プログラミングを完了して安定な状態になったら、ユーザ生成スナップショットを作成することをお勧めします。その後、新しい after_maintenance スナップショットを before_maintenance スナップショットと比較することができます。

システム生成およびユーザ生成スナップショットは、スナップショット リポジトリに保存されます。

図 *8*：スナップショット リポジトリ



次の表に、対応する show コマンドを含むスナップショット セクションを示します。

セクションの名前	対応する **show** コマンド
bgp セッション	show bgp sessions vrf all
eigrp	show ip eigrp topology summary
eigrpv6	show ipv6 eigrp topology summary
interface	show interface
ospf	show ip ospf vrf all
ospfv3	show ipv6 ospfv3 vrf all
isis	show isis database detail vrf all
rip	show ip rip vrf all
route-summary	show ip route summary vrf all
routev6-summary	show ipv6 route summary vrf all
vpc	show vpc

FIB 保留の抑制

転送情報ベース（FIB）保留の抑制機能は、ボーダー ゲートウェイ プロトコルのルーティング情報ベース（BGP-RIB）および拡張内部ゲートウェイ ルーティング プロトコルのルーティング情報ベース（EIGRP-RIB）のフィードバック メカニズムを使用して、ネットワーク内の尚早なルートアドバタイズメントと後続のパケット損失を防ぎます。このメカニズムはデフォルトでイネーブルであり、これにより、ルートがネイバーにアドバタイズされる前にローカルに組み込まれるようになります。

BGP および EIGRP は RIB からのフィードバックを待ちます。このフィードバックには、EIGRP または BGP によって RIB に組み込まれたルートが、EIGRP または BGP がネイバーにアップデートを送信する前に転送情報ベース（FIB）に組み込まれたことが示されています。EIGRP または BGP がアップデートを送信するのは、FIB が組み込んだバージョン以下のバージョンのルートだけです。この選択的なアップデートにより、EIGRP または BGP は尚早なアップデートを送信しなくなり、その結果、スイッチのリロード後、ライン カードのリロード後、またはスイッチがメンテナンス モードから通常モードに移行するときにデータ プレーンがプログラムされる前であっても、トラフィックが収集されます。

GIR の注意事項と制約事項

- 自動またはシステム生成プロファイルでサポートされないカスタムのトポロジおよびプロトコルには、カスタム メンテナンス プロファイルを使用する必要があります。
- メンテナンスを開始する前に、スイッチをメンテナンス モードにした後にスイッチがデータ トラフィックを収集していないことを確認してください。カウンタと統計情報を使用して、スイッチにデータ トラフィックがないことを確認できます。
- カスタム プロファイルを使用する場合にカスタム プロファイルがシステム生成プロファイルによって上書きされないようにするには、**system mode maintenance always-use-custom-profile** コマンドを使用します。
- デュアル スーパーバイザ システムでは、スナップショット情報はスタンバイ スーパーバイザに自動的にコピーされません。
- 特定のトポロジと設定では、GIR により、アプリケーション トラフィックの損失がゼロにならない場合があります。
- Cisco NX-OS Release 7.3(0)D1(1) 以降では **configure profile [maintenance-mode | normal-mode] type admin** コマンドを使用しないことを推奨します。**configure maintenance profile [maintenance-mode | normal-mode]** コマンドの使用を強く推奨します。
- メンテナンス モードでは、インサービス ソフトウェア アップグレード（ISSU）、インサービス ソフトウェア ダウングレード（ISSD）は実行できません。

カスタム メンテナンス モード プロファイルおよびカスタム通常モード プロファイルの設定

グレースフル削除またはグレースフル挿入時に適用できる設定コマンドを使用して、メンテナンス モード プロファイルまたは通常モード プロファイルを作成できます。カスタム メンテナンス モード プロファイルおよびカスタム通常モード プロファイルを設定したら、**system mode maintenance always-use-custom-profile** コマンドを使用して、メンテナンス モードの動作中は常にカスタム プロファイルが使用されるようにすることをお勧めします。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure maintenance profile** [**maintenance-mode** | **normal-mode**]	メンテナンス モード プロファイルまたは通常モード プロファイルの設定セッションを開始します。 （注） 設定しているプロトコルに応じて、プロトコルを停止する適切なコマンドを入力します。
ステップ 2	switch# **end**	メンテナンス モード プロファイルを閉じます。

次に、カスタム メンテナンス モード プロファイルを作成する例を示します。

```
switch# configure maintenance profile maintenance-mode
Please configure 'system mode maintenance always-use-custom-profile' if you want to use
custom profile always for maintenance mode.
Enter configuration commands, one per line. End with CNTL/Z.
switch(config-mm-profile)# router bgp 100
switch(config-mm-profile-router)# isolate
switch(config-mm-profile-router)# exit
switch(config-mm-profile)# sleep instance 1 10
switch(config-mm-profile)# interface ethernet 1/1
switch(config-mm-profile-if-verify)# shutdown
switch(config-mm-profile-if-verify)# end
Exit maintenance profile mode.
```

次に、カスタム通常モード プロファイルを作成する例を示します。

```
switch# configure maintenance profile normal-mode
Please configure 'system mode maintenance always-use-custom-profile' if you want to use
custom profile always for maintenance mode.
Enter configuration commands, one per line. End with CNTL/Z.
switch(config-mm-profile)# interface ethernet 1/1
switch(config-mm-profile-if-verify)# no shutdown
switch(config-mm-profile-if-verify)# exit
switch(config-mm-profile)# sleep instance 1 20
switch(config-mm-profile)# router bgp 100
switch(config-mm-profile-router)# no isolate
switch(config-mm-profile-router)# end
```

```
Exit maintenance profile mode.

switch# show maintenance profile
[Normal Mode]
interface Ethernet1/1
no shutdown
sleep instance 1 20
router bgp 100
no isolate
[Maintenance Mode]
router bgp 100
isolate
sleep instance 1 20
interface Ethernet1/1
shutdown
```

スナップショットの作成

選択した機能の実行状態のスナップショットを作成できます。スナップショットを作成する場合、定義済みの一連の show コマンドが実行され、出力が保存されます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **snapshot create***name description*	スナップショットを作成します。*name* 変数は最大 64 文字です。*description* 変数は最大 256 文字です。 すべてのスナップショットまたは特定のスナップショットを削除するには、**snapshot delete** {**all** | *snapshot-name*} コマンドを使用します。
ステップ 2	switch# **show snapshots**	（任意） スイッチ上に存在するスナップショットを表示します。
ステップ 3	switch# **show snapshots compare***snapshot-name-1 snapshot-name-2* [**summary**]	（任意） 2 つのスナップショットの比較を表示します。**summary** キーワードは、2 つのスナップショット間の全体的な変更を確認するのに十分な情報のみ表示します。

次に、スナップショットを作成する例を示します。

```
switch# snapshot create before_maint taken before maint
Executing 'show interface'... Done
Executing 'show ip route summary vrf all'... Done
Executing 'show ipv6 route summary vrf all'... Done
Executing 'show bgp sessions vrf all'... Done
Executing 'show ip eigrp topology summary'... Done
Executing 'show ipv6 eigrp topology summary'... Done
Executing 'show vpc'... Done
Executing 'show ip ospf vrf all'... Done
Feature 'ospfv3' not enabled, skipping...
```

```
Executing 'show isis database detail vrf all'... Done
Executing 'show ip rip vrf all'... Done
Executing user-specified 'show ip route detail vrf all'... Done
Snapshot 'before_maint' created
```

次に、スイッチ上に存在するスナップショットを表示する方法を示します。

```
switch# show snapshots
Snapshot Name           Time                            Description
--------------------------------------------------------------------------------
before_maint            Wed Oct 14 10:56:50 2015        taken before maint
```

次に、2 つのスナップショット間の比較を表示します。

```
switch# show snapshots compare before_maintenance after_maintenance summary
================================================================================
Feature changed                        before_maintenance after_maintenance
================================================================================
basic summary
   # of interfaces                              50               50
   # of vlans                                   0                0
   # of ipv4 routes  vrf default                13               13
   # of ipv4 paths   vrf default                13               13
   # of ipv4 routes  vrf management             14               14
   # of ipv4 paths   vrf management             14               14
   # of ipv6 routes  vrf default                3                3
   # of ipv6 paths   vrf default                3                3

interfaces
   # of eth interfaces                          48               48
   # of eth interfaces up                       1                1
   # of eth interfaces down                     47               47
   # of eth interfaces other                    0                0

   # of vlan interfaces                         0                0
   # of vlan interfaces up                      0                0
   # of vlan interfaces down                    0                0
   # of vlan interfaces other                   0                0
```

次に、スナップショットを削除する例を示します。

```
switch# snapshot delete before_maint
switch# show snapshots
Snapshot Name           Time                            Description
--------------------------------------------------------------------------------
```

スナップショットへの show コマンドの追加

スナップショットでキャプチャされる追加の **show** コマンドを指定できます。それらの **show** コマンドは、ユーザ指定のスナップショット セクションで定義されます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **snapshot section add***section "show-command" row-id*	ユーザ指定のセクションをスナップショットに追加します。*section* は、**show** コマンドの出力に名前を付けるために使用されます。任意の単語を使用して、セクションに名前を付けることができます。

	コマンドまたはアクション	目的
	element-key1 [*element-key2*]	**show** コマンドは、引用符で囲む必要があります。**show** 以外のコマンドは拒否されます。 *row-id* 引数では、**show** コマンドの XML 出力の各行エントリのタグを指定します。*element-key1* および *element-key2* 引数では、行エントリ間を区別するために使用されるタグを指定します。ほとんどの場合、行エントリ間を区別するために指定する必要があるのは *element-key1* 引数だけです。 （注） スナップショットからユーザ指定のセクションを削除するには、**snapshot section delete***section* section コマンドを使用します。
ステップ 2	switch# **show snapshots sections**	（任意） ユーザ指定のスナップショット セクションを表示します。

次の例では、スナップショットに **show ip route detail vrf all** コマンドを追加する方法を示します。

```
switch# snapshot section add v4route "show ip route detail vrf all" ROW_prefix ipprefix
switch# show snapshots sections
user-specified snapshot sections
--------------------------------
[v4route]
show command: show ip route detail vrf all
row id: ROW_prefix
key1: ipprefix
key2: -
```

次の例では、スナップショットに **show ipv6 route detail vrf all** コマンドを追加する方法を示します。

```
switch# snapshot section add routev6 "show ipv6 route detail vrf all" ROW_prefix ipprefix
added section "routev6"

switch# show snapshots sections
user-specified snapshot sections
--------------------------------
[routev6]
show command: show ipv6 route detail vrf all
row id: ROW_prefix
key1: ipprefix
key2: -
```

次に、ユーザ指定のスナップショット セクションを削除する例を示します。

```
switch# snapshot section delete v4route
deleted section ”v4route"

switch# show snapshots sections
user-specified snapshot sections
--------------------------------
none
```

次に、**show ip route detail vrf all** コマンドの XML 出力例を表示します。

```
switch(config)# show ip route detail vrf all | xml
<?xml version="1.0" encoding="ISO-8859-1"?>
<nf:rpc-reply xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns="http://w
ww.cisco.com/nxos:7.3.0.D1.1.:urib">
 <nf:data>
  <show>
   <ip>
       <__readonly__>
         <TABLE_vrf>
          <ROW_vrf>
           <vrf-name-out>default</vrf-name-out>
           <TABLE_addrf>
            <ROW_addrf>
             <addrf>ipv4</addrf>
             <TABLE_prefix>
              <ROW_prefix>
               <ipprefix>0.0.0.0/32</ipprefix>
               <ucast-nhops>1</ucast-nhops>
               <mcast-nhops>0</mcast-nhops>
               <attached>false</attached>
              … <snip>
              </ROW_prefix>
```

スナップショット セクションのダンプ

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **show snapshots dump***snapshot-name*	生成されたスナップショットのさまざまなセクションの内容を表示します。

次に、生成されたスナップショットのさまざまなセクションの内容をダンプする例を示します。

```
switch# show snapshots dump new
File:  interface.xml        Snapshot:  new
================================================================================
<?xml version="1.0" encoding="ISO-8859-1"?>
<nf:rpc-reply xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns="http://w
ww.cisco.com/nxos:7.3.0.D1.1.:if_manager">
 <nf:data>
  <show>
   <interface>
    <__readonly__>
     <TABLE_interface>
      <ROW_interface>
       <interface>mgmt0</interface>
       <state>up</state>
       <admin_state>up</admin_state>
       <eth_hw_desc>GigabitEthernet</eth_hw_desc>
       <eth_hw_addr>5cfc.666d.3b34</eth_hw_addr>
       <eth_bia_addr>5cfc.666d.3b34</eth_bia_addr>
       <eth_ip_addr>5.24.100.101</eth_ip_addr>
       <eth_ip_mask>16</eth_ip_mask>
       <eth_ip_prefix>5.24.0.0</eth_ip_prefix>
       <eth_mtu>1500</eth_mtu>
    … <snip> …
```

メンテナンス モードの開始

system mode maintenance コマンドを使用してシステムに生成を任せるのでなく、ユーザが独自のプロファイルを作成するには、「カスタム メンテナンス モード プロファイルおよびカスタム通常モード プロファイルの設定」の項を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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	switch(config)# **system mode maintenance** [**shutdown** | **timeout***value* | **on-reload reset-reason***reason* | **dont-generate-profile** | **always-use-custom-profile**]	すべての有効なプロトコルをメンテナンス モードにします（**isolate** コマンドを使用）。 **dont-generate-profile** および **shutdown** オプションを使用して、スイッチをメンテナンス モードにします。 • **dont-generate-profile**：有効なプロトコルの動的な検索が回避され、メンテナンス モード プロファイルに設定されているコマンドが実行されます。システムによりカスタム メンテナンス モード プロファイルのコマンドが実行されるようにするには、このオプションを使用します。 • **shutdown**：すべてのプロトコルおよび管理インターフェイスを除くインターフェイスをシャットダウンします（**shutdown** コマンドを使用）。このオプションを指定すると中断が発生しますが、デフォルト（**isolate** コマンドを使用）の場合、中断は発生しません。 メンテナンス モード パラメータを設定するには、**on-reload reset-reason**、**timeout** および **always-use-custom-profile** オプションを使用します。これによってスイッチがメンテナンス モードになることはありません。 • **timeout***value*：指定した分数の間、スイッチをメンテナンス モードのままにします。範囲は 5 ～ 65535 です。タイムアウト値は、少なくとも 60 分に設定することを推奨します。設定した時間が経過すると、スイッチは自動的に通常モードに戻ります。**no system mode maintenance timeout** コマンドは、タイマーを無効にします。 • **on-reload reset-reason***reason*：指定されているシステム クラッシュが発生した場合、スイッチは自動的にメンテナンス モードで起動します。**no system mode maintenance**

	コマンドまたはアクション	目的
		on-reload reset-reason コマンドを使用すると、システム クラッシュ時にスイッチがメンテナンス モードで起動するのを回避できます。メンテナンス モードのリセット理由は次のとおりです。 • HW_ERROR：ハードウェア エラー • SVC_FAILURE：重大なサービス障害 • KERN_FAILURE：カーネル パニック • WDOG_TIMEOUT：ウォッチドッグ タイムアウト • FATAL_ERROR：致命的なエラー • MANUAL_RELOAD：手動リロード • MAINTENANCE：リロード前にスイッチがすでにメンテナンス モードである場合に、メンテナンス モードでスイッチをリロードします。 • MATCH_ANY：上記のいずれかの理由 • ANY_OTHER：上記で指定されていないリロードの理由。 続行を促すプロンプトが表示されます。続行する場合は y、プロセスを終了する場合は n を入力します。 （注） リセット理由を設定してスタートアップ コンフィギュレーションに保存することをお勧めします。これにより、どのような理由でも、スイッチがリロードしたら、スイッチをメンテナンス モードにすることができます。 • **always-use-custom-profile**：既存のカスタム メンテナンス モードプロファイルを適用し、自動生成メンテナンス モードプロファイルが作成されるのを防ぐ場合、このオプションを使用します。このオプションにより、**system mode maintenance** コマンドで指定されていない場合にも、dont-generate-profile オプションが適用されます。このオプションが使用されている場合は、shutdown オプションを使用できません。

	コマンドまたはアクション	目的
ステップ 3	switch# **show system mode**	（任意） 現在のシステム モードを表示します。また、このコマンドは、スイッチがメンテナンス モードの場合に、メンテナンス モード タイマーの現在の状態を表示します。

次に、**system mode maintenance** コマンドを使用してすべてのプロトコルをメンテナンス モードにする例を示します。

```
switch# configure terminal
switch(config)# system mode maintenance
Following configuration will be applied:

router bgp 100
  isolate
router ospf 100
  isolate
router isis 100
  isolate

Do you want to continue (y/n)? [no] y

Generating a snapshot before going into maintenance mode

Starting to apply commands...

Applying : router bgp 100
Applying :   isolate
Applying : router ospf 100
Applying :   isolate
Applying : router isis 100
Applying :   isolate

Maintenance mode operation successful.
```

次に、スイッチのすべてのプロトコルおよびインターフェイスをシャットダウンする例を示します。

```
switch# configure terminal
switch(config)# system mode maintenance shutdown
Following configuration will be applied:

router bgp 64581
  shutdown
router eigrp p2
  shutdown
  address-family ipv6 unicast
    shutdown
router eigrp 0
  shutdown
  address-family ipv6 unicast
    shutdown
router ospf 200
  shutdown
router isis 70
  shutdown
vpc domain 2
  shutdown
system interface shutdown

NOTE: 'system interface shutdown' will shutdown all interfaces excluding mgmt 0
```

```
Do you want to continue (yes/no)? [no] yes

Generating a snapshot before going into maintenance mode

Starting to apply commands...

Applying : router bgp 64581
Applying :   shutdown
Applying : router eigrp p2
Applying :   shutdown
Applying :   address-family ipv6 unicast
Applying :     shutdown
Applying : router eigrp 0
Applying :   shutdown
Applying :   address-family ipv6 unicast
Applying :     shutdown
Applying : router ospf 200
Applying :   shutdown
Applying : router isis 70
Applying :   shutdown
Applying : vpc domain 2
Applying :   shutdown2016 Jan 15 11:10:36.080386 CP-BL26-N7K-1A %$ VDC-1 %$
%VPC-2-VPC_SHUTDOWN: vPC shutdown status is ON

Applying : system interface shutdown

Maintenance mode operation successful.
switch(config)# 2016 Jan 15 11:10:42.057678 CP-BL26-N7K-1A %$ VDC-1 %$ %MMODE-2-MODE_CHANGED:
 System changed to "maintenance" mode.
2016 Jan 15 11:10:42.058167 CP-BL26-N7K-1A %$ VDC-1 %$ %MMODE-2-MODE_CHANGE_WARN: System
will be moved to "normal" mode in 5 minutes
```

次に、スイッチを指定の期間（分）メンテナンス モードに保持する例を示します。

```
switch# configure terminal
switch (config)# system mode maintenance timeout 25

switch# show system mode
System Mode: Maintenance
Maintenance Mode Timer: 24 minutes 55 seconds remaining
```

次に、致命的なエラーが発生した場合に、スイッチを自動的にメンテナンス モードで起動する例を示します。

```
switch# configure terminal
switch(config)# system mode maintenance on-reload reset-reason fatal_error
```

次に、以前に作成したメンテナンス モード プロファイルを使用してスイッチをメンテナンス モードにする例を示します。

```
switch# configure terminal
switch(config)# system mode maintenance dont-generate-profile

Following configuration will be applied:

router bgp 100
  isolate
sleep instance 1 10
interface Ethernet1/1
  shutdown

Do you want to continue (y/n)? [no] y

Generating a snapshot before going into maintenance mode

Starting to apply commands...

Applying : router bgp 100
Applying :   isolate
```

```
Applying : sleep instance 1 10
Applying : interface Ethernet1/1
Applying :   shutdown

Maintenance mode operation successful.
```

次に、既存のカスタム メンテナンス モード プロファイルを適用し、自動生成メンテナンス モード プロファイルが作成されるのを防ぐ例を示します。

```
switch# configure terminal
switch(config)# system mode maintenance always-use-custom-profile
```

通常モードへの復帰

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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	switch# **no system mode maintenance** [**dont-generate-profile**]	以前に作成した通常モード プロファイル ファイルを実行するか、または動的に通常モード プロファイル ファイルを作成します。**dont-generate-profile** オプションは、通常モード メンテナンス プロファイルの作成を抑制し、既存の通常モード メンテナンス プロファイルの再利用も防ぎます。 続行を促すプロンプトが表示されます。続行する場合は **y**、プロセスを終了する場合は **n** を入力します。 （注） 大規模な設定の場合、インターフェイスは一定の期間の後に起動します。

次に、メンテナンス モードから通常モードに戻す例を示します。

```
switch# configure terminal
switch(config)# no system mode maintenance
Following configuration will be applied:

interface Ethernet1/1
  no shutdown
sleep instance 1 20
router bgp 100
  no isolate

Do you want to continue (y/n)? [no] yes

Starting to apply commands...

Applying : interface Ethernet1/1
Applying :   no shutdown
Applying : sleep instance 1 20
Applying : router bgp 100
Applying :   no isolate
```

```
Maintenance mode operation successful.

Generating Current Snapshot

Please use 'show snapshots compare before_maintenance after_maintenance' to check the health
 of the system
switch(config)#


switch(config)# show system mode
System Mode: Normal
```

メンテナンス プロファイルの削除

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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	switch# **no configure maintenance profile** {**normal-mode** | **maintenance-mode**}	通常モードまたはメンテナンス モード プロファイルを削除します。

次に、メンテナンス プロファイルを削除する例を示します。

```
switch# configure terminal
switch(config)# no configure maintenance profile maintenance-mode
```

GIR の設定例

次に、カスタム メンテナンス モード プロファイルを作成する例を示します。

```
switch# configure maintenance profile maintenance-mode
Please configure 'system mode maintenance always-use-custom-profile' if you want to use
custom
profile always for maintenance mode.
Enter configuration commands, one per line. End with CNTL/Z.
switch(config-mm-profile)# router bgp 100
switch(config-mm-profile-router)# isolate
switch(config-mm-profile-router)# exit
switch(config-mm-profile)# sleep instance 1 10
switch(config-mm-profile)# interface ethernet 1/1
switch(config-mm-profile-if-verify)# shutdown
switch(config-mm-profile-if-verify)# end
Exit maintenance profile mode.
```

次に、カスタム通常モード プロファイルを作成する例を示します。

```
switch# configure maintenance profile normal-mode
Please configure 'system mode maintenance always-use-custom-profile' if you want to use
custom
profile always for maintenance mode.
Enter configuration commands, one per line. End with CNTL/Z.
switch(config-mm-profile)# interface ethernet 1/1
```

```
switch(config-mm-profile-if-verify)# no shutdown
switch(config-mm-profile-if-verify)# exit
switch(config-mm-profile)# sleep instance 1 20
switch(config-mm-profile)# router bgp 100
switch(config-mm-profile-router)# no isolate
switch(config-mm-profile-router)# end
Exit maintenance profile mode.
```

次に、IPv6 プロトコルで、カスタム メンテナンス モード プロファイルおよびカスタム通常モード プロファイルを作成する例を示します。

```
switch# configure terminal
switch(config)# configure maintenance profile maintenance-mode
Please configure 'system mode maintenance always-use-custom-profile' if you want to use
custom
profile always for maintenance mode.
switch(config-mm-profile)# router ospfv3 ospf_ipv6
switch(config-mm-profile-router)# shutdown
switch(config-mm-profile-router)# exit
switch(config-mm-profile)# router eigrp 660
switch(config-mm-profile-router)# address-family ipv6 unicast
switch(config-mm-profile-router-af)# shutdown
switch(config-mm-profile-router-af)# exit
switch(config-mm-profile)# router isis isp
switch(config-mm-profile-router)# set-overload-bit always
switch(config-mm-profile-router)# address-family ipv6 unicast
switch(config-mm-profile-router-af)# shutdown
switch(config-mm-profile-router-af)# exit


switch# configure terminal
switch(config)# configure maintenance profile normal-mode
Please configure 'system mode maintenance always-use-custom-profile' if you want to use
custom
profile always for maintenance mode.
switch(config-mm-profile)# router isis isp
switch(config-mm-profile-router)# no set-overload-bit always
switch(config-mm-profile-router)# address-family ipv6 unicast
switch(config-mm-profile-router-af)# no shutdown
switch(config-mm-profile-router-af)# exit
switch(config-mm-profile)# router eigrp 660
switch(config-mm-profile-router)# address-family ipv6 unicast
switch(config-mm-profile-router-af)# no shutdown
switch(config-mm-profile-router-af)# exit
switch(config-mm-profile)# router ospfv3 ospf_ipv6
switch(config-mm-profile-router)# no shutdown
switch(config-mm-profile-router)# exit


switch# show maintenance profile
[Normal mode]
router isis isp
  no set-overload-bit always
  address-family ipv6 unicast
   no shutdown
router eigrp 660
  address-family ipv6 unicast
   no shutdown
router ospfv3 ospf_ipv6
   no shutdown
[Maintenance Mode]
router ospfv3 ospf_ipv6
  shutdown
router eigrp 660
  address-family ipv6 unicast
   shutdown
router isis isp
  set-overload-bit always
  address-family ipv6 unicast
   shutdown
```

次に、VPC で、カスタム メンテナンス モード プロファイルおよびカスタム通常モード プロファイルを作成する例を示します。

```
switch# configure terminal
switch(config)# configure maintenance profile maintenance-mode
switch(config-mm-profile)# router bgp 100
switch(config-mm-profile-router)# isolate
switch(config-mm-profile-router)# exit
switch(config-mm-profile)# interface port channel 5
switch(config-mm-profile-if-verify)# vpc orphan port suspend
switch(config-mm-profile-if-verify)# exit
switch(config-mm-profile)# interface port channel 6
switch(config-mm-profile-if-verify)# vpc orphan port
suspend switch(config-mm-profile-if-verify)# exit
switch(config-mm-profile)# sleep instance 1 5
switch(config-mm-profile)# vpc domain 1
switch(config-mm-profile-vpc-domain)# shutdown


switch# configure terminal
switch(config)# configure maintenance profile normal-mode
switch(config-mm-profile)# vpc domain 1
switch(config-mm-profile-vpc-domain)# no shutdown
switch(config-mm-profile-vpc-domain)# exit
switch(config-mm-profile)# sleep instance 1 60
switch(config-mm-profile)# interface port channel 5
switch(config-mm-profile-if-verify)# no vpc orphan port suspend
switch(config-mm-profile-if-verify)# exit
switch(config-mm-profile)# interface port channel 6
switch(config-mm-profile-if-verify)# no vpc orphan port suspend
switch(config-mm-profile-if-verify)# exit
switch(config-mm-profile)# router bgp 100
switch(config-mm-profile-router)# no isolate


switch# show maintenance profile
[Normal Mode]
vpc domain 1
  no shutdown
sleep instance 1 60
interface port-channel 5
  no vpc orphan-port suspend
interface port-channel 6
  no vpc orphan-port suspend router
bgp 100
  no isolate

[Maintenance Mode]
router bgp 100
  isolate
interface port-channel 5 vpc
  orphan-port suspend
interface port-channel 6 vpc
  orphan-port suspend
sleep instance 1 5
  vpc domain 1 shutdown
```

次に、**isolate** コマンドを使用して、すべてのプロトコルをメンテナンス モードにする例を示します。

```
switch(config)# system mode maintenance

Following configuration will be applied:

router bgp 100
  isolate
router ospf 100
  isolate
router isis 100
  isolate
```

```
Do you want to continue (y/n)? [no] y

Generating a snapshot before going into maintenance mode

Starting to apply commands...

Applying : router bgp 100
Applying :   isolate
Applying : router ospf 100
Applying :   isolate
Applying : router isis 100
Applying :   isolate

Maintenance mode operation successful.
```

次に、スイッチのすべてのプロトコルおよびインターフェイスをシャットダウンする例を示します。

```
switch# configure terminal
switch(config)# system mode maintenance shutdown

Following configuration will be applied:

router bgp 64581
  shutdown
router eigrp p2
  shutdown
  address-family ipv6 unicast
    shutdown
router eigrp 0
  shutdown
  address-family ipv6 unicast
    shutdown
router ospf 200
  shutdown
router isis 70
  shutdown
vpc domain 2
  shutdown
system interface shutdown

NOTE: 'system interface shutdown' will shutdown all interfaces excluding mgmt 0
Do you want to continue (yes/no)? [no] yes

Generating a snapshot before going into maintenance mode

Starting to apply commands...

Applying : router bgp 64581
Applying :   shutdown
Applying : router eigrp p2
Applying :   shutdown
Applying :   address-family ipv6 unicast
Applying :     shutdown
Applying : router eigrp 0
Applying :   shutdown
Applying :   address-family ipv6 unicast
Applying :     shutdown
Applying : router ospf 200
Applying :   shutdown
Applying : router isis 70
Applying :   shutdown
Applying : vpc domain 2
Applying :   shutdown2016 Jan 15 11:10:36.080386 CP-BL26-N7K-1A %$ VDC-1 %$
%VPC-2-VPC_SHUTDOWN: vPC shutdown status is ON

Applying : system interface shutdown

Maintenance mode operation successful.
switch(config)# 2016 Jan 15 11:10:42.057678 CP-BL26-N7K-1A %$ VDC-1 %$ %MMODE-2-MODE_CHANGED:
 System changed to "maintenance" mode.
```

```
2016 Jan 15 11:10:42.058167 CP-BL26-N7K-1A %$ VDC-1 %$ %MMODE-2-MODE_CHANGE_WARN: System
will be moved to "normal" mode in 5 minutes
```

次に、メンテナンス モードから通常モードに戻す例を示します。

```
switch# configure terminal
switch(config)# no system mode maintenance dont-generate-profile

Following configuration will be applied:
interface Ethernet1/1
  no shutdown
  sleep instance 1 20
router bgp 100
  no isolate
Do you want to continue (y/n)? [no] yes
Starting to apply commands...
Applying : interface Ethernet1/1
Applying :   no shutdown
Applying : sleep instance 1 20
Applying : router bgp 100
Applying :   no isolate
Maintenance mode operation successful.
Generating Current Snapshot
Please use 'show snapshots compare before_maintenance after_maintenance' to check the
health of the system
```

次に、FabricPath で、カスタム メンテナンス モード プロファイルおよびカスタム通常モード プロファイルを作成する例を示します。

```
switch# configure maintenance profile maintenance-mode
Enter configuration commands, one per line. End with CNTL/Z.
switch(config-mm-profile)# fabricpath domain default
switch(config-mm-profile-fabricpath-isis)# set-overload-bit always
switch(config-mm-profile-fabricpath-isis)# end
Exit maintenance profile mode.
switch#

switch# configure maintenance profile normal-mode
Enter configuration commands, one per line. End with CNTL/Z.
switch(config-mm-profile)# fabricpath domain default
switch(config-mm-profile-fabricpath-isis)# no set-overload-bit always
switch(config-mm-profile-fabricpath-isis)# end
Exit maintenance profile mode.
switch#


switch# show maintenance profile
[Normal Mode]
fabricpath domain default
  no set-overload-bit always
[Maintenance Mode]
fabricpath domain default
  set-overload-bit always
```

次に、仮想ポート チャネル（vPC）で、カスタム メンテナンス モード プロファイルおよびカスタム通常モード プロファイルを作成する例を示します。

```
switch# configure maintenance profile maintenance-mode
Enter configuration commands, one per line. End with CNTL/Z.
switch(config-mm-profile)# vpc domain 1
switch(config-mm-profile-vpc-domain)# shutdown
switch(config-mm-profile-vpc-domain)# exit
switch(config-mm-profile)# system interface shutdown
switch(config-mm-profile)# end
Exit maintenance profile mode.
switch#


switch# configure maintenance profile normal-mode
```

```
Enter configuration commands, one per line. End with CNTL/Z.
switch(config-mm-profile)# vpc domain 1
switch(config-mm-profile-vpc-domain)# no shutdown
switch(config-mm-profile-vpc-domain)# exit
switch(config-mm-profile)# no system interface shutdown
switch(config-mm-profile)# end
Exit maintenance profile mode.
switch#
```

```
switch# show maintenance profile
[Normal Mode]
vpc domain 1
  no shutdown
no system interface shutdown
[Maintenance Mode]
vpc domain 1
  shutdown
system interface shutdown
```

次に、vPC VLAN トラフィックを伝送するポートチャネルまたは通常の L2 イーサネットインターフェイス（vPC ピア リンクを除く）が存在し、対応するスイッチ仮想インターフェイス（SVI）の状態がこれらのインターフェイスにより制御されないようにする必要がある場合に必要な設定の例を示します。

```
Port-channel configuration
switch(config)# interface port-channel3
switch(config-if)# description "L2-Cross Link eth3/3 eth4/3 eth5/3 eth6/3"
switch(config-if)# switchport
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk allowed vlan 1101-1500
switch(config-if)# spanning-tree port type network
switch(config-if)# lacp min-links 2
switch(config-if)# switchport autostate exclude vlan 1101-1500
```

```
L2 Ethernet configuration
switch(config)# interface ethernet 3/3
switch(config-if)# switchport
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk allowed vlan 1101-1500
switch(config-if)# switchport autostate exclude vlan 1101-1500
```

ボーダー ゲートウェイ プロトコル（BGP）の **isolate** モードではダイレクト ルートが撤回されないため、BGP での「redistribute direct」の設定でトラフィックは収集されます。 次に、**route-map** コマンドを使用して BGP をイネーブルにし、**isolate** モードでダイレクト ルートを撤回する例を示します。

ポリシーの設定

メンテナンス モードで **route-map my-rmap-deny** を使用して、タグ 200 が設定された SVI を除外します。

```
switch(config)# route-map my-rmap-deny deny 10
switch(config-route-map)# match tag 200
switch(config-route-map)# exit
switch(config)# route-map my-rmap-deny permit 20
```

通常モードで **route-map my-rmap-permit** を使用して、タグ 200 が設定された SVI を含めます。

```
switch(config)# route-map my-rmap-permit permit 10
switch(config-route-map)# match tag 200
switch(config-route-map)# exit
switch(config)# route-map my-rmap-permit permit 20
```

仮想 IP（vIP）/スイッチ仮想インターフェイス（SVI）の設定

```
switch(config)# interface loopback 200
switch(config-if)# ip address 192.0.2.100/8 tag 200
switch(config)# interface vlan 2
switch(config-if)# ip address 192.0.2.108/8 tag 200
....
switch(config)# interface vlan 3
switch(config-if)# ip address 192.0.2.102/8 tag 200
```

BGP の設定

```
switch(config)# feature bgp
switch(config)# router bgp 100
switch(config-router)# neighbor 192.0.2.100
....
```

メンテナンス モード プロファイル

```
switch# configure maintenance profile maintenance-mode
switch(config-mm-profile)# router bgp 200
switch(config-mm-profile-router)# address-family ipv4 unicast
switch(config-mm-profile-router-af)# redistribute direct route-map my-rmap-deny
switch(config-mm-profile-router-af)# exit
switch(config-mm-profile)# sleep instance 1 10
```

通常モード プロファイル

```
switch# configure maintenance profile normal-mode
switch(config-mm-profile)# router bgp 100
switch(config-mm-profile-router)# address-family ipv4 unicast
switch(config-mm-profile-router-af)# redistribute direct route-map my-rmap-permit
switch(config-mm-profile-router-af)# exit
switch(config-mm-profile)# sleep instance 1 20
```

GIR の確認

設定を確認するには、次のコマンドを使用します。

コマンド	目的
show interface brief	インターフェイスの要約情報を表示します。
show maintenance on-reload reset-reason	スイッチがメンテナンス モードで起動されることになる、リセット理由を表示します。
show maintenance profile [maintenance-mode | normal-mode]	メンテナンス モード プロファイルまたは通常モード プロファイルの詳細を表示します。
show maintenance timeout	メンテナンスモードのタイムアウト期間を表示します。この期間後、スイッチは自動的に通常モードに戻ります。
show tech-support mmode	シスコのテクニカル サポートのメンテナンス モード情報を表示します。

コマンド	目的
show {running-□config | startup-□config} mmode [all]	実行コンフィギュレーションまたはスタートアップ コンフィギュレーションのメンテナンス モードのセクションを表示します。**all** オプションには、デフォルト値が含まれます。
show snapshots	スイッチ上に存在するスナップショットを表示します。
show snapshots compare*snapshot-name-1 snapshot-name-2* [**summary | ipv4routes | ipv6routes**]	2 つのスナップショットの比較を表示します。**summary** オプションは、2 つのスナップショット間の全体的な変更を確認するのに十分な情報のみ表示します。**ipv4routes** および **ipv6routes** オプションは、2 つのスナップショット間の IPv4 および IPv6 ルートの変更を表示します。
show snapshots dump*snapshot-name*	生成されたスナップショットのさまざまなセクションの内容を表示します。
show snapshots sections	ユーザ指定のスナップショット セクションを表示します。
show system mode	現在のシステム モードを表示します。また、このコマンドは、スイッチがメンテナンス モードの場合に、メンテナンス モード タイマーの現在の状態を表示します。

プロトコル レベルでの GIR の確認

BGP（メンテナンス モード）

メンテナンス モードで BGP ステータスを表示するには、**show bgp process** コマンドを使用します。

```
switch# show bgp process

BGP Process Information
BGP Process ID                 : 11725
BGP Protocol Started, reason:  : configuration
BGP Protocol Tag               : 100
BGP Protocol State          : Running (Isolate)
BGP MMODE                   : Initialized
BGP Memory State               : OK
BGP asformat                   : asplain

BGP attributes information
Number of attribute entries    : 1
HWM of attribute entries       : 1
Bytes used by entries          : 100
Entries pending delete         : 0
```

```
HWM of entries pending delete  : 0
BGP paths per attribute HWM    : 3
BGP AS path entries            : 0
Bytes used by AS path entries  : 0
```

プログラムされている BGP IPv4 および IPv6 プレフィックスの数と、プログラムされていない BGP IPv4 および IPv6 プレフィックスの数を表示するには、**show bgp internal all statistics** コマンドを使用します。

```
BGP internal statistics information for VRF default, address family IPv4 Unicast
  Total prefixes in BGP Table: 3
  Total prefixes pending programming in HW: 0
BGP internal statistics information for VRF default, address family IPv6 Unicast
  Total prefixes in BGP Table: 0
  Total prefixes pending programming in HW: 0
```

EIGRP（メンテナンス モード）

メンテナンス モードで EIGRP ステータスを表示するには、**show ip eigrp** コマンドを使用します。

```
switch# show ip eigrp
IP-EIGRP AS 100 ID 30.1.1.1 VRF default
  Process-tag: 100
  Instance Number: 1
  Status: running (isolate)
  Authentication mode: none
  Authentication key-chain: none
  Metric weights: K1=1 K2=0 K3=1 K4=0 K5=0
  IP proto: 88 Multicast group: 224.0.0.10
  Int distance: 90 Ext distance: 170
  Max paths: 8
  Number of EIGRP interfaces: 1 (0 loopbacks)
  Number of EIGRP passive interfaces: 0
  Number of EIGRP peers: 1
  Redistributing:
    direct route-map passall
    static route-map passall
  Graceful-Restart: Enabled
  Stub-Routing: Disabled
  NSF converge time limit/expiries: 120/0
  NSF route-hold time limit/expiries: 240/6
  NSF signal time limit/expiries: 20/0
  Redistributed max-prefix: Disabled
  MMODE: Initialized
  Suppress-FIB-Pending Configured
```

ISIS（メンテナンス モード）

メンテナンス モードで ISIS ステータスを表示するには、**show isis protocol** コマンドを使用します。

```
switch# show isis protocol
ISIS process : 100
 Instance number :  1
 UUID: 1090519320
 Process ID 6969
VRF: default
  System ID : 0300.0000.0004  IS-Type : L2
  SAP : 412  Queue Handle : 16
  Maximum LSP MTU: 1492
  Stateful HA enabled
  Graceful Restart enabled. State: Inactive
  Last graceful restart status : none
  Start-Mode Complete
  BFD IPv4 is globally disabled for ISIS process: 100
  BFD IPv6 is globally disabled for ISIS process: 100
  Topology-mode is base
  Metric-style : advertise(wide), accept(narrow, wide)
```

```
  Area address(es) :
    10
  Process is up and running (isolate)
  VRF ID: 1
  Stale routes during non-graceful controlled restart
  Interfaces supported by IS-IS :
    Ethernet1/2
```

OSPF（メンテナンス モード）

メンテナンス モードで OSPF ステータスを表示するには、**show ip ospf internal** コマンドを使用します。

```
switch# show ip ospf internal

ospf 100
ospf process tag 100
ospf process instance number 1
ospf process uuid 1090519321
ospf process linux pid 6968
ospf process state running (isolate)
System uptime 6d06h
SUP uptime 2 6d06h

Server up : L3VM|IFMGR|RPM|AM|CLIS|URIB|U6RIB|IP|IPv6|SNMP|MMODE
Server required  : L3VM|IFMGR|RPM|AM|CLIS|URIB|IP|SNMP
Server registered: L3VM|IFMGR|RPM|AM|CLIS|URIB|IP|SNMP|MMODE
Server optional  : MMODE

Early hello : OFF
Force write PSS: FALSE
OSPF mts pkt sap 324
OSPF mts base sap 320
```

GIR の機能の履歴

次の表に、このマニュアルの新機能および変更された機能を要約し、各機能がサポートされているリリースを示します。ご使用のソフトウェア リリースで、本書で説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。

機能名	リリース	Information
グレースフル挿入と削除（GIR）	7.3(0)D1(1)	GIR のデフォルト モードは isolate です。計画外メンテナンス、メンテナンス モード タイマー、FIB保留の抑制、スナップショットへの Show コマンドの追加、およびスナップショット セクションのダンプをサポートします。

機能名	リリース	Information
グレースフル挿入と削除（GIR）	7.2(0)D1(1)	この機能が導入されました。GIR のデフォルト モードは shutdown です。「GIR の設定（Cisco NX-OS Release 7.2(0)D1(1)）」を参照してください。

第 23 章

GIRの設定（Cisco NX-OS Release 7.2(0)D1(1)）

この章の内容は、次のとおりです。

- GIR について，493 ページ
- GIR の注意事項と制約事項，494 ページ
- GIR サイクルの実行，494 ページ
- 通常モード プロファイル ファイルの設定，495 ページ
- スナップショットの作成，496 ページ
- メンテナンス モードの開始，497 ページ
- 通常モードへの復帰，498 ページ
- メンテナンス モード プロファイル ファイルの設定，498 ページ
- GIR の確認，500 ページ

GIR について

デバッグやアップグレードを実行するために、グレースフル挿入と削除（GIR）を使用して、スイッチをネットワークから分離することができます。スイッチのメンテナンスが完了したら、スイッチを通常モードに戻すことができます。

スイッチをメンテナンス モードにすると、すべてのプロトコルはグレースフルに（正常に）ダウン状態になり、すべての物理ポートがシャットダウンします。通常モードに戻すと、すべてのプロトコルおよびポートが起動状態に戻ります。

次のプロトコルがサポートされています。

- Border Gateway Protocol（BGP）
- BGPv6
- Enhanced Interior Gateway Routing Protocol（EIGRP）

- EIGRPv6
- Intermediate System-to-Intermediate System（ISIS）
- Open Shortest Path First（OSPF）
- OSPFv3

以下もサポートされます。

- 仮想ポート チャネル（vPC）
- インターフェイス
- FabricPath

スイッチをメンテナンス モードにする前にメンテナンス モード プロファイル ファイルを作成できます。または **[no] system mode maintenance** コマンドを入力する際に、システムによりメンテナンス モード プロファイル ファイルを作成するようにすることができます。

snapshot コマンドを使用して、選択した機能の実行状態をキャプチャし、永続ストレージ メディアに保存します。

スナップショットは、メンテナンス モードになる前と通常モードに戻った後に、スイッチの状態を比較するのに便利です。スナップショット プロセスは、次の 3 つの部分で構成されます。

- 事前に選択したスイッチの一部機能の状態のスナップショットを作成し、永続ストレージメディアに保存する。
- さまざまな時間間隔で取得したスナップショットを一覧にして、管理する。
- スナップショットを比較し、各機能の概要と詳細を表示する。

GIR の注意事項と制約事項

グレースフル挿入と削除（GIR）には、次の注意事項と制約事項があります。

- メンテナンス モード プロファイル、通常モード プロファイルは、それぞれ、**config profile maintenance-mode type admin** および **config profile normal-mode type admin** コマンドを使用して作成できます。

GIR サイクルの実行

手順

ステップ 1 （任意） メンテナンス モード プロファイル ファイルを作成します。
メンテナンス モード プロファイル ファイルの設定, （498 ページ）を参照してください。

ステップ 2 （任意） 通常モード プロファイル ファイルを作成します。
通常モード プロファイル ファイルの設定, （495 ページ）を参照してください。

ステップ 3 メンテナンス モードに入る前にスナップショットを作成します。
スナップショットの作成, （496 ページ）を参照してください。

ステップ 4 スイッチをメンテナンス モードにします。
メンテナンス モードの開始, （497 ページ） を参照してください。

ステップ 5 （任意） **copy running-config startup-config** コマンドを入力します。

ステップ 6 スイッチを通常モードに戻します。
通常モードへの復帰, （498 ページ）を参照してください。

ステップ 7 通常モードに戻ったら、スナップショットを作成します。
スナップショットの作成, （496 ページ）を参照してください。

通常モード プロファイル ファイルの設定

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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	switch(config)# **configure profile normal-mode type admin**	通常モードプロファイルファイルの設定セッションを開始します。 （注） 設定しているプロトコルに応じて、プロトコルを起動する適切なコマンドを入力する必要があります。
ステップ 3	switch# **end**	通常モード プロファイル ファイルを閉じます。

次に、通常モード プロファイル ファイルを作成する例を示します。

```
switch# configure terminal
switch(config)# configure profile normal-mode type admin
switch(config-profile)# router ospf 100
switch(config-profile-router)# no shutdown
switch(config-profile-router)# exit
switch(config-profile)# router eigrp 101
switch(config-profile-router)# no shutdown
switch(config-profile-router)# exit
switch(config-profile)# router isis 102
switch(config-profile-router)# no shutdown
switch(config-profile-router)# no set-overload-bit always
switch(config-profile-router)# exit
```

```
switch(config-profile)# router bgp 103
switch(config-profile-router)# no shutdown
switch(config-profile-router)# exit
switch(config-profile)# vpc domain 20
switch(config-profile-router)# no shutdown
switch(config-profile-router)# exit
switch(config-profile)# no system interface shutdown
switch(config-profile)# end
Exit configure profile mode.
switch#
```

次に、通常モード カスタム プロファイル ファイルを作成する例を示します。

```
switch# configure terminal
switch(config)# configure profile normal-mode type admin
switch(config-profile)# router bgp 65501
switch(config-profile-router)# no shutdown
switch(config-profile-router)# exit
switch(config-profile)# router eigrp 100
switch(config-profile-router)# no shutdown
switch(config-profile-router)# exit
switch(config-profile)# address-family ipv6 unicast
switch(config-profile)# no shutdown
switch(config-profile)# router eigrp 600
switch(config-profile-router)# no shutdown
switch(config-profile-router)# exit
switch(config-profile)# address-family ipv6 unicast
switch(config-profile-router)# no shutdown
switch(config-profile-router)# exit
switch(config-profile)# router ospf 100
switch(config-profile-router)# no shutdown
switch(config-profile-router)# exit
switch(config-profile)# router ospfv3 ospf_ipv6
switch(config-profile-router)# no shutdown
switch(config-profile-router)# exit
switch(config-profile)# router isis isp
switch(config-profile-router)# no set-overload-bit always
switch(config-profile-router)# exit
switch(config-profile)# vpc domain 2
switch(config-profile-router)# no shutdown
switch(config-profile-router)# exit
switch(config-profile)# no system interface shutdown
switch(config-profile)# end
Exit configure profile mode.
switch#
```

スナップショットの作成

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **snapshot create***namedescription*	スナップショットを作成します。*name* 変数は最大 64 文字です。*description* 変数は最大 256 文字です。

次に、スナップショットを作成する例を示します。

```
switch# snapshot create snap1 For documentation purposes.
Executing show interface... Done
```

```
Executing show bgp sessions vrf all... Done
Executing show ip eigrp topology summary... Done
Executing show ipv6 eigrp topology summary... Done
Executing show vpc... Done
Executing show ip ospf vrf all... Done
Feature 'ospfv3' not enabled, skipping...
Executing show isis vrf all... Done
Snapshot 'snap1' created
switch#
```

メンテナンス モードの開始

はじめる前に

system mode maintenance コマンドで生成するのでなく独自のプロファイルを作成する場合は、メンテナンス モード プロファイル ファイルの設定，（498 ページ）を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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	switch(config)# **system mode maintenance** [**dont-generate-profile**]	以前に作成したメンテナンス モード プロファイル ファイルを実行するか、または動的にメンテナンス モード プロファイル ファイルを作成します。 **dont-generate-profile** オプションは、メンテナンス モード プロファイル ファイルの作成を抑制します。 （注） 続行を促すプロンプトが表示されます。続行する場合は y、プロセスを終了する場合は n を入力します。

これにより、スイッチはメンテナンス モードになります。

（注） メンテナンス モードでは、インサービス ソフトウェア ダウングレード（ISSD）を行うことはできません。

次に、以前に作成したメンテナンス モード プロファイル ファイルを使用してスイッチをメンテナンス モードにする例を示します。

```
switch# configure terminal
switch(config)# system mode maintenance dont-generate-profile
Do you want to continue (y/n)? [n] y

Progressing.....................................................Done.

System mode operation completed successfully
switch(config)#
```

通常モードへの復帰

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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	switch(config)# **no system mode maintenance** [**dont-generate-profile**]	以前に作成した通常モード プロファイル ファイルを実行するか、または動的に通常モード プロファイル ファイルを作成します。**dont-generate-profile** オプションは、通常モードプロファイルファイルの作成を抑制します。 （注） 続行を促すプロンプトが表示されます。続行する場合はy、プロセスを終了する場合はnを入力します。 これにより、スイッチは通常モードになります。

次に、メンテナンス モードから通常モードに戻す例を示します。

```
switch# configure terminal
switch(config)# no system mode maintenance dont-generate-profile
Do you want to continue (y/n)? [n] y

Progressing.............Done.

System mode operation completed successfully

switch(config)#
```

メンテナンス モード プロファイル ファイルの設定

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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	switch(config)# **configure profile maintenance-mode type admin**	メンテナンス モード プロファイル ファイルの設定セッションを開始します。 （注） 設定しているプロトコルに応じて、プロトコルを停止する適切なコマンドを入力する必要があります。

	コマンドまたはアクション	目的
ステップ 3	switch# **end**	メンテナンス モード プロファイル ファイルを閉じます。

次に、メンテナンス モード プロファイル ファイルを作成する例を示します。

```
switch# configure terminal
switch(config)# configure profile maintenance-mode type admin
switch(config-profile)# router ospf 100
switch(config-profile-router)# shutdown
switch(config-profile-router)# exit
switch(config-profile)# router eigrp 101
switch(config-profile-router)# shutdown
switch(config-profile-router)# exit
switch(config-profile)# router isis 102
switch(config-profile-router)# shutdown
switch(config-profile-router)# set-overload-bit always
switch(config-profile-router)# exit
switch(config-profile)# router bgp 103
switch(config-profile-router)# shutdown
switch(config-profile-router)# exit
switch(config-profile)# vpc domain 20
switch(config-profile-router)# shutdown
switch(config-profile-router)# exit
switch(config-profile)# system interface shutdown
switch(config-profile)# end
Exit configure profile mode.
switch#
```

次に、メンテナンス モード カスタム プロファイル ファイルを作成する例を示します。

```
switch# configure terminal
switch(config)# configure profile maintenance-mode type admin
switch(config-profile)# router bgp 65501
switch(config-profile-router)# shutdown
switch(config-profile-router)# exit
switch(config-profile)# address-family ipv6 unicast
switch(config-profile)# shutdown
switch(config-profile)# router eigrp 600
switch(config-profile-router)# shutdown
switch(config-profile-router)# exit
switch(config-profile)# address-family ipv6 unicast
switch(config-profile-router)# shutdown
switch(config-profile-router)# exit
switch(config-profile)# router ospf 100
switch(config-profile-router)# shutdown
switch(config-profile-router)# exit
switch(config-profile)# router ospfv3 ospf_ipv6
switch(config-profile-router)# shutdown
switch(config-profile-router)# exit
switch(config-profile)# router isis isp
switch(config-profile-router)# set-overload-bit always
switch(config-profile-router)# exit
switch(config-profile)# vpc domain 2
switch(config-profile-router)# shutdown
switch(config-profile-router)# exit
switch(config-profile)# system interface shutdown
switch(config-profile)# end
Exit configure profile mode.
switch#
```

次に、IPv6 プロトコルで、メンテナンス モード プロファイルを作成する例を示します。

```
switch# configure terminal
switch(config)# configure profile maintenance-mode type admin
switch(config-profile)# router ospfv3 ospf_ipv6
switch(config-profile-router)# shutdown
switch(config-profile-router)# exit
switch(config-profile)# router eigrp 660
switch(config-profile-router)# address-family ipv6 unicast
switch(config-profile-router-af)# shutdown
switch(config-profile-router-af)# exit
switch(config-profile-router)# router isis isp
switch(config-profile-router)# set-overload-bit always
switch(config-profile-router)# exit
switch(config-profile)# router bgp 655551
switch(config-profile)# address-family ipv6 unicast
switch(config-profile-router)# shutdown
switch(config-profile-router)# exit
switch(config-profile)#
```

GIR の確認

次のいずれかのコマンドを使用して、設定を確認します。

コマンド	目的
show system mode	現在のシステム モードを表示します。
show interface brief	インターフェイスの要約情報を表示します。
show snapshots*before-maintenance-mode description*	スイッチ上に存在するスナップショットを表示します。
show config-profile*name*	config-profile ファイルの詳細を表示します。

show system mode コマンド

```
switch# show system mode
System Mode : Maintenance
```

show interface brief コマンド

```
switch# show interface brief

--------------------------------------------------------------------------------
Ehternet       VLAN     Type Mode   Status  Reason               Speed   Port
Interface                                                                Ch #
--------------------------------------------------------------------------------
Eth1/1         - -      eth  routed  down   sysIntfShut           10G(D) - -
Eth1/2         - -      eth  routed  down   sysIntfShut           10G(D) - -
Eth1/3         - -      eth  routed  down   sysIntfShut           10G(D) - -
Eth1/4         - -      eth  routed  down   sysIntfShut           10G(D) - -
Eth1/5         - -      eth  routed  down   sysIntfShut           10G(D) - -
Eth1/6         - -      eth  routed  down   sysIntfShut           10G(D) - -
Eth1/7         - -      eth  routed  down   SFP not inserted      10G(D) - -
Eth1/8         - -      eth  routed  down   SFP not inserted      10G(D) - -
Eth1/9         - -      eth  routed  down   SFP not inserted      10G(D) - -
Eth1/10        - -      eth  routed  down   SFP not inserted      10G(D) - -
```

```
Eth1/12        - -      eth  routed  down   SFP not inserted      10G(D) - -
Eth1/13        - -      eth  routed  down   SFP not inserted      10G(D) - -
Eth1/14        - -      eth  routed  down   SFP not inserted      10G(D) - -
Eth1/15        - -      eth  routed  down   SFP not inserted      10G(D) - -
Eth1/16        - -      eth  routed  down   SFP not inserted      10G(D) - -

--------------------------------------------------------------------------------
Port-channel  VLAN    Type Mode    Status  Reason                   Speed   Protocol
Interface
--------------------------------------------------------------------------------
Po1           1       eth  access  down    No operational members   auto(I)  none
Po100         1       eth  access  down    No operational members   auto(I)  none

--------------------------------------------------------------------------------
Port     VRF         Status IP Address                              Speed    MTU
--------------------------------------------------------------------------------
mgmt0    - -         up     192.0.0.1                               1000     1500
switch#
```

show snapshots コマンド

```
switch# show snapshots
Snapshot Name
-----------------------------------------------------------------------------------------------
snapshot_before_maintenance      Wed Sep 10 20:19:31 2014      system-internal-snapshot
snapshot_after_maintenance       Wed Sep 10 20:29:54 2014      system-internal-snapshot
snap1                            Wed Sep 10 20:36:15 2014      For testing
```

show config-profile コマンド

```
switch# show config-profile

config-profile maintenance-mode type admin
  router ospf 100
   shutdown
  router eigrp 101
   shutdown
  router isis 102
   set-overload-bit always
  router bgp 103
   shutdown
  vpc domain 20
   shutdown
  system interface shutdown exclude fex-fabric

config-profile normal-mode type admin
  router ospf 100
   no shutdown
  router eigrp 101
   no shutdown
  router isis 102
   no set-overload-bit always
  router bgp 103
   no shutdown
  vpc domain 20
   no shutdown
  no system interface shutdown
```

第 24 章

ソフトウェア メンテナンス アップグレードの実行

この章では、Cisco NX-OS デバイスでソフトウェア メンテナンス アップグレードを実行する方法について説明します。

この章の内容は、次のとおりです。

- SMU の前提条件，503 ページ
- SMU の注意事項と制約事項，504 ページ
- ソフトウェア メンテナンス アップグレードの実行に関する情報，505 ページ
- Cisco NX-OS のソフトウェア メンテナンス アップグレードの実行，507 ページ
- 次の作業，519 ページ
- その他の参考資料，520 ページ
- ソフトウェア メンテナンス アップグレードを実行するための機能情報，521 ページ

SMU の前提条件

アクティブ化または非アクティブ化するパッケージでは、これらの前提条件が満たされている必要があります。

- 適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。ユーザ グループの割り当てが原因でコマンドを使用できないと考えられる場合、AAA 管理者に連絡してください。
- すべてのライン カードが取り付けられ、正常に動作していることを確認します。たとえば、ライン カードのブート中、ライン カードのアップグレード中または交換中、または自動スイッチオーバー アクティビティが予想される場合は、パッケージのアクティブ化や非アクティブ化はできません。

- デュアル スーパーバイザ システムでは、アクティブおよびスタンバイ スーパーバイザ モジュールの両方を、相互に同期する必要があります。

SMU の注意事項と制約事項

SMU に関する注意事項および制約事項は次のとおりです。

- パッケージによっては、他のパッケージのアクティブ化または非アクティブ化が必要です。SMU に相互に依存関係がある場合は、前の SMU をまずアクティブにしないとそれらをアクティブ化できません。
- アクティブ化するパッケージは、現在のアクティブなソフトウェアのセットと互換性がある必要があります。
- 1 つのコマンドで複数の SMU をアクティブにできません。
- VDC ごとの SMU はサポートされません。
- パッケージの互換性が確認できた場合に限り、アクティブ化が実行されます。競合がある場合は、エラー メッセージが表示されます。
- ソフトウェアパッケージをアクティブ化する間、その他の要求はすべての影響のあるノードで実行できません。これと同様のメッセージが表示されると、パッケージのアクティブ化は完了します。

```
Install operation 1 completed successfully at Thu Jan 9 01:19:24 2014
```

- 各 CLI インストール要求には要求 ID が割り当てられます。これは後でイベントを確認するのに使用できます。
- SMU は物理デバイスに依存します。つまり、Cisco Nexus 7000 シリーズ用の SMU は Cisco Nexus 7700 シリーズで使用できず、逆もまた同様です。
- ソフトウェア メンテナンス アップグレードを実行後、デバイスを新しい Cisco NX-OS ソフトウェア リリースにアップグレードする場合、新しいイメージで以前の Cisco NX-OS リリースと SMU パッケージ ファイルの両方が上書きされます。
- SMU は、インストールされている Cisco NX-OS ソフトウェア リリースのバージョンに依存します。使用中のリリースと互換性のある SMU をインストールする必要があります。リロードまたは ISSU を使用して他の Cisco NX-OS ソフトウェア リリースに移行すると、以前にインストールされていた Cisco NX-OS ソフトウェア リリースにインストールした SMU は非アクティブになります。たとえば、Supervisor 2 セットアップで、Cisco NX-OS Release 7.2.0 で SMU を使用していた場合、Cisco NX-OS Release 7.2.2 などの他のリリースのイメージに移行すると、SMU は非アクティブになります。
- SMU をサポートしない NX-OS Release 7.2.0 以前の Cisco NX-OS ソフトウェア リリースのイメージをロードすると、SMU は無効になります。ただし、Cisco NX-OS Release 7.2.0 に戻ると SMU はアクティブになります。

ソフトウェアメンテナンスアップグレードの実行に関する情報

SMU の概要

通常、SMU がデバイスの動作に大きな影響を及ぼすことはありません。SMU のバージョンは、アップグレードするパッケージのメジャー、マイナー、およびメンテナンス バージョンに同期されます。

SMUは、メンテナンス リリースの代わりになるものではありません。直近の問題に対する迅速な解決策を提供します。SMUで修正された障害は、メンテナンス リリースにすべて統合されます。

SMU の実際の導入はデバイスによって異なります。通常、プロセスを再起動するだけでソフトウェアはパッチされます。ただし、デバイスによってはパッチしたプロセスが再起動せず、その場合、リロードまたは ISSU によって SMU を導入します。

SMU の影響は次のタイプによって異なります。

- プロセスの再起動SMU：アクティベーション時にプロセスまたはプロセスのグループの再起動を引き起こします。
- リロード SMU：スイッチ全体のリロード、スーパーバイザとライン カードの並列リロードを引き起こします。
- ラインカード SMU：ライン カードのタイプに基づきます。スーパーバイザは、影響を受けるすべてのライン カードにこの SMU をプッシュします。ラインカード SMU をアクティブ化するには、スイッチのリロードが必要です。
- ISSU SMU：ISSU オーケストレーションを使用して導入されます。
- 前提条件 SMU：依存する SMU をロードする前にアクティブ化が必要です。1 つの SMU に、前提条件としての SMU を 1 つ以上含めることができます。
- 置き換え SMU：以前にロードされた SMU の累積的な修正を含み、以前の SMU を置き換えます。

デバイスを新しい機能やメンテナンス リリースにアップグレードする詳細については、『*Cisco Nexus 7000 Series NX-OS Software Upgrade and Downgrade Guide*』を参照してください。

SMU は、SMU バイナリ ファイル、および関連する警告を含む添付の README.txt から構成されます。SMU の命名規則を次に示します。

<platform>-<pkg-type>.<release_version>.<CDET>.<file-type>

次に例を示します。

n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin

n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.txt

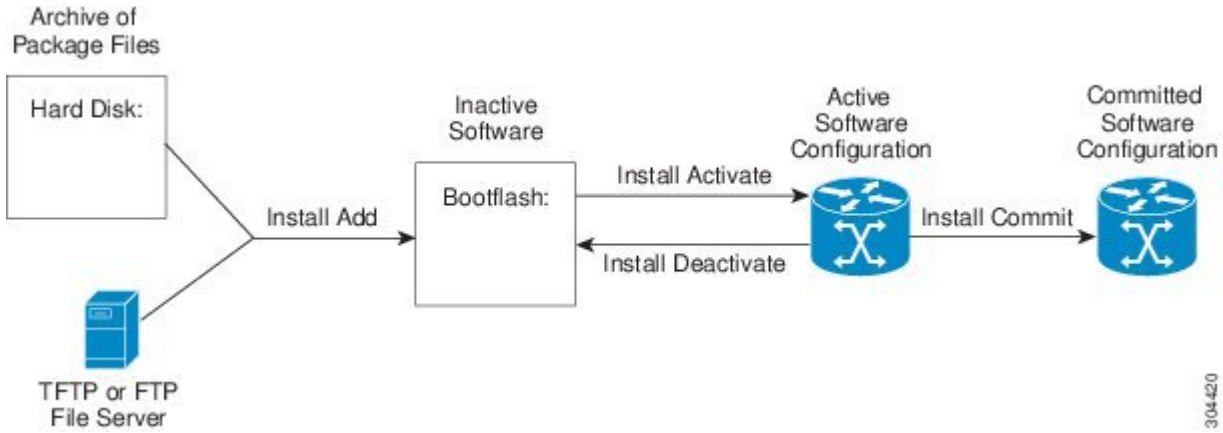
パッケージ管理

デバイスでの SMU パッケージの追加およびアクティブ化の一般的な手順は次のとおりです。

1. パッケージ ファイルをローカル ストレージ デバイスまたはファイル サーバにコピーします。
2. **install add** コマンドを使用してデバイス上でパッケージを追加します。
3. **install activate** コマンドを使用して、デバイス上でパッケージをアクティブ化します。
4. **install commit** コマンドを使用して、現在のパッケージのセットをコミットします。ただし、SMU をリロードまたは ISSU する場合は、リロードまたは ISSU の後にパッケージをコミットします。
5. （任意）必要に応じて、パッケージを非アクティブ化して削除します。

次の図は、パッケージの管理プロセスの主要な手順について説明します。

図 *9*：*SMU* パッケージを追加、アクティブ化およびコミットするプロセス



パッケージのアクティブ化と非アクティブ化の影響

SMUパッケージのアクティブ化または非アクティブ化は、システムにすぐさま影響を与える可能性があります。システムは次のように影響を受ける場合があります。

- 新しいプロセスが開始する場合があります。
- 実行しているプロセスが停止または再起動する場合があります。
- ライン カード上のすべてのプロセスがパッチされる場合があり、再起動可能なプロセスのみが再起動します。ライン カードのプロセスの再起動は、ソフト リセットと同等です。
- ラインカード SMU の場合、システムはアップグレードの動作と似た動作をします。
- ライン カードがリロードする場合があります。
- システム全体がリロードする場合があります。
- ライン カードのプロセスは影響を受けない場合があります。

（注） 必要に応じて、改訂されたコンフィギュレーションおよびコンフィギュレーションの再適用によって起こる問題に対処する必要があります。

ヒント パッケージをアクティブ化する際に**test**オプションを使用すると、稼働中のシステムに影響を与えることなく、コマンドの効果をテストすることができます。アクティブ化プロセスが完了したら、**show install log** コマンドを入力してプロセスの結果を表示します。

Cisco NX-OS のソフトウェア メンテナンス アップグレードの実行

パッケージ インストールの準備

SMU パッケージのインストールの準備に関する情報を収集するには、複数の **show** コマンドを使用する必要があります。

はじめる前に

ソフトウェアの変更が必要かどうかを確認します。

使用中のシステムで新しいパッケージがサポートされていることを確認する。ソフトウェア パッケージによっては、他のパッケージまたはパッケージ バージョンをアクティブにする必要があり、特定のライン カードのみをサポートするパッケージもあります。

そのリリースに関連する重要な情報についてリリース ノートを確認し、そのパッケージとデバイス設定の互換性の有無を判断する。

システムの動作が安定していて、ソフトウェアの変更に対応できることを確認する。

手順

	コマンドまたはアクション	目的
ステップ 1	**show install active** 例： `switch# show install active`	デバイス上のアクティブなソフトウェアを表示します。デバイスに追加する必要があるソフトウェアを確認するには、次のコマンドを使用します。
ステップ 2	**show module** 例： `switch# show module`	すべてのモジュールが安定状態であることを確認します。

	コマンドまたはアクション	目的
ステップ 3	**show clock** 例： `switch# show clock`	システム クロックが正しいことを確認します。ソフトウェア操作は、デバイス クロックの時刻に基づいて証明書を使用します。
ステップ 4	**show install pkg-info***SMU_name* 例： `Device# show install pkg-info n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin`	SMU のコンテンツ、つまり、SMU 再起動タイプ、プラットフォーム、影響されるプロセスなどに関する詳細を表示します。

次に、システム全体のアクティブなパッケージを表示する例を示します。この情報を使用して、ソフトウェアの変更が必要かどうかを判断します。

SMU のインストール前：

```
switch# show install active

Boot Images:

Kickstart Image: bootflash:/ n7700-s2-kickstart.7.2.0.D1.1.bin
System Image: bootflash:/ n7700-s2-dk9.7.2.0.D1.1.bin

Active Packages:
Active Packages on Module #1:
```

SMU のインストール後：

```
Switch# show install active

Boot Images:

Kickstart Image: bootflash:/n7700-s2-kickstart.7.2.0.D1.1.bin
System Image: bootflash:/n7700-s2-dk9.7.2.0.D1.1.bin

Active Packages:

  n7700-s2-dk9.7.2.0.D1.1.CSCuo7721.bin

Active Packages on Module #1:
  n7700-s2-dk9.7.2.0.D1.1.CSCuo7721.bin
```

次に、現在のシステム クロックの設定を表示する例を示します。

```
switch# show clock

02:14:51.474 PST Wed Jan 04 2014
```

次に、インストールしたパッケージの詳細を表示する例を示します。この情報を使用して、ソフトウェアの変更が必要かどうかを判断します。

```
switch# show install pkg-info n7700-s2-dk9.7.2.0.D1.1. CSCuo07721.bin

Contents of Package file 'n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin'
            Expiry date: Sun Oct 22 11:39:35 2017
            Uncompressed size: 224905
            Vendor: Cisco Systems
            Restart type: restart
            Desc: Bug Fix for CDET: CSCuo07721
            Build: Built on Tue Aug  4 01:12:10 2015
            Source: By Unknown
            Platform: Nexus7700
```

```
Supersedes: None
Superseded By: None
Pre-requisite: None
Restart information: Ethpm
Pre-install activate scripts: None
Post-install activate scripts: None
Pre-install deactivate scripts: None
Post-install deactivate scripts: None
```

Cisco.com からの SMU パッケージ ファイルのダウンロード

SMU パッケージ ファイルをダウンロードするには、次の手順に従ってください。

手順

ステップ 1 Cisco.com にログインします。

ステップ 2 次の URL から [Download Software] ページに移動します。 http://software.cisco.com/download/navigator.html

ステップ 3 [Select a Product] リストから、[**Switches**] > [**Data Center Switches**] > [**Cisco Nexus 7000 Series Switches**] > [*model*] を選択します。

ステップ 4 デバイスに適した SMU ファイルを選択し、[**Download**] をクリックします。

ローカルストレージデバイスまたはネットワークサーバへのパッケージ ファイルのコピー

デバイスがアクセスできるローカル ストレージ デバイスまたはネットワーク ファイル サーバに SMU パッケージ ファイルをコピーする必要があります。この作業が完了したら、パッケージをデバイスに追加しアクティブにできます。

デバイスにパッケージ ファイルを保存する必要がある場合は、ハードディスクにファイルを保存することを推奨します。ブートデバイスは、パッケージを追加しアクティブするローカルディスクです。デフォルトのブート デバイスは bootflash: です。

ヒント ローカル ストレージ デバイスにパッケージ ファイルをコピーする前に、**dir** コマンドを使用して、必要なパッケージ ファイルがデバイスに存在するかどうかを確認します。

ヒント ブートフラッシュに十分なスペースがあることを確認します。

SMU パッケージ ファイルがリモート TFTP、FTP、SCP、または SFTP サーバにある場合、ローカル ストレージ デバイスにファイルをコピーできます。ファイルがローカル ストレージ デバイスに置かれた後、パッケージをそのストレージ デバイスからデバイスに追加しアクティブにできます。次のサーバ プロトコルがサポートされます。

- TFTP：ネットワークを介して、あるコンピュータから別のコンピュータへファイルを転送できるようにします。通常は、クライアント認証（たとえば、ユーザ名およびパスワード）を使用しません。これは FTP の簡易版です。

（注） パッケージ ファイルによっては、大きさが 32 MB を超える場合もありますが、一部のベンダーにより提供される TFTP サービスではこの大きさのファイルがサポートされていない場合があります。32 MB を超えるファイルをサポートする TFTP サーバにアクセスできない場合は、FTP を使用してファイルをダウンロードします。

- ファイル転送プロトコル：FTP は TCP/IP プロトコル スタックの一部であり、ユーザ名とパスワードが必要です。
- セキュア コピー：SCP は、セキュア シェル（SSH）をサポートするネットワーク サーバからファイルが転送されるようにします。セキュア コピープロトコル（SCP）を使用します。
- SSH ファイル転送プロトコル：SFTP は、セキュリティ パッケージの SSHv2 機能の一部で、セキュアなファイル転送を提供します。詳細については、『*Cisco Nexus 7000 Series NX-OS Security Configuration Guide*』を参照してください。

（注） お使いのネットワーク サーバの場所と可用性については、システム管理者に問い合わせてください。

ファイル転送プロトコルを使用してサーバからデバイスに SMU パッケージ ファイルをコピーするには、次の表のコマンドを使用します。

表 *44*：*SMU* パッケージ ファイルをデバイスにコピーするためのコマンド

コマンド	目的
copy tftp://*hostname-or-ipaddress*/*directory-path*/*filename***bootflash:** `switch# copy tftp://10.1.1.1/images/ n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin bootflash:`	TFTP サーバから bootflash: にパッケージ ファイルをコピーします。 • *hostname-or-ipaddress*：ネットワーク ファイル サーバのホスト名または IP アドレス。 • *directory-path*：追加されるパッケージ ファイルに導くネットワーク ファイルのサーバ パス。 • *filename*：追加するパッケージ ファイルの名前。

コマンド	目的
copy ftp://*username***:***password***@***hostname-or-ipaddress***/***directory-path***/***filename***bootflash:** `switch# copy ftp://john:secret@10.1.1.1/images/ n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin bootflash:`	FTP サーバから bootflash: にパッケージ ファイルをコピーします。 • *username*：パッケージ ファイルを保存するディレクトリへのアクセス権を持つユーザのユーザ名。 • *password*：パッケージ ファイルを保存するディレクトリへのアクセス権を持つユーザのユーザ名に関連付けられたパスワード。パスワードを指定しないと、ネットワーキング デバイスは、anonymous FTP を受け入れます。 • *hostname-or-ipaddress*：ネットワーク ファイル サーバのホスト名または IP アドレス。 • *directory-path*：追加されるパッケージ ファイルに導くネットワーク ファイルのサーバパス。指定されるディレクトリは、ユーザのホームディレクトリの下のディレクトリである必要があります。この例では、ダウンロードされたファイルはユーザ「john」のホーム ディレクトリ内の「images」というサブディレクトリにあります。 （注） FTP サービスの場合、*directory-path* は *username* ホーム ディレクトリの相対パスです。ディレクトリの絶対パスを指定するには、サーバ アドレスの後ろに「/」を追加する必要があります。 • *filename*：追加するパッケージ ファイルの名前。

コマンド	目的
copy sftp://*hostname-or-ipaddress*/*directory-path*/*filename***bootflash:** `switch# copy sftp://10.1.1.1/images n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin bootflash:`	SFTP サーバから bootflash: にパッケージ ファイルをコピーします。 • *username*：パッケージ ファイルを保存するディレクトリへのアクセス権を持つユーザのユーザ名。 • *directory-path*：追加されるパッケージ ファイルに導くネットワーク ファイルのサーバ パス。 • *filename*：追加するパッケージ ファイルの名前。
copy scp://*username@scpserver.cisco.com*//*directory-path*/*filename***bootflash:** `switch# copy scp://john@10.1.1.1//download/n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin bootflash:n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin`	SCP サーバから bootflash: にパッケージ ファイルをコピーします。 • *hostname-or-ipaddress*：ネットワーク ファイル サーバのホスト名または IP アドレス。 • *directory-path*：追加されるパッケージ ファイルに導くネットワーク ファイルのサーバ パス。 • *filename*：追加するパッケージ ファイルの名前。

SMU パッケージ ファイルをネットワーク ファイル サーバまたはローカル ストレージ デバイスに転送した後に、ファイルを追加しアクティブ化することができます。

パッケージの追加とアクティブ化

ローカル ストレージ デバイスまたはリモート TFTP、FTP、SFTP サーバに保存されている SMU パッケージ ファイルをデバイスに追加できます。

（注） アクティブ化する SMU パッケージは、現在アクティブで動作可能なソフトウェアと互換性がなければなりません。アクティブ化が試行されると、システムは自動互換性チェックを実行し、パッケージがデバイス上で他のアクティブなソフトウェアと互換性があることを確認します。競合がある場合は、エラー メッセージが表示されます。アクティブ化が実行されるのは、すべての互換性が確認できた場合だけです。

（注） あるプロセスの SMU のアクティブ化によって他のプロセスに適用されている SMU が非アクティブ化されることはありません。ただし、同じプロセスで以前アクティブだった SMU は非アクティブ化されます。

はじめる前に

追加するすべてのパッケージがローカル ストレージ デバイスまたはネットワーク ファイル サーバにあることを確認します。

パッケージのアクティブ化の前提条件をすべて満たしていることを確認します。

「ローカル ストレージ デバイスまたはネットワーク サーバへのパッケージ ファイルのコピー」に記載されている手順を完了します。

手順

	コマンドまたはアクション	目的
ステップ 1	コンソール ポートに接続して、ログインします。	コンソール ポートに CLI 管理セッションを確立します。
ステップ 2	**dir bootflash:**	（任意） 追加可能なパッケージ ファイルを表示します。 （注） このプロシージャを使用して追加およびアクティきるのは SMU パッケージ ファイルだけです。
ステップ 3	**install add***filename* [**activate**] 例： `switch# install add bootflash: n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin`	ローカル ストレージ デバイスまたはネットワーク サーバケージ ソフトウェア ファイルを解凍して、アクティブ スイザおよびスタンバイ スーパーバイザ上のブートフラッシします。 *filename* 引数は、次の形式をとることができます。 • **bootflash:***filename* • **tftp:**//*hostname-or-ipaddress*/*directory-path*/*filename* • **ftp:**//*username*:*password*@*hostname-or-ipaddress*/*directory-pa* • **sftp:**//*hostname-or-ipaddress*/*directory-path*/*filename* • **usb1:***filename*

	コマンドまたはアクション	目的
		現在実行中のソフトウェアに影響を与えずに、複数バージョ SMU パッケージをストレージ デバイスに追加できます。た アクティブ化できるのは 1 つのバージョンのパッケージだけ
ステップ 4	**show install inactive** 例： `switch# show install inactive`	（任意） デバイス上の非アクティブなパッケージを表示します。前述 で追加されたパッケージが表示に出ることを確認します。

ステップ 5	**install activate***filename* [**test**]
	
	例：
	`switch# install activate n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin`
	
	`Install operation 158 completed successfully at Tue Jun 9 19:09:33 2015`
		デバイスに追加されたパッケージをアクティブにします。SM
		ケージは、アクティブにされるまで無効のままです。（**instal**
		activate コマンドを使用して、パッケージが前にアクティブに
		た場合は、この手順を省略します。）
		（注） パッケージ名を部分的に入力してから？を押すと、
		ティブ化に使用できるすべての候補が表示されます
		補が 1 つしかない場合に Tab キーを押すと、パック
		名の残りの部分が自動入力されます。
		ヒント パッケージをアクティブ化する際に **test** キーワード
		用すると、稼働中のシステムに影響を与えることな
		コマンドの効果をテストすることができます。アク
		ブ化プロセスが終了したら、**show install log** コマン
		力してプロセスの結果を表示します。

ステップ 6	すべてのパッケージがアクティブ化されるまで手順 5 を繰り返します。	必要に応じて他のパッケージもアクティブ化します。
ステップ 7	**show install active** 例： `switch# show install active`	（任意） すべてのアクティブなパッケージを表示します。このコマン 用して、正しいパッケージがアクティブであるかどうかを判 す。

アクティブなパッケージ セットのコミット

SMUパッケージがデバイス上でアクティブになると、それは現在の実行コンフィギュレーションの一部になります。パッケージのアクティブ化をシステム全体のリロード間で持続させるには、デバイス上でパッケージをコミットする必要があります。

SMU のリロードおよび ISSU では、スイッチのリロードまたは ISSU の完了後、パッケージをコミットする必要があります。

（注） 起動時に、デバイスはコミットされたパッケージ セットをロードします。現在のアクティブなパッケージがコミットされる前にシステムがリロードされると、以前にコミットされたパッケージ セットが使用されます。

はじめる前に

パッケージ セットをコミットする前に、デバイスが正常に動作し、想定どおりにパットを転送していることを検証します。

パッケージの追加とアクティブ化, （512 ページ） に記載されている手順を完了します。

手順

	コマンドまたはアクション	目的
ステップ 1	**install commit***filename* 例： `switch# install commit n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin`	現在のパッケージのセットをコミットして、デバイスが再起動したときにこれらのパッケージが使用されるようにします。
ステップ 2	**show install committed** 例： `switch# show install committed`	（任意） コミットされたパッケージを表示します。

次に、デバイス上でアクティブなSMUパッケージをコミットして、次にコミットされたパッケージを確認する例を示します。

```
switch#  install commit n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin
Install operation 2 completed successfully at Thu Jan 9 01:20:46 2014

switch# show install committed
Boot Images:
      Kickstart Image: bootflash:/n7700-s2-kickstart.7.2.0.D1.1.bin
      System Image: bootflash:/ n7700-s2-dk9.7.2.0.D1.1.bin

Committed Packages:
      n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin
```

パッケージの非アクティブ化と削除

パッケージを非アクティブ化すると、そのデバイスではアクティブではなくなりますが、パッケージ ファイルはブート ディスクに残ります。パッケージ ファイルは、後で再アクティブ化できます。また、ディスクから削除もできます。

Cisco NX-OS ソフトウェアでは、選択されたパッケージ セットを前に保存されたパッケージ セットにロールバックする柔軟性も提供されます。現在アクティブなパッケージ セットよりも以前の

パッケージ セットの方が好ましい場合は、**install deactivate** および **install commit** コマンドを使用して、現在のパッケージを非アクティブ化し、install active および install commit コマンドを使用して、以前のパッケージをアクティブ化できます。

はじめる前に

別のアクティブなパッケージに必要なパッケージを非アクティブ化することはできません。パッケージを非アクティブ化しようとすると、システムがそのパッケージが他のアクティブなパッケージによって必要とされていないかを自動的にチェックします。非アクティブ化を実行するのは、すべての互換性が確認できた場合だけです。

デバイスの実行中のソフトウェアまたはコミットされたソフトウェアの一部であるパッケージは削除できません。

手順

	コマンドまたはアクション	目的
ステップ 1	コンソール ポートに接続して、ログインします。	コンソール ポートにCLI管理セッションを確立します。
ステップ 2	**install deactivate***filename* **例**： `switch# install deactivate n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin`	デバイスに追加されたパッケージを非アクティブ化し、ライン カードのパッケージ機能をオフにします。 **（注）** パッケージ名を部分的に入力してから?を押すと、非アクティブ化に使用できるすべての候補が表示されます。候補が 1 つしかない場合に Tab キーを押すと、パッケージ名の残りの部分が自動入力されます。
ステップ 3	**show install inactive** **例**： `switch# show install inactive`	（任意） デバイス上の非アクティブなパッケージを表示します。
ステップ 4	**install commit** **例**： `switch# install commit`	（任意） 現在のパッケージのセットをコミットして、デバイスが再起動したときにこれらのパッケージが使用されるようにします。 **（注）** パッケージを削除できるのは、非アクティブ化操作がコミットされた場合だけです。

ステップ 5	**install remove** {*filename* | **inactive**}
	
	例：
	`switch# install remove n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin`
	`Proceed with removing n7700-s2-`
		（任意）
		非アクティブなパッケージを削除します。
		• 削除できるのは非アクティブなパッケージだけです。

	コマンドまたはアクション	目的
	dk9.7.2.0.D1.1.CSCuo07721.bin? (y/n)? [n] y 例： switch# install remove inactive Proceed with removing? (y/n)? [n] y	• パッケージは、デバイスのすべてのライン カードから非アクティブにされた場合にのみ削除できます。 • パッケージの非アクティブ化はコミットする必要があります。 • ストレージ デバイスから特定の非アクティブなパッケージを削除するには、**install remove** コマンドに*filename* 引数を指定して使用します。 • システムのすべてのノードから非アクティブなパッケージをすべて削除するには、**install remove** コマンドと **inactive** キーワードを使用します。

次に、パッケージを非アクティブ化し、変更内容をコミットし、デバイスから非アクティブなパッケージを削除する例を示します。

```
switch# install deactivate n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin
Install operation 3 completed successfully at Thu Jan 9 01:20:36 2014

switch# show install inactive
Inactive Packages: n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin

switch# install commit
Install operation 4 completed successfully at Thu Jan 9 01:20:46 2014

switch# install remove n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin
Proceed with removing n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin? (y/n)? [n] y
Install operation 5 completed successfully at Thu Jan 9 01:20:57 2014
```

インストール ログ情報の表示

インストール ログは、インストール動作の履歴についての情報を提供します。インストール動作が実行されるたびに、その動作に対して番号が割り当てられます。

- **show install log** コマンドを使用して、インストール動作の成功および失敗の両方について情報を表示します。
- 引数を指定しない **show install log** コマンドを使用して、すべてのインストール動作のサマリーを表示します。ある動作に固有の情報を表示するには、*request-id* 引数を指定します。ファイルの変更、リロードできなかったノード、その他プロセスに影響する操作など、特定の操作の詳細を表示するには、**detail** キーワードを使用します。

次に、すべてのインストール要求の情報を表示する例を示します。

```
switch# show install log
Thu Jan 9 01:26:09 2014
Install operation 1 by user 'admin' at Thu Jan 9 01:19:19 2014
Install add bootflash: n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin
Install operation 1 completed successfully at Thu Jan 9 01:19:24 2014
----------------------------------------
Install operation 2 by user 'admin' at Thu Jan 9 01:19:29 2014
Install activate n7700-s2-dk9.7.2.0.D1.1.bin
Install operation 2 completed successfully at Thu Jan 9 01:19:45 2014
----------------------------------------
Install operation 3 by user 'admin' at Thu Jan 9 01:20:05 2014
Install commit n7700-s2- dk9.7.2.0.D1.1.bin
Install operation 3 completed successfully at Thu Jan 9 01:20:08 2014
----------------------------------------
Install operation 4 by user 'admin' at Thu Jan 9 01:20:21 2014
Install deactivate n7700-s2-dk9.7.2.0.D1.1.bin
Install operation 4 completed successfully at Thu Jan 9 01:20:36 2014
----------------------------------------
Install operation 5 by user 'admin' at Thu Jan 9 01:20:43 2014
Install commit n7700-s2-dk9.7.2.0.D1.1.bin
Install operation 5 completed successfully at Thu Jan 9 01:20:46 2014
----------------------------------------
Install operation 6 by user 'admin' at Thu Jan 9 01:20:55 2014
Install remove n7700-s2-dk9.7.2.0.D1.1.bin
Install operation 6 completed successfully at Thu Jan 9 01:20:57 2014
----------------------------------------
Install operation 7 by user 'admin' at Thu Jan 9 01:21:07 2014
Install remove
Install operation 7 completed successfully at Thu Jan 9 01:21:10 201
```

次に、ノードやプロセスへの影響を含む追加情報を表示する例を示します。

```
switch# show install log detail
Thu Jan 9 01:24:03 2014
Install operation 1 by user 'admin' at Thu Jan 9 01:19:19 2014
Installer started downloading the package: / n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin
via bootflash
Install add bootflash: n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin
Copying file at Thu Jan 9 01:19:20 2014
Download success, 238545 bytes received
Verifying package
Checking MD5 at Thu Jan 9 01:19:21 2014
MD5 checksum OK
Checking HW platform at Thu Jan 9 01:19:22 2014
Checking SW platform at Thu Jan 9 01:19:23 2014
Package verified successfully
Sending patch file to plugin manager at Thu Jan 9 01:19:23 2014
The following package is now available to be activated: n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin

Install operation 1 completed successfully at Thu Jan 9 01:19:24 2014
----------------------------------------
Install operation 2 by user 'admin' at Thu Jan 9 01:19:29 2014
Install activate n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin
Install activate action started
The software will be activated with process restart
2 processes affected
sysinfo (modified)
vman (modified)
Install operation 2 completed successfully at Thu Jan 9 01:19:45 2014
----------------------------------------
Install operation 3 by user 'admin' at Thu Jan 9 01:20:05 2014
Install commit n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin
MD5 checksum OK for patch: n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin
Install operation 3 completed successfully at Thu Jan 9 01:20:08 2014
----------------------------------------
Install operation 4 by user 'admin' at Thu Jan 9 01:20:21 2014
Install deactivate n7700-s2-dk9.7.2.0.D1.1.bin
Install deactivate action started
The software will be deactivated with process restart
2 processes affected
```

```
sysinfo (modified)
vman (modified)
Install operation 4 completed successfully at Thu Jan 9 01:20:36 2014
----------------------------------------
Install operation 5 by user 'admin' at Thu Jan 9 01:20:43 2014
Install commit n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin
MD5 checksum OK for patch: n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin
Install operation 5 completed successfully at Thu Jan 9 01:20:46 2014
----------------------------------------
Install operation 6 by user 'admin' at Thu Jan 9 01:20:55 2014
Install remove n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin
Install operation 6 completed successfully at Thu Jan 9 01:20:57 2014
----------------------------------------
Install operation 7 by user 'admin' at Thu Jan 9 01:21:07 2014
Install remove
Install operation 7 completed successfully at Thu Jan 9 01:21:10 2014
```

次に、SMU パッケージが起動した後、スイッチがリロードされる前の出力の例を示します。

```
switch# show install log detail
Install operation 18 by user 'admin' at Sun Mar 9 00:42:10 2014
Install activate n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin
Install activate action started
The software will be activated with system reload
Install operation 18 !!WARNING!!
This patch will get activated only after a reload of the switch. at Sun Mar 9 00:42:12 2014
```

次の例では、特定の SMU の詳細を示します。

```
switch# show install package
Boot Images:
     Kickstart Image: bootflash:/ n7700-s2-kickstart.7.2.0.D1.1.bin
     System Image: bootflash:/ n7700-s2-dk9.7.2.0.D1.1.bin
------------------------------------------------------------------
n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin              Active Committed

Modules

       Module #3: Active Committed

       Module #4: Active Committed

n7700-s2-dk9.7.2.0.D1.1.CSCuo07721.bin              Inactive

Modules

       Module #3: Inactive

       Module #4: Inactive
```

次の作業

制御ポリシーの設定の詳細については、「Configuring ISG Control Policies」モジュールを参照してください。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
ソフトウェア アップグレード	『*Cisco Nexus 7000 Series NX-OS Software Upgrade and Downgrade Guide*』
システム管理コマンド	『*System Management Command Reference*』

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

関連資料

関連項目	マニュアル タイトル
ソフトウェア アップグレード	『*Cisco Nexus 7000 Series NX-OS Software Upgrade and Downgrade Guide*』

ソフトウェアメンテナンスアップグレードを実行するための機能情報

次の表に、このソフトウェアでサポートされる SMU パッケージ ファイルのリリース情報を示します。次の表には、特定の SMU パッケージのサポートが導入されているソフトウェア リリースだけを示します。特に明記されていない限り、記載のソフトウェアの後続のリリースでも SMU パッケージをサポートします。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、http://www.cisco.com/go/cfnに進みます。Cisco.com のアカウントは必要ありません。

SMU パッケージ ファイル	リリース	説明
n7000-s2-dk9.7.2.0.D1.1.CSCuo07721.bin	7.2(0)	再起動タイプ：再起動 プラットフォーム：Nexus7700 置き換え：なし 被置き換え：なし 再起動情報：*CSCuo07721* アクティブ化スクリプトのプリインストール：なし アクティブ化スクリプトのポストインストール：なし 非アクティブ化スクリプトのプリインストール：なし 非アクティブ化スクリプトのポストインストール：なし

第 25 章

CLIコマンドのネットワーク設定形式への変換

この章では、CLI コマンドを Network Configuration Protocol（NETCONF）に変換するために XMLIN ツールをインストールして使用する方法について説明します。

- 機能情報の確認，523 ページ
- XMLIN について，524 ページ
- XMLIN のライセンス要件，524 ページ
- XMLIN ツールのインストールおよび使用，524 ページ
- show コマンド出力の XML への変換，525 ページ
- XMLIN の設定例，526 ページ
- 関連資料，528 ページ
- XMLIN の機能の履歴，528 ページ

機能情報の確認

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

XMLIN について

XMLIN ツールは、CLI コマンドをネットワーク設定（NETCONF）プロトコル形式に変換します。NETCONF は、ネットワーク デバイスの設定をインストール、処理、削除する機能を提供するネットワーク管理プロトコルです。これは、設定データとプロトコル メッセージに XML ベースのエンコーディングを使用します。NETCONF プロトコルの NX-OS 実装は、<get>、<edit-config>、<close-session>、<kill-session>、および <exec-command> のプロトコル操作をサポートします。

XMLIN ツールは、show、EXEC、およびコンフィギュレーション コマンドを対応する NETCONF <get>、<exec-command>、および<edit-config> リクエストに変換します。複数のコンフィギュレーション コマンドを単一の NETCONF <edit-config> インスタンスにまとめることができます。

XMLIN ツールはまた、show コマンドの出力を XML 形式に変換します。

XMLIN のライセンス要件

表 *45* : ***XMLIN*** のライセンス要件

製品	ライセンス要件
Cisco NX-OS	XMLIN にはライセンスは必要ありません。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。NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

XMLIN ツールのインストールおよび使用

XMLIN ツールをインストールして、コンフィギュレーション コマンドを NETCONF 形式に変換するために使用できます。

はじめる前に

XMLIN ツールは通常、対応する機能セットまたは必要なハードウェア機能がデバイス上で使用できない場合でもコマンドの NETCONF インスタンスを生成できますが、**xmlin** コマンドを入力する前に機能セットの一部をインストールする必要がある場合があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **xmlin**	
ステップ 2	switch(xmlin)# **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 3	コンフィギュレーション コマンド	コンフィギュレーション コマンドを NETCONF 形式に変換します。
ステップ 4	switch(config)(xmlin)# **end**	（任意） 対応する <edit-config> 要求を生成します。 （注） **show** コマンドに対して XML インスタンスを生成する前に、**end** コマンドを入力して現在の XML 設定を終了する必要があります。
ステップ 5	switch(config-if-verify)(xmlin)# **show***commands*	（任意） **show** コマンドを NETCONF 形式に変換します。
ステップ 6	switch(config-if-verify)(xmlin)# **exit**	（任意） EXEC モードに戻ります。

show コマンド出力の XML への変換

show コマンドの出力を XML に変換できます。

はじめる前に

変換するコマンドのすべての機能がインストールされ、デバイス上で有効になっていることを確認します。そうしない場合、コマンドは失敗します。

terminal verify-only コマンドを使用すると、デバイスに入力しなくても機能が有効になっていることを確認できます。

コマンドに対するすべての必須ハードウェアがデバイス上に存在することを確認します。そうしない場合、コマンドは失敗します。

XMLIN ツールがインストールされていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# *show-command* | **xmlin**	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。 （注） コンフィギュレーション コマンドと一緒にこのコマンドを使用することはできません。

XMLIN の設定例

次の例は、XMLINツールがデバイス上にどのようにインストールされ、一連のコンフィギュレーション コマンドを <edit-config> インスタンスに変換するためにどのように使用されるかを示しています。

```
switch# xmlin
****************************************
Loading the xmlin tool. Please be patient.
****************************************
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright ©) 2002-2013, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php

switch(xmlin)# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)(xmlin)# interface ethernet 2/1
% Success
switch(config-if-verify)(xmlin)# cdp enable
% Success
switch(config-if-verify)(xmlin)# end
<?xml version="1.0"?>
<nf:rpc xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns="http://www.cisco.com/nxos:6.2.2.:configure_"
xmlns:m="http://www.cisco.com/nxos:6.2.2.:_exec"
xmlns:m1="http://www.cisco.com/nxos:6.2.2.:configure__if-eth-base" message-id="1">
  <nf:edit-config>
     <nf:target>
      <nf:running/>
  </nf:target>
  <nf:config>
    <m:configure>
      <m:terminal>
        <interface>
           <__XML__PARAM__interface>
             <__XML__value>Ethernet2/1</__XML__value>
             <m1:cdp>
               <m1:enable/>
             </m1:cdp>
```

```
            </__XML__PARAM__interface>
           </interface>
          </m:terminal>
         </m:configure>
        </nf:config>
       </nf:edit-config>
      </nf:rpc>
     ]]>]]>
```

次の例は、**show** コマンドに対して XML インスタンスを生成する前に現在の XML 設定を終了するために **end** コマンドを入力する必要があることを示しています。

```
switch(xmlin)# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)(xmlin)# interface ethernet 2/1
switch(config-if-verify)(xmlin)# show interface ethernet 2/1
****************************************************
Please type "end" to finish and output the current XML document before building a new one.
****************************************************
% Command not successful

switch(config-if-verify)(xmlin)# end
<?xml version="1.0"?>
<nf:rpc xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns="http://www.cisco.com/nxos:6.2.2.:configure_"
xmlns:m="http://www.cisco.com/nxos:6.2.2.:_exec" message-id="1">
    <nf:edit-config>
      <nf:target>
         <nf:running/>
      </nf:target>
      <nf:config>
         <m:configure>
           <m:terminal>
              <interface>
                 <__XML__PARAM__interface>
                    <__XML__value>Ethernet2/1</__XML__value>
                 </__XML__PARAM__interface>
              </interface>
           </m:terminal>
           </m:configure>
         </nf:config>
      </nf:edit-config>
    </nf:rpc>
   ]]>]]>

switch(xmlin)# show interface ethernet 2/1
<?xml version="1.0"?>
<nf:rpc xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns="http://www.cisco.com/nxos:6.2.2.:if_manager" message-id="1">
  <nf:get>
    <nf:filter type="subtree">
      <show>
      <interface>
        <__XML__PARAM__ifeth>
          <__XML__value>Ethernet2/1</__XML__value>
        </__XML__PARAM__ifeth>
      </interface>
     </show>
   </nf:filter>
  </nf:get>
</nf:rpc>
]]>]]>
switch(xmlin)# exit
switch#
```

次の例は、**show interface brief** コマンドの出力を XML に変換する方法を示しています。

```
switch# show interface brief | xmlin
<?xml version="1.0"?>
<nf:rpc xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns="http://www.cisco.com/nxos:6.2.2.:if_manager"
```

```
message-id="1">
  <nf:get>
    <nf:filter type="subtree">
       <show>
          <interface>
              <brief/>
          </interface>
       </show>
     </nf:filter>
   </nf:get>
</nf:rpc>
]]>]]>
```

関連資料

関連項目	マニュアル タイトル
XMLIN コマンド：コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト設定、使用上のガイドライン、および例	『*Cisco Nexus 7000 Series NX-OS System Management Command Reference*』

XMLIN の機能の履歴

次の表に、このマニュアルの新機能および変更された機能を要約し、各機能がサポートされているリリースを示します。ご使用のソフトウェア リリースで、本書で説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。

表 *46*：*XMLIN* の機能の履歴

機能名	リリース	機能情報
XMLIN	6.2(2)	この機能が導入されました。

付 録 A

Cisco NX-OS システム管理でサポートされている IETF RFC

Cisco NX-OS でサポートされているシステム管理に関する IETF RFC は次のとおりです。

- Cisco NX-OS システム管理でサポートされている IETF RFC, 529 ページ

Cisco NX-OS システム管理でサポートされている IETF RFC

Cisco NX-OS でサポートされているシステム管理に関する IETF RFC は次のとおりです。

RFC	タイトル
RFC 2819	『*Remote Network Monitoring Management Information Base*』
RFC 3164	『*The BSD syslog Protocol*』
RFC 3411 および RFC 3418	『*An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks*』
RFC 3954	『*Cisco Systems NetFlow Services Export Version 9*』

Cisco NX-OS システム管理でサポートされている IETF RFC

付 録 B

Embedded Event Manager システム イベントおよびコンフィギュレーション例

この付録では、Embedded Event Manager（EEM）システム ポリシー、イベント、およびポリシーのコンフィギュレーション例について説明します。

この付録は、次の項で構成されています。

- EEM システム ポリシー，531 ページ
- EEM イベント，534 ページ
- EEM ポリシーのコンフィギュレーション例，536 ページ

EEM システム ポリシー

次の表に、Embedded Event Manager（EEM）のシステム ポリシーを示します。

イベント	説明
__PortLoopback	CallHome を実行し、Syslog、OBFL、または例外ログにエラーを記録し、GOLD "PortLoopback" テストに 10 回連続で失敗した場合は、その後影響を受けたポートでの HM テストをディセーブルにします。
__RewriteEngineLoopback	CallHome を実行し、Syslog、OBFL、または例外ログにエラーを記録し、GOLD "RewriteEngine" テストに 10 回連続で失敗した場合は、その後影響を受けたポートでの HM テストをディセーブルにします。

イベント	説明
__asic_register_check	CallHome を実行し、エラーを記録し、GOLD "ASICRegisterCheck" テストに 20 回連続で失敗した場合は、その後その ASIC デバイスおよびインスタンスの HM テストをディセーブルにします。
__compact_flash	CallHome を実行し、エラーを記録し、GOLD "CompactFlash" テストに 20 回連続で失敗した場合は、その後 HM テストをディセーブルにします。
__crypto_device	CallHome を実行し、GOLD "CryptoDevice" テストに失敗するとエラーを記録します。
__eobc_port_loopback	CallHome を実行し、GOLD "EOBCPortLoopback" テストに失敗するとエラーを記録します。
__ethpm_debug_1	アクション：なし
__ethpm_debug_2	アクション：なし
__ethpm_debug_3	アクション：なし
__ethpm_debug_4	アクション：なし
__ethpm_link_flap	420 秒間隔でリンク フラップが 30 を超えています。アクション：エラー。ポートをディセーブルにします。
__external_compact_flash	CallHome を実行し、エラーを記録し、GOLD "ExternalCompactFlash" テストに 20 回連続で失敗した場合は、その後 HM テストをディセーブルにします。
__lcm_module_failure	2 度電源を切って入れ直し、電源を切ります。
__management_port_loopback	CallHome を実行し、GOLD "ManagementPortLoopback" テストに失敗するとエラーを記録します。
__nvram	CallHome を実行し、エラーを記録し、GOLD "NVRAM" テストに 20 回連続で失敗した場合は、その後 HM テストをディセーブルにします。

イベント	説明
__pfm_fanabsent_all_systemfan	両方のファン トレイ（f1 と f2）が 2 分間存在しない場合は、シャットダウンします。
__pfm_fanbad_all_systemfan	ファンで障害が発生した場合シスログに記録します。
__pfm_fanbad_any_singlefan	ファンで障害が発生した場合シスログに記録します。
__pfm_power_over_budget	不十分な電力超過バジェットに対するシスログ警告
__pfm_tempev_major	TempSensor メジャーしきい値アクション：シャットダウン
__pfm_tempev_minor	TempSensorマイナーしきい値アクション：シスログ
__primary_bootrom	CallHome を実行し、エラーを記録し、GOLD "PrimaryBootROM" テストに 20 回連続で失敗した場合は、その後 HM テストをディセーブルにします。
__pwr_mgmt_bus	CallHome を実行し、エラーを記録し、GOLD "PwrMgmtBus" テストに 20 回連続で失敗した場合は、モジュールまたはスパインカードの HM テストをディセーブルにします。
__real_time_clock	CallHome を実行し、エラーを記録し、GOLD "RealTimeClock" テストに 20 回連続で失敗した場合は、その後 HM テストをディセーブルにします。
__secondary_bootrom	CallHome を実行し、エラーを記録し、GOLD "SecondaryBootROM" テストに 20 回連続で失敗した場合は、その後 HM テストをディセーブルにします。
__spine_control_bus	CallHome を実行し、エラーを記録し、GOLD "SpineControlBus" テストに 20 回連続で失敗した場合は、そのモジュールまたはスパインカードの HM テストをディセーブルにします。

イベント	説明
__standby_fabric_loopback	CallHome を実行し、エラーを記録し、10 回連続で失敗した場合は、その後 HM テストをディセーブルにします。
__status_bus	CallHome を実行し、エラーを記録し、GOLD "StatusBus" テストに 5 回連続で失敗した場合は、その後 HM テストをディセーブルにします。
__system_mgmt_bus	CallHome を実行し、エラーを記録し、GOLD "SystemMgmtBus" テストに 20 回連続で失敗した場合は、そのファンまたは電源の HM テストをディセーブルにします。
__usb	CallHome を実行し、GOLD "USB" テストに失敗するとエラーを記録します。

EEM イベント

次の表は、デバイスで使用できる EEM イベントについて説明します。

EEM イベント	説明
アプリケーション	アプリケーション固有のイベントをパブリッシュします。
cli	ワイルドカードを使用したパターンを照合する CLI コマンドが入力されます。
counter	EEM カウンタが指定された値または範囲に達します。
fanabsent	システム ファン トレイがありません。
fanbad	システム ファンで障害が生成されます。
fib	ユニキャスト FIB のルートまたは TCAM の使用状況をモニタします。
Gold	GOLD テスト失敗条件がヒットします。

EEM イベント	説明
interface	インターフェイス カウンタがしきい値を超えます。
メモリ	使用可能なシステム メモリがしきい値を超えます。
module	指定したモジュールが、選択したステータスになります。
module-failure	モジュール障害が生成されます。
none	指定されたイベントがないポリシー イベントを実行します。
oir	活性挿抜が発生します。
policy-default	デフォルトのパラメータおよびしきい値が、上書きするシステム ポリシーのイベントに使用されます。
poweroverbudget	プラットフォーム ソフトウェアが電力バジェット条件を検出します。
snmp	SNMP オブジェクト ID（OID）の状態が変化します。
storm-control	プラットフォーム ソフトウェアがイーサネット パケット ストーム条件を検出します。
syslog	syslog メッセージを監視し、ポリシーの検索文字列に基づいてポリシーを呼び出します。
sysmgr	システム マネージャがイベントを生成します。
temperature	システムの温度レベルがしきい値を超えます。
timer	指定された時間に到達します。
track	トラッキング対象オブジェクトの状態が変化します。

EEM ポリシーのコンフィギュレーション例

CLI イベントのコンフィギュレーション例

インターフェイス シャットダウンのモニタリング

インターフェイスのシャットダウンをモニタする例を示します。

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# event manager applet monitorShutdown
switch(config-applet)#
switch(config-applet)# description "Monitors interface shutdown."
switch(config-applet)# event cli match "conf t; interface *; shutdown"
switch(config-applet)# action 1.0 cli show interface e 3/1
switch(config)# copy running-config startup-config
```

（注） EEM ポリシーの一部として入力された **show** コマンドの出力は、「eem_archive_」というプレフィックスが付加されたテキスト ファイルとして logflash にアーカイブされます。アーカイブされている出力を表示するには、**show file logflash:eem_archive_***n* コマンドを使用します。

モジュール パワーダウンのモニタリング

モジュールのパワーダウンをモニタする例を示します。

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# event manager applet monitorPoweroff
switch(config-applet)#
switch(config-applet)# description "Monitors module power down."
switch(config-applet)# event cli match "conf t ; poweroff *"
switch(config-applet)# action 1.0 cli show module
switch(config)# copy running-config startup-config
```

ロールバックを開始するトリガーの追加

ロールバックを開始するトリガーを追加する例を示します。

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)#
switch(config)# event manager applet rollbackTrigger
switch(config-applet)#
switch(config-applet)# description "Rollback trigger."
switch(config-applet)# event cli match "rollback *"
switch(config-applet)# action 1.0 cli copy running-config bootflash:last_config
switch(config)# copy running-config startup-config
```

メジャーしきい値を上書き（ディセーブル）するコンフィギュレーション例

メジャーしきい値に達したときにシャットダウンを防ぐ方法

メジャーしきい値に達したことによるシャットダウンを防ぐ例を示します。

```
switch# configure terminal
switch(config)# event manager applet myappletname override __pfm_tempev_major
switch(config)# end
```

デフォルト コンフィギュレーションに戻す例を示します。

```
switch# configure terminal
switch(config)# no event manager applet myappletname override __pfm_tempev_major
switch(config)# end
```

1 つの不良センサーをディセーブルにする方法

センサー 3 で障害が発生した場合（他のセンサーに影響なし）に、モジュール 2 でセンサー 3 だけをディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# event manager applet myappletname override __pfm_tempev_major
switch(config-applet)# event temperature module 2 sensor 3 threshold major
switch(config-applet)# end
```

デフォルト コンフィギュレーションに戻す例を示します。

```
switch# configure terminal
switch(config)# no event manager applet myappletname override __pfm_tempev_major
switch(config)# end
```

複数の不良センサーをディセーブルにする方法

モジュール 2 のセンサー 5、6、7 で障害が発生した場合（他のセンサーに影響なし）に、これらのセンサーをディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# event manager applet myappletname override __pfm_tempev_major
switch(config-applet)# event temperature module 2 sensor 5 threshold major
switch(config-applet)# end
switch# configure terminal
switch(config)# event manager applet myappletname override __pfm_tempev_major
switch(config-applet)# event temperature module 2 sensor 6 threshold major
switch(config-applet)# end
switch# configure terminal
switch(config)# event manager applet myappletname override __pfm_tempev_major
switch(config-applet)# event temperature module 2 sensor 7 threshold major
switch(config-applet)# end
```

デフォルト コンフィギュレーションに戻す例を示します。

```
switch# configure terminal
switch(config)# no event manager applet myappletname override __pfm_tempev_major
```

```
switch(config)# end
```

モジュール全体の上書き（ディセーブル）

誤動作するモジュール 2 をディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# event manager applet myappletname override __pfm_tempev_major
switch(config-applet)# event temperature module 2 threshold major
switch(config-applet)# end
```

デフォルト コンフィギュレーションに戻す例を示します。

```
switch# configure terminal
switch(config)# no event manager applet myappletname override __pfm_tempev_major
switch(config)# end
```

複数のモジュールおよびセンサーの上書き（ディセーブル）

誤動作するモジュール 2 のセンサー 3、4、7 とモジュール 3 のすべてのセンサーをディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# event manager applet myappletname override __pfm_tempev_major
switch(config-applet)# event temperature module 2 sensor 3 threshold major
switch(config-applet)# end
switch# configure terminal
switch(config)# event manager applet myappletname override __pfm_tempev_major
switch(config-applet)# event temperature module 2 sensor 4 threshold major
switch(config-applet)# end
switch# configure terminal
switch(config)# event manager applet myappletname override __pfm_tempev_major
switch(config-applet)# event temperature module 2 sensor 7 threshold major
switch(config-applet)# end
switch# configure terminal
switch(config)# event manager applet myappletname override __pfm_tempev_major
switch(config-applet)# event temperature module 3 threshold major
switch(config-applet)# end
```

デフォルト コンフィギュレーションに戻す例を示します。

```
switch# configure terminal
switch(config)# no event manager applet myappletname override __pfm_tempev_major
switch(config)# end
```

1 つのセンサーをイネーブルにして、すべてのモジュールの残りのセンサーをすべてディセーブルにする方法

モジュール 9 のセンサー 4 を除くすべてのモジュールのすべてのセンサーをディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# event manager applet myapplet1 override __pfm_tempev_major
switch(config-applet)# end
switch# configure terminal
switch(config)# event manager applet myapplet2 override __pfm_tempev_major
switch(config-applet)# event temperature module 9 sensor 4 threshold major
switch(config-applet)# action 2 policy-default
```

```
switch(config-applet)# end
```

複数のセンサーをイネーブルにして、すべてのモジュールの残りのセンサーをすべてディセーブルにする方法

モジュール 9 のセンサー 4、6、7 を除くすべてのモジュールのすべてのセンサーをディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# event manager applet myapplet1 override __pfm_tempev_major
switch(config-applet)# end
switch# configure terminal
switch(config)# event manager applet myapplet2 override __pfm_tempev_major
switch(config-applet)# event temperature module 9 sensor 4 threshold major
switch(config-applet)# action 2 policy-default
switch(config-applet)# end
switch# configure terminal
switch(config)# event manager applet myapplet3 override __pfm_tempev_major
switch(config-applet)# event temperature module 9 sensor 6 threshold major
switch(config-applet)# action 3 policy-default
switch(config-applet)# end
switch# configure terminal
switch(config)# event manager applet myapplet4 override __pfm_tempev_major
switch(config-applet)# event temperature module 9 sensor 7 threshold major
switch(config-applet)# action 4 policy-default
switch(config-applet)# end
```

1 つのモジュールのすべてのセンサーをイネーブルにして、残りのモジュールのすべてのセンサーをディセーブルにする方法

モジュール 9 のすべてのセンサーを除く残りのモジュールのすべてのセンサーをディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# event manager applet myapplet1 override __pfm_tempev_major
switch(config-applet)# end
switch# configure terminal
switch(config)# event manager applet myapplet2 override __pfm_tempev_major
switch(config-applet)# event temperature module 9 threshold major
switch(config-applet)# action 2 policy-default
switch(config-applet)# end
```

モジュールのセンサーを組み合わせてイネーブルにして、残りのモジュールのすべてのセンサーをディセーブルにする方法

モジュール 2 の センサー 3、4、7 とモジュール 3 のすべてのセンサーを除くすべてのモジュールのすべてのセンサーをディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# event manager applet myapplet1 override __pfm_tempev_major
switch(config-applet)# end
switch# configure terminal
switch(config)# event manager applet myapplet2 override __pfm_tempev_major
switch(config-applet)# event temperature module 2 sensor 3 threshold major
switch(config-applet)# action 2 policy-default
switch(config-applet)# end
switch# configure terminal
```

```
switch(config)# event manager applet myapplet3 override __pfm_tempev_major
switch(config-applet)# event temperature module 2 sensor 4 threshold major
switch(config-applet)# action 3 policy-default
switch(config-applet)# end
switch# configure terminal
switch(config)# event manager applet myapplet4 override __pfm_tempev_major
switch(config-applet)# event temperature module 2 sensor 7 threshold major
switch(config-applet)# action 4 policy-default
switch(config-applet)# end
switch# configure terminal
switch(config)# event manager applet myapplet5 override __pfm_tempev_major
switch(config-applet)# event temperature module 3 threshold major
switch(config-applet)# action 5 policy-default
switch(config-applet)# end
```

ファントレイ取り外しのためのシャットダウンを上書き（ディセーブル）するコンフィギュレーション例

1つまたは複数のファントレイを取り外すためのシャットダウンの上書き（ディセーブル）

1つまたは複数（またはすべて）のファン トレイを取り外せるように、シャットダウンをディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# event manager applet myappletname override __pfm_fanabsent_any_singlefan
switch(config-applet)# end
```

デフォルト コンフィギュレーションに戻す例を示します。

```
switch# configure terminal
switch(config)# no event manager applet myappletname override __pfm_fanabsent_any_singlefan
switch(config-applet)# end
```

指定したファントレイを取り外すためのシャットダウンの上書き（ディセーブル）

指定したファン トレイ（ファン トレイ 3）を取り外せるように、シャットダウンをディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# event manager applet myappletname override __pfm_fanabsent_any_singlefan
switch(config-applet)# event fanabsent fan 3 time 60
switch(config-applet)# end
```

デフォルト コンフィギュレーションに戻す例を示します。

```
switch# configure terminal
switch(config) no event manager applet myappletname override __pfm_fanabsent_any_singlefan
switch(config)# end
```

指定した複数のファントレイを取り外すためのシャットダウンの上書き（ディセーブル）

指定した複数のファン トレイ（ファン トレイ 2、3、4）を取り外せるように、シャットダウンをディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# event manager applet myapplet1 override __pfm_fanabsent_any_singlefan
switch(config-applet)# event fanabsent fan 2 time 60
switch(config-applet)# end
switch# configure terminal
switch(config)# event manager applet myapplet2 override __pfm_fanabsent_any_singlefan
switch(config-applet)# event fanabsent fan 3 time 60
switch(config-applet)# end
switch# configure terminal
switch(config)# event manager applet myapplet3 override __pfm_fanabsent_any_singlefan
switch(config-applet)# event fanabsent fan 4 time 60
switch(config-applet)# end
```

デフォルト コンフィギュレーションに戻す例を示します。

```
switch# configure terminal
switch(config)# no event manager applet myappletname override __pfm_fanabsent_any_singlefan
switch(config)# end
```

1 つを除くすべてのファン トレイを取り外すためのシャットダウンの上書き（ディセーブル）

1台（ファントレイ2）を除くすべてのファントレイを取り外せるように、シャットダウンをディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# event manager applet myapplet1 override __pfm_fanabsent_any_singlefan
switch(config-applet)# end
switch# configure terminal
switch(config)# event manager applet myapplet2 override __pfm_fanabsent_any_singlefan
switch(config-applet)# event fanabsent fan 2 time 60
switch(config-applet)# action 2 policy-default
switch(config-applet)# end
```

ファントレイの指定したセットを除くファントレイを取り外すためのシャットダウンの上書き（ディセーブル）

指定したファン トレイのセット（ファン 2、3、4）を除くファン トレイを取り外せるように、シャットダウンをディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# event manager applet myapplet1 override __pfm_fanabsent_any_singlefan
switch(config-applet)# end
switch(config)# event manager applet myapplet2 override __pfm_fanabsent_any_singlefan
switch(config-applet)# event fanabsent fan 2,3,4 time 60
switch(config-applet)# action 2 policy-default
switch(config-applet)# end
```

ファントレイのセットから1台を除くすべてのファントレイを取り外すためのシャットダウンの上書き（ディセーブル）

指定したファン トレイのセット（ファン トレイ 2、3、4）の 1 台を除くすべてのファン トレイを取り外せるように、シャットダウンをディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# event manager applet myapplet1 override __pfm_fanabsent_any_singlefan
switch(config-applet)# end
switch# configure terminal
switch(config)# event manager applet myapplet2 override __pfm_fanabsent_any_singlefan
switch(config-applet)# event fanabsent fan 2 time 60
switch(config-applet)# action 2 policy-default
switch(config-applet)# end
switch# configure terminal
switch(config)# event manager applet myapplet3 override __pfm_fanabsent_any_singlefan
switch(config-applet)# event fanabsent fan 3 time 60
switch(config-applet)# action 3 policy-default
switch(config-applet)# end
switch# configure terminal
switch(config)# event manager applet myapplet4 override __pfm_fanabsent_any_singlefan
switch(config-applet)# event fanabsent fan 4 time 60
switch(config-applet)# action 4 policy-default
switch(config-applet)# end
```

補足ポリシーを作成するコンフィギュレーション例

ファン トレイが存在しないイベントの補足ポリシーの作成

event fanabsent コマンドを使用して、補足ポリシーを作成する例を示します。

[**no**] **event fanabsent** [**fan***fan-tray-number*] **time***time-interval*

ファン トレイ 1 が 60 秒間存在しない場合に、デフォルトのポリシーに加えて、ポリシー myappletname とアクション 3 を実行する例を示します。

```
switch# configure terminal
switch(config)# event manager applet myappletname
switch(config-applet)# event fanabsent fan 1 time 60
switch(config-applet)# action 3 cli "show env fan"
switch(config-applet)# end
```

温度しきい値イベントの補足ポリシーの作成

event temperature コマンドを使用して、補足ポリシーを作成する例を示します。

[**no**] **event temperature** [**mod***module-number*] [**sensor***sensor-number*] **threshold** {**major** | **minor** | **any**}

モジュール 2 のセンサー 3 で温度がマイナーしきい値を超えた場合に、デフォルトのポリシーに加えて、ポリシー myappletname とアクション 1 を実行する例を示します。

```
switch# configure terminal
switch(config)# event manager applet myappletname
switch(config-applet)# event temperature module 2 sensor 3 threshold minor
switch(config-applet)# action 1 cli "show environ temperature"
switch(config-applet)# end
```

電力のバジェット超過ポリシーのコンフィギュレーション例

電力のバジェット超過ポリシーは、使用可能な電力がゼロ未満に低下し、前に起動されたモジュールを起動状態で維持できなくなった場合に開始します。デフォルトのアクションでは、ユーザに電力のバジェット超過が発生したことを通知する syslog を出力します。

利用可能な電力が赤（負）のゾーンから回復するまでモジュールの電源を落とす追加アクションをイネーブルにできます。

モジュールのシャットダウン

モジュールを指定しない場合、電力のバジェット超過シャットダウンはスロット 1 から始まり、電力が赤（負）のゾーンから回復するまでモジュールをシャットダウンします。空のスロットやスーパーバイザ、スタンバイ スーパーバイザ、スパイン、クロスバーを含むスロットは飛ばされます。

利用可能な電力がゼロ未満に低下した場合に、モジュール 1 からモジュールをシャットダウンする例を示します。

```
switch# configure terminal
switch(config)# event manager applet <myappletname4a> override __pfm_power_over_budget
switch(config-applet)# event poweroverbudget
switch(config-applet)# action 4 overbudgetshut
switch(config-applet)# end
```

指定された一連のモジュールのシャットダウン

電力のバジェット超過アクションによって、電力が赤（負）のゾーンから回復するまでシャットダウンされるモジュールのリストを指定できます。空のスロットやスーパーバイザ、スタンバイ スーパーバイザ、スパイン、クロスバーを含むスロットは飛ばされます。

利用可能な電力がゼロ未満に低下した場合に、指定されたモジュールのリスト（1、2、7、8）からモジュールをシャットダウンする例を示します。

```
switch# configure terminal
switch(config)# event manager applet <myappletname4b> override __pfm_power_over_budget
switch(config-applet)# event poweroverbudget
switch(config-applet)# action 5 overbudgetshut module 1,2,7,8
switch(config-applet)# end
```

シャットダウンするモジュールを選択するコンフィギュレーション例

デフォルトでシャットダウンに非上書きモジュールを選択するポリシーの使用

メジャーしきい値を超えた場合に、デフォルトで非上書きモジュールをシャットダウンするよう選択するポリシーを使用する例を示します。

```
switch# configure terminal
switch(config)# event manager applet my5a1 override __pfm_tempev_major
switch(config-applet)# end
```

```
switch# configure terminal
switch(config)# event manager applet my5a2 override __pfm_tempev_major
switch(config-applet)# event temperature module 1-3 sensor 4 threshold major
switch(config-applet)# action 5 policy-default
switch(config-applet)# end
```

シャットダウンに非上書きモジュールを選択するパラメータ置き換えの使用

メジャーしきい値を超えた場合に、パラメータの置き換えを使用してシャットダウンする非上書きモジュールを選択する例を示します。

```
switch# configure terminal
switch(config)# event manager applet my5b1 override __pfm_tempev_major
switch(config-applet)# end
switch# configure terminal
switch(config)# event manager applet my5b2 override __pfm_tempev_major
switch(config-applet)# event temperature module 1-3 sensor 8 threshold major
switch(config-applet)# action 6 forceshut module my_module_list reset "temperature-sensor
policy trigger"
switch(config-applet)# end
```

イベント マネージャ パラメータを作成するには、**event manager environment** コマンドを使用します。イベント マネージャ パラメータの値を表示するには、**show event manager environment all** コマンドを使用します。

活性挿抜イベントのコンフィギュレーション例

活性挿抜イベント（OIR）には、デフォルトのポリシーがありません。

event oir コマンドを使用して、OIR イベントを設定する例を示します。

event oir*device-typeevent-type* [*device-number*]

device-type は、**fan**、**module** または **powersupply** です。

event-type は、**insert**、**remove**、または **anyoir**（装着または取り外し）です。

オプションの *device-number* では 1 台のデバイスを指定します。省略すると、すべてのデバイスが選択されます。

装着イベントを設定する例を示します。

```
switch# configure terminal
switch(config)# event manager applet myoir
switch(config-applet)# event oir module insert
switch(config-applet)# action 1 syslog priority critical msg "OIR insert event: A Module
is inserted"
```

取り外しイベントを設定する例を示します。

```
switch# configure terminal
switch(config)# event manager applet myoir
switch(config-applet)# event oir module remove
switch(config-applet)# action 1 syslog priority critical msg "OIR remove event: A Module
is removed"
```

ユーザ syslog を生成するコンフィギュレーション例

action syslog コマンドを使用して、ユーザ syslog を生成する例を示します。

```
switch# configure terminal
switch(config)# event manager applet myoir
switch(config-applet)# event oir module remove
switch(config-applet)# action 1 syslog priority critical msg "Module is removed"
```

このイベントが発生すると、次の syslog が生成されます。

```
switch(config)# 2013 May 20 00:08:27 p1b-57 %$ VDC-1 %$ %EEM_ACTION-2-CRIT: "Module is
removed"
```

Syslog メッセージをモニタする設定例

次に、スイッチからの Syslog メッセージをモニタする例を示します。

```
switch(config)# event manager applet a1
switch(config-applet)# event syslog occurs 6 period 4294967 pattern "authentication failed"
```

このイベントがトリガーされると、ポリシーで定義されているアクションが実行されます。

SNMP 通知のコンフィギュレーション例

SNMP OID のポーリングによる EEM イベントの生成

スイッチの CPU 使用率を問い合わせるには、SNMP オブジェクト ID（OID）CISCO-SYSTEM-EXT-MIB::cseSysCPUUtilization が使用されます。

```
cseSysCPUUtilization OBJECT-TYPE
SYNTAX Gauge32 (0..100 )
UNITS "%"
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The average utilization of CPU on the active supervisor."
::= { ciscoSysInfoGroup 1 }
```

10 秒間隔でポーリングされ、しきい値が 95 % の SNMP OID を使用する例を示します。

```
switch# configure terminal
switch(config)# event manager applet test_policy
switch(config-applet)# event snmp oid 1.3.6.1.4.1.9.9.305.1.1.1.0 get-type exact entry-op
gt entry-val 95 exit-op lt exit-val 90 poll-interval 10
```

イベント ポリシーのイベントへの応答で SNMP 通知を送信

このタイプのコンフィギュレーションを使用して、重大なイベント トリガーで SNMP 通知を生成できます。

イベント マネージャのアプレット コンフィギュレーション モードからイベントに対して SNMP 通知を送信する例を示します。

```
switch(config-applet)# action 1.1 snmp-trap intdata1 100 intdata2 300 strdata "CPU Hogging
 at switch1"
switch(config-applet)# action 1.1 snmp-trap intdata1 100 intdata2 300 strdata "Port Failure
 eth9/1"
```

このコンフィギュレーションでは、スイッチから SNMP ホストに SNMP 通知（トラップ）を行います。SNMP ペイロードには、ユーザ定義フィールド intdata1、intdata2、および strdata の値が含まれます。

ポート トラッキングのコンフィギュレーション例

1 つのポートの状態を別のポートの状態と一致させるように設定する例を示します（ポート トラッキング）。

イーサネット インターフェイス 1/2 によるイーサネット インターフェイス 3/23 のポート トラッキングを設定するには、次のステップに従います。

手順

ステップ 1 イーサネット インターフェイス 3/23 のステータスを追跡するオブジェクトを作成します。

例：

```
switch# configure terminal
switch(config)# track 1 interface ethernet 3/23
switch(config-track)# end
```

ステップ 2 トラッキング オブジェクトがシャットダウンされたらイーサネット インターフェイス 1/2 をシャットダウンする EEM イベントを設定します。

例：

```
switch(config)# event manager applet track_3_23_down
switch(config-applet)# event track 1 state down
switch(config-applet)# action 1 syslog msg EEM applet track_3_23_down shutting down port
eth1/2 due to eth3/23 being down
switch(config-applet)# action 2 cli conf term
switch(config-applet)# action 3 cli interface ethernet 1/2
switch(config-applet)# action 4 cli shut
switch(config-applet)# end
```

ステップ 3 イーサネット インターフェイス 3/23 が起動したらイーサネット インターフェイス 1/2 を起動する EEM イベントを設定します。

例：

```
switch# configure terminal
switch(config)# event manager applet track_3_23_up
switch(config-applet)# event track 1 state up
switch(config-applet)# action 1 syslog msg EEM applet track_3_23_down bringing up port
eth1/2 due to eth3/23 being up
switch(config-applet)# action 2 cli conf term
switch(config-applet)# action 3 cli interface ethernet 1/2
switch(config-applet)# action 4 cli no shut
```

```
switch(config-applet)# end
```

EEM によって EEM ポリシーを登録する設定例

次に、EEM によって EEM ポリシーを登録する例を示します。

基本的なスイッチ設定：

```
event manager applet vpc_check_peer_at_startup
event track 101 state up
action 1.0 cli copy bootflash:eem/user_script_policies/load_schedules running-config

feature scheduler

!!## 2 x dummy loopbacks are required ##!!
interface loopback 101
interface loopback 102

track 1 list boolean or
object 13
object 12
object 102
track 2 list boolean and
object 13
object 12
track 12 interface Ethernet 2/24 line-protocol
track 13 interface port-channel 3000 line-protocol
track 101 interface loopback 101 line-protocol
track 102 interface loopback 102 line-protocol
```

（注） この例では、ポート チャネル 3000 が vPC ピア リンクで、イーサネット 2/24 が vPC キープアライブ リンクです。

ブートフラッシュに次のファイルをコピーする必要があります。

- スーパーバイザのブートフラッシュに作成する必要がある、/eem/user_script_policies と呼ばれるディレクトリ。
- 次の 5 つのファイルを上記のディレクトリに作成してロードする必要があります。
  - load_schedules
  - remove_vpc_if_peer_failed
  - clean_up
  - unload_schedules
  - restore_vpc

load_schedules ファイルの設定

```
feature scheduler

configure terminal
scheduler job name vpc_check
configure terminal
```

```
event manager policy remove_vpc_if_peer_failed
end

configure terminal
scheduler job name clean_up
configure terminal
event manager policy clean_up
end

configure terminal
scheduler job name trigger
configure terminal
interface loopback 102
shutdown
no shutdown
end

configure terminal
scheduler schedule name load_vpc_check
time start +00:00:04
job name vpc_check

scheduler schedule name trigger_vpc_check
time start +00:00:05
job name trigger

scheduler schedule name load_clean_up
time start +00:00:08
job name clean_up


scheduler schedule name trigger_clean_up
time start +00:00:10
job name trigger
```

remove_vpc_if_peer_failed ファイルの設定

```
event manager applet remove_vpc_if_peer_failed
event track 1 state down
action 1.0 cli show run vpc > bootflash://sup-active/eem/user_script_policies/vpc_saved.cfg
action 2.0 cli show run vpc > bootflash://sup-standby/eem/user_script_policies/vpc_saved.cfg
action 3.0 cli configure terminal
action 4.0 cli no feature vpc
action 5.0 syslog msg severity alert "##### WARNING!!!! PEER SWITCH FAILED TO COME ONLINE.
 VPC CONFIG REMOVED #####"
action 6.0 cli event manager policy restore_vpc
action 7.0 cli copy bootflash:eem/user_script_policies/unload_schedules running-config
action 8.0 cli no event manager applet remove_vpc_if_peer_failed
action 9.0 cli end
```

clean_up ファイルの設定

```
event manager applet clean_up
event track 102 state up
action 1.0 cli configure terminal
action 2.0 cli no event manager applet remove_vpc_if_peer_failed
action 3.0 cli copy bootflash:eem/user_script_policies/unload_schedules running
action 4.0 cli no event manager applet clean_up
action 5.0 end
```

unload_schedules ファイルの設定

```
no scheduler schedule name load_vpc_check
no scheduler schedule name trigger_vpc_check
no scheduler schedule name load_clean_up
no scheduler schedule name trigger_clean_up
no scheduler job name vpc_check
no scheduler job name trigger
no scheduler job name clean_up
```

restore_vpc ファイルの設定

```
event manager applet restore_vpc
event track 2 state up
action 1.0 cli copy bootflash:eem/user_script_policies/vpc_saved.cfg running-config
action 2.0 syslog msg severity alert "##### VPC PEER DETECTED. VPC CONFIG RESTORED #####"
action 3.0 cli configure terminal
action 4.0 cli copy bootflash:eem/user_script_policies/unload_schedules running-config
action 5.0 cli no event manager applet restore_vpc
action 6.0 cli end
```

付 録 C

Cisco NX-OS システム管理の設定制限事項

設定の制限は、『*Cisco Nexus 7000 Series NX-OS Verified Scalability Guide*』に記載されています。

- Cisco NX-OS システム管理の設定制限事項，551 ページ

Cisco NX-OS システム管理の設定制限事項

設定の制限は、『*Cisco Nexus 7000 Series NX-OS Verified Scalability Guide*』に記載されています。

Cisco NX-OS システム管理の設定制限事項