



Cisco Nexus 9000 シリーズ NX-OS システム管理設定ガイド、リリース 9.3(x)

初版：2019年7月20日

最終更新：2022年2月8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。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS REFERENCED IN THIS DOCUMENTATION ARE SUBJECT TO CHANGE WITHOUT NOTICE. EXCEPT AS MAY OTHERWISE BE AGREED BY CISCO IN WRITING, ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENTATION ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED.

The Cisco End User License Agreement and any supplemental license terms govern your use of any Cisco software, including this product documentation, and are located at: <http://www.cisco.com/go/softwareterms>. Cisco product warranty information is available at <http://www.cisco.com/go/warranty>. US Federal Communications Commission Notices are found here <http://www.cisco.com/c/en/us/products/us-fcc-notice.html>.

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

Any products and features described herein as in development or available at a future date remain in varying stages of development and will be offered on a when-and-if-available basis. Any such product or feature roadmaps are subject to change at the sole discretion of Cisco and Cisco will have no liability for delay in the delivery or failure to deliver any products or feature roadmap items that may be set forth in this document.

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

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

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

© 2019–2022 Cisco Systems, Inc. All rights reserved.



目次

Trademarks ?

はじめに :

はじめに xxv

対象読者 xxv

表記法 xxv

Cisco Nexus 9000 シリーズ スイッチの関連資料 xxvi

マニュアルに関するフィードバック xxvi

通信、サービス、およびその他の情報 xxvii

第 1 章

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

第 2 章

システム管理機能のプラットフォーム サポート 5

システム管理機能のプラットフォーム サポート 5

第 3 章

概要 9

ライセンス要件 9

ソフトウェア イメージ 10

Cisco NX-OS デバイスのコンフィギュレーション方式 10

CLI または XML 管理インターフェイスで設定する 11

Cisco DCNM での設定 11

ネットワーク タイム プロトコル 11

Cisco Discovery Protocol 11

セッションマネージャ 12

スケジューラ	12
SNMP	12
オンライン診断	12
オンボード障害ロギング	12
SPAN	13
ERSPAN	13
LLDP	13
MPLS ストリッピング	13
sFlow	13
SMU	13
仮想デバイス コンテキスト	14
トラブルシューティング機能	14

第 4 章

スイッチ プロファイルの設定 15

スイッチ プロファイルの概要	15
スイッチ プロファイル：コンフィギュレーション モード	16
コンフィギュレーション同期モード	16
スイッチ プロファイルモード	16
スイッチ プロファイル インポート モード	16
コンフィギュレーションの検証	16
相互排除チェック	17
マージチェック	17
スイッチ プロファイルを使用したソフトウェアのアップグレードとダウングレード	17
スイッチ プロファイルの注意事項および制約事項	18
スイッチ プロファイルの設定	19
スイッチ プロファイルのコマンドの追加または変更	22
スイッチ プロファイルのインポート	23
vPC トポロジでの設定のインポート	25
ピア スイッチの分離	26
スイッチ プロファイルの削除	26
ミューテックスとマージの失敗の手動修正	27
スイッチ プロファイル設定の確認	28

スイッチプロファイルの設定例	28
ローカルおよびピア スイッチでのスイッチ プロファイルの作成...	28
同期ステータスの確認	31
実行中のコンフィギュレーションの表示	32
ローカルとピア スイッチ間のスイッチ プロファイルの同期の表示	32
ローカルおよびピア スイッチでの確認とコミットの表示	33
ローカルおよびピア スイッチ間の成功および失敗した同期の表示	34
スイッチ プロファイル バッファの表示	35
設定のインポート	36
ファブリック エクステンダのストレート型トポロジでの Cisco NX-OS リリース 7.0(3)I2(1) 以降への移行	38
Cisco Nexus 9000 シリーズ スイッチの交換	38
設定の同期	40
Cisco Nexus 9000 シリーズ スイッチのリブート後の設定の同期化	40
mgmt0 インターフェイスの接続が失われた場合の設定の同期化	40
グローバル コンフィギュレーション モードでレイヤ 2 からレイヤ 3 への不注意による ポート モードの変更を元に戻す	40

 第 5 章

PTP の設定 43

PTP について	43
PTP オフロード	44
PTP デバイス タイプ	44
クロック	45
PTP プロセス	46
PTP のハイ アベイラビリティ	47
PTP の注意事項および制約事項	48
PTP のデフォルト設定	50
PTP の設定	51
PTP のグローバルな設定	51
インターフェイスでの PTP の設定	55
ユニキャストモードでの PTP の設定	59

ユニキャスト モードの設定	59
マスター ロールの割り当て	59
スレーブ ロールの割り当て	60
ユニキャスト送信元アドレスの設定	61
PTP 混合モード	61
PTP インターフェイスがマスター ステートを維持する設定	62
タイムスタンプ タギング	63
タイムスタンプ タギングの設定	63
TTAG マーカー パケットと時間間隔の設定	64
PTP 設定の確認	66
PTP の設定例	67
その他の参考資料	70
関連資料	70

第 6 章

NTP の設定 71

NTP の詳細	71
NTP アソシエーション	72
時間サーバとしての NTP	72
クロック マネージャ	72
高可用性	73
仮想化のサポート	73
NTP の前提条件	73
NTP の注意事項と制約事項	73
NTP のデフォルト設定	75
NTP の設定	75
NTP の有効化または無効化	75
正規の NTP サーバとしてのデバイスの設定	76
NTP サーバおよびピアの設定	76
NTP 認証の設定	78
NTP アクセス制限の設定	80
NTP ソース IP アドレスの設定	83

NTP ソース インターフェイスの設定	83
NTP ログインの設定	84
NTP の設定確認	85
NTP の設定例	85
その他の参考資料	86
関連資料	86
MIB	87

第 7 章

CDP の設定	89
CDP について	89
VTP 機能のサポート	90
高可用性	91
仮想化のサポート	91
CDP の注意事項と制約事項	91
CDP のデフォルト設定	91
CDP の設定	91
CDP のグローバルな有効化または無効化	92
インターフェイス上での CDP の有効化または無効化	92
CDP オプション パラメータの設定	93
CDP コンフィギュレーションの確認	94
CDP のコンフィギュレーション例	95

第 8 章

システムメッセージロギングの設定	97
システム メッセージ ロギングの詳細	97
Syslogサーバ	98
セキュアな Syslog サーバ	98
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	99
システム メッセージ ロギングのデフォルト設定	99
システムメッセージロギングの設定	100
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	100
Syslog メッセージの送信元 ID の設定	102

ファイルへのシステム メッセージの記録	103
モジュールおよびファシリティ メッセージのログgingsの設定	104
syslog サーバの設定	107
セキュアな Syslog サーバの設定	109
CA 証明書の設定	110
CA 証明書の登録	111
UNIX または Linux システムでの syslog サーバの設定	112
ログ ファイルの表示およびクリア	113
システム メッセージ ログgingsの設定確認	114
システム メッセージ ログgingsの設定例	115
その他の参考資料	115
関連資料	115

第 9 章

Smart Call Home の設定	117
Smart Call Home の概要	117
宛先プロファイル	118
Smart Call Home アラート グループ	118
Smart Call Home のメッセージ レベル	122
Smart Call Home の取得	123
データベース マージの注意事項	123
高可用性	124
仮想化のサポート	124
Smart Call Home の前提条件	124
Smart Call Home の注意事項および制約事項	124
Smart Call Home のデフォルト設定	125
Smart Call Home の設定	125
連絡先情報の設定	126
宛先プロファイルの作成	128
宛先プロファイルの変更	129
アラート グループと宛先プロファイルのアソシエート	131
アラート グループへの show コマンドの追加	132

電子メール サーバの設定	133
HTTP を使用したメッセージ送信のための VRF 設定	135
HTTP プロキシ サーバの設定	136
定期的なインベントリ通知の設定	137
重複メッセージ抑制のディセーブル化	138
Smart Call Home のイネーブル化またはディセーブル化	139
Smart Call Home 設定のテスト	140
Smart Call Home 設定の確認	141
Smart Call Home の設定例	141
その他の参考資料	142
イベント トリガ	142
メッセージフォーマット	144
ショートテキストメッセージフォーマット	144
共通のイベントメッセージフィールド	145
アラート グループメッセージフィールド	148
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	148
インベントリ イベントメッセージのフィールド	149
ユーザが作成したテストメッセージのフィールド	149
フルテキスト形式での syslog アラート通知の例	150
XML 形式での syslog アラート通知の例	152
MIB	156

 第 10 章

Session Manager の設定	157
セッション マネージャについて	157
高可用性	158
セッション マネージャの前提条件	158
Session Manager の注意事項および制約事項	158
Session Manager の設定	158
セッションの作成	159
セッションでの ACL の設定	159
セッションの確認	160

セッションのコミット	160
セッションの保存	160
セッションの廃棄	161
Session Manager 設定の確認	161
Session Manager のコンフィギュレーション例	161
その他の参考資料	162
関連資料	162

第 11 章

スケジューラの設定 163

スケジューラについて	163
リモート ユーザ認証	164
ログ	164
高可用性	164
スケジューラの前提条件	164
スケジューラの注意事項および制約事項	165
スケジューラのデフォルト設定	165
スケジューラの設定	165
スケジューラの有効化または無効化	165
スケジューラ ログ ファイル サイズの定義	166
リモート ユーザ認証の設定	167
ジョブの定義	168
ジョブの削除	169
タイムテーブルの定義	170
スケジューラ ログ ファイルの消去	172
スケジューラの設定確認	172
スケジューラの設定例	172
スケジューラ ジョブの作成	172
スケジューラ ジョブのスケジューリング	173
ジョブ スケジュールの表示	173
スケジューラ ジョブの実行結果の表示	173

第 12 章

SNMP の設定 175

SNMP について 175

SNMP 機能の概要 175

SNMP 通知 176

SNMPv3 177

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 178

ユーザベースのセキュリティ モデル 179

CLI および SNMP ユーザの同期 180

グループベースの SNMP アクセス 180

SNMP および Embedded Event Manager 181

マルチ インスタンス サポート 181

SNMP のハイ アベイラビリティ 181

SNMP の仮想化サポート 182

SNMP の注意事項および制約事項 182

SNMP のデフォルト設定 183

SNMP の設定 183

SNMP ユーザの設定 183

SNMP メッセージ暗号化の適用 184

SNMPv3 ユーザに対する複数のロールの割り当て 184

SNMP コミュニティの作成 185

SNMP 要求のフィルタリング 186

SNMP 通知レシーバの設定 187

SNMP 通知用の発信元 インターフェイスの設定 188

通知ターゲット ユーザの設定 190

VRF を使用する SNMP 通知レシーバの設定 191

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 192

SNMP 通知のイネーブル化 194

インターフェイスでのリンク通知のディセーブル化 203

インターフェイスの SNMP ifIndex の表示 204

TCP による SNMP のワンタイム認証の有効化 204

SNMP スイッチのコンタクト（連絡先）およびロケーション情報の指定	205
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	205
SNMP のディセーブル化	207
SNMP サーバカウンタ キャッシュ更新タイマーの管理	207
AAA 同期時間の変更	208
SNMP ローカル エンジン ID の設定	209
SNMP の設定の確認	210
SNMP の設定例	211
その他の参考資料	212
関連資料	212
RFC	213
MIB	213

第 13 章

RMON の設定	215
RMON について	215
RMON アラーム	216
RMON イベント	216
RMON のハイ アベイラビリティ	217
RMON の仮想化サポート	217
RMON の注意事項と制約事項	217
RMON のデフォルト設定	217
RMON の設定	218
RMON アラームの設定	218
RMON イベントの設定	219
RMON 設定の確認	220
RMON の設定例	220
その他の参考資料	221
MIB	221

第 14 章

オンライン診断の設定	223
オンライン診断について	223

ブートアップ診断	223
ランタイムまたはヘルス モニタリング診断	225
オンデマンド診断	234
高可用性	234
仮想化のサポート	234
オンライン診断の注意事項と制約事項	234
オンライン診断のデフォルト設定	235
オンライン診断の設定	236
起動診断レベルの設定	236
診断テストのアクティブ化	237
オンデマンド診断テストの開始または中止	238
診断結果のシミュレーション	239
診断結果の消去	239
オンライン診断設定の確認	240
オンライン診断のコンフィギュレーション例	240

第 15 章

Embedded Event Manager の設定 243

EEM について	243
ポリシー	244
イベント文	245
アクション文	246
VSH スクリプト ポリシー	247
環境変数	247
EEM イベント相関	247
高可用性	247
仮想化のサポート	248
EEM の前提条件	248
EEM の注意事項と制約事項	248
EEM のデフォルト設定	249
EEM の設定	250
環境変数の定義	250

CLIによるユーザ ポリシーの定義	250
イベント文の設定	252
アクション文の設定	258
VSHスクリプトによるポリシーの定義	260
VSHスクリプト ポリシーの登録およびアクティブ化	260
ポリシーの上書き	260
メモリのしきい値の設定	262
EEMパブリッシャとしてのsyslogの設定	263
EEMの設定確認	265
EEMの設定例	266
イベントログの自動収集とバックアップ	267
拡張ログファイルの保持	267
すべてのサービスの拡張ログファイル保持のイネーブル化	267
すべてのサービスの拡張ログファイル保持の無効化	268
単一サービスの拡張ログファイル保持の有効化	268
拡張ログファイルの表示	270
単一サービスに対する拡張ログファイル保持の無効化	270
トリガーベースのイベントログの自動収集	272
トリガーベースのログファイルの自動収集の有効化	272
自動収集YAMLファイル	272
コンポーネントあたりの自動収集の量の制限	275
自動収集ログファイル	275
トリガーベースのログ収集の確認	279
トリガーベースのログファイル生成の確認	279
ローカルログファイルのストレージ	279
最近のログファイルのローカルコピーの生成	280
外部ログファイルのストレージ	282
第 16 章	
オンボード障害ロギングの設定	285
OBFLの概要	285
OBFLの前提条件	286

OBFL の注意事項と制約事項	286
OBFL のデフォルト設定	286
OBFL の設定	286
OBFL 設定の確認	289
OBFL のコンフィギュレーション例	290
その他の参考資料	291
関連資料	291

 第 17 章

SPAN の設定	293
SPAN の概要	293
SPAN ソース	293
送信元ポートの特性	294
SPAN 宛先	295
宛先ポートの特性	295
SPAN セッション	295
ローカライズされた SPAN セッション	296
SPAN 切り捨て	296
ACL TCAM リージョン	296
高可用性	296
SPAN の前提条件	297
SPAN の注意事項および制約事項	297
Cisco Nexus 3000 プラットフォーム スイッチの SPAN の制限	301
Cisco Nexus 9200 プラットフォーム スイッチの SPAN の制限事項	301
Cisco Nexus 9300 プラットフォーム スイッチの SPAN の制限事項	302
Cisco Nexus 9500 プラットフォーム スイッチの SPAN の制限事項	305
SPAN のデフォルト設定	307
SPAN の設定	307
SPAN セッションの設定	307
UDF ベース SPAN の設定	311
SPAN 切り捨ての設定	314
異なる LSE スライス間のマルチキャスト Tx トラフィックの SPAN の設定	315

SPAN セッションのシャットダウンまたは再開	316
SPAN 設定の確認	317
SPAN のコンフィギュレーション例	318
SPAN セッションのコンフィギュレーション例	318
単一方向 SPAN セッションの設定例	318
SPAN ACL の設定例	319
UDF ベース SPAN の設定例	319
SPAN 切り捨ての設定例	320
LSE スライス間のマルチキャスト Tx SPAN の設定例	321
その他の参考資料	322
関連資料	322

第 18 章

ERSPAN の設定	323
ERSPAN について	323
ERSPAN 送信元	323
ERSPAN の宛先	324
ERSPAN セッション	324
ローカライズされた ERSPAN セッション	325
ERSPAN の切り捨て	325
ERSPAN の前提条件	325
ERSPAN の注意事項および制約事項	325
デフォルト設定	329
ERSPAN の設定	329
ERSPAN 送信元セッションの設定	330
ERSPAN セッションのシャットダウンまたはアクティブ化	333
ERSPAN ACL の設定	335
UDF ベース ERSPAN の設定	338
ERSPAN 切り捨ての設定	340
ERSPAN 宛先セッションの設定	342
ERSPAN 設定の確認	345
ERSPAN の設定例	346

単一方向 ERSPAN セッションの設定例	346
ERSPAN ACL の設定例	346
マーカー パケットの設定例	347
UDF ベース ERSPAN の設定例	347
ERSPAN 切り捨ての設定例	348
IPv4 上の構成例	349

第 19 章**LLDP の設定 351**

LLDP について 351

DCBXP について 352

高可用性 353

仮想化のサポート 353

LLDP に関する注意事項および制約事項 353

LLDP のデフォルト設定 354

LLDP の設定 354

LLDP をグローバルに有効化または無効化する 355

インターフェイス上での LLDP の有効化または無効化 355

DCBXP プロトコルバージョンの設定 356

物理インターフェイスごとの複数の LLDP ネイバー 358

LLDP マルチネイバー サポートのイネーブル化またはディセーブル化 358

ポート チャネル インターフェイスでの LLDP サポートの有効化または無効化 360

LLDP オプション パラメータの設定 362

LLDP 設定の確認 364

LLDP の設定例 365

第 20 章**NetFlow の設定 367**

NetFlow について 367

デュアルレイヤ NetFlow の実装 368

フロー レコード 368

フロー エクスポート 369

エクスポート形式 369

レイヤ 2 NetFlow キー	369
フロー モニタ	370
NetFlow 出力インターフェイス	370
高可用性	370
NetFlow の前提条件	371
NetFlow に関する注意事項および制約事項	371
NetFlow の設定	375
NetFlow 機能の有効化	375
フロー レコードの作成	376
match パラメータの指定	377
collect パラメータの指定	378
フロー エクスポートの作成	379
フロー モニタの作成	380
インターフェイスへのフロー モニタの適用	381
VLAN 上でのブリッジ型 NetFlow の設定	382
レイヤ 2 NetFlow キーの設定	383
NetFlow タイムアウトの設定	384
NetFlow 設定の確認	385
NetFlow のモニタリング	386
NetFlow の表示例	386
NetFlow のコンフィギュレーション例	386

第 21 章

sFlow の設定	387
sFlow について	387
sFlow エージェント	387
sFlow の前提条件	388
sFlow の注意事項および制約事項	388
sFlow のデフォルト設定	389
sFlow の設定	390
sFlow の有効化	390
サンプリング レートの設定	391

最大サンプリング サイズの設定	391
カウンタのポーリング間隔の設定	392
最大データグラム サイズの設定	393
sFlow コレクタ アドレスの設定	393
sFlow コレクタ ポートの設定	395
sFlow エージェント アドレスの設定	396
sFlow サンプリング データ ソースの設定	396
sFlow 設定の確認	397
sFlow 統計情報のモニタリングとクリア	398
sFlow の設定例	398
その他の参考資料	399
関連資料	399

第 22 章

『Configuring TAP Aggregation and MPLS Stripping』	401
TAP アグリゲーションについて	401
ネットワーク TAP	401
TAP アグリゲーション	402
TAP 集約の注意事項と制約事項	403
MPLS ストリッピングについて	404
MPLS ストリッピングに関する注意事項と制限事項	405
TAP アグリゲーションの設定	406
ラインカードの TAP 集約のイネーブル化	406
TAP 集約ポリシーの設定	407
TAP アグリゲーション ポリシーのインターフェイスへのアタッチ	409
TAP アグリゲーションの設定の確認	410
TAP アグリゲーションの設定例	410
MPLS ストリッピングの設定	411
MPLS ストリッピングの有効化	411
VLAN タグの着信ポートの設定	412
MPLS ラベルの追加と削除	414
宛先 MAC アドレスの設定	415

MPLS ラベル エージングの設定	415
MPLS ストリッピング設定の確認	416
MPLS ストリッピング カウンタおよびラベル エントリのクリア	417
MPLS ストリッピングの設定例	418
その他の参考資料	418
関連資料	418

第 23 章

MPLS アクセス リストの構成	421
MPLS アクセス リストの構成	421
MPLS アクセス リスト構成の検証	422
MPLS アクセス リストの構成例	422

第 24 章

グレースフル挿入と削除の設定	423
グレースフル挿入と削除について	423
プロファイル	424
スナップショット	426
GIR の注意事項と制限事項	426
GIR ワークフロー	427
メンテナンス モードプロファイルの設定	427
通常モードプロファイルの設定	429
スナップショットの作成	430
スナップショットへの show コマンドの追加	432
グレースフル削除のトリガー	434
グレースフル挿入のトリガー	437
メンテナンス モードの強化	438
GIR 設定の確認	439
GIR の設定例	441

第 25 章

ソフトウェア メンテナンス アップグレードの実行	443
SMU について	443
RPM パッチ	444

パッケージ管理	445
パッケージのアクティブ化と非アクティブ化の影響	445
SMU の前提条件	446
SMU の注意事項と制約事項	446
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	447
パッケージインストールの準備	447
Cisco.com からの SMU パッケージファイルのダウンロード	449
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	449
パッケージの追加とアクティブ化	453
アクティブなパッケージセットのコミット	456
RPM パッケージのインストール	457
パッケージの非アクティブ化と削除	458
機能 RPM のダウングレード	461
インストール ログ情報の表示	462
Guest Shell Bash のソフトウェア メンテナンス アップグレードの実行	464
その他の参考資料	466
関連資料	466
SMU の履歴	466

 第 26 章

コンフィギュレーションの置換の実行	469
コンフィギュレーションの置換とコミットタイムアウトについて	469
概要	470
コンフィギュレーションの置換の利点	471
コンフィギュレーションの置換に関する注意事項と制限事項	472
コンフィギュレーションの置換の推奨ワークフロー	474
コンフィギュレーションの置換の実行	475
コンフィギュレーションの置換の確認	477
コンフィギュレーションの置換の例	478

 第 27 章

ロールバックの設定	485
------------------	-----

ロールバックについて	485
システム チェックポイントの自動生成	486
高可用性	486
仮想化のサポート	487
ロールバックの前提条件	487
ロールバックの注意事項と制約事項	487
ロールバックのデフォルト設定	488
ロールバックの設定	488
チェックポイントの作成	488
ロールバックの実装	489
ロールバック コンフィギュレーションの確認	490
ロールバックの設定例	491
その他の参考資料	491
関連資料	491
<hr/>	
付録 A :	Cisco NX-OS システム管理でサポートされている IETF RFC 493
	Cisco NX-OS システム管理でサポートされている IETF RFC 493
<hr/>	
付録 B :	Embedded Event Manager システム イベントおよび設定例 495
	EEM システム ポリシー 495
	EEM イベント 499
	EEM ポリシーの設定例 500
	CLI イベントの設定例 500
	インターフェイス シャットダウンのモニタリング 500
	モジュールパワーダウンのモニタリング 501
	ロールバックを開始するトリガーの追加 501
	メジャーしきい値を上書き（無効化）する設定例 501
	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 501
	One Bad センサーの無効化 501
	複数の不良センサーを無効にする方法 502
	モジュール全体の上書き（無効化） 502

複数のモジュールおよびセンサーの上書き（無効）	502
1つのセンサーを有効にして、すべてのモジュールの残りのセンサーをすべて無効にする方法	503
複数のセンサーを有効にして、すべてのモジュールの残りのセンサーをすべて無効にする方法	503
1つのモジュールのすべてのセンサーを有効にして、残りのモジュールのすべてのセンサーを無効にする方法	504
モジュールのセンサーを組み合わせて有効にして、残りのモジュールのすべてのセンサーを無効にする方法	504
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（無効化）するコンフィギュレーション例	504
1つまたは複数のファントレイ取り外しのためのシャットダウンの上書き（無効）	504
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（無効）	505
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（無効化）	505
1つを除くすべてのファンを取り外すためのシャットダウンの上書き（無効）	505
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（無効）	506
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（無効）	506
補足ポリシーを作成するコンフィギュレーション例	506
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	506
温度しきい値イベントの補足ポリシーの作成	507
電力のバジェット超過ポリシーの設定例	507
モジュールのシャットダウン	507
指定された一連のモジュールのシャットダウン	507
シャットダウンするモジュールを選択する設定例	508
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	508
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	508
活性挿抜イベントのコンフィギュレーション例	508
ユーザ syslog を生成するコンフィギュレーション例	509
Syslog メッセージをモニタする設定例	509
SNMP 通知の設定例	509

SNMP OID のポーリングによる EEM イベントの生成 509
イベント ポリシーのイベントへの応答で SNMP 通知を送信 510
ポート トラッキングの設定例 510
EEM によって EEM ポリシーを登録する設定例 511

付録 C : Cisco NX-OS システム管理の設定制限 515
Cisco NX-OS システム管理の設定制限 515



はじめに

この前書きは、次の項で構成されています。

- [対象読者](#) (xxv ページ)
- [表記法](#) (xxv ページ)
- [Cisco Nexus 9000 シリーズ スイッチの関連資料](#) (xxvi ページ)
- [マニュアルに関するフィードバック](#) (xxvi ページ)
- [通信、サービス、およびその他の情報](#) (xxvii ページ)

対象読者

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

表記法

コマンドの説明には、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。
<i>italic</i>	イタリック体の文字は、ユーザが値を指定する引数です。
[x]	省略可能な要素（キーワードまたは引数）は、角かっこで囲んで示しています。
[x y]	いずれか1つを選択できる省略可能なキーワードや引数は、角かっこで囲み、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、波かっこで囲み、縦棒で区切って示しています。

表記法	説明
[x {y z}]	角かっこまたは波かっこが入れ子になっている箇所は、任意または必須の要素内の任意または必須の選択肢であることを表します。角かっこ内の波かっこと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。
variable	ユーザが値を入力する変数であることを表します。イタリック体が使用できない場合に使用されます。
string	引用符を付けない一組の文字。string の前後には引用符を使用しないでください。引用符を使用すると、その引用符も含めて string と見なされます。

例では、次の表記法を使用しています。

表記法	説明
screen フォント	スイッチが表示する端末セッションおよび情報は、スクリーンフォントで示しています。
太字の screen フォント	ユーザが入力しなければならない情報は、太字の 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。

Cisco Nexus 9000 シリーズ スイッチの関連資料

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

http://www.cisco.com/en/US/products/ps13386/tsd_products_support_series_home.html

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。ご協力をよろしくお願いいたします。

通信、サービス、およびその他の情報

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

Cisco バグ検索ツール

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



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 9000 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 9.3(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

表 1: 新機能および変更された機能

特長	説明	変更が行われたリリース	参照先
SNMPv3 の認証プロトコル	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。 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。	9.3(8)	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 (178 ページ) ユーザベースのセキュリティモデル (179 ページ)

特長	説明	変更が行われたリリース	参照先
Config-replace : 1回目と2回目のロールバックが失敗した場合のログの収集とリロード	CRの失敗に加えて、以前の実行コンフィギュレーションへの復元に失敗した場合、以前に保存したスタートアップコンフィギュレーションにスイッチをリロードするオプションの on-failure reload コマンドがサポートされます。このコマンドの後に、 save-startup-config コマンドを実行して、実行コンフィギュレーションをスタートアップに保存します。	9.3(7)	コンフィギュレーションの置換の実行 (475 ページ) システム管理機能のプラットフォームサポート (5 ページ)
イベントログの自動収集とバックアップ	拡張オンスイッチおよびオフスイッチイベントロギングファイルストレージのサポートが導入されました。	9.3(3)	イベントログの自動収集とバックアップ (267 ページ)
PTP サポート	Cisco Nexus 93360YC-FX2 および 93216TC-FX2 スイッチの PTP サポートが追加されました。	9.3(3)	システム管理機能のプラットフォームサポート (5 ページ)
スイッチプロファイルのインターフェイスでの MTU 設定	スイッチプロファイル設定での MTU 設定のサポートが導入されました。	9.3(3)	スイッチプロファイルの注意事項および制約事項 (18 ページ)
sFlow および SPAN のサポート	Cisco Nexus 9300-GX プラットフォームスイッチは、同じインターフェイスで sFlow と SPAN の両方をサポートします。	9.3(3)	sFlow の注意事項および制約事項 (388 ページ) Cisco Nexus 9300 プラットフォームスイッチの SPAN の制限事項 (302 ページ)

特長	説明	変更が行われたリリース	参照先
Netflow サポート	Netflow は Cisco Nexus 9300-GX プラットフォームスイッチではサポートされません。	9.3(3)	システム管理機能のプラットフォームサポート (5 ページ)
Netflow ND-ISSU の制限	ND-ISSU 中にエクスポートの損失が予想されます。	9.3(3)	NetFlow に関する注意事項および制約事項 (371 ページ)
ASIC Register ヘルス モニタ チェック	ASICRegisterCheck は、ヘルスマニタ診断として追加されます。	9.3(3)	ランタイムまたはヘルスマニタリング診断 (225 ページ)
ISSU RPM パッチ	ISSU RPM パッチのサポートが追加されました。	9.3(1)	RPM パッチ (444 ページ) RPM パッケージのインストール (457 ページ)
設定の置換	設定の置換コマンドのセマンティック検証のサポートが追加されました。	9.3(1)	コンフィギュレーションの置換の推奨ワークフロー (474 ページ) コンフィギュレーションの置換の実行 (475 ページ)
ERSPAN	Cisco Nexus 9200、9300-EX、9300-FX プラットフォームスイッチにサポートが追加されました。	9.3(1)	ERSPAN の注意事項および制約事項 (325 ページ)
NetFlow	9300-FX ラインカードを搭載した Cisco Nexus 9500 p プラットフォームスイッチ	9.3(1)	NetFlow に関する注意事項および制約事項 (371 ページ)
オンライン診断および EEM	AsicMemory、BootupPortLoopback、FpgaRegTest、および L2ACLRedirect テストの修正アクションが導入されました。	9.3(1)	ランタイムまたはヘルスマニタリング診断 (225 ページ) EEM システム ポリシー (495 ページ)

特長	説明	変更が行われたリリース	参照先
PTP オフロード	X9700-EX および X9700-FX ラインカードを搭載したCisco Nexus 9500 プラットフォームスイッチのサポートが追加されました。	9.3(1)	PTP オフロード (44 ページ)
PTP ワンステップ クロック モード	Cisco Nexus 9636C-R および 9636Q-R ラインカードで設定可能。	9.3(1)	クロック モード (46 ページ) PTP の注意事項および制約事項 (48 ページ)
PTP タイムスタンプ タギング	Cisco Nexus 9200, 9300-EX、9300-FX スイッチと、9700-EX および 9700-FX ラインカードを搭載した Cisco Nexus 9500 プラットフォームスイッチにサポートが追加されました。	9.3(1)	PTP の注意事項および制約事項 (48 ページ)
sFlow と SPAN の組み合わせ	Cisco Nexus 9336C-FX2、93240YC-FX2、および 93360YC-FX2 スイッチのサポートが追加されました。	9.3(1)	Cisco Nexus 9300 プラットフォームスイッチの SPAN の制限事項 (302 ページ) sFlow の注意事項および制約事項 (388 ページ)
SPAN 切り捨て	X9700-EX および X9700-FX ラインカードを搭載したCisco Nexus 9500 プラットフォームスイッチのサポートが追加されました。	9.3(1)	Cisco Nexus 9500 プラットフォームスイッチの SPAN の制限事項 (305 ページ)



第 2 章

システム管理機能のプラットフォームサポート

この章では、Cisco プラットフォームスイート全体でサポートされていない機能のプラットフォームサポートについて定義します。

- [システム管理機能のプラットフォームサポート \(5 ページ\)](#)

システム管理機能のプラットフォームサポート

次の表に、各機能でサポートされるプラットフォームと、それらが最初に導入されたリリースを示します。最初の製品リリースでサポートされるプラットフォームの詳細については、リリースノートを参照してください。

NetFlow

NetFlow の詳細については、[NetFlow の設定 \(367 ページ\)](#) を参照してください。

機能	サポートされるプラットフォームまたはラインカード	サポートされるようになった最初のリリース
NetFlow	• Cisco Nexus 9300-GX プラットフォーム スイッチ	Cisco NX-OS リリース 9.3(3)
NetFlow	• Cisco Nexus 92348GC-X • Cisco Nexus 9700-EX ラインカードおよび FM-E ファブリック モジュールを搭載した Cisco Nexus 9500 プラットフォーム スイッチ。 • Cisco Nexus 93360YC-FX2	Cisco NX-OS リリース 9.3(1)

機能	サポートされるプラットフォームまたはラインカード	サポートされるようになった最初のリリース
NetFlow	<ul style="list-style-type: none"> • Cisco Nexus 9300-EX および 9300-FX プラットフォーム スイッチ • Cisco Nexus 9300-FX2 プラットフォーム スイッチ • Cisco Nexus N9K-C93240YC-FX2 プラットフォーム スイッチ 	
NetFlow	<ul style="list-style-type: none"> • 9700-EX ラインカード搭載の Cisco Nexus 9500 プラットフォーム スイッチ 	Cisco NX-OS リリース 9.2(2)

高精度時間プロトコル

Precision Time Protocol (PTP) の詳細については、[PTP の設定 \(43 ページ\)](#) を参照してください。

機能	サポートされるプラットフォームまたはラインカード	サポートされるようになった最初のリリース
タイムスタンプ タギング (TTAG)	Cisco Nexus 9300-FX プラットフォーム スイッチ	Cisco NX-OS リリース 7.0(3)I7(3)
タイムスタンプ タギング (TTAG)	Cisco Nexus 9300-FX2 プラットフォーム スイッチ	Cisco NX-OS リリース 9.3(3)
タイムスタンプ タギング (TTAG)	-EX または FX ラインカード搭載の Cisco Nexus 9500 プラットフォーム スイッチ	
タイムスタンプ タギング (TTAG)	Cisco Nexus 9300-EX プラットフォーム スイッチ	Cisco NX-OS リリース 7.0(3)I6(1)
タイムスタンプ タギング (TTAG)	Cisco Nexus 9364C	Cisco NX-OS リリース 7.0(3)I7(3)
タイムスタンプ タギング (TTAG)	Cisco Nexus 9332C	gbhvisco NX-OS リリース 9.2(3)
タイムスタンプ タギング (TTAG)	Cisco Nexus 9200 プラットフォーム スイッチ	Cisco NX-OS リリース 7.0(3)I6(1)
PTP	Cisco Nexus 93360YC-FX2 Cisco Nexus 93216TC-FX2	Cisco NX-OS リリース 9.3(3)

機能	サポートされるプラットフォームまたはラインカード	サポートされるようになった最初のリリース
PTP	Cisco Nexus 9504-FM-R プラットフォーム スイッチ	Cisco NX-OS リリース 9.2(3)

sFlow

sFlow の詳細については、[sFlow の設定 \(387 ページ\)](#) を参照してください。

機能	サポートされるプラットフォームまたはラインカード	サポートされるようになった最初のリリース
sFlow	Cisco Nexus 92348GC-X	Cisco NX-OS リリース 9.3(1)
sFlow	Cisco Nexus 9736C-FX ラインカード搭載の Cisco Nexus 9500 プラットフォーム スイッチ	Cisco NX-OS リリース 7.0(3)I7(3)
sFlow	Cisco Nexus 9788TC-FX または 9732C-FX ラインカード搭載の Cisco 9500 プラットフォーム スイッチ	Cisco NX-OS リリース 7.0(3)I7(3)

SPAN

SPAN の詳細については、[SPAN の設定 \(293 ページ\)](#) を参照してください。

機能	サポートされるプラットフォームまたはラインカード	サポートされるようになった最初のリリース
VLAN Tx SPAN	<p>Cisco Nexus 9200 プラットフォーム スイッチ、Cisco Nexus 9300-EX プラットフォーム スイッチ、Cisco Nexus 9300-FX プラットフォーム スイッチ、Cisco Nexus 9300-GX プラットフォーム スイッチ</p> <p>次のラインカードを備えた Cisco Nexus 9500 プラットフォーム スイッチ</p> <ul style="list-style-type: none"> • Cisco Nexus 97160YC-EX • Cisco Nexus 9732C-EX • Cisco Nexus 9732C-FX • Cisco Nexus 9736C-EX • Cisco Nexus 9736C-FX • Cisco Nexus 9736Q-FX • Cisco Nexus 9788TC-FX 	

スイッチ プロファイル

スイッチ プロファイルの詳細については、[スイッチ プロファイルの設定 \(15 ページ\)](#) を参照してください。

機能	サポートされるプラットフォームまたはラインカード	サポートされるようになった最初のリリース
スイッチ プロファイル	Cisco Nexus 9300 プラットフォーム スイッチ	

TAP アグリゲーション

タップ アグリゲーションの詳細については、[『Configuring TAP Aggregation and MPLS Stripping』 \(401 ページ\)](#) を参照してください。

機能	サポートされるプラットフォームまたはラインカード	サポートされるようになった最初のリリース
タップ アグリゲーションおよび MPLS ストリッピング	<ul style="list-style-type: none"> • 9700-EX および 9700-FX ラインカードを搭載した Cisco Nexus 9500 プラットフォーム スイッチ • Cisco Nexus 9200 プラットフォーム スイッチ • Cisco Nexus 9300 プラットフォーム スイッチ 	Cisco NX-OS リリース 9.2(1)



CHAPTER 3

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。

- [ライセンス要件 \(9 ページ\)](#)
- [ソフトウェア イメージ \(10 ページ\)](#)
- [Cisco NX-OS デバイスのコンフィギュレーション方式 \(10 ページ\)](#)
- [ネットワーク タイム プロトコル \(11 ページ\)](#)
- [Cisco Discovery Protocol \(11 ページ\)](#)
- [セッションマネージャ \(12 ページ\)](#)
- [スケジューラ \(12 ページ\)](#)
- [SNMP \(12 ページ\)](#)
- [オンライン診断 \(12 ページ\)](#)
- [オンボード障害ロギング \(12 ページ\)](#)
- [SPAN \(13 ページ\)](#)
- [ERSPAN \(13 ページ\)](#)
- [LLDP \(13 ページ\)](#)
- [MPLS ストリッピング \(13 ページ\)](#)
- [sFlow \(13 ページ\)](#)
- [SMU \(13 ページ\)](#)
- [仮想デバイス コンテキスト \(14 ページ\)](#)
- [トラブルシューティング機能 \(14 ページ\)](#)

ライセンス要件

Cisco NX-OS ライセンス方式の推奨の詳細と、ライセンスの取得および適用の方法については、『[Cisco NX-OS Licensing Guide](#)』を参照してください。

ソフトウェアイメージ

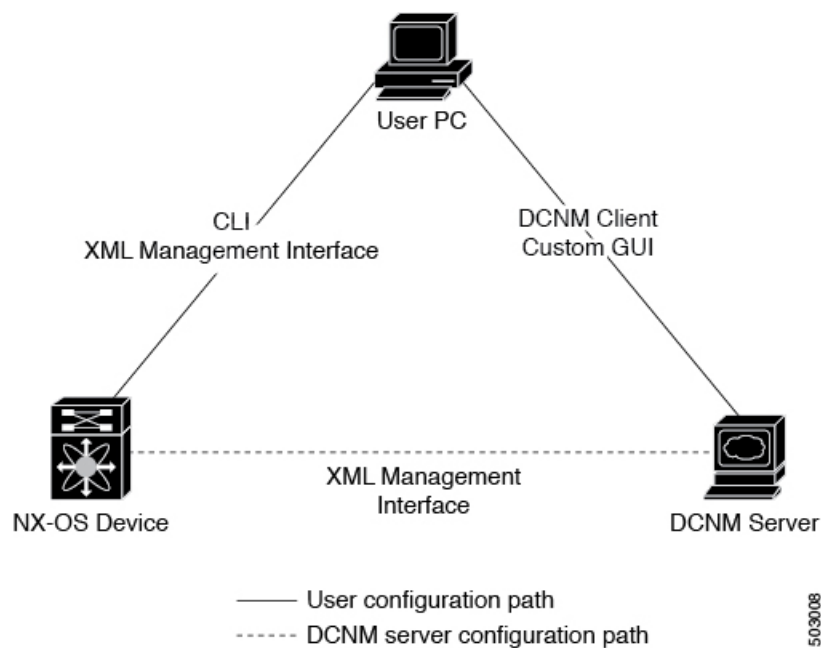
Cisco NX-OS ソフトウェアは、1つの NXOS ソフトウェアイメージで構成されています。このイメージは、すべての Cisco Nexus 3400 シリーズ スイッチで実行されます。

Cisco NX-OS デバイスの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 デバイスのコンフィギュレーション方式



この表に、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 2: コンフィギュレーション方式および参考資料

設定方法	ドキュメント
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 3400 シリーズ NX-OS 基本設定ガイド』
Cisco DCNM クライアント	Cisco DCNM 基本ガイド

CLI または XML 管理インターフェイスで設定する

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から CLI : SSH セッション、Telnet セッション、またはコンソールポート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 9000 シリーズ NX-OS 基本設定ガイド』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 管理ユーザガイド』を参照してください。

Cisco DCNM での設定

Cisco DCNM クライアントを使用して Cisco NX-OS 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、『Cisco DCNM Fundamentals Guide』を参照してください。

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。

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。

セッションマネージャ

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。

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。

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 送信元セッションを設定するには、送信元ポートまたは VLAN のセットを、宛先 IP アドレス、ERSPANID 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。(VRF) 名に対応付けます。

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せん。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。

MPLS ストリッピング

MPLS ストリッピングは、MPLS ラベルをパケットから除去する機能を提供し、非 MPLS 対応 ネットワーク モニタリング ツールでパケットをモニタできるようにします。

sFlow

サンプリングされたフロー (sFlow) では、スイッチとルータを含むデータ ネットワークのリアルタイムトラフィックをモニタし、中央データ コレクタにサンプルデータを転送できます。

SMU

ソフトウェア メンテナンス アップグレード (SMU) は、特定の障害の修正を含むパッケージ ファイルです。SMU は、直近の問題に対処するために作成され、新しい機能は含まれていません。SMU は、メンテナンス リリースの代わりに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。

仮想デバイス コンテキスト

Cisco NX-OS では、仮想デバイスをエミュレートする Virtual Device Context (VDCs) に、OS およびハードウェアリソースを分割できます。Cisco Nexus 9000 シリーズスイッチは、現在のところ、複数の VDC をサポートしていません。すべてのスイッチリソースはデフォルト VDC で管理されます。

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、Trivial File Transfer Protocol (TFTP) のファイル転送ユーティリティを使用して、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 4 章

スイッチ プロファイルの設定

この章では、Cisco Nexus 9000 シリーズ スイッチでスイッチ プロファイルを設定する方法を説明します。

- [スイッチ プロファイルの概要 \(15 ページ\)](#)
- [スイッチ プロファイルの注意事項および制約事項 \(18 ページ\)](#)
- [スイッチ プロファイルの設定 \(19 ページ\)](#)
- [スイッチ プロファイルのコマンドの追加または変更 \(22 ページ\)](#)
- [スイッチ プロファイルのインポート \(23 ページ\)](#)
- [vPC トポロジでの設定のインポート \(25 ページ\)](#)
- [ピア スイッチの分離 \(26 ページ\)](#)
- [スイッチ プロファイルの削除 \(26 ページ\)](#)
- [ミューテックスとマージの失敗の手動修正 \(27 ページ\)](#)
- [スイッチ プロファイル設定の確認 \(28 ページ\)](#)
- [スイッチ プロファイルの設定例 \(28 ページ\)](#)

スイッチ プロファイルの概要

複数のアプリケーションは、ネットワーク内のデバイス間で整合性のある設定が必要です。たとえば、仮想ポート チャンネル (vPC) のコンフィギュレーションを同じにする必要があります。コンフィギュレーションが一致しない場合、エラーやコンフィギュレーションエラーが生じる可能性があります。その結果、サービスが中断することがあります。設定の同期 (config-sync) 機能では、1つのスイッチ プロファイルを設定し、設定を自動的にピア スイッチに同期させることができます。

スイッチ プロファイルには次の利点があります。

- スイッチ間でコンフィギュレーションを同期化できます。
- 2つのスイッチ間で接続が確立されると、コンフィギュレーションがマージされます。
- どのコンフィギュレーションを同期化するかを完全に制御できます。
- マージチェックおよび相互排除チェックを使用して、ピア全体でコンフィギュレーションの一貫性を確保します。

- verify 構文および commit 構文を提供します。
- 既存の vPC 設定をスイッチ プロファイルに移行できます。

スイッチ プロファイル：コンフィギュレーションモード

スイッチ プロファイル機能には、次のコンフィギュレーションモードがあります。

- コンフィギュレーション同期モード (config-sync)
- スイッチ プロファイル モード (config-sync-sp)
- スイッチ プロファイル インポート モード (config-sync-sp-import)

コンフィギュレーション同期モード

コンフィギュレーション同期化モード (config-sync) を使用してスイッチ プロファイルを作成できます。

スイッチ プロファイル モード

スイッチ プロファイルモード (config-sync-sp) では、後でピアスイッチと同期化されるスイッチ プロファイル一時バッファに、サポートされているコンフィギュレーション コマンドを追加できます。スイッチ プロファイルモードで入力するコマンドは、**commit** コマンドを入力するまで実行されません。コマンドを入力すると、コマンドの構文が検証されますが、**commit** コマンドを入力したときにコマンドが正常に実行される保証はありません。

スイッチ プロファイル インポート モード

スイッチ プロファイル インポート モード (config-sync-sp-import) では、既存のスイッチ設定を実行コンフィギュレーションからスイッチ プロファイルインポートし、どのコマンドをプロファイルに含めるかを指定できます。このオプションは、スイッチ プロファイルをサポートしていない Cisco NX-OS リリースからサポートしているリリースにアップグレードする場合に特に役立ちます。

スイッチ プロファイル インポート モードを使用して実行コンフィギュレーションから必要な設定をインポートし、スイッチ プロファイルまたはグローバル コンフィギュレーション モードで追加の変更を行う前に変更を確定することを推奨します。そうしないと、インポートが危険にさらされ、現在のインポートセッションを放棄してプロセスを再実行する必要がある場合があります。詳細については、[スイッチ プロファイルのインポート \(23 ページ\)](#) を参照してください。

コンフィギュレーションの検証

2種類のコンフィギュレーション検証チェックを使用して、スイッチ プロファイルエラーを識別できます。

- 相互排除チェック

- マージ チェック

相互排除チェック

コンフィギュレーション コマンドの相互排除は、`config-sync` およびグローバル コンフィギュレーション モードでのコマンドの重複を避けるために適用されます。スイッチ プロファイルの設定をコミットすると、相互排除 (`mutex`) チェックがローカル スイッチとピア スイッチ (設定されている場合) で実行されます。両方のスイッチで障害が報告されない場合、コミットは受け入れられ、実行コンフィギュレーションにプッシュされます。

スイッチ プロファイルに含まれるコマンドは、スイッチ プロファイル外に設定できます。

`mutex` チェックがエラーを識別すると、`mutex` の障害として報告され、手動で修正する必要があります。詳細は、[ミューテックスとマージの失敗の手動修正 \(27 ページ\)](#) を参照してください。

相互排除ポリシーには、次の例外が適用されます。

- インターフェイス コンフィギュレーション：インターフェイス コンフィギュレーションは、競合しない限り、スイッチプロファイルと実行コンフィギュレーションのそれぞれに部分的に含まれることができます。
- shutdown/no shutdown
- System QoS

マージ チェック

マージ チェックは、コンフィギュレーションを受信する側のピア スイッチで実行されます。マージチェックは、受信したコンフィギュレーションが、受信側のスイッチにすでに存在するスイッチ プロファイル コンフィギュレーションと競合しないようにします。マージ チェックは、確認プロセスまたはコミット プロセス中に実行されます。エラーはマージエラーとして報告され、手動で修正する必要があります。詳細は、[ミューテックスとマージの失敗の手動修正 \(27 ページ\)](#) を参照してください。

1 つまたは両方のスイッチがリロードされ、コンフィギュレーションが初めて同期化される際には、マージ チェックによって、両方のスイッチのスイッチ プロファイル コンフィギュレーションが同じであることが検証されます。スイッチ プロファイルの相違はマージ エラーとして報告され、手動で修正する必要があります。

スイッチプロファイルを使用したソフトウェアのアップグレードとダウングレード

スイッチ プロファイルをサポートする Cisco NX-OS リリースからスイッチ プロファイルをサポートしない Cisco NX-OS リリースにダウングレードする場合、スイッチ プロファイルを削除する必要があります。

旧リリースからスイッチ プロファイルをサポートする Cisco NX-OS リリースにアップグレードする場合、実行コンフィギュレーション コマンドの一部をスイッチ プロファイルに移動することができます。詳細は、[スイッチ プロファイルインポート モード \(16 ページ\)](#) を参照してください。

バッファされた（コミットされていない）設定が存在する場合でもアップグレードを実行できますが、コミットされていないコンフィギュレーションは失われます。

スイッチ プロファイルの注意事項および制約事項

スイッチ プロファイルの注意事項および制約事項

- Cisco NX-OS リリース 9.3(3) 以降、**mtu** コマンドは、インターフェイス コンフィギュレーションモードでスイッチ プロファイル コンフィギュレーションモードを介してサポートされます。
- スイッチ プロファイルは Cisco Nexus 9300 シリーズ スイッチでのみサポートされます。Cisco Nexus 9500 シリーズ スイッチは、スイッチ プロファイルをサポートしていません。
- **mgmt0** インターフェイスを使用するのみ設定同期化をイネーブルにできます。
- 仮想ピアリンク環境で **config-sync** を使用する場合は、次の制限事項に注意してください。
 - 仮想ピアリンクで **config-sync** セッションを開始するには、ピア スイッチ間で管理 IP アドレスの代わりにループバック IP アドレスを設定します。
 - マルチシャード EtherChannel トランク (MCT) 設定と仮想ピアリンク設定の間で設定の同期を実行することはできません。この **config-sync** 操作はサポートされていません。
- 同じスイッチ プロファイル名で同期されたピアを設定する必要があります。
- スイッチ プロファイル設定で使用可能なコマンドを、設定スイッチ プロファイル モード (**config-sync-sp**) で設定できます。
- サポートされているスイッチ プロファイル コマンドは、**vPC** コマンドに関連します。
- 1つのスイッチ プロファイルセッションのみを一度に進行できます。別のセッションの開始を試みると失敗します。
- スイッチ プロファイルセッションの進行中は、グローバル コンフィギュレーションモードから実行されたサポートされているコマンドの変更はブロックされます。
- **commit** コマンドを入力し、ピア スイッチに到達可能である場合、設定は、両方のピア スイッチに適用されるか、いずれのスイッチにも適用されません。コミットの障害が発生した場合、コマンドは、スイッチ プロファイルバッファに残ります。その場合、必要な修正をし、コミットを再試行します。
- コンフィギュレーション同期 (**config-sync**) モードは、コンフィギュレーションターミナルモード (**config t**) と同等の L2 モードです。 **config-sync** は、スイッチ プロファイルを使

用して、ピアスイッチと同じスイッチの **config t** モードを更新します。 **switch-profile** モードでの同期の問題を防ぐために、現在の CLI コマンドを上書きまたは置換する前に、各 CLI コマンドの後にコミットアクションを実行することを推奨します。

たとえば、 **CLI_command_A** を上書きして **CLI_command_B** に変更する場合は、まず **CLI_command_A** をコミットしてから、 **CLI_command_B** を設定し、別のコミットアクションを実行します。

```
switch# conf sync
Enter configuration commands, one per line. End with CNTL/Z.
switch(config-sync)# switch-profile test
Resyncing db before starting Switch-profile.Re-synchronization of switch-profile db
takes a few minutes...
Re-synchronize switch-profile db completed successfully.
Switch-Profile started, Profile ID is 1
switch(config-sync-sp)#
switch(config-sync-sp)# int e 1/3
switch(config-sync-sp-if)# switchport trunk allowed vlan 100-150
switch(config-sync-sp-if)# commit
Verification successful...
Proceeding to apply configuration. This might take a while depending on amount of
configuration in buffer.
Please avoid other configuration changes during this time.
Commit Successful
switch(config-sync)#
switch(config-sync)# switch-profile test
Resyncing db before starting Switch-profile.Re-synchronization of switch-profile db
takes a few minutes...
Re-synchronize switch-profile db completed successfully.
Switch-Profile started, Profile ID is 1
switch(config-sync-sp)#
switch(config-sync-sp)# int e 1/3
switch(config-sync-sp-if)# switchport trunk allowed vlan 45-90
switch(config-sync-sp-if)# commit
Verification successful...
Proceeding to apply configuration. This might take a while depending on amount of
configuration in buffer.
Please avoid other configuration changes during this time.
Commit Successful
switch(config-sync)# end
switch#
```

- レイヤ 3 コマンドはサポートされていません。

スイッチ プロファイルの設定

ローカルスイッチでスイッチ プロファイルを作成および設定し、同期に含まれる 2 番目のスイッチを追加することができます。

スイッチ プロファイルは、各スイッチで同じ名前を使用して作成する必要があります。また、スイッチは互いにピアとして設定する必要があります。同じアクティブなスイッチ プロファイルが設定されたスイッチ間で接続が確立されると、スイッチ プロファイルが同期化されます。

手順

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 必須: cfs ipv4 distribute

例 :

```
switch(config)# cfs ipv4 distribute
```

ピア スイッチ間の Cisco Fabric Services (CFS) 配信を有効にします。

ステップ 3 必須: config sync

例 :

```
switch(config)# config sync
switch(config-sync)#
```

コンフィギュレーション同期モードを開始します。

ステップ 4 必須: switch-profile name

例 :

```
switch(config-sync)# switch-profile abc
switch(config-sync-sp)#
```

スイッチ プロファイルを設定し、スイッチ プロファイルの名前を設定し、スイッチ プロファイル コンフィギュレーション モードを開始します。

ステップ 5 必須: [no] sync-peers destination ip-address

例 :

```
switch(config-sync-sp)# sync-peers destination 10.1.1.1
```

スイッチ プロファイルにスイッチを追加します。宛先 IP アドレスは、同期するスイッチの IP アドレスです。

このコマンドの **no** 形式でスイッチ プロファイルから指定のスイッチを削除します。

(注) コミットが完了する前に、ピア スイッチがスイッチ プロファイル ステータス 「In sync」 を表示するまで待機する必要があります。

ステップ 6 必須: Cisco Nexus 3164Q スイッチの場合のみ、次の手順を実行します。**a) interface type slot/port**

例 :

```
switch(config-sync-sp)# interface ethernet 1/1
switch(config-sync-sp-if)#
```

スイッチ プロファイル 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。

b) switchport

例 :

```
switch(config-sync-sp-if)# switchport
```

レイヤ 3 インターフェイスをレイヤ 2 インターフェイスに変更します。

c) exit

例 :

```
switch(config-sync-sp-if)# exit  
switch(config-sync-sp)#
```

スイッチ プロファイル 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。

d) commit

例 :

```
switch(config-sync-sp)# commit
```

現在の設定をコミットします。

(注) コミットが完了する前に、スイッチ プロファイルのステータスが「Insync」と表示されていることを確認します。

ステップ 7 (任意) end

例 :

```
switch(config-sync-sp)# end  
switch#
```

スイッチ プロファイル コンフィギュレーション モードを終了し、EXEC モードに戻ります。

ステップ 8 (任意) show switch-profile name status

例 :

```
switch# show switch-profile abc status
```

ローカル スイッチのスイッチ プロファイルおよびピア スイッチ情報を表示します。

ステップ 9 (任意) show switch-profile name peer ip-address

例 :

```
switch# show switch-profile abc peer 10.1.1.1
```

スイッチ プロファイルのピアの設定を表示します。

ステップ 10 (任意) copy running-config startup-config

例 :

```
switch# copy running-config startup-config
```

実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

スイッチ プロファイルのコマンドの追加または変更

ローカルおよびピア スイッチでスイッチ プロファイルを設定したら、スイッチ プロファイルにサポートされているコマンドを追加し、コミットする必要があります。

追加または変更されたコマンドは、**commit** コマンドを入力するまでバッファに格納されます。コマンドは、バッファリングされた順序で実行されます。特定のコマンドに順序の依存関係がある場合（たとえば、QoS ポリシーは適用前に定義する必要がある）、その順序を維持する必要があります。そうしないとコミットに失敗する可能性があります。**show switch-profile name buffer** コマンド、**buffer-delete** コマンド、**buffer-move** コマンドなどのユーティリティ コマンドを使用して、バッファを変更し、入力済みのコマンドの順序を修正できます。

手順

	コマンドまたはアクション	目的
ステップ 1	必須: config sync 例 : <pre>switch# config sync switch(config-sync)#</pre>	コンフィギュレーション同期モードを開始します。
ステップ 2	必須: switch-profile name 例 : <pre>switch(config-sync)# switch-profile abc switch(config-sync-sp)#</pre>	スイッチプロファイルを設定し、スイッチプロファイルの名前を設定し、スイッチプロファイル 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	必須: <i>command</i> 例 : <pre>switch(config-sync-sp)# interface Port-channel100 switch(config-sync-sp-if)# speed 1000 switch(config-sync-sp-if)# interface Ethernet1/1 switch(config-sync-sp-if)# speed 1000 switch(config-sync-sp-if)# channel-group 100 switch(config-sync-sp-if)# exit switch(config-sync-sp)#</pre>	スイッチ プロファイルにコマンドを追加します。
ステップ 4	(任意) show switch-profile name buffer 例 : <pre>switch(config-sync-sp)# show switch-profile abc buffer</pre>	スイッチ プロファイルバッファ内のコンフィギュレーション コマンドを表示します。
ステップ 5	必須: verify 例 : <pre>switch(config-sync-sp)# verify</pre>	スイッチ プロファイルバッファ内のコマンドを確認します。

	コマンドまたはアクション	目的
ステップ 6	<p>必須: commit</p> <p>例 :</p> <pre>switch(config-sync-sp) # commit</pre>	<p>スイッチ プロファイルにコマンドを保存し、ピア スイッチと設定を同期します。このコマンドは、次のことも行います。</p> <ul style="list-style-type: none"> • mutex チェックとマージチェックを起動し、同期を確認します。 • ロールバック インフラストラクチャでチェックポイントを作成します。 • スイッチ プロファイル内の任意のスイッチでアプリケーション障害がある場合は、すべてのスイッチでロールバックを実行します。 • チェックポイントを削除します。
ステップ 7	<p>(任意) end</p> <p>例 :</p> <pre>switch(config-sync-sp) # end switch#</pre>	<p>スイッチ プロファイル コンフィギュレーションモードを終了し、EXEC モードに戻ります。</p>
ステップ 8	<p>(任意) show switch-profile name status</p> <p>例 :</p> <pre>switch# show switch-profile abc status</pre>	<p>ローカル スイッチのスイッチ プロファイルのステータスとピア スイッチのステータスを表示します。</p>
ステップ 9	<p>(任意) copy running-config startup-config</p> <p>例 :</p> <pre>switch# copy running-config startup-config</pre>	<p>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。</p>

スイッチ プロファイルのインポート

インポートするコマンドのセットに基づいてスイッチ プロファイルをインポートできます。

始める前に

コマンドをスイッチ プロファイルにインポートする前に、スイッチ プロファイルバッファが空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	<p>(任意) ステップ 4 でインポートするインターフェイスを設定します。</p> <p>例 :</p> <pre>switch(config)# interface ethernet 1/2 switch(config-if)# switchport switch(config-if)# switchport mode trunk switch(config-if)# switchport trunk allowed vlan 12 switch(config-if)# speed 10000 switch(config-if)# spanning-tree port type edge trunk switch(config)# end switch#</pre>	<p>コンフィギュレーション同期モードを開始します。</p>
ステップ 2	<p>config sync</p> <p>例 :</p> <pre>switch# config sync switch(config-sync)#</pre>	<p>コンフィギュレーション同期モードを開始します。</p>
ステップ 3	<p>必須: switch-profile name</p> <p>例 :</p> <pre>switch(config-sync)# switch-profile abc switch(config-sync-sp)#</pre>	<p>スイッチプロファイルを設定し、スイッチプロファイルの名前を設定し、スイッチプロファイル コンフィギュレーションモードを開始します。</p>
ステップ 4	<p>必須: import [interface interface port/slot running-config]</p> <p>例 :</p> <pre>switch(config-sync-sp)# import interface ethernet 1/2 switch(config-sync-sp-import)#</pre>	<p>インポートするコマンドを識別し、スイッチプロファイルインポートモードを開始します。次のオプションを使用できます。</p> <ul style="list-style-type: none"> • オプションを指定せずに import コマンドを入力すると、選択したコマンドがスイッチプロファイルに追加されます。 • import interface オプションは、指定されたインターフェイスでサポートされるコマンドを追加します。 • running-config オプションでは、サポートされるシステムレベル コマンドを追加します。

	コマンドまたはアクション	目的
		(注) 新しいコマンドがインポート中に追加されると、スイッチ プロファイルが保存されていないままになり、スイッチはスイッチ プロファイルインポート モードのままになります。
ステップ 5	必須: commit 例 : <code>switch(config-sync-sp-import)# commit</code>	コマンドをインポートし、スイッチ プロファイルにコマンドを保存します。
ステップ 6	(任意) abort 例 : <code>switch(config-sync-sp-import)# abort</code>	インポート プロセスを中止します。
ステップ 7	(任意) end 例 : <code>switch(config-sync-sp-import)# end</code> <code>switch#</code>	スイッチ プロファイルインポート モードを終了し、EXEC モードに戻ります。
ステップ 8	(任意) show switch-profile 例 : <code>switch# show switch-profile</code>	スイッチ プロファイル コンフィギュレーションを表示します。
ステップ 9	(任意) copy running-config startup-config 例 : <code>switch# copy running-config startup-config</code>	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。

vPC トポロジでの設定のインポート

2 スイッチ vPC トポロジで設定をインポートできます。



(注) 次の手順の詳細については、この章の該当する項を参照してください。

1. 両方のスイッチで、同じ名前を持つスイッチ プロファイルを設定します。
2. 両方のスイッチに設定を個別にインポートします。



(注) 両方のスイッチで、スイッチプロファイルに移動された設定が同じであることを確認します。同じでない場合、マージチェックの障害が発生する場合があります。

3. **sync-peer destination** コマンドを入力してスイッチを設定します。
4. 適切な **show** コマンドを入力して、スイッチプロファイルが同一であることを確認します。

ピア スイッチの分離

スイッチプロファイルを変更するためにピア スイッチを分離できます。このプロセスは、設定の同期をブロックしたり、設定をデバッグしたり、設定同期機能が同期しなくなった状況から回復したりする場合に使用できます。

ピア スイッチを分離するには、スイッチプロファイルからピア接続をブレイクし、スイッチプロファイルにピア スイッチを追加する必要があります。



(注) 次の手順の詳細については、この章の該当する項を参照してください。

1. 両方のスイッチでスイッチプロファイルからピア スイッチを削除できます。
2. **no sync-peers destination** コマンドをスイッチプロファイルに追加し、両方のスイッチで変更をコミットします。
3. 必要なトラブルシューティング設定を追加します。
4. **show running switch-profile** が両方のスイッチで同一であることを確認します。
5. **sync-peers destination ip-address** コマンドを両方のスイッチに追加して、変更をコミットします。
6. ピアが同期中であることを確認します。

スイッチ プロファイルの削除

スイッチプロファイルを削除できます。

手順

	コマンドまたはアクション	目的
ステップ 1	config sync 例 :	コンフィギュレーション同期モードを開始します。

	コマンドまたはアクション	目的
	switch# config sync switch(config-sync)#	
ステップ 2	<p>必須: no switch-profile name {all-config local-config}</p> <p>例 :</p> <pre>switch(config-sync)# no switch-profile abc local-config switch(config-sync-sp) #</pre>	<p>次の手順に従って、スイッチ プロファイルを削除します。</p> <ul style="list-style-type: none"> • all-config : ローカル スイッチおよびピア スイッチのスイッチ プロファイルを削除します。ピア スイッチが到達可能でない場合は、ローカル スイッチ プロファイルだけが削除されます。 • local-config : スイッチ プロファイルおよびローカル コンフィギュレーションを削除します。 <p>(注) スイッチ プロファイルを削除する前に、resync-database を実行することを推奨します。</p> <pre>switch(config-sync) # resync-database</pre>
ステップ 3	<p>(任意) end</p> <p>例 :</p> <pre>switch(config-sync-sp) # end switch#</pre>	スイッチ プロファイル コンフィギュレーション モードを終了し、EXEC モードに戻ります。
ステップ 4	<p>(任意) copy running-config startup-config</p> <p>例 :</p> <pre>switch# copy running-config startup-config</pre>	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。このコマンドを入力すると、 config-sync 機能がピア スイッチで同じ動作をトリガします。

ミューテックスとマージの失敗の手動修正

ミューテックスとマージの障害が発生した場合は、手動で修正できます。



(注) ピア スイッチで競合が発生している場合は、[ピア スイッチの分離 \(26 ページ\)](#) の手順に従ってそのスイッチの問題を修正します。

1. スイッチ プロファイル インポート モードを使用して、問題のコマンドをスイッチ プロファイルにインポートします。

2. 必要に応じて動作を変更します。

スイッチ プロファイル設定の確認

スイッチ プロファイルに関する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
<code>show switch-profile name</code>	スイッチ プロファイル中のコマンドを表示します。
<code>show switch-profile name buffer</code>	スイッチ プロファイル中のコミットされていないコマンド、移動されたコマンド、削除されたコマンドを表示します。
<code>show switch-profile name peer ip-address</code>	ピア スイッチの同期ステータスが表示されます。
<code>show switch-profile name session-history</code>	最後の 20 のスイッチ プロファイルセッションのステータスを表示します。
<code>show switch-profile name status</code>	ピア スイッチのコンフィギュレーション同期ステータスを表示します。
<code>show running-config switch-profile</code>	ローカル スイッチのスイッチ プロファイルの実行コンフィギュレーションを表示します。
<code>show startup-config switch-profile</code>	ローカル スイッチのスイッチ プロファイル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。

スイッチ プロファイルの設定例

ローカルおよびピア スイッチでのスイッチ プロファイルの作成...

次に、ローカルおよびピア スイッチで正常にスイッチ プロファイル設定を作成する例を示します。これには QoS ポリシー（vPC ピアリンクおよびスイッチ プロファイル中の vPC）の設定が含まれます。

1. ローカルおよびピア スイッチで CFS 配信を有効にし、スイッチの管理インターフェイスなど、同期するスイッチの宛先 IP アドレスを設定します。

```
-Local switch-1#---
switch-1# configure terminal
switch-1(config)# cfs ipv4 distribute
switch-1(config)# interface mgmt 0
switch-1(config-if)# ip address 30.0.0.81/8

-Peer switch-2#--
```



```
switch-2# configure terminal
switch-2(config)# cfs ipv4 distribute
switch-2(config)# interface mgmt 0
switch-2(config-if)# ip address 30.0.0.82/8
```

2. ローカルおよびピア スイッチで新しいスイッチ プロファイルを作成します。

```
-Local switch-1#---
switch-1# config sync
switch-1(config-sync)# switch-profile A
Switch-Profile started, Profile ID is 1
switch-1(config-sync-sp)# sync-peers destination 30.0.0.82
switch-1(config-sync-sp)# end

-Peer switch-2#--
switch-1# config sync
switch-1(config-sync)# switch-profile A
Switch-Profile started, Profile ID is 1
switch-1(config-sync-sp)# sync-peers destination 30.0.0.81
switch-1(config-sync-sp)# end
```

3. スイッチプロファイルが、ローカルおよびピア スイッチで同じであることを確認します。

```
switch-1(config-sync-sp)# show switch-profile status

switch-profile : A
-----

Start-time: 843992 usecs after Wed Aug 19 17:00:01 2015
End-time: 770051 usecs after Wed Aug 19 17:00:03 2015

Profile-Revision: 1
Session-type: Initial-Exchange
Session-subtype: Init-Exchange-All
Peer-triggered: Yes
Profile-status: Sync Success

Local information:
-----
Status: Commit Success
Error(s):

Peer information:
-----
IP-address: 30.0.0.82
Sync-status: In sync
Status: Commit Success
Error(s):
```

4. ローカル スイッチでスイッチ プロファイルにコンフィギュレーション コマンドを追加します。コマンドがコミットされたときに、コマンドがピア スイッチに適用されます。

```
switch-1# config sync
switch-1(config-sync)# switch-profile A
Switch-Profile started, Profile ID is 1
switch-1(config-sync-sp)# interface port-channel 10
switch-1(config-sync-sp-if)# switchport
switch-1(config-sync-sp-if)# commit
Verification successful...
Proceeding to apply configuration. This might take a while depending on amount of
configuration in buffer.
```

```

Please avoid other configuration changes during this time.
Commit Successful
switch-1(config-sync)# switch-profile A
Switch-Profile started, Profile ID is 1
switch-1(config-sync-sp)# interface port-channel 10
switch-1(config-sync-sp-if)# switchport mode trunk
switch-1(config-sync-sp-if)# switchport trunk allowed vlan 10
switch-1(config-sync-sp-if)# spanning-tree port type network
switch-1(config-sync-sp-if)# vpc peer-link
switch-1(config-sync-sp-if)# switch-profile switching-mode switchname
switch-1(config-sync-sp-if)# show switch-profile buffer

switch-profile : A
-----
Seq-no Command
-----

1 interface port-channel10
1.1 switchport mode trunk
1.2 switchport trunk allowed vlan 10
1.3 spanning-tree port type network
1.4 vpc peer-link

switch-1(config-sync-sp-if)# commit
Verification successful...
Proceeding to apply configuration. This might take a while depending on amount of
configuration in buffer.
Please avoid other configuration changes during this time.
Commit Successful
switch-1(config-sync)# switch-profile A
Switch-Profile started, Profile ID is 1
switch-1(config-sync-sp)# interface ethernet 2/1
switch-1(config-sync-sp-if)# switchport mode trunk
switch-1(config-sync-sp-if)# switchport trunk allowed vlan 10
switch-1(config-sync-sp-if)# spanning-tree port type network
switch-1(config-sync-sp-if)# channel-group 10 mode active

```

5. バッファリングされたコマンドを表示します。

```

switch-1(config-sync-sp-if)# show switch-profile buffer

switch-profile : A
-----
Seq-no Command
-----

1 interface Ethernet2/1
1.1 switchport mode trunk
1.2 switchport trunk allowed vlan 10
1.3 spanning-tree port type network
1.4 channel-group 10 mode active

```

6. スイッチ プロファイルのコマンドを検証します。

```

switch-1(config-sync-sp-if)# verify
Verification Successful

```

7. スイッチ プロファイルにコマンドを適用し、ローカルとピアスイッチ間の設定を同期させます。

```

-Local switch-2#--
switch-1(config-sync-sp)# commit
Verification successful...

```

```

Proceeding to apply configuration. This might take a while depending on amount of
configuration in buffer.
Please avoid other configuration changes during this time.
Commit Successful
switch-1(config-sync)# end

switch-1# show running-config switch-profile

switch-profile A
sync-peers destination 30.0.0.82

interface port-channel10
switchport mode trunk
switchport trunk allowed vlan 10
spanning-tree port type network
vpc peer-link

interface Ethernet2/1
switchport mode trunk
switchport trunk allowed vlan 10
spanning-tree port type network
channel-group 10 mode active

--Peer switch-2#--
switch-2# show running-config switch-profile

switch-profile A
sync-peers destination 30.0.0.81

interface port-channel10
switchport mode trunk
switchport trunk allowed vlan 10
spanning-tree port type network
vpc peer-link

interface Ethernet2/1
switchport mode trunk
switchport trunk allowed vlan 10
spanning-tree port type network
channel-group 10 mode active

```

同期ステータスの確認

次に、ローカルとピア スイッチ間の同期ステータスを確認する例を示します。

```

switch-1# show switch-profile status

switch-profile : A
-----switch-1-----

Start-time: 912776 usecs after Wed Aug 19 17:03:43 2015
End-time: 868379 usecs after Wed Aug 19 17:03:48 2015

Profile-Revision: 4
Session-type: Commit
Session-subtype: -
Peer-triggered: No
Profile-status: Sync Success

Local information:

```

```

-----
Status: Commit Success
Error(s):

Peer information:
-----
IP-address: 30.0.0.82
Sync-status: In sync
Status: Commit Success
Error(s):

```

実行中のコンフィギュレーションの表示

次に、ローカルスイッチでスイッチ プロファイルの実行コンフィギュレーションを表示する方法の例を示します。

```

— PEER SWITCH-1 —
switch-1# show running-config switch-profile

```

```

switch-profile A
sync-peers destination 30.0.0.82

interface port-channel10
switchport mode trunk
switchport trunk allowed vlan 10
spanning-tree port type network
vpc peer-link

interface Ethernet2/1
switchport mode trunk
switchport trunk allowed vlan 10
spanning-tree port type network
channel-group 10 mode active
switch-1#

```

```

— PEER SWITCH-2 —
switch-2# show running-config switch-profile

```

```

switch-profile A
sync-peers destination 30.0.0.81

interface port-channel10
switchport mode trunk
switchport trunk allowed vlan 10
spanning-tree port type network
vpc peer-link

interface Ethernet2/1
switchport mode trunk
switchport trunk allowed vlan 10
spanning-tree port type network
channel-group 10 mode active
switch-2#

```

ローカルとピアスイッチ間のスイッチ プロファイルの同期の表示

次に、2 台のピア間の最初の正常な同期を表示する例を示します。

```
switch1# show switch-profile sp status

Start-time: 491815 usecs after Mon Jul 20 11:54:51 2015
End-time: 449475 usecs after Mon Jul 20 11:54:58 2015

Profile-Revision: 1
Session-type: Initial-Exchange
Peer-triggered: No
Profile-status: Sync Success

Local information:
-----
Status: Commit Success
Error(s):

Peer information:
-----
IP-address: 10.193.194.52
Sync-status: In Sync.
Status: Commit Success
Error(s):

switch2# show switch-profile sp status

Start-time: 503194 usecs after Mon Jul 20 11:54:51 2015
End-time: 532989 usecs after Mon Jul 20 11:54:58 2015

Profile-Revision: 1
Session-type: Initial-Exchange
Peer-triggered: Yes
Profile-status: Sync Success

Local information:
-----
Status: Commit Success
Error(s):

Peer information:
-----
IP-address: 10.193.194.51
Sync-status: In Sync.
Status: Commit Success
Error(s):
```

ローカルおよびピア スイッチでの確認とコミットの表示

次に、ローカル スイッチおよびピア スイッチで正常に確認とコミットを実行する例を示します。

```
switch1# config sync
switch1(config-sync)# switch-profile sp
Switch-Profile started, Profile ID is 1
switch1(config-sync-sp)# interface Ethernet1/1
switch1(config-sync-sp-if)# description foo
switch1(config-sync-sp-if)# exit
switch1(config-sync-sp)# verify
Verification Successful
switch1(config-sync-sp)# commit
Commit Successful
switch1(config-sync)# show running-config switch-profile
```

```

switch-profile sp
  sync-peers destination 10.193.194.52
  interface Ethernet1/1
    description foo
switch1(config-sync)# show switch-profile sp status

Start-time: 171513 usecs after Wed Jul 20 17:51:28 2015
End-time: 676451 usecs after Wed Jul 20 17:51:43 2015

Profile-Revision: 3
Session-type: Commit
Peer-triggered: No
Profile-status: Sync Success

Local information:
-----
Status: Commit Success
Error(s):

Peer information:
-----
IP-address: 10.193.194.52
Sync-status: In Sync.
Status: Commit Success
Error(s):

switch1(config-sync)#

switch2# show running-config switch-profile
switch-profile sp
  sync-peers destination 10.193.194.51
  interface Ethernet1/1
    description foo
switch2# show switch-profile sp status

Start-time: 265716 usecs after Mon Jul 20 16:51:28 2015
End-time: 734702 usecs after Mon Jul 20 16:51:43 2015

Profile-Revision: 3
Session-type: Commit
Peer-triggered: Yes
Profile-status: Sync Success

Local information:
-----
Status: Commit Success
Error(s):

Peer information:
-----
IP-address: 10.193.194.51
Sync-status: In Sync.
Status: Commit Success
Error(s):

```

ローカルおよびピア スイッチ間の成功および失敗した同期の表示

次に、ピア スイッチでスイッチ プロファイルの同期ステータスを設定する例を示します。最初の例は正常な同期を示し、2 番目の例はピアの到達不能な状態を示します。

```

switch1# show switch-profile sp peer

switch1# show switch-profile sp peer 10.193.194.52
Peer-sync-status      : In Sync.
Peer-status           : Commit Success
Peer-error(s)        :
switch1#

switch1# show switch-profile sp peer 10.193.194.52
Peer-sync-status      : Not yet merged. pending-merge:1 received_merge:0
Peer-status           : Peer not reachable
Peer-error(s)        :

```

スイッチ プロファイルバッファの表示

次に、スイッチ プロファイルバッファの設定、バッファ移動、バッファ削除を設定する例を示します。

```

switch1# config sync
switch1(config-sync)# switch-profile sp
Switch-Profile started, Profile ID is 1
switch1(config-sync-sp)# vlan 101
switch1(config-sync-sp-vlan)# ip igmp snooping querier 10.101.1.1
switch1(config-sync-sp-vlan)# exit
switch1(config-sync-sp)# mac address-table static 0000.0000.0001 vlan 101 drop
switch1(config-sync-sp)# interface Ethernet1/2
switch1(config-sync-sp-if)# switchport mode trunk
switch1(config-sync-sp-if)# switchport trunk allowed vlan 101
switch1(config-sync-sp-if)# exit
switch1(config-sync-sp)# show switch-profile sp buffer
-----
Seq-no  Command
-----
1       vlan 101
1.1     ip igmp snooping querier 10.101.1.1
2       mac address-table static 0000.0000.0001 vlan 101 drop
3       interface Ethernet1/2
3.1     switchport mode trunk
3.2     switchport trunk allowed vlan 101

switch1(config-sync-sp)# buffer-move 3 1
switch1(config-sync-sp)# show switch-profile sp buffer
-----
Seq-no  Command
-----
1       interface Ethernet1/2
1.1     switchport mode trunk
1.2     switchport trunk allowed vlan 101
2       vlan 101
2.1     ip igmp snooping querier 10.101.1.1
3       mac address-table static 0000.0000.0001 vlan 101 drop

switch1(config-sync-sp)# buffer-delete 1
switch1(config-sync-sp)# show switch-profile sp buffer
-----
Seq-no  Command
-----
2       vlan 101
2.1     ip igmp snooping querier 10.101.1.1
3       mac address-table static 0000.0000.0001 vlan 101 drop

```

```
switch1(config-sync-sp)# buffer-delete all
switch1(config-sync-sp)# show switch-profile sp buffer
```

設定のインポート

次に、インターフェイス コンフィギュレーションをインポートする例を示します。

```
switch# show running-config interface Ethernet1/3

!Command: show running-config interface Ethernet1/3
!Time: Wed Jul 20 18:12:44 2015

version 7.0(3)I2(1)

interface Ethernet1/3
  switchport mode trunk
  switchport trunk allowed vlan 1-100

switch# config sync
switch(config-sync)# switch-profile sp
Switch-Profile started, Profile ID is 1

switch(config-sync-sp)# import interface Ethernet1/3
switch(config-sync-sp-import)# show switch-profile sp buffer
-----
Seq-no  Command
-----
1       interface Ethernet1/3
1.1     switchport mode trunk
1.2     switchport trunk allowed vlan 1-100

switch(config-sync-sp-import)# verify
Verification Successful
switch(config-sync-sp-import)# commit
Commit Successful
```

次に、実行コンフィギュレーションにサポートされるコマンドをインポートする例を示します。

```
switch(config-sync)# switch-profile sp
Switch-Profile started, Profile ID is 1
switch(config-sync-sp)# import running-config
switch(config-sync-sp-import)# show switch-profile sp buffer
-----
Seq-no  Command
-----
1       logging event link-status default
2       vlan 1
3       interface port-channel 3
3.1     switchport mode trunk
3.2     vpc peer-link
3.3     spanning-tree port type network
4       interface port-channel 30
4.1     switchport mode trunk
4.2     vpc 30
4.3     switchport trunk allowed vlan 2-10
5       interface port-channel 31
5.1     switchport mode trunk
5.2     vpc 31
```



```
5.3      switchport trunk allowed vlan 11-20
6        interface port-channel 101
6.1      switchport mode fex-fabric
6.2      fex associate 101
7        interface port-channel 102
7.1      switchport mode fex-fabric
7.2      vpc 102
7.3      fex associate 102
8        interface port-channel 103
8.1      switchport mode fex-fabric
8.2      vpc 103
8.3      fex associate 103
9        interface Ethernet1/1
10       interface Ethernet1/2
11       interface Ethernet1/3
12       interface Ethernet1/4
12.1     switchport mode trunk
12.2     channel-group 3
13       interface Ethernet1/5
13.1     switchport mode trunk
13.2     channel-group 3
14       interface Ethernet1/6
14.1     switchport mode trunk
14.2     channel-group 3
15       interface Ethernet1/7
15.1     switchport mode trunk
15.2     channel-group 3
16       interface Ethernet1/8
17       interface Ethernet1/9
17.1     switchport mode trunk
17.2     switchport trunk allowed vlan 11-20
17.3     channel-group 31 mode active
18       interface Ethernet1/10
18.1     switchport mode trunk
18.2     switchport trunk allowed vlan 11-20
18.3     channel-group 31 mode active
19       interface Ethernet1/11
20       interface Ethernet1/12
...
45       interface Ethernet2/4
45.1     fex associate 101
45.2     switchport mode fex-fabric
45.3     channel-group 101
46       interface Ethernet2/5
46.1     fex associate 101
46.2     switchport mode fex-fabric
46.3     channel-group 101
47       interface Ethernet2/6
47.1     fex associate 101
47.2     switchport mode fex-fabric
47.3     channel-group 101
48       interface Ethernet2/7
48.1     fex associate 101
48.2     switchport mode fex-fabric
48.3     channel-group 101
49       interface Ethernet2/8
49.1     fex associate 101
...
89       interface Ethernet100/1/32
90       interface Ethernet100/1/33
91       interface Ethernet100/1/34
92       interface Ethernet100/1/35
93       interface Ethernet100/1/36
...
```

```
105      interface Ethernet100/1/48
```

ファブリック エクステンダのストレート型トポロジでの Cisco NX-OS リリース 7.0(3)I2(1) 以降への移行

この例では、ファブリック エクステンダのアクティブ/アクティブ トポロジまたはストレート型トポロジで Cisco NX-OS リリース 7.0(3)I2(1) 以降に移行するために使用するタスクを示します。タスクの詳細については、この章の該当する項を参照してください。

1. 両方のスイッチで設定が同じであることを確認します。
2. 両方のスイッチで、同じ名前を持つスイッチ プロファイルを設定します。
3. 両方のスイッチのすべての vPC ポート チャンネルについて、**import interface port-channel x-y, port-channel z** コマンドを入力します。
4. **show switch-profile name buffer** コマンドを入力し、すべての設定が両方のスイッチで正しくインポートされていることを確認します。
5. バッファを編集して不要な設定を削除します。
6. 両方のスイッチで **commit** コマンドを入力します。
7. **sync-peers destination ip-address** コマンドを入力して、両方のスイッチでピアスイッチを設定します。
8. **show switch-profile name status** コマンドを入力して、両方のスイッチが同期状態であることを確認します。

Cisco Nexus 9000 シリーズ スイッチの交換

Cisco Nexus 9000 シリーズ スイッチを交換する場合、交換するスイッチで次の設定手順を実行し、既存の Cisco Nexus 9000 シリーズ スイッチと同期する必要があります。この手順は、ハイブリッドファブリック エクステンダのアクティブ/アクティブトポロジとファブリック エクステンダストレート型トポロジで実行できます。

1. ピアリンク、vPC、アクティブ/アクティブ、またはストレート型のトポロジファブリック ポートを交換用スイッチに接続しないでください。
2. 交換するスイッチを起動します。スイッチは設定なしで起動します。
3. 交換スイッチを設定します。
 - 実行コンフィギュレーションがオフラインで保存された場合は、手順4～8に進み、設定を適用します。
 - 実行コンフィギュレーションがオフラインで保存されなかった場合で、設定同期機能がイネーブルの場合、ピアスイッチから実行コンフィギュレーションを取得でき

ます（ローカルおよびピア スイッチでのスイッチ プロファイルの作成...（28 ページ））の手順 1 および 2 を参照してください。その後、手順 9 から開始します）。

- いずれの条件にも当てはまらない場合は、手動で設定を追加し、以下の手順 9 に進みます。

4. 設定同期機能を使用している場合は、コンフィギュレーション ファイルを編集し、**sync-peer** コマンドを削除します。
5. mgmt ポート IP アドレスを設定し、コンフィギュレーション ファイルをダウンロードします。
6. 実行コンフィギュレーションに、コンフィギュレーション ファイルをコピーします。
7. **show running-config** コマンドを入力して、コンフィギュレーションが正しいことを確認します。
8. 交換スイッチが動作していない間に、ピア スイッチでスイッチ プロファイルの設定が変更された場合、スイッチ プロファイルでこれらの設定を適用して、**commit** コマンドを入力します。
9. vPC トポロジに含まれるすべてのファブリック エクステンダ ストレート型 トポロジ ポートをシャットダウンします。
10. ファブリック エクステンダ ストレート型 トポロジ ファブリック ポートを接続します。
11. ファブリック エクステンダ ストレート型 トポロジ スイッチがオンラインになるまで待ちます。
12. 既存スイッチの vPC のロールプライオリティが、交換スイッチよりも上位であることを確認します。
13. ピア リンク ポートをピア スイッチに接続します。
14. スイッチ vPC ポートを接続します。
15. すべてのファブリック エクステンダ ストレート型 vPC ポートで、**no shutdown** コマンドを入力します。
16. 交換スイッチにあるすべての vPC スイッチおよびファブリック エクステンダ がオンラインになり、トラフィックに中断がないことを確認します。
17. 設定同期機能を使用している場合、手順 3 で有効にされなかった場合は、**sync-peer** の設定をスイッチ プロファイルに追加します。
18. コンフィギュレーション同期機能を使用している場合、**show switch-profile name status** コマンドを使用し、両方のスイッチが同期されるようにします。

設定の同期

Cisco Nexus 9000 シリーズ スイッチのリブート後の設定の同期化

スイッチプロファイルを使用して新しい設定がピアスイッチでコミットされている中で Cisco Nexus 9000 シリーズ スイッチがリブートする場合、これらの手順に従いリロード後にピアスイッチを同期します。

1. 両方のスイッチでスイッチプロファイルからピアスイッチを削除できます。
2. **no sync-peers destination** コマンドをスイッチプロファイルに追加し、両方のスイッチで変更をコミットします。
3. 欠落または変更されたコマンドを追加します。
4. `show running switch-profile` が両方のスイッチで同一であることを確認します。
5. **sync-peers destination ip-address** コマンドを両方のスイッチに追加して、変更をコミットします。
6. ピアが同期中であることを確認します。

mgmt0 インターフェイスの接続が失われた場合の設定の同期化

mgmt0 インターフェイスの接続が失われ、設定変更が必要な場合は、スイッチプロファイルを使用して、両方のスイッチに設定変更を適用します。mgmt0 インターフェイスへの接続が復元されると、両方のスイッチが同期されます。

このシナリオで設定変更が1台のスイッチのみで実行された場合、マージは、mgmt0 インターフェイスが起動し、設定が他のスイッチに適用されたときに成功します。

グローバル コンフィギュレーション モードでレイヤ 2 からレイヤ 3 への不注意によるポート モードの変更を元に戻す

config-sync モードでインポートされたポートに関連する設定は、グローバルコンフィギュレーション モードで設定しないでください。通常、そのような試みは config-sync 機能によって拒否され、mutex 警告が表示されます。ただし、mutex チェックの制限により、config-sync モードでレイヤ 2 として設定されたポートが、グローバル コンフィギュレーション モードでレイヤ 3 (スイッチポートなし) に変更された場合、config-sync 機能は検出および防止できません。その結果、config-sync モードがグローバル コンフィギュレーション モードと同期しなくなる可能性があります。この場合は、次の手順に従って変更を元に戻します。

1. 両方のスイッチでスイッチプロファイルからピアスイッチを削除できます。
2. **no sync-peers destination** コマンドをスイッチプロファイルに追加し、両方のスイッチで変更をコミットします。
3. 現在のインターフェイス設定をインポートします。
4. 必要な変更を加えてコミットします。

5. `show running switch-profile` が両方のスイッチで同一であることを確認します。
6. `sync-peers destination ip-address` コマンドを両方のスイッチに追加して、変更をコミットします。
7. ピアが同期中であることを確認します。

■ グローバル コンフィギュレーション モードでレイヤ 2 からレイヤ 3 への不注意によるポート モードの変更を元に戻す



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。

- [PTP について \(43 ページ\)](#)
- [PTP の注意事項および制約事項 \(48 ページ\)](#)
- [PTP のデフォルト設定 \(50 ページ\)](#)
- [PTP の設定 \(51 ページ\)](#)
- [タイムスタンプ タギング \(63 ページ\)](#)
- [PTP 設定の確認 \(66 ページ\)](#)
- [PTP の設定例 \(67 ページ\)](#)
- [その他の参考資料 \(70 ページ\)](#)

PTP について

PTP は、ネットワークに分散したノード間で時刻同期を行うプロトコルで、IEEE 1588 に定義されています。PTP を使用すると、イーサネットネットワークを介して 1 マイクロ秒未満の精度で、分散したクロックを同期できます。さらに、PTP のハードウェア タイムスタンプ機能は、ERSPAN タイプ III ヘッダのタイムスタンプ情報を提供します。この情報は、エッジスイッチ、集約スイッチ、およびコアスイッチ間のパケット遅延の計算に使用できます。

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 は次の機能をサポートしています。

- マルチキャストおよびユニキャスト PTP 転送：マルチキャスト転送モードでは、PTP はデバイス間の通信に IEEE 1588 標準に従ってマルチキャスト宛先 IP アドレス 224.0.1.129 を使用します。送信元 IP アドレスの場合、PTP ドメインでユーザが設定可能なグローバル IP アドレスを使用します。ユニキャストトランスポートモードでは、PTP はインターフェイスで設定可能な設定可能なユニキャスト送信元および宛先 IP アドレスを使用します。ユニキャストモードとマルチキャストモードの両方で、PTP は UDP ポートを使用します。イベントメッセージには 319、デバイス間の一般的なメッセージ通信には 320 を使用します。
- PTP マルチキャスト設定は、L2 または L3 の物理インターフェイスでのみサポートされます。L3 物理インターフェイスでのみサポートされるユニキャスト PTP 設定。PTP は、ポートチャネル、SVI、トンネルなどの仮想インターフェイスではサポートされません。
- IP over UDP over PTP カプセル化：PTP は、IP 上のトランスポートプロトコルとして UDP を使用します。ユニキャストモードとマルチキャストモードの両方で、PTP はイベントメッセージに UDP ポート 319 を使用し、デバイス間の一般的なメッセージ通信に 320 を使用します。L2 カプセル化モードは、ではサポートされていません。
- PTP プロファイル：PTP はデフォルト (1588)、AES67、および SMPTE 2059-2 プロファイルをサポートします。すべての同期要求間隔と遅延要求間隔が異なります。デフォルトプロファイルの詳細については、IEEE 1588 を参照してください。AES67 および SMPTE 2059-2 の詳細については、それぞれの仕様を参照してください。
- パス遅延測定：マスターとスレーブのデバイス間の遅延を測定する遅延要求および応答メカニズムをサポートします。ピア遅延要求および応答メカニズムは、ではサポートされていません。
- メッセージ間隔：デバイス間でアナウンス、同期、および遅延要求メッセージを送信する必要がある間隔を設定できます。
- ベスト マスター クロック (BMC) の選択：BMC アルゴリズムは、1588 仕様に従って受信したアナウンスメッセージに基づいて、PTP 対応インターフェイスのマスター、スレーブ、およびパッシブ状態を選択するために使用されます。

PTP オフロード

この機能により、ラインカードに PTP 機能が分散され、システムでサポートされる PTP セッション数のスケーリングが可能になります。この機能は、9700-EX、9700-FX、9636C-R、9636Q-R、および 9636C-RX ラインカードを搭載した Cisco Nexus 9500 プラットフォーム スイッチで使用できます。

PTP デバイス タイプ

PTP デバイス タイプは設定可能で、クロック タイプの設定に使用できます。

クロック

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) 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 (10 MHz) 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。

クロック モード

IEEE 1588 規格は、PTP をサポートするデバイスが 1 ステップと 2 ステップで動作するための 2 つのクロックモードを指定しています。

1 ステップ モード :

1 ステップモードでは、クロック同期メッセージに、マスターポートがメッセージを送信した時刻が含まれます。ASIC は、同期メッセージがポートを出るときにタイムスタンプを追加します。1 ステップモードで動作するマスターポートは、Cisco Nexus 9508-FM-R および 9504-FM-R ファブリック モジュール、および Cisco Nexus 9636C-R、9636Q-R、および 9636C-RX ラインカードで使用できます。

スレーブポートは、同期メッセージの一部として送信されるタイムスタンプを使用します。

2 ステップ モード :

2 ステップモードでは、同期メッセージがポートを出た時刻は後続のフォローアップメッセージで送信されます。これは、デフォルトのモードです。

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

オーディナリクロックと境界クロックは、**Sync**、**Delay_Req**、**Follow_Up**、**Delay_Resp** イベントメッセージを使用してタイミング情報を生成し、伝えます。

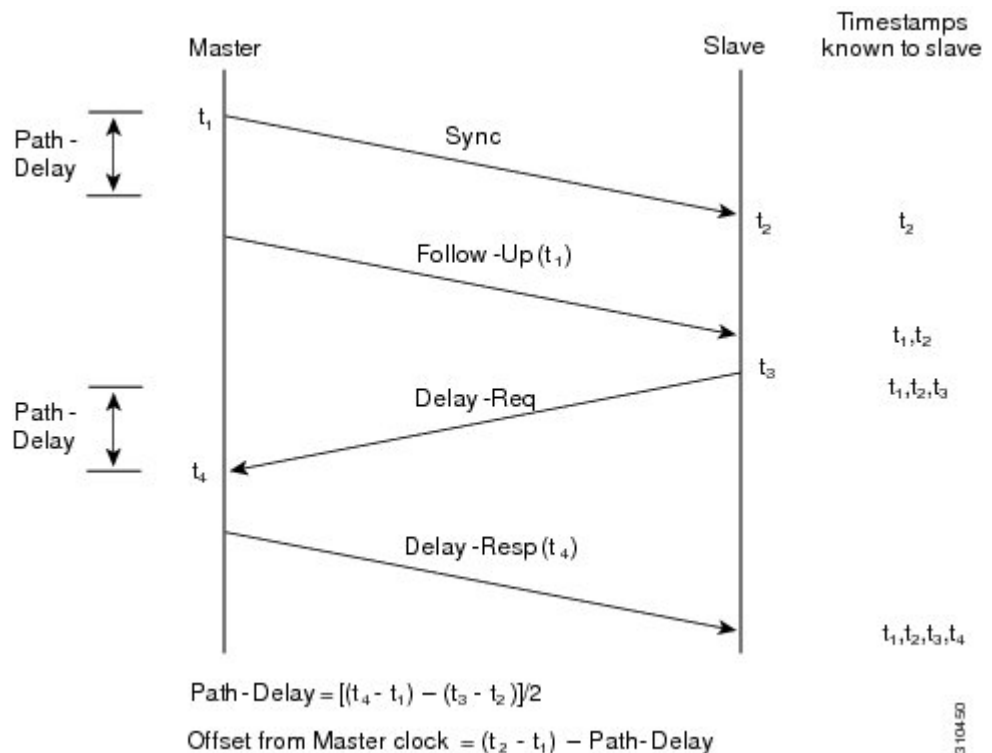
これらのメッセージは、次のシーケンスで送信されます。

1. マスターが、スレーブに **Sync** メッセージを送信し、それが送信された時刻 (t_1) を記録します。1 ステップ **Sync** メッセージの場合、メッセージはマスターから送り出された時刻を示します。2 ステップメッセージの場合、この時刻は、後続の **Follow-Up** イベントメッセージで送信されます。
2. スレーブは、**Sync** メッセージを受信し、受信した時刻 (t_2) を記録します。
3. マスターはスレーブに対し、タイムスタンプ t_1 を、**Follow_Up** イベントメッセージに埋め込むことにより送信します。
4. スレーブはマスターに対し、**Delay_Req** メッセージを送信し、送信した時刻 t_3 を記録します。

5. マスターは **Delay_Req** メッセージを受信し、受信した時刻、 t_4 を記録します。
6. マスターはスレーブに対し、タイムスタンプ t_4 を、**Delay_Resp** メッセージに埋め込むことによって送信します。
7. このシーケンスの後、スレーブは4つすべてのタイムスタンプを所有します。これらのタイムスタンプを使用して、マスターに対するスレーブクロックのオフセットと、2つのクロック間のメッセージの平均伝達時間を計算できます。

次の図は、タイミング情報を生成して通信する PTP プロセスのイベントメッセージを示しています。

図 2: PTP プロセス



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はサポートされません。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 シリーズ NX-OS ハイアベイラビリティおよび冗長性ガイド](#)』を参照してください。

PTP の注意事項および制約事項



(注) スケールの情報については、リリース特定の『Cisco Nexus 9000 Series NX-OS Verified Scalability Guide』を参照してください。

PTP 用 Cisco Nexus 9000 シリーズスイッチの注意事項と制約事項は次のとおりです。

- PTP が正常に機能するには、最新の SUP およびラインカードの FPGA バージョンを使用する必要があります。FPGA のアップグレードについては、リリースノートのランディングページにアクセスし、「FPGA/EPLD アップグレードリリースノート (NX-OS モードスイッチ)」セクションに移動して、ご使用のソフトウェアバージョンの FPGA/EPLD アップグレードリリースノートを参照してください。 <https://www.cisco.com/c/en/us/support/switches/nexus-9000-series-switches/products-release-notes-list.html> 「インストールガイドライン」のトピックを参照してください。
- 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。
- ユーザ データグラム プロトコル (UDP) 上の PTP 転送がサポートされます。Transport over Ethernet はサポートされません。
- PTP はマルチキャスト通信をサポートします。PTP はユニキャスト通信もサポートしていますが、ユニキャストモードはオプションです。
- PTP は境界クロック モードをサポートします。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 デバイスにはマルチキャストまたはユニキャスト PTP モードを設定することを推奨しますが、マルチキャストモードとユニキャストモードの両方を一緒に設定することは推奨しません。
- PTP はポートチャネル メンバー ポートで有効にできます。
- スレーブ ポートから受信したすべての管理メッセージは、すべての PTP 対応ポートに転送されます。スレーブ ポートから受信した管理メッセージは処理されません。
- タイムスタンプタギング (TTAG) は、次のプラットフォームスイッチでサポートされています。
 - Cisco Nexus 9200 プラットフォーム スイッチ : Cisco NX-OS リリース 7.0(3)I6(1) 以降
 - Cisco Nexus 9364C : Cisco NX-OS リリース 7.0(3)I7(2) 以降
 - Cisco Nexus 9332C : Cisco NX-OS リリース 9.2(3) 以降
 - Cisco Nexus 9300-EX プラットフォーム スイッチ : Cisco NX-OS リリース 7.0(3)I6(1) 以降

- Cisco Nexus 9300-FX プラットフォーム スイッチ : Cisco NX-OS リリース 7.0(3)I7(3) 以降
 - Cisco Nexus 9300-FX2 プラットフォーム スイッチ : Cisco NX-OS リリース 9.3(3) 以降
 - -EX/-FX ライン カード搭載の Cisco Nexus 9500 プラットフォーム スイッチ
- RACL を使用して PTP 制御パケットを照合するには、L3 インターフェイスで PIM を有効にします。
 - Cisco Nexus 9000 シリーズ スイッチに PTP を設定する場合は、`clock protocol ptp vdc 1` コマンドを使用して、PTP を使用するようにクロックプロトコルを設定します。NTP は、Cisco Nexus 9000 シリーズ スイッチに設定された PTP と共存できません。
 - PTP は、100G 9408PC ライン カードおよび 100G M4PC 汎用拡張モジュール (GEM) を除き、すべての Cisco Nexus 9000 シリーズおよび 3164Q ハードウェアでは利用できません。
 - Cisco NX-OS リリース 9.3(3) 以降、Cisco Nexus 9504-FM-R プラットフォーム スイッチでは PTP が利用できます。
 - PTP `correction-range`、PTP `correction-range logging`、および PTP `mean-path-delay` コマンドは、Cisco Nexus 9508-R ライン カードでサポートされます。
 - Cisco Nexus 31108PC-V および 31108TC-V スイッチの場合、100 G の速度で動作するポートでは PTP はサポートされません。
 - Cisco Nexus 9000 シリーズ スイッチでは、マスター PTP ポートで操作の混合非ネゴシエートモードがサポートされます。つまり、スレーブ クライアントがユニキャスト遅延要求 PTP パケットを送信すると、Cisco Nexus 9000 はユニキャスト遅延応答パケットで応答することを意味します。また、スレーブ クライアントがマルチキャスト遅延要求 PTP パケットを送信すると、Cisco Nexus 9000 はマルチキャスト遅延応答パケットで応答します。混合非ネゴシエートモードが機能するには、BC デバイスの `ptp 送信元 IP` アドレス設定で使用される送信元 IP アドレスが、BC デバイスの物理または論理インターフェイスでも設定されている必要があります。推奨されるベストプラクティスは、デバイスのループバックインターフェイスを使用することです。
 - Cisco NX-OS リリース 9.2(1) 以降では、Cisco Nexus 9732C-EX、9736C-EX、および 97160YC-EX ライン カードが PTP オフロードをサポートしています。
 - Cisco NX-OS リリース 9.3(1) からリリース 7.0(3)I7 にダウングレードする際には、その前に、PTP オフロードを設定解除する必要があります。Cisco NX-OS リリース 7.0(3)I7 の場合、PTP オフロードは、9636PQ、9564PX、9464PX、および 9536PQ ライン カード上の Cisco Nexus 9000 プラットフォーム スイッチではサポートされません。
 - Cisco Nexus 93108TC-EX および 93180YC-EX スイッチは、混合モードおよびユニキャストモードでの PTP をサポートします。Cisco Nexus 9396 スイッチは PTP 混合モードをサポートします。
 - 同期間隔 -3 での PTP は、Cisco Nexus 9508-R ファミリー ライン カードでのみサポートされます。より高い同期間隔はサポートされません。

- PTP ユニキャストはデフォルトの VRF でのみサポートされます (PTP ユニキャストはオフロードモードではサポートされません)。
- PTP は、ステートフル高可用性ではサポートされません。
- PTP は、管理インターフェイスではサポートされません。
- PTP は、PTP メッセージを配信するための混合モードをサポートします。これは、接続されたクライアントから受信した遅延要求メッセージのタイプに基づいて Cisco Nexus デバイスが自動的に検出するものなので、設定は不要です。
- ワンステップ PTP は、Cisco Nexus 9000-R シリーズプラットフォーム スイッチでのみサポートされます。
- PTP は、FEX インターフェイスではサポートされません。
- 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。
- 9636C-R、9636C-RX、または 9636Q-R ラインカードを搭載した Cisco Nexus 9504 および 9508 プラットフォームスイッチでは、マスターポートとスレーブポートはワンステップモードで動作できます。これらのラインカードでは、ワンステップモードを設定できます。ワンステップモードでのスレーブポート動作がデフォルトです。
- PTP ワンステップモードは、9636C-R、9636C-RX、または 9636Q-R ラインカードを搭載した Cisco Nexus 9504 および 9508 プラットフォームスイッチの PTP オフロードモードでのみサポートされます。Cisco NX-OS リリース 9.3(3) 以降では、ワンステップモードが設定されると、PTP オフロードが自動的に有効になります。
- PTP が有効になっているトポロジで、GrandMaster デバイスにプロファイルが設定され、冗長 GrandMaster がネットワークに展開されている場合、GrandMaster のプロファイルを変更するには、最初にスイッチへの GrandMaster に設定されているポートをシャットダウンし、プロファイルを変更してから、ポートを再度有効にする必要があります。例えば、AES7 プロファイルから SMPTE プロファイルに、またはその逆の移動です。
- 各ポートは、サポートされている任意の PTP プロファイルを使用して個別に構成できます。異なる PTP プロファイルは、インターフェイス上で共存できます。デフォルトの 1588 と SMPTE-2059-2 または AES67 プロファイルの組み合わせがサポートされています。ただし、SMPTE-2059-2 と AES67 プロファイルの組み合わせは、同じインターフェイスではサポートされていません。

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 3: 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
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 遅延要求間隔	<ul style="list-style-type: none"> • 0 ログ秒 • Cisco Nexus 3232C、3264Q、および 9500 プラットフォーム スイッチの場合、-1 ログ秒
PTP 同期間隔	<ul style="list-style-type: none"> • -2 ログ秒 • Cisco Nexus 3232C、3264Q、および 9500 プラットフォーム スイッチでは -3 ログ秒
PTP VLAN	gPTP はデフォルトの VLAN 1 だけをサポートし、他のユーザ設定 VLAN はサポートしません。

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。



- (注) PTP が正常に機能するには、最新の SUP および LC FPGA バージョンを使用する必要があります。FPGA のアップグレードについては、リリースノートのランディングページにアクセスし、「FPGA/EPLD アップグレードリリースノート (NX-OS モードスイッチ)」セクションに移動して、ご使用のソフトウェアバージョンの FPGA/EPLD アップグレードリリースノートを参照してください。 <https://www.cisco.com/c/en/us/support/switches/nexus-9000-series-switches/products-release-notes-list.html> 「インストールガイドライン」のトピックを参照してください。



- (注) 1 ステップ モードまたは 2 ステップ モードに関係なく、PTP プロトコルによって更新されるローカルクロックのクロック プロトコル PTP vdc1 を常に設定する必要があります。設定は、**show running-config clock_manager** コマンドを使用して確認できます。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： <pre>switch# configure terminal switch(config)#</pre>	グローバル設定モードを開始します。
ステップ 2	[no] feature ptp 例： <pre>switch(config)# feature ptp</pre>	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。 dot1x (feature dot1x) または NV オーバーレイ (feature nv overlay) のいずれかの機能のみが設定されていることを確認します。これらの機能が設定されると、ダイナミック ifacl ラベルが予約されます。ただし、使用可能なダイナミック ifacl ラベル ビットは 2 つだけです。これらの機能の両方がすでに設定されている場合、ダイナミック ifacl ラベルは PTP で使用できず、機能を有効にす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	<p>[no] ptp device-type [generalized-ptp boundary-clock]</p> <p>例 :</p> <pre>switch(config)# ptp device-type generalized-ptp</pre>	<p>デバイス タイプを gPTP または境界クロックとして設定します。この generalized-ptp オプションは、Cisco NX-OS リリース 7.0(3)PTP0(15) 以降の -R シリーズ ラインカード。</p>
ステップ 4	<p>[no] ptp source ip-address</p> <p>例 :</p> <pre>switch(config)# ptp source 10.10.10.1</pre>	<p>マルチキャスト PTP モードのすべての PTP パケットに、送信元 IPv4 アドレスを設定します。</p>
ステップ 5	<p>(任意) [no] ptp domain number</p> <p>例 :</p> <pre>switch(config)# ptp domain 1</pre>	<p>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。</p> <p>指定できる数の範囲は 0 ~ 127 です。</p>
ステップ 6	<p>(任意) [no] ptp offload</p> <p>例 :</p> <pre>switch(config)# ptp offload</pre>	<p>一部のタイマーをラインカードにオフロードすることで、PTP セッションの数を増やします。</p> <p>この手順は、1 ステップ モードでは必須であり、2 ステップ モードではオプションです。</p> <p>(注) dot1x (feature dot1x) と NV オーバーレイ (feature nv overlay) のどちらの機能も設定されていないことを確認します。これらの機能が設定されると、ダイナミック ifacl ラベルが予約されます。ただし、使用可能なダイナミック ifacl ラベルビットは2つだけです。これらの機能のいずれかがすでに設定されている場合、ダイナミック ifacl ラベルは PTP オフロードに使用できず、機能を有効にすることはできません。PTP (feature ptp) は1つの ifacl ラベルを消費することに注意してください。</p>

	コマンドまたはアクション	目的
		<p>(注) Cisco NX-OS リリース 9.3(3) 以降、9636C-R、9636C-RX、または 9636Q-R ラインカードを搭載した Cisco Nexus 9504 および 9508 プラットフォームスイッチは、1 ステップのクロック動作でのみオフロードをサポートします。PTP オフロードは、ワンステップクロック動作が有効または無効になると、自動的に有効または無効になります。</p>
ステップ 7	<p>(任意) [no] ptp clock-operation one-step</p> <p>例 :</p> <pre>switch(config)# ptp clock-operation one-step</pre>	<p>PTP クロック動作を 1 ステップ モードに設定します。この場合、タイムスタンプメッセージは同期メッセージの一部として送信されます。このモードでは、フォローアップメッセージは送信されません。</p>
ステップ 8	<p>(任意) [no] ptp priority1 value</p> <p>例 :</p> <pre>switch(config)# ptp priority1 1</pre>	<p>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。</p> <p><i>value</i> の範囲は 0 ~ 255 です。</p>
ステップ 9	<p>(任意) [no] ptp priority2 value</p> <p>例 :</p> <pre>switch(config)# ptp priority2 1</pre>	<p>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。</p> <p><i>value</i> の範囲は 0 ~ 255 です。</p>

	コマンドまたはアクション	目的
ステップ 10	[no] ptp management 例 : <pre>switch(config)# ptp management switch(config-ptp-profile)#</pre>	PTP 管理パケットのサポートを設定します。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。 no : 管理パケットのサポートを無効にします。
ステップ 11	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	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 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。

始める前に

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	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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 slot/port 例 : <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre>	PTP を有効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	[no] ptp 例 : <pre>switch(config-if)# ptp</pre>	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	(任意) [no] ptp master ipv6-address 例 :	インターフェイスの PTP ロールが「slave」に設定されている場合に、マ

	コマンドまたはアクション	目的
	<pre>switch(config-if)# ptp master 10.10.10.1 switch(config-if)#</pre>	<p>スタークロックの IP アドレスを設定します。</p> <p>このオプションは、Cisco Nexus 93180YC-FX3S スイッチの PTP Telecom Profile でのみ使用できます。</p> <p>(注) このコマンドは、Cisco NX-OS リリース 10.2(1)F 以降でサポートされます。</p>
ステップ 5	<p>(任意) ptp transport ipv4 ucast master</p> <p>例 :</p> <pre>switch(config)# ptp transport ipv4 ucast master</pre>	ユニキャストモード (PTP マスター使用) のインターフェイスで PTP を有効にします。
ステップ 6	<p>(任意) ptp transport ipv4 ucast slave</p> <p>例 :</p> <pre>switch(config)# ptp transport ipv4 ucast slave</pre>	ユニキャストモードのインターフェイスで PTP を有効にします (PTP スレーブ使用)。
ステップ 7	<p>(任意) ptp ucast-source ipv4-address [vrf vrf-name]</p> <p>例 :</p> <pre>switch(config)# ptp ucast-source 10.1.1.40</pre>	<p>ユニキャストメッセージの送信元 IP アドレスを設定します。</p> <p><i>ipv4-address</i> : ユニキャスト送信元の IPv4 アドレス。</p> <p><i>vrf vrf-name</i> : hello メッセージに使用される VRF の名前。</p>
ステップ 8	<p>(任意) [no] ptp announce {interval log-seconds timeout count}</p> <p>例 :</p> <pre>switch(config-if)# ptp announce interval 3</pre>	<p>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。</p> <p>PTP アナウンス間隔の範囲は 0 ~ 4 ログ秒で、間隔のタイムアウトの範囲は 2 ~ 4 間隔です。</p>
ステップ 9	<p>(任意) [no] ptp announce interval [aes67 smpte-2059] log-seconds</p> <p>例 :</p>	インターフェイスで PTP アナウンスメッセージの間隔を設定します。

	コマンドまたはアクション	目的												
	<pre>switch(config-if)# ptp announce interval aes67 3</pre>	<p>表 4: PTP アナウンス間隔の範囲とデフォルト値</p> <table border="1"> <thead> <tr> <th>オプション</th> <th>範囲</th> <th>デフォルト値</th> </tr> </thead> <tbody> <tr> <td>aes67-2015</td> <td>0 ~ 4 ログ秒</td> <td>1 ログ秒</td> </tr> <tr> <td>smpte-2059-2</td> <td>-3 ~ -1 ログ秒</td> <td>1 ログ秒</td> </tr> <tr> <td>aes67 または smpte-2059 オプションなし</td> <td>0 ~ 4 ログ秒</td> <td>1 ログ秒</td> </tr> </tbody> </table>	オプション	範囲	デフォルト値	aes67-2015	0 ~ 4 ログ秒	1 ログ秒	smpte-2059-2	-3 ~ -1 ログ秒	1 ログ秒	aes67 または smpte-2059 オプションなし	0 ~ 4 ログ秒	1 ログ秒
オプション	範囲	デフォルト値												
aes67-2015	0 ~ 4 ログ秒	1 ログ秒												
smpte-2059-2	-3 ~ -1 ログ秒	1 ログ秒												
aes67 または smpte-2059 オプションなし	0 ~ 4 ログ秒	1 ログ秒												
ステップ 10	<p>(任意) [no] ptp delay-request minimum interval log-seconds</p> <p>例 :</p> <pre>switch(config-if)# ptp delay-request minimum interval -1</pre>	<p>ポートがマスター ステートの場合に PTP 遅延メッセージ間で許可される最小間隔を設定します。</p> <p>範囲は log (-1) ~ log (6) 秒です。ここで、log (-1) は毎秒 2 フレームです。</p>												
ステップ 11	<p>(任意) [no] ptp delay-request minimum interval [aes67-2015 smpte-2059-2] log-seconds</p> <p>例 :</p> <pre>switch(config-if)# ptp delay-request minimum interval aes67-2015-1</pre>	<p>ポートがマスター ステートの場合に PTP 遅延メッセージ間で許可される最小間隔を設定します。</p> <p>表 5: PTP 遅延要求の最小間隔の範囲とデフォルト値</p> <table border="1"> <thead> <tr> <th>オプション</th> <th>範囲</th> <th>デフォルト値</th> </tr> </thead> <tbody> <tr> <td>aes67-2015</td> <td>-4 ~ 5 ログ秒</td> <td>0 ログ秒</td> </tr> <tr> <td>smpte-2059-2</td> <td>-4 ~ 5 ログ秒</td> <td>0 ログ秒</td> </tr> <tr> <td>aes67-2015 または smpte-2059-2 オプションなし</td> <td>-1 ~ 6 ログ秒 (ここで、-1 = 2 フレーム毎秒)</td> <td>0 ログ秒</td> </tr> </tbody> </table>	オプション	範囲	デフォルト値	aes67-2015	-4 ~ 5 ログ秒	0 ログ秒	smpte-2059-2	-4 ~ 5 ログ秒	0 ログ秒	aes67-2015 または smpte-2059-2 オプションなし	-1 ~ 6 ログ秒 (ここで、-1 = 2 フレーム毎秒)	0 ログ秒
オプション	範囲	デフォルト値												
aes67-2015	-4 ~ 5 ログ秒	0 ログ秒												
smpte-2059-2	-4 ~ 5 ログ秒	0 ログ秒												
aes67-2015 または smpte-2059-2 オプションなし	-1 ~ 6 ログ秒 (ここで、-1 = 2 フレーム毎秒)	0 ログ秒												

	コマンドまたはアクション	目的												
ステップ 12	<p>(任意) [no] ptp sync interval <i>log-seconds</i></p> <p>例 :</p> <pre>switch(config-if)# ptp sync interval 1</pre>	<p>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。</p> <p>範囲は、log (-3) ~ log (1) 秒です。メディア関連のプロファイル情報については、『メディア ソリューションガイド向け Cisco NX-OS IP ファブリック』を参照してください。</p>												
ステップ 13	<p>(任意) [no] ptp sync interval [aes67-2015 smpte-2059-2] log-seconds</p> <p>例 :</p> <pre>switch(config-if)# ptp sync interval aes67 1</pre>	<p>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。</p> <p>表 6: PTP 同期間隔の範囲とデフォルト値</p> <table border="1"> <thead> <tr> <th>オプション</th> <th>範囲</th> <th>デフォルト値</th> </tr> </thead> <tbody> <tr> <td>aes67-2015</td> <td>-4 ~ -1 ログ秒</td> <td>-2 ログ秒</td> </tr> <tr> <td>smpte-2059-2</td> <td>-4 ~ -1 ログ秒</td> <td>-2 ログ秒</td> </tr> <tr> <td>aes67-2015 または smpte-2059-2 オプションなし</td> <td>-3 ~ -1 ログ秒</td> <td>-2 ログ秒</td> </tr> </tbody> </table>	オプション	範囲	デフォルト値	aes67-2015	-4 ~ -1 ログ秒	-2 ログ秒	smpte-2059-2	-4 ~ -1 ログ秒	-2 ログ秒	aes67-2015 または smpte-2059-2 オプションなし	-3 ~ -1 ログ秒	-2 ログ秒
オプション	範囲	デフォルト値												
aes67-2015	-4 ~ -1 ログ秒	-2 ログ秒												
smpte-2059-2	-4 ~ -1 ログ秒	-2 ログ秒												
aes67-2015 または smpte-2059-2 オプションなし	-3 ~ -1 ログ秒	-2 ログ秒												
ステップ 14	<p>(任意) [no] ptp vlan <i>vlan-id</i></p> <p>例 :</p> <pre>switch(config-if)# ptp vlan 1</pre>	<p>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。</p> <p>指定できる範囲は 1 ~ 4094 です。</p>												
ステップ 15	<p>(任意) show ptp brief</p> <p>例 :</p> <pre>switch(config-if)# show ptp brief</pre>	<p>PTP のステータスを表示します。</p>												
ステップ 16	<p>(任意) show ptp port interface <i>interface slot/port</i></p> <p>例 :</p> <pre>switch(config-if)# show ptp port interface ethernet 2/1</pre>	<p>PTP ポートのステータスを表示します。</p>												

	コマンドまたはアクション	目的
ステップ 17	(任意) copy running-config startup-config 例 : <pre>switch(config-if)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

ユニキャストモードでの PTP の設定

ユニキャストモードの設定

従来の PTP メッセージは、PTP マルチキャストメッセージを受信できるノードに配信されます。(たとえば、**announce**、**sync**、**delay_req**、**delay_resp** および **follow_up**)。ユニキャストモードでは、すべての PTP メッセージが特定の PTP ノードにのみ配信されます。マルチキャストアドレスは使用されません。ユニキャストモードでは、マスター/スレーブロールを設定し、対応するピア スレーブ/マスター IP アドレスを割り当てることができます。

スレーブユニキャストポートには最大 8 個のマスター IP を設定でき、マスターポートには最大 64 個のスレーブ IP を設定でき、すべてのポートで最大 256 個のスレーブ IP を設定できます。ユニキャストスレーブ IP とユニキャストマスター IP を設定するには、次のコマンドを使用します。ユニキャストパケットは、これらの IP との間でのみ送受信されます。他の IP から受信したパケットは無視されます。

```
switch(config-if)# ptp transport ipv4 ucast master
switch(config-if-ptp-master)# slave ipv4 10.10.10.2
```

```
switch(config-if)# ptp transport ipv4 ucast slave
switch(config-if-ptp-slave)# master ipv4 10.10.10.1
```

マスターロールの割り当て

マスターロールを割り当てするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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 slot/port 例 : <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre>	PTP を有効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。

	コマンドまたはアクション	目的
ステップ 3	[no] ptp transport ipv4 ucast master 例： switch(config-if)# ptp transport ipv4 ucast master switch(config-if-ptp-master)#	特定のポート（レイヤ3インターフェイス）で PTP マスターをイネーブルにします。マスターサブモードでは、スレーブ IPv4 アドレスを入力できます。
ステップ 4	slave ipv4 <IP_address> 例： switch-1(config)# interface ethernet 1/1 switch-1(config-if)# ptp transport ipv4 ucast master switch-1(config-if-ptp-master)# slave ipv4 1.2.3.1 switch-1(config-if-ptp-master)# slave ipv4 1.2.3.2 switch-1(config-if-ptp-master)# slave ipv4 1.2.3.3 switch-1(config-if-ptp-master)# slave ipv4 1.2.3.4 switch-1(config-if-ptp-master)#	スレーブ IPv4 アドレスを入力します。マスターごとに最大 64 個の IP アドレスを使用できますが、実際の数は同期間隔の設定に応じて変わります。マスターは、これらのスレーブアドレスにのみ、アナウンス、同期、フォローアップ、および delay_resp を送信します。スレーブ IP が到達可能であることを確認する必要があります。

スレーブ ロールの割り当て

スレーブ ロールを割り当てるには、次の手順を実行します。

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	interface ethernet slot/port 例： switch(config)# interface ethernet 2/1 switch(config-if)#	PTP を有効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	[no] ptp transport ipv4 ucast slave 例： switch(config-if)# ptp transport ipv4 ucast slave switch(config-if-ptp-slave)#	特定のポート（レイヤ3インターフェイス）で PTP スレーブをイネーブルにします。スレーブ サブモードでは、ユーザーはマスター IPv4 アドレスを入力できます。
ステップ 4	master ipv4 <IP_address> 例：	マスター IPv4 アドレスを入力します。

	コマンドまたはアクション	目的
	<pre>switch-1(config)# interface ethernet 1/1 switch-1(config-if)# ptp transport ipv4 ucast slave switch-1(config-if-ptp-slave)# master ipv4 4.4.4.1 switch-1(config-if-ptp-slave)# master ipv4 4.4.4.2 switch-1(config-if-ptp-slave)# master ipv4 4.4.4.3</pre>	

ユニキャスト送信元アドレスの設定



- (注) Cisco NX-OS リリース 9.3(4) までのすべてのリリースで、インターフェイスの PTP 設定がユニキャストからマルチキャストまたはユニキャスト スレーブからユニキャスト マスターに変更された場合は、ユニキャスト送信元アドレスを再設定する必要があります。

ユニキャスト送信元アドレスを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	<p>configure terminal</p> <p>例 :</p> <pre>switch# configure terminal switch(config)#</pre>	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	<p>interface ethernet slot/port</p> <p>例 :</p> <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre>	PTP を有効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	<p>[no] ptp ucast-source ipv4-address</p> <p>例 :</p> <pre>switch(config-if)# ptp ucast-source 10.10.10.20 switch(config-if)#</pre>	インターフェイス レベルごとに PTP 送信元アドレスを設定します。この IP アドレスは、ユニキャスト PTP メッセージにのみ使用されます。PTP ユニキャスト送信元 IP アドレスが到達可能である必要があります。

PTP 混合モード

PTP は、接続されたクライアントから受信した **delay_req** メッセージのタイプに基づいて、Cisco Nexus デバイスによって自動的に検出される PTP メッセージを配信するための混合モー

ドをサポートします。このモードでは、スレーブがユニキャストメッセージで **delay_req** を送信すると、マスターもユニキャスト **delay_resp** メッセージで応答します。

PTP インターフェイスがマスター ステートを維持する設定

この手順では、エンドポイントによってポートがスレーブ ステートに移行するのを防ぐ方法について説明します。

始める前に

- 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。
- 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。

手順

	コマンドまたはアクション	目的
ステップ 1	<code>switch # configure terminal</code>	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	<code>switch(config) # interface ethernet slot/port</code>	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	<code>switch(config-if) # ptp</code>	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	<code>switch(config-if) # ptp multicast master-only</code>	マスターステートを維持するようにポートを設定します。

例

この例では、インターフェイス上に PTP を設定し、インターフェイスがマスター ステートを維持するように設定する方法を示しています。

```
switch(config)# show ptp brief
```

```
PTP port status
```

```
-----  
Port                State
```

```
-----  
Eth1/1              Slave
```

```
switch(config)# interface ethernet 1/1
```

```
switch(config-if)# ptp multicast master-only
```

```
2001 Jan 7 07:50:03 A3-MTC-CR-1 %$ VDC-1 %$ %PTP-2-PTP_GM_CHANGE: Grandmaster clock has changed  
from 60:73:5c:ff:fe:62:a1:41 to 58:97:bd:ff:fe:0d:54:01 for the PTP protocol
```

```

2001 Jan 7 07:50:03 A3-MTC-CR-1 %$ VDC-1 %$ %PTP-2-PTP_STATE_CHANGE: Interface Eth1/1 change from
PTP_BMC_STATE_SLAVE to PTP_BMC_STATE_PRE_MASTER
2001 Jan 7 07:50:03 A3-MTC-CR-1 %$ VDC-1 %$ %PTP-2-PTP_TIMESYNC_LOST: Lost sync with master clock
2001 Jan 7 07:50:07 A3-MTC-CR-1 %$ VDC-1 %$ %PTP-2-PTP_STATE_CHANGE: Interface Eth1/1 change from
PTP_BMC_STATE_PRE_MASTER to PTP_BMC_STATE_MASTER

```

タイムスタンプタギング

タイムスタンプタギング機能は、リモートデバイスでパケットが到達したときに正確な時間情報を提供し、実際の時間を追跡できるようにします。パケットは、PTPを使用してナノ秒の精度で切り捨てられ、タイムスタンプが付けられます。Cisco Nexus Data Broker とともにスイッチの TAP 集約機能を使用すると、SPAN を使用してネットワークトラフィックをコピーし、トラフィックをフィルタリングしてタイムスタンプを付け、記録および分析のために送信できます。

タイムスタンプタギングの設定



- (注) 9636C-R、9636C-RX、および 9636Q-R ラインカードを搭載した Cisco Nexus 9508 スイッチでは、タイムスタンプタギングの設定はサポートされていません。



- (注) VXLAN EVPN マルチサイト展開で ttag 機能を使用する場合は、クラウドに接続する BGW の DCI インターフェイスで ttag が削除されていることを確認します (**ttag-strip**)。詳細に説明すると、ttag が、ether-type 0x8905 をサポートしない Nexus 9000 以外のデバイスに接続されている場合、ttag の除去が必要です。ただし、DCI の BGW バックツーバックモデルでは ttag の削除は必要ありません。

始める前に

PTP オフロードがグローバルに有効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 : <pre>switch# configure terminal switch(config)#</pre>	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 <i>type slot/port</i> 例： switch(config)# interface ethernet 2/2 switch(config-if)#	指定したインターフェイスに対してインターフェイス 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] ttag 例： switch(config-if)# ttag	レイヤ 2 またはレイヤ 3 出力インターフェイスでタイムスタンプ タギングを設定します。

TTAG マーカー パケットと時間間隔の設定

ttag タイムスタンプ フィールドは、マーカー パケットに 48 ビットのタイムスタンプを付加します。この 48 ビットのタイムスタンプは、人間の読み取りやすい ASCII ベースのタイムスタンプではありません。この 48 ビットのタイムスタンプを人間が読み取れるようにするために、ttag マーカー パケットを使用して、48 ビットのタイムスタンプ情報をデコードするための追加情報を提供できます。

フィールド	位置 (バイト : ビット)	長さ	定義
Magic		16	デフォルトでは、このフィールドには A6A6 と表示されます。これにより、パケットストリーム上の ttag-marker パケットを識別できます。
バージョン		8	バージョン番号。デフォルトのバージョンは 1 です。
精度		8	このフィールドは、48 ビットのタイムスタンプサイズの粒度を表します。デフォルトの値は 04 で、これは 100 ピコ秒つまり 0.1 ナノ秒を表します。
UTc_offset		8	ASIC と UTC クロック間の utc_offset 値です。デフォルト値は 0 です。
Timestamp_hi		32	48 ビットの ASIC ハードウェア タイムスタンプの上位 16 ビットです。

Timestamp_lo		32	48 ビットの ASIC ハードウェア タイムスタンプの下位 32 ビットです。
UTC sec		32	Cisco Nexus 9000 シリーズ スイッチの CPU クロックに基づく UTC タイムスタンプの秒の部分です。
UTC sec		32	Cisco Nexus 9000 シリーズ スイッチの CPU クロックに基づく UTC タイムスタンプのナノ秒の部分です。
予約済み		32	将来的な使用のために予約されています。
署名 (Signature)		32	デフォルト値は 0xA5A5A5A5 です。これにより、マーカーパケットの前方検索が可能になり、UTC タイムスタンプへの参照が提供されるため、クライアントソフトウェアはその参照 UTC を使用して、各パケットヘッダーの 32 ビットのハードウェアタイムスタンプを回復できます。
パッド		8	これは、ttag-marker の位置を合わせを 4 バイト境界に変換するための位置合わせバイトです。

始める前に

PTP オフロードがグローバルにイネーブル化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	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	ttag-marker-interval seconds 例：	スイッチが ttag-marker パケットを発信ポートに送信するまでの秒数を設定しま

	コマンドまたはアクション	目的
	<code>switch(config-if)# ttag-marker-interval 90</code>	す。これはスイッチのグローバル設定です。デフォルトでは、 <code>ttag-marker</code> パケットを 60 秒ごとに送信します。seconds の範囲は 1 ~ 25200 です。
ステップ 3	interface type slot/port 例： <code>switch(config)# interface ethernet 2/2</code> <code>switch(config-if)#</code>	指定したインターフェイスに対してインターフェイス コンフィギュレーションモードを開始します。
ステップ 4	[no] ttag-marker enable 例： <code>switch(config-if)# ttag-marker enable</code>	<code>ttag-marker</code> パケットを発信ポートに送信します。
ステップ 5	ttag-strip 例： <code>switch(config-if)# ttag-strip</code>	インターフェイスの出力パケットから TTAG を削除します。

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。
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 counters [all interface ethernet slot/port]	すべてのインターフェイスまたは指定したインターフェイスの PTP パケットカウンタを表示します。
show ptp parent	PTP の親のプロパティを表示します。

コマンド	目的
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。
show ptp time-property	PTP クロック プロパティを表示します。
show ttag brief	タイムアウト タグ付け設定のステータスを表示します。 (注) 9636C-R、9636C-RX、および 9636Q-R ライン カードを搭載した Cisco Nexus 9508 スイッチでは、タイムスタンプタグ付け設定はサポートされません。
show running-config ptp [all]	PTP の実行コンフィギュレーションを表示します。
clear ptp counters [all interface ethernet slot/port]	特定のインターフェイスまたは PTP が有効になっているすべてのインターフェイスで送受信されるすべての PTP メッセージをクリアします。
clear ptp corrections	PTP 修正の履歴をクリアします。

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# 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:Mon Dec 22 14:13:24 2014

```

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 1/1
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 smpte-2059-2 -3
switch(config-if)# ptp sync interval smpte-2059-2 -3
switch(config-if)# no shutdown
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

```

個の例では、マスター/スレーブ ロールを設定し、対応するピア スレーブ/マスター IP アドレスを割り当てる方法を示します。

```

For Cisco NX-OS Release 9.3(4) and earlier:
switch-1(config)# interface ethernet 1/1
switch-1(config-if)# ptp transport ipv4 ucast master
switch-1(config-if-ptp-master)# slave ipv4 1.2.3.1
switch-1(config-if-ptp-master)# slave ipv4 1.2.3.2
switch-1(config-if-ptp-master)# slave ipv4 1.2.3.3
switch-1(config-if-ptp-master)# slave ipv4 1.2.3.4
switch-1(config-if-ptp-master)#

switch-1(config-if)# ptp transport ipv4 ucast slave
switch-1(config-if-ptp-slave)# master ipv4 4.4.4.1
switch-1(config-if-ptp-slave)# master ipv4 4.4.4.2
switch-1(config-if-ptp-slave)# master ipv4 4.4.4.3

switch-1(config-if-ptp-slave)# ptp ucast-source 9.9.9.9

switch-1(config-if)# sh running-config ptp

```



```
!Command: show running-config ptp
!Time: Tue Feb  7 17:37:09 2017

version 7.0(3)I4(6)
feature ptp

ptp source 1.1.1.1

interface Ethernet1/1
  ptp transport ipv4 ucast master
  slave ipv4 1.2.3.1
  slave ipv4 1.2.3.2
  slave ipv4 1.2.3.3
  slave ipv4 1.2.3.4

interface Ethernet1/2
  ptp transport ipv4 ucast slave
  master ipv4 4.4.4.1
  master ipv4 4.4.4.2
  master ipv4 4.4.4.3
  ptp ucast-source 9.9.9.9

switch-1(config-if)#
```

次に、マスター ポートまたはスレーブ ポートでクロック動作モードで PTP を設定する例を示します。

```
PLTFM-A(config)# show ptp clock
PTP Device Type : boundary-clock
PTP Device Encapsulation : layer-3
PTP Source IP Address : 1.1.1.1
Clock Identity : 74:26:ac:ff:fe:fd:de:ff
Clock Domain: 0
Slave Clock Operation : One-step
Master Clock Operation : One-step
Slave-Only Clock Mode : Disabled
Number of PTP ports: 142
Priority1 : 200
Priority2 : 200
Clock Quality:
  Class : 248
  Accuracy : 254
  Offset (log variance) : 65535
Offset From Master : -32
Mean Path Delay : 105
Steps removed : 1
Correction range : 200
MPD range : 100
Local clock time : Wed Jul  3 18:57:23 2019
Hardware frequency correction : NA
```

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
1588 IEEE	1588 IEEE 標準



第 6 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。

- [NTP の詳細 \(71 ページ\)](#)
- [NTP の前提条件 \(73 ページ\)](#)
- [NTP の注意事項と制約事項 \(73 ページ\)](#)
- [NTP のデフォルト設定 \(75 ページ\)](#)
- [NTP の設定 \(75 ページ\)](#)
- [NTP の設定確認 \(85 ページ\)](#)
- [NTP の設定例 \(85 ページ\)](#)
- [その他の参考資料 \(86 ページ\)](#)

NTP の詳細

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 ではストラタム (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

NTP 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。

時間サーバとしての 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。

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。プロトコルを指定すると、システムクロック更新が開始します。クロック マネージャの設定の詳細については『Cisco Nexus 9000 シリーズ NX-OS 基本設定ガイド』を参照してください。

高可用性

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 9000 シリーズ NX-OS ハイアベイラビリティおよび冗長性ガイド](#)』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

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 の詳細については、『[Cisco Nexus 9000 シリーズ NX-OS ユニキャストルーティング設定ガイド](#)』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。

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。

- NTP サーバ機能はサポートされます。
- デフォルト以外の VRF で名前ベースの NTP サーバ (FQDN) を設定する前に、その特定の VRF で DNS サーバを設定する必要があります。オプションを使用してグローバルコンフィギュレーションモードから DNS サーバを設定する場合、その名前ベースの NTP サーバ設定は実行コンフィギュレーションに追加されません。 **use-vrf** この方法を使用して NTP サーバを設定しようとした場合は、コマンドの **no** バージョンを使用して NTP 設定を削除し、その VRF の下に DNS サーバを追加してから、VRF に名前ベースの NTP サーバを追加する必要があります。
- 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）に限り、別のデバイスとの間にピアアソシエーションを設定することを推奨します。
- 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ことを推奨します。
- 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します。
- スイッチをエッジデバイスとして使用して NTP を利用したい場合は、**ntp access-group** コマンドを使用して必要なエッジデバイスにのみ NTP をフィルタリングすることを推奨します。
- システムに **ntp passive**、**ntp broadcast client**、または **ntp multicast client** コマンドが設定されている場合、対称アクティブの着信パケット、ブロードキャストパケット、マルチキャストパケットを NTP が受信する際に、送信者と同期させるための一時的なピアアソシエーションを設定できます。



(注) 上記コマンドのいずれかを有効にする前に必ず **ntp authenticate** b を指定してください。そうしないと、上記のパケットタイプのいずれかを送信する任意のデバイス（悪意のある攻撃者に制御されたデバイスを含む）とデバイスが同期される可能性があります。

- **ntp authenticate** コマンドが指定されている場合、対称アクティブパケット、ブロードキャストパケット、マルチキャストパケットが受信されても、**ntp trusted-key** グローバルコンフィギュレーションコマンドで指定された認証キーの1つがパケットで運ばれていない限り、システムとピアの同期は行われません。
- **ntp access-group** コマンドなど他の方法で、デバイスの NTP サービスと非承認ホストとの通信防止の措置が取られている場合を除き、非承認のネットワークホストとの同期を避けるには、**ntp passive**、**ntp broadcast client**、**ntp multicast client** コマンドを指定した段階で随時 **ntp authenticate** コマンドを指定する必要があります。
- The **ntp authenticate** コマンドは、**ntp server** および **ntp peer** コンフィギュレーションコマンドで設定されたピアアソシエーションを認証しません。**ntp server** および **ntp peer** アソシエーションを認証するには、**key** キーワードを指定します。
- 1つの NTP アクセスグループに最大4つの IP ACL を設定できます。IPv4 および IPv6 ACL がサポートされています。

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	イネーブル
NTP 認証	ディセーブル
NTP アクセス	イネーブル
NTP access group match all	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りますので注意してください。

NTP の有効化または無効化

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)#	グローバル設定モードを開始します。
ステップ 2	[no] feature ntp 例： switch(config)# feature ntp	NTP を有効または無効にします。
ステップ 3	(任意) copy running-config startup-config 例： switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

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	(任意) show running-config ntp 例： switch(config)# show running-config ntp	NTP コンフィギュレーションを表示します。
ステップ 4	(任意) copy running-config startup-config 例： switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

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。

始める前に

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：	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
	switch# configure terminal switch(config)#	
ステップ 2	<p>[no] ntp server {<i>ip-address</i> <i>ipv6-address</i> <i>dns-name</i>} [key <i>key-id</i>] [maxpoll <i>max-poll</i>] [minpoll <i>min-poll</i>] [prefer] [use-vrf <i>vrf-name</i>]</p> <p>例 :</p> <pre>switch(config)# ntp server 192.0.2.10</pre>	<p>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。</p> <p>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。<i>key-id</i> 引数の範囲は 1 ~ 65535 です。</p> <p>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。<i>max-poll</i> および <i>min-poll</i> 引数の範囲は 4~16 (2 の累乗として設定されます。つまり、実質的に 16~65536 秒) で、デフォルト値はそれぞれ 6 と 4 です (<i>maxpoll</i> デフォルト=64 秒、<i>minpoll</i> デフォルト=16 秒)。</p> <p>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。</p> <p>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。<i>vrf-name</i> 引数には、default、management、または大文字と小文字が区別される最大 32 文字の任意の英数字文字列を指定できます。</p> <p>(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。</p>
ステップ 3	<p>[no] ntp peer {<i>ip-address</i> <i>ipv6-address</i> <i>dns-name</i>} [key <i>key-id</i>] [maxpoll <i>max-poll</i>] [minpoll <i>min-poll</i>] [prefer] [use-vrf <i>vrf-name</i>]</p> <p>例 :</p> <pre>switch(config)# ntp peer 2001:0db8::4101</pre>	<p>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。</p> <p>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。<i>key-id</i> 引数の範囲は 1 ~ 65535 です。</p>

	コマンドまたはアクション	目的
		<p>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。<i>max-poll</i> および <i>min-poll</i> 引数の範囲は 4～16 (2 の累乗として設定されます。つまり、実質的に 16～131072 秒) で、デフォルト値はそれぞれ 6 と 4 です (<i>maxpoll</i> デフォルト=64秒、<i>minpoll</i> デフォルト=16秒)。</p> <p>デバイスに対して対象の NTP ピアを優先にするには、prefer キーワードを使用します。</p> <p>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。<i>vrf-name</i> 引数には、default、management、または大文字と小文字が区別される最大 32 文字の任意の英数字文字列を指定できます。</p>
ステップ 4	<p>(任意) show ntp peers</p> <p>例 :</p> <pre>switch(config)# show ntp peers</pre>	<p>設定されたサーバおよびピアを表示します。</p> <p>(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。</p>
ステップ 5	<p>(任意) copy running-config startup-config</p> <p>例 :</p> <pre>switch(config)# copy running-config startup-config</pre>	<p>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。</p>

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。

始める前に

この手順で指定する予定の認証キーによって、NTP サーバが設定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	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 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 個の 15 文字の英数字を指定できます。
ステップ 3	ntp server ip-address key key-id 例： switch(config)# ntp server 192.0.2.1 key 1001	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。 認証を必須とする場合は、 key キーワードを使用する必要があります。 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。
ステップ 4	(任意) show ntp authentication-keys 例： switch(config)# show ntp authentication-keys	設定済みの NTP 認証キーを表示します。
ステップ 5	[no] ntp trusted-key number 例： switch(config)# ntp trusted-key 42	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。デバイスを時刻源と同期させるには、未設定のリモートシンメトリック、ブロードキャスト、およびマルチキャストの時刻源を

	コマンドまたはアクション	目的
		NTP パケット内に入力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 6	(任意) show ntp trusted-keys 例： switch(config)# 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。
ステップ 7	[no] ntp authenticate 例： switch(config)# ntp authenticate	ntp passive、ntp broadcast client、および ntp multicast で認証を有効または無効にします。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 8	(任意) show ntp authentication-status 例： switch(config)# show ntp authentication-status	NTP 認証の状況を表示します。
ステップ 9	(任意) copy running-config startup-config 例： switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

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、デバイスで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。

Cisco NX-OS リリース 7.0(3)I7(3) 以降では、アクセスグループは次の方法で評価されます。

- **match-all** キーワードがない場合、パケットは **permit** が見つかるまでアクセスグループに対して（以下に示す順で）評価されます。**permit** が検出されない場合、パケットはドロップされます。
- **match-all** キーワードがある場合、パケットはすべてのアクセスグループに対して（以下に示す順で）評価され、最後に成功した評価（ACL が設定されている最後のアクセスグループ）に基づいてアクションが実行されます。

アクセスグループとパケットのタイプのマッピングは次のとおりです。

- **peer** : クライアント、対称アクティブ、対称パッシブ、サービス、コントロール、およびプライベートパケット (すべてのタイプ) を処理
- **serve** : クライアント、コントロール、およびプライベートパケットを処理
- **serve-only** : クライアントパケットだけを処理
- **query-only** : コントロールおよびプライベートパケットだけを処理

アクセスグループは、次の降順で評価されます。

1. **peer** (すべてのパケットタイプ)
2. **serve** (クライアント、コントロール、およびプライベートパケット)
3. **query only** (クライアントパケット) または **query-only** (コントロールおよびプライベートパケット)

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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 match-all {{peer serve serve-only query-only} access-list-name} 例 : <pre>switch(config)# ntp access-group match-all switch(config)# ntp access-group peer peer-acl switch(config)# ntp access-group serve serve-acl</pre>	<p>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。</p> <p>設定ピアの遅延 ACL 1 ルールに NTP が一致する場合、ACL 処理は停止し、次のアクセスグループ オプションへと継続しません。</p> <ul style="list-style-type: none"> • 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。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • serve-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時刻要求だけを受信するようにします。 • 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。 • match-all キーワードを使用すると、アクセス グループ オプションが、制限の最も緩いものから最も厳しいもの、peer、serve、serve-only、query-only の順序でスキャンされるようにできます。着信パケットが peer アクセス グループの ACL に一致しない場合、パケットは serve アクセス グループに送信され、処理されます。パケットが serve アクセス グループの ACL に一致しない場合、serve-only アクセス グループに送られ、これが継続されます。 <p>(注) match-all キーワードは、Cisco NX-OS リリース 7.0(3)I6(1)以降で利用可能なもので、Cisco Nexus 9000 シリーズ スイッチと、Cisco Nexus 3164Q、31128PQ、3232C、および 3264Q スイッチでサポートされています。</p> <ul style="list-style-type: none"> • access-list-name 変数は、NTP アクセスグループの名前です。名前は、特殊文字を含む、最大 64 文字の英数字ストリングで指定できます。
ステップ 3	(任意) show ntp access-groups 例： <pre>switch(config)# show ntp access-groups</pre>	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。

	コマンドまたはアクション	目的
ステップ 4	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	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 : <pre>switch# configure terminal switch(config)#</pre>	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 : <pre>switch(config)# ntp source 192.0.2.1</pre>	すべての NTP パケットにソース IP アドレスを設定します。 <i>ip-address</i> には IPv4 または IPv6 形式を使用できます。
ステップ 3	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	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 : <pre>switch# configure terminal switch(config)#</pre>	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 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。サポートされているインターフェイスのリストを表示するには、? キーワードを使用します。
ステップ 3	(任意) copy running-config startup-config 例： switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

NTP ログイングの設定

重要な NTP イベントでシステム ログを生成するよう、NTP ログイングを設定できます。NTP ログイ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)#	グローバル設定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 ログイ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	(任意) show ntp logging-status 例： switch(config)# show ntp logging-status	NTP ログイ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	(任意) copy running-config startup-config 例： switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

NTP の設定確認

NTP 設定を表示するには、次のタスクのうちのいずれかを実行します。

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 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。
ntp ソースを表示する	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 パケット内で認証キー 42 を提示している時刻源とだけ同期するようデバイス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)# ntp authentication-key 42 md5 aNiceKey
switch(config)# ntp server 192.0.2.105 key 42
switch(config)# ntp trusted-key 42
switch(config)# ntp authenticate
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
クロック マネージャ	『 Cisco Nexus 9000 Series NX-OS Fundamentals 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。 ftp://ftp.cisco.com/pub/mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html



第 7 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。

- [CDP について \(89 ページ\)](#)
- [CDP の注意事項と制約事項 \(91 ページ\)](#)
- [CDP のデフォルト設定 \(91 ページ\)](#)
- [CDP の設定 \(91 ページ\)](#)
- [CDP コンフィギュレーションの確認 \(94 ページ\)](#)
- [CDP のコンフィギュレーション例 \(95 ページ\)](#)

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、メディアにもプロトコルにも依存しないプロトコルです。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。

- デバイス ID

- アドレス
- ポート ID
- 機能
- バージョン
- プラットフォーム
- ネイティブ VLAN
- 全二重/半二重
- MTU
- SysName
- SysObjectID
- 管理アドレス
- 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 9000 シリーズ NX-OS レイヤ 2 スイッチング設定ガイド』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ます。
- VTP 機能がイネーブルになっています。
- VTP ドメイン名が設定されています。

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

高可用性

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 9000 シリーズ NX-OS ハイアベイラビリティおよび冗長性ガイド』を参照してください。

仮想化のサポート

Cisco NX-OS は、CDP のインスタンスを 1 つサポートします。

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ンネル上に限られます。

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	バージョン 2
CDP device ID	シリアル番号
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ります。

CDP のグローバルな有効化または無効化

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)#	グローバル設定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 機能を有効または無効にします。デフォルトでは有効。
ステップ 3	(任意) copy running-config startup-config 例： switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

インターフェイス上での CDP の有効化または無効化

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。

	コマンドまたはアクション	目的
ステップ 2	interface interface slot/port 例： switch(config)# interface ethernet 1/2 switch(config-if) #	インターフェイス設定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 を有効または無効にします。デフォルトでは有効。 (注) CDP がデバイス上でグローバルに有効になっていることを確認します。
ステップ 4	(任意) show cdp interface interface slot/port 例： switch(config-if) # show cdp interface ethernet 1/2	インターフェイスの CDP 情報を表示します。
ステップ 5	(任意) copy running-config startup-config 例： switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

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。
ステップ 2	(任意) cdp advertise {v1 v2} 例： switch(config)# cdp advertise v1	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	(任意) cdp format device-id {mac-address serial-number system-name}	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。

	コマンドまたはアクション	目的
	例： switch(config)# cdp format device-id mac-address	<ul style="list-style-type: none"> • mac-address : シャーシの MAC アドレスを指定します。 • 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 デフォルトは system-name です。
ステップ 4	(任意) cdp holdtime seconds 例： switch(config)# cdp holdtime 150	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	(任意) cdp timer seconds 例： switch(config)# cdp timer 50	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	(任意) copy running-config startup-config 例： switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

CDP コンフィギュレーションの確認

CDP 設定を表示するには、次のタスクのうちのいずれかを実行します。

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。
show cdp global	CDP グローバル パラメータを表示します。
show cdp interface interface slot/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 interface slot/port} [detail]	CDP ネイバーのステータスを表示します。
show cdp interface interface slot/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。

show cdp neighbors detail コマンドを（**show cdp neighbors** コマンドの代わりに）使用することを推奨します。**show cdp neighbors** コマンドが表示するのは、プラットフォーム名の 13 文字だけです。完全なプラットフォーム名を表示するには、**show cdp neighbors detail** 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 機能を有効にして、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。

```
configure terminal
cdp enable
cdp timer 50
cdp holdtime 100
```




第 8 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。

この章は、次の内容で構成されています。

- システムメッセージロギングの詳細, on page 97
- 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 (99 ページ)
- システムメッセージロギングのデフォルト設定, on page 99
- システムメッセージロギングの設定 (100 ページ)
- システムメッセージロギングの設定確認, on page 114
- システムメッセージロギングの設定例 (115 ページ)
- その他の参考資料 (115 ページ)

システムメッセージロギングの詳細

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記録します。

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。

Table 8: 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

レベル	説明
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。



Note 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。

セキュアな Syslog サーバ

Cisco NX-OS リリース 9.2(1) 以降では、リモート ロギング サーバへのセキュアな TLS トランスポート接続をサポートするように Syslog サーバを設定できます。さらに、相互認証の設定によって NX-OS スイッチ (クライアント) のアイデンティティを強化することができます。NX-OS スイッチの場合、この機能は TLSv1.1 および TLSv1.2 をサポートします。

セキュアな Syslog サーバの機能では、デバイス認証および暗号化を提供するために TCP/TLS トランスポートおよびセキュリティプロトコルを使用します。この機能を使用すると、(クライアントとして機能している) Cisco NX-OS デバイスが、ロギングにセキュアな接続をサポートする (サーバとして機能している) リモート Syslog サーバに対してセキュアな暗号化されたアウトバウンド接続を確立できるようになります。認証と暗号化により、この機能では、セキュリティ保護されていないネットワーク上でもセキュアな通信を実現できます。

システムメッセージロギングの注意事項および制約事項

システムメッセージロギングには次の設定上の注意事項と制約事項があります。

- 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。
- syslog サーバに到達する前に出力されるシステムメッセージ（スーパーバイザアクティブメッセージやオンラインメッセージなど）は、syslog サーバに送信できません。
- Cisco NX-OS リリース 9.2(1) 以降では、リモートロギングサーバへのセキュアな TLS トランスポート接続をサポートするように Syslog サーバを設定できます。この機能は、TLSv1.1 および TLSv1.2 をサポートします。
- セキュアな syslog サーバがインバンド（非管理）インターフェイスを介して到達できるようにするには、CoPP プロファイルに調整が必要な場合があります。特に、複数のロギングサーバが設定されている場合、および短時間で多数の syslog が生成される場合（ブートアップや設定アプリケーションなど）。

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。

Table 9: 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
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	秒
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。



Note コンソールのボーレートが 9600 ボー (デフォルト) の場合、現在の Critical (デフォルト) ログレベルが維持されます。コンソールログレベルを変更しようとする、必ずエラーメッセージが生成されます。ログレベルを上げる (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。

Procedure

	Command or Action	Purpose
ステップ 1	terminal monitor Example: 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 Example: 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] Example: 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。 <ul style="list-style-type: none"> • 0 : 緊急 • 1 : アラート • 2 : クリティカル • 3 : エラー

	Command or Action	Purpose
		<ul style="list-style-type: none"> • 4 : 警告 • 5 : 通知 • 6 : 情報 • 7 : デバッグ <p>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。</p>
ステップ 4	<p>(Optional) show logging console</p> <p>Example:</p> <pre>switch(config)# show logging console</pre>	コンソールロギング設定を表示します。
ステップ 5	<p>[no] logging monitor [severity-level]</p> <p>Example:</p> <pre>switch(config)# logging monitor 3</pre>	<p>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。</p> <ul style="list-style-type: none"> • 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 <p>設定は Telnet および SSH セッションに適用されます。</p> <p>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。</p>

	Command or Action	Purpose
ステップ 6	(Optional) show logging monitor Example: switch(config)# show logging monitor	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 Example: 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	(Optional) copy running-config startup-config Example: switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Syslog メッセージの送信元 ID の設定

リモート syslog サーバに送信される syslog メッセージにホスト名、IP アドレス、またはテキスト文字列を付加するように 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	必須: logging origin-id {hostname ip ip-address string text-string} 例： switch(config)# logging origin-id string n9k-switch-abc	リモート syslog サーバに送信される syslog メッセージに追加するホスト名、IP アドレス、またはテキスト文字列を指定します。
ステップ 3	(任意) show logging origin-id 例：	リモート syslog サーバに送信される syslog メッセージに付加される、設定済

	コマンドまたはアクション	目的
	switch(config)# show logging origin-id Logging origin_id : enabled (string: n9k-switch-abc)	みのホスト名、IP アドレス、またはテキスト文字列を表示します。
ステップ 4	(任意) copy running-config startup-config 例 : switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

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 /logflash/log/logfilename 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	非永続的ログファイルパラメータを設定します。 <i>logfile-name</i> : システムメッセージの保存に使用するログファイルの名前を設定します。デフォルトのファイル名は「message」です。 <i>severity-level</i> : ログに記録する最小の重大度レベルを設定します。小さい値は、より高い重大度を示します。デフォルトは 5 です。範囲は 0 ～ 7 です。 <ul style="list-style-type: none"> • 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

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • 6 : 情報 • 7 : デバッグ <p>size bytes : オプションとして、最大ファイルサイズを指定します。範囲は 4096 ~ 4194304 バイトです。</p>
ステップ 3	logging event {link-status trunk-status} {enable default} 例 : <pre>switch(config)# logging event link-status default</pre>	インターフェイス イベントをロギングします。 <ul style="list-style-type: none"> • 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 : すべてのトランク ステータス メッセージをロギングします。 • 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い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。
ステップ 4	(任意) show logging info 例 : <pre>switch(config)# show logging info</pre>	ロギング設定を表示します。
ステップ 5	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	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。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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] Example: <pre>switch(config)# logging module 3</pre>	<p>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。</p> <ul style="list-style-type: none"> • 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 <p>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。</p>
ステップ 3	(Optional) show logging module Example: <pre>switch(config)# show logging module</pre>	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 Example: <pre>switch(config)# logging level aaa 2</pre>	<p>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。</p> <ul style="list-style-type: none"> • 0 : 緊急 • 1 : アラート • 2 : クリティカル • 3 : エラー • 4 : 警告

	Command or Action	Purpose
		<ul style="list-style-type: none"> • 5 : 通知 • 6 : 情報 • 7 : デバッグ <p>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。</p> <p>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。</p>
ステップ 5	(Optional) show logging level [facility] Example: <pre>switch(config)# show logging level aaa</pre>	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	(Optional) [no] logging level ethpm Example: <pre>switch(config)# logging level ethpm ? <0-7> 0-emg,1-ale,2-crit,3-err,4-warn,5-notif,6-inform,7-debug link-down Configure logging level for link down syslog messages link-up Configure logging level for link up syslog messages switch(config)#logging level ethpm link-down ? error ERRORS notif NOTICE (config)# logging level ethpm link-down error ? <CR> (config)# logging level ethpm link-down</pre>	レベル 3 のイーサネット ポート マネージャ リンクアップ/リンクダウン syslog メッセージのロギングを有効にします。 no オプションを使用すると、イーサネット ポート マネージャの syslog メッセージにデフォルトのロギング レベルが使用されます。

	Command or Action	Purpose
	<pre> notif ? <CR> switch(config)#logging level ethpm link-up ? error ERRORS notif NOTICE (config)# logging level ethpm link-up error ? <CR> (config)# logging level ethpm link-up notif ? <CR> </pre>	
ステップ 7	<p>[no] logging timestamp {microseconds milliseconds seconds}</p> <p>Example:</p> <pre> switch(config)# logging timestamp milliseconds </pre>	<p>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。</p> <p>Note 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。</p>
ステップ 8	<p>(Optional) show logging timestamp</p> <p>Example:</p> <pre> switch(config)# show logging timestamp </pre>	<p>設定されたロギング タイムスタンプ単位を表示します。</p>
ステップ 9	<p>(Optional) copy running-config startup-config</p> <p>Example:</p> <pre> switch(config)# copy running-config startup-config </pre>	<p>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。</p>

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。



Note

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 9000 シリーズ NX-OS ユニキャストルーティング設定ガイド』を参照してください。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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]] Example: <pre>switch(config)# logging server 192.0.2.253</pre> Example: <pre>switch(config)# logging server 2001::)db*::3 5 use-vrf red</pre>	<p>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。</p> <ul style="list-style-type: none"> • 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 <p>デフォルトの発信ファシリティは local7 です。</p> <p>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。</p> <p>この最初の例では、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。</p>
ステップ 3	Required: logging source-interface loopback virtual-interface Example: <pre>switch(config)# logging source-interface loopback 5</pre>	<p>リモート Syslog サーバの送信元インターフェイスをイネーブルにします。 virtual-interface 引数の範囲は 0 ～ 1023 です。</p>
ステップ 4	(Optional) show logging server Example: <pre>switch(config)# show logging server</pre>	Syslog サーバ設定を表示します。

	Command or Action	Purpose
ステップ 5	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	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。

セキュアな Syslog 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： <pre>switch# configure terminal switch(config)#</pre>	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 [port port-number]][secure[trustpoint client-identity trustpoint-name]][use-vrf vrf-name]] 例： <pre>switch(config)# logging server 192.0.2.253 secure</pre> 例： <pre>switch(config)# logging server 2001::3 5 secure trustpoint client-identity myCA use-vrf red</pre>	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。必要に応じて、CA によって署名されるクライアント アイデンティティ証明書をインストールし、trustpoint client-identity オプションを使用することで相互認証を適用できます。 セキュアな TLS 接続のデフォルト宛先ポートは 6514 です。
ステップ 3	(任意) logging source-interface interface name 例： <pre>switch(config)# logging source-interface lo0</pre>	リモート Syslog サーバの送信元インターフェイスをイネーブルにします。
ステップ 4	(任意) show logging server 例： <pre>switch(config)# show logging server</pre>	Syslog サーバ設定を表示します。secure オプションを設定する場合、出力のエントリにトランスポート情報が含まれるようになります。デフォルトでは、secure オプションが設定されていない場合、トランスポートは UDP です。

	コマンドまたはアクション	目的
ステップ 5	(任意) copy running-config startup-config 例： switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

CA 証明書の設定

セキュアな Syslog 機能のサポートには、トラストポイントの設定によってリモートサーバを認証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	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] crypto ca trustpoint trustpoint-name 例： switch(config)# crypto ca trustpoint winca switch(config-trustpoint)#	トラストポイントを設定します。 (注) トラストポイントの設定の前に ip domain-name を設定する必要があります。
ステップ 3	必須: crypto ca authenticate trustpoint-name 例： switch(config-trustpoint)# crypto ca authenticate winca	トラストポイントの CA 証明書を設定します。
ステップ 4	(任意) show crypto ca certificate 例： switch(config)# show crypto ca certificates	設定されている証明書/チェーンと、関連付けられているトラストポイントを表示します。
ステップ 5	(任意) copy running-config startup-config 例： switch(config)# copy running-config startup-config	デバイスのリロード後にトラストポイントが持続されるように、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ます。

CA 証明書の登録

NX-OS スイッチ（クライアント）が識別するようリモートサーバによって要求される相互認証では、ピア認証が必須であるため、これは証明書をスイッチに登録するための追加設定です。

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	必須: crypto key generate rsa label key name exportable modules 2048 例： switch(config-trustpoint)# crypto key generate rsa label myKey exportable modulus 2048	RSA キー ペアを設定します。デフォルトでは、Cisco NX-OS ソフトウェアは 1024 ビットの RSA キーを作成します。
ステップ 3	[no] crypto ca trustpoint trustpoint-name 例： switch(config)# crypto ca trustpoint myCA switch(config-trustpoint)#	トラストポイントを設定します。 (注) トラストポイントの設定の前に ip domain-name を設定する必要があります。
ステップ 4	必須: rsa keypair key-name 例： switch(config-trustpoint)# rsa keypair myKey	トラストポイント CA に生成されたキー ペアを関連付けます。
ステップ 5	crypto ca trustpoint trustpoint-name 例： switch(config)# crypto ca authenticate myCA	トラストポイントの CA 証明書を設定します。
ステップ 6	[no] crypto ca enroll trustpoint-name 例： switch(config)# crypto ca enroll myCA	CA に登録するスイッチのアイデンティティ証明書を生成します。
ステップ 7	crypto ca import trustpoint-name certificate 例： switch(config-trustpoint)# crypto ca import myCA certificate	CA によって署名されたアイデンティティ証明書をスイッチにインポートします。

	コマンドまたはアクション	目的
ステップ 8	(任意) show crypto ca certificates 例： switch# show crypto ca certificates	設定されている証明書またはチェーンと、関連付けられているトラストポイントを表示します。
ステップ 9	必須: copy running-config startup-config 例： switch# copy running-config startup-config	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

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 10: *syslog.conf* の *syslog* フィールド

フィールド	説明
Facility	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。
Level	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。

Procedure

	Command or Action	Purpose
ステップ 1	Required: show logging last <i>number-lines</i> Example: 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 duration <i>hh:mm:ss</i> Example: switch# show logging logfile duration 15:10:0	入力された時間内のタイム スタンプを持つログ ファイルのメッセージを表示します。
ステップ 3	show logging logfile last-index Example: switch# show logging logfile last-index	ログファイルの最後のメッセージのシーケンス番号を表示します。
ステップ 4	show logging logfile [start-time <i>yyyy mmm dd hh:mm:ss</i>] [end-time <i>yyyy mmm dd hh:mm:ss</i>]	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

	Command or Action	Purpose
	Example: <pre>switch# show logging logfile start-time 2013 oct 1 15:10:0</pre>	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 5	show logging logfile [start-seqn number] [end-seqn number] Example: <pre>switch# show logging logfile start-seqn 100 end-seqn 400</pre>	シーケンス番号の範囲内である、発生したメッセージを表示します。終了シーケンス番号を指定しなかった場合は、ログファイルの、開始番号から最後のメッセージまでのメッセージが表示されます。
ステップ 6	show logging nvram [last number-lines] Example: <pre>switch# show logging nvram last 10</pre>	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 7	clear logging logfile [persistent] Example: <pre>switch# clear logging logfile</pre>	ログファイルの内容をクリアします。 persistent : 永続的な場所から、ログファイルの内容をクリアします。
ステップ 8	clear logging nvram Example: <pre>switch# clear logging nvram</pre>	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 duration hh:mm:ss	入力された時間内のタイムスタンプを持つログファイルのメッセージを表示します。
show logging logfile last-index	ログファイルの最後のメッセージのシーケンス番号を表示します。

コマンド	目的
show logging logfile [start-time yyyy mmm dd hh:mm:ss] [end-time yyyy mmm dd hh:mm:ss]	開始日時と終了日時に基づいてログファイルのメッセージを表示します。
show logging logfile [start-seqn number] [end-seqn number]	シーケンス番号の範囲内で発生したメッセージを表示します。終了シーケンス番号を含めない場合は、開始番号から最後のメッセージまで、ログファイルのメッセージが表示されます。
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 origin-id	リモート syslog サーバに送信される syslog メッセージに付加される、設定済みのホスト名、IP アドレス、またはテキスト文字列を表示します。
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設定例

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	『Cisco NX-OS System Messages Reference』



第 9 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。

この章は、次の内容で構成されています。

- [Smart Call Home の概要, on page 117](#)
- [Smart Call Home の前提条件, on page 124](#)
- [Smart Call Home の注意事項および制約事項 \(124 ページ\)](#)
- [Smart Call Home のデフォルト設定, on page 125](#)
- [Smart Call Home の設定 \(125 ページ\)](#)
- [Smart Call Home 設定の確認, on page 141](#)
- [Smart Call Home の設定例 \(141 ページ\)](#)
- [その他の参考資料 \(142 ページ\)](#)

Smart Call Home の概要

Smart Call Home により、重要なシステム ポリシーについ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 エンジニアやネットワーク オペレーション センターを呼び出せます。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。

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

- 複数のメッセージ宛先への同時配信が可能。各宛先プロファイルには最大50件の電子メール宛先アドレスを設定できます。

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つまたは複数の電子メール宛先：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重大度よりも低い場合、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。

Table 11: アラートグループおよび実行されるコマンド

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。
設定	設定に関連した定期的なイベント。	show module show version
診断	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 <i>number</i> 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 <i>number</i> detail show module show tech-support gold show tech-support ha show tech-support platform

アラートグループ	説明	実行されるコマンド
環境	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
インベントリ	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 sptom all show system uptime show version
ライセンス	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
ラインカードハードウェア	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 sptom all show tech-support ethpm show tech-support gold show tech-support ha show tech-support platform show version

アラートグループ	説明	実行されるコマンド
スーパーバイザハードウェア	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
システム	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
テスト	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 **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。



Note 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 レベルを示します。

Table 12: 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	警告	警告 (4)	警告状態。
2	通知	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	標準	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マ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転送が、ご使用のデバイスから直接、または HTTP プロキシサーバやダウンロード可能な転送ゲートウェイ（TG）を経由して行われます。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、関連するフィールドの注意事項、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
- お使いの 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

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 E 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。

高可用性

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

Smart Call Home のインスタンスが 1 つサポートされます。次の URL から、Smart Call Home の Web サイトでお客様の連絡先を登録できます。https://supportforums.cisco.com/community/netpro/solutions/smart_services/smartcallhome

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。

Smart Call Home は Virtual Routing and Forwarding (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。
- デバイスは電子メール 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。

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フォワーディング (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 には最大 5 個までの SMTP サーバを設定できます。
- Link up/down syslog メッセージは、Smart Call Home メッセージまたはアラート通知をトリガーしません。

- 住所、顧客 ID、サイト ID などの Smart Call Home コマンドを設定する場合は、これらのコマンドをセミコロン区切りでグループ化するのではなく、個別のコマンドとして設定する必要があります。

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。

Table 13: 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アソシエート	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 のメッセージレベル	0 (ゼロ)
HTTP プロキシサーバの使用	無効であり、プロキシサーバは設定されていません。

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ります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 \(126 ページ\)](#)
2. [宛先プロファイルの作成 \(128 ページ\)](#)
3. [アラートグループと宛先プロファイルのアソシエート \(131 ページ\)](#)
4. (任意) [アラートグループへの show コマンドの追加 \(132 ページ\)](#)
5. [Smart Call Home のイネーブル化またはディセーブル化 \(139 ページ\)](#)
6. (省略可) [Smart Call Home 設定のテスト \(140 ページ\)](#)

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。

これらの Smart Call Home コマンドは、セミコロン区切りでグループ化するのではなく、個別のコマンドとして設定する必要があります。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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 <i>sys-contact</i> Example: <pre>switch(config)# snmp-server contact personname@companyname.com</pre>	SNMP sysContact を設定します。
ステップ 3	callhome Example: <pre>switch(config)# callhome switch(config-callhome)#</pre>	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 <i>email-address</i> Example: <pre>switch(config-callhome)# email-contact admin@Mycompany.com</pre>	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。 <i>email-address</i> 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。 Note 任意の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。

	Command or Action	Purpose
ステップ 5	phone-contact <i>international-phone-number</i> Example: <pre>switch(config-callhome)# phone-contact +1-800-123-4567</pre>	デバイスの担当者の電話番号を国際電話フォーマットで設定します。 <i>international-phone-number</i> 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。 Note 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 <i>address</i> Example: <pre>switch(config-callhome)# streetaddress 123 Anystreet st. Anytown,AnyWhere</pre>	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。 <i>address</i> 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	(Optional) contract-id <i>contract-number</i> Example: <pre>switch(config-callhome)# contract-id Contract5678</pre>	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。 契約番号は、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	(Optional) customer-id <i>customer-number</i> Example: <pre>switch(config-callhome)# customer-id Customer123456</pre>	サービス契約からこのデバイスのカスタマー番号を設定します。 カスタマー番号は、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	(Optional) site-id <i>site-number</i> Example: <pre>switch(config-callhome)# site-id Site1</pre>	このデバイスのサイト番号を設定します。 <i>site-number</i> 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	(Optional) switch-priority <i>number</i> Example: <pre>switch(config-callhome)# switch-priority 3</pre>	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。
ステップ 11	commit Example:	Smart Call Home 設定コマンドをコミットします。

	Command or Action	Purpose
	<code>switch(config-callhome)# commit</code>	
ステップ 12	(Optional) show callhome Example: <code>switch(config-callhome)# show callhome</code>	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	(Optional) copy running-config startup-config Example: <code>switch(config)# copy running-config startup-config</code>	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。

What to do next

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： <code>switch# configure terminal</code> <code>switch(config)#</code>	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： <code>switch(config)# callhome</code> <code>switch(config-callhome)#</code>	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： <code>switch(config-callhome)# destination-profile Noc101</code>	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： <code>switch(config-callhome)# destination-profile Noc101 format full-txt</code>	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。

	コマンドまたはアクション	目的
ステップ 5	commit 例： <code>switch(config-callhome)# commit</code>	Smart Call Home 設定コマンドをコミットします。
ステップ 6	(任意) show callhome destination-profile [profile name] 例： <code>switch(config-callhome)# show callhome destination-profile profile Noc101</code>	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	(任意) copy running-config startup-config 例： <code>switch(config)# copy running-config startup-config</code>	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。

次のタスク

1つの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：E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 Eメールアドレスに送信された Smart Call Home メッセージの長さ。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example:	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

	Command or Action	Purpose
	switch# configure terminal switch(config)#	
ステップ 2	callhome Example: 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 { <i>name</i> CiscoTAC-1 full-txt-destination short-txt-destination } email-addr <i>address</i> Example: 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 E 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 { <i>name</i> CiscoTAC-1 full-txt-destination short-txt-destination } http <i>address</i> Example: switch(config-callhome)# destination-profile CiscoTAC-1 http https://tools.cisco.com/its/service/aitte/services/IDEService	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 { <i>name</i> CiscoTAC-1 full-txt-destination short-txt-destination } transport-method { email http } Example: 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。
ステップ 6	destination-profile { <i>name</i> CiscoTAC-1 full-txt-destination short-txt-destination } message-level <i>number</i> Example: 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 では、Smart Call Home 重大度が一致する、またはそれ以上であるアラートのみが、このプロファイルの宛先に送信されます。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 { <i>name</i> CiscoTAC-1 full-txt-destination short-txt-destination } message-size <i>number</i> Example:	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。

	Command or Action	Purpose
	<pre>switch(config-callhome)# destination-profile full-txt-destination message-size 100000</pre>	
ステップ 8	commit Example: <pre>switch(config-callhome)# commit</pre>	Smart Call Home 設定コマンドをコミットします。
ステップ 9	(Optional) show callhome destination-profile [profile name] Example: <pre>switch(config-callhome)# show callhome destination-profile profile full-text-destination</pre>	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	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	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。

What to do next

1 つの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アソシエート

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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 Example: <pre>switch(config)# callhome switch(config-callhome)#</pre>	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 	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。

	Command or Action	Purpose
	Supervisor-Hardware Syslog-group-port System Test} Example: <pre>switch(config-callhome)# destination-profile Noc101 alert-group All</pre>	
ステップ 4	commit Example: <pre>switch(config-callhome)# commit</pre>	Smart Call Home 設定コマンドをコミットします。
ステップ 5	(Optional) show callhome destination-profile [profile name] Example: <pre>switch(config-callhome)# show callhome destination-profile profile Noc101</pre>	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	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	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。

What to do next

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 グループには、最大 5 個のユーザー定義 CLI **show** コマンドを割り当てることができます。



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

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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

	Command or Action	Purpose
ステップ 2	callhome Example: <pre>switch(config)# callhome switch(config-callhome)#</pre>	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 Example: <pre>switch(config-callhome)# alert-group Configuration user-def-cmd show ip route</pre>	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 Example: <pre>switch(config-callhome)# commit</pre>	Smart Call Home 設定コマンドをコミットします。
ステップ 5	(Optional) show callhome user-def-cmds Example: <pre>switch(config-callhome)# show callhome user-def-cmds</pre>	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	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	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。

What to do next

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 E メール アドレスも設定できます。

Smart Call Home には最大 5 個までの 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。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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 Example: <pre>switch(config)# callhome switch(config-callhome)#</pre>	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] Example: <pre>switch(config-callhome)# transport email mail-server 192.0.2.1 use-vrf Red</pre>	<p>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。デフォルトポート番号は、25 です。</p> <p>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。</p> <p>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。</p>
ステップ 4	(Optional) transport email from email-address Example: <pre>switch(config-callhome)# transport email from person@company.com</pre>	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	(Optional) transport email reply-to email-address Example: <pre>switch(config-callhome)# transport email reply-to person@company.com</pre>	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 Example: <pre>switch(config-callhome)# commit</pre>	Smart Call Home 設定コマンドをコミットします。

	Command or Action	Purpose
ステップ 7	(Optional) show callhome transport Example: switch(config-callhome)# 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。
ステップ 8	(Optional) copy running-config startup-config Example: switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

What to do next

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 を使用すると、HTTP で 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	(任意) show callhome 例:	Smart Call Home 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
	<code>switch(config-callhome)# show callhome</code>	
ステップ 6	<p>(任意) copy running-config startup-config</p> <p>例 :</p> <pre>switch(config)# copy running-config startup-config</pre>	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。

次のタスク

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	<p>configure terminal</p> <p>例 :</p> <pre>switch# configure terminal switch(config)#</pre>	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	<p>callhome</p> <p>例 :</p> <pre>switch(config)# callhome switch(config-callhome)#</pre>	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	<p>transport http proxy server ip-address [port number]</p> <p>例 :</p> <pre>switch(config-callhome)# transport http proxy server 192.0.2.1</pre>	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。デフォルトのポート番号は 8080 です。
ステップ 4	<p>transport http proxy enable</p> <p>例 :</p> <pre>switch(config-callhome)# transport http proxy enable</pre>	<p>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。</p> <p>(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。</p>

	コマンドまたはアクション	目的
		(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	(任意) show callhome transport 例： switch(config-callhome)# 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。
ステップ 7	(任意) copy running-config startup-config 例： switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次のタスク

任意で、定期的な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

デバイス上で現在有効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な送信するように、デバイスを設定できます。デバイスは 2 つの Smart Call Home 通知（定期的な設定メッセージと定期的なインベントリ メッセージ）を生成します。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: 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 Example: 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。

	Command or Action	Purpose
ステップ 3	periodic-inventory notification [interval days] [timeofday time] Example: <pre>switch(config-callhome)# periodic-inventory notification interval 20</pre>	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 Example: <pre>switch(config-callhome)# commit</pre>	Smart Call Home 設定コマンドをコミットします。
ステップ 5	(Optional) show callhome Example: <pre>switch(config-callhome)# show callhome</pre>	Smart Call Home に関する情報を表示します。
ステップ 6	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	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。

What to do next

任意で重複メッセージ スロットリングを無効にします。

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け取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 : <pre>switch# configure terminal switch(config)#</pre>	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 :	Smart Call Home 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
	switch(config)# callhome switch(config-callhome)#	
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。
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	(任意) copy running-config startup-config 例： switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

次のタスク

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	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。

	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	(任意) copy running-config startup-config 例： switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

次のタスク

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の 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	(任意) copy running-config startup-config 例：	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。

コマンドまたはアクション	目的
switch(config)# copy running-config startup-config	

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 <i>name</i>	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 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。
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、コンタクト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。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、コンタクト情報と電子メールの情報を設定した後で、HTTP を介して 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
```

次に、複数の SMTP サーバを Smart Call Home メッセージに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

次の表に、イベントトリガおよび 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 (Configuration)	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
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

アラートグループ	イベント名	説明	Smart Call Home 重大度
Line module Hardware 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
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 (注) Link up/down syslog メッセージは、Smart Call Home メッセージ またはアラート通知をトリガーしません。	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

データ項目	説明
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 (Cisco Nexus 9000 シリーズスイッチなど)。	/aml/header/source

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）
デバイス ID	<p>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、<i>type@Sid@serial</i> です。</p> <ul style="list-style-type: none"> • <i>type</i> は、バックプレーン IDPROM からの製品の型番です。 • <i>@</i> は区切り文字です。 • <i>Sid</i> は C で、シリアル ID をシャースシリアル番号として特定します。 • <i>serial</i> は、Sid フィールドによって識別される番号です。 <p>例：N9K-C9508@C@12345678</p>	/aml/ header/deviceId
カスタマー 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
連絡先 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

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）
Server ID	<p>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、<i>type@Sid@serial</i> です。</p> <ul style="list-style-type: none"> • <i>type</i> は、バックプレーン IDPROM からの製品の型番です。 • <i>@</i> は区切り文字です。 • <i>Sid</i> 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。 • <i>serial</i> は、Sid フィールドによって識別される番号です。 <p>例：N9K-C9508@C@12345678</p>	/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
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
[連絡先電子メール（Contact email）]	この装置の担当者の電子メールアドレス。	/aml/body/sysContactEmail
連絡先電話番号	このユニットの連絡先である人物の電話番号	/aml/body/sysContactPhoneNumber
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（製品ファミリー名に含まれる具体的なモデル）。	/aml/body/chassis/name
シリアル番号	ユニットのシャーシのシリアル番号	/aml/body/chassis/serialNo

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）
Command output name	実行されたCLI コマンドの正確な名前。	/aml/attachments/attachment/name
添付ファイルの種類	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
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 モジュールの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名	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

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）
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 ソフトウェアのバージョン	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

次の表に、フルテキストまたはXMLメッセージのコンポーネント 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の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 名	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 ソフトウェアのバージョン	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
プロセス状態	プロセスの状態（実行中、中止など）	/aml/body/process/processState

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）
プロセス例外	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:Nexus9000
Switch Priority:0
Device Id:N9K-C9508C@TXX12345678
Server Id:N9K-C9508C@TXX12345678
Time of Event:2013-05-17 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 2013 May 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:N9K-C9508
Affected Chassis Serial Number:TXX12345678 Affected Chassis Hardware Version:0.405
Affected Chassis Software Version:6.1(2) Affected Chassis Part No:11-11111-11 end chassis
information:
start attachment
  name:show logging logfile | tail -n 200
  type:text
  data:
    2013 May 17 10:57:51 dc3-test %SYSLOG-1-SYSTEM_MSG : Logging logfile (messages) cleared
    by user
    2013 May 17 10:57:53 dc3-test %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configuring console from
    /dev/ttyS0 /dev/ttyS0_console
    2013 May 17 10:58:35 dc3-test %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configuring console from
    /dev/ttyS0 /dev/ttyS0_console
    2013 May 17 10:59:00 dc3-test %DAEMON-3-SYSTEM_MSG: error: setsockopt IP_TOS 16:
    Invalid argument: - sshd[14484]
    2013 May 17 10:59:05 dc3-test %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configuring console from
    /dev/ttyS0 /dev/ttyS0_console
    2013 May 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).
    2013 May 17 16:28:03 dc3-test %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configuring console from
    /dev/ttyS0 /dev/ttyS0_console
    2013 May 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 .
    2013 May 17 16:28:44 dc3-test %SYSMGR-2-SERVICE_CRASHED: Service "eltm" (PID 3504)
    hasn't caught signal 9 (no core).
    2013 May 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.
    2013 May 17 16:29:08 dc3-test %SYSMGR-2-SERVICE_CRASHED: Service "eltm" (PID 23210)
    hasn't caught signal 9 (no core).
    2013 May 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.
    2013 May 17 16:29:17 dc3-test %SYSMGR-2-SERVICE_CRASHED: Service "eltm" (PID 23294)
```

```
hasn't caught signal 9 (no core).
 2013 May 17 16:29:25 dc3-test %SYSMGR-2-HASWITCHOVER_PRE_START: This supervisor is
becoming active (pre-start phase).
 2013 May 17 16:29:25 dc3-test %SYSMGR-2-HASWITCHOVER_START: This supervisor is becoming
active.
 2013 May 17 16:29:26 dc3-test %USER-3-SYSTEM_MSG: crdcfg_get_srvinfo: mts_send failed
- device_test
 2013 May 17 16:29:27 dc3-test %NETSTACK-3-IP_UNK_MSG_MAJOR: netstack [4336] Unrecognized
message from MRIB. Major type 1807
 2013 May 17 16:29:27 dc3-test %IM-5-IM_INTF_STATE: mgmt0 is DOWN
 2013 May 17 16:29:28 dc3-test %SYSMGR-2-SWITCHOVER_OVER: Switchover completed.
 2013 May 17 16:29:28 dc3-test %DAEMON-3-SYSTEM_MSG: ntp:socket family : 2 - ntpd[19045]

 2013 May 17 16:29:28 dc3-test %DAEMON-3-SYSTEM_MSG: ntp:socket family : 10 - ntpd[19045]

 2013 May 17 16:29:28 dc3-test %DAEMON-3-SYSTEM_MSG: ntp:ipv6 only defined - ntpd[19045]

 2013 May 17 16:29:28 dc3-test %DAEMON-3-SYSTEM_MSG: ntp:bindv6 only defined -
ntpd[19045]
 2013 May 17 16:29:28 dc3-test %DAEMON-3-SYSTEM_MSG: ntp:socket family : 2 - ntpd[19045]

 2013 May 17 16:29:28 dc3-test %DAEMON-3-SYSTEM_MSG: ntp:socket family : 0 - ntpd[19045]

 2013 May 17 16:29:28 dc3-test %DAEMON-3-SYSTEM_MSG: ntp:socket family : 0 - ntpd[19045]

 2013 May 17 16:29:28 dc3-test %NETSTACK-3-CLIENT_GET: netstack [4336] HA client filter
recovery failed (0)
 2013 May 17 16:29:28 dc3-test %NETSTACK-3-CLIENT_GET: netstack [4336] HA client filter
recovery failed (0)
 2013 May 17 16:29:29 dc3-test %DAEMON-3-SYSTEM_MSG: ssh disabled, removing -
dcos-xinetd[19072]
 2013 May 17 16:29:29 dc3-test %DAEMON-3-SYSTEM_MSG: Telnet disabled, removing -
dcos-xinetd[19072]
 2013 May 17 16:29:31 dc3-test %DAEMON-3-SYSTEM_MSG: Telnet disabled, removing -
dcos-xinetd[19073]
 2013 May 17 16:29:32 dc3-test %DAEMON-3-SYSTEM_MSG: ssh disabled, removing -
dcos-xinetd[19079]
 2013 May 17 16:29:32 dc3-test %DAEMON-3-SYSTEM_MSG: Telnet disabled, removing -
dcos-xinetd[19079]
 2013 May 17 16:29:34 dc3-test %IM-5-IM_INTF_STATE: mgmt0 is UP
 2013 May 17 16:29:34 dc3-test %DAEMON-3-SYSTEM_MSG: ssh disabled, removing -
dcos-xinetd[19105]
 2013 May 17 16:29:34 dc3-test %DAEMON-3-SYSTEM_MSG: Telnet disabled, removing -
dcos-xinetd[19105]
 2013 May 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
 2013 May 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
 2013 May 17 16:29:38 dc3-test %CALLHOME-2-EVENT: SUP_FAILURE
 2013 May 17 16:29:46 dc3-test vsh[19166]: CLIC-3-FAILED_EXEC: Can not exec command
<more> return code <14>
 2013 May 17 16:30:24 dc3-test vsh[23810]: CLIC-3-FAILED_EXEC: Can not exec command
<more> return code <14>
 2013 May 17 16:30:24 dc3-test vsh[23803]: CLIC-3-FAILED_EXEC: Can not exec command
<more> return code <14>
 2013 May 17 16:30:24 dc3-test vsh[23818]: CLIC-3-FAILED_EXEC: Can not exec command
<more> return code <14>
 2013 May 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 .
 2013 May 17 16:30:47 dc3-test %SYSMGR-2-SERVICE_CRASHED: Service "eltm" (PID 4820)
hasn't caught signal 9 (no core).
 2013 May 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 .
 2013 May 17 16:31:02 dc3-test %SYSMGR-2-SERVICE_CRASHED: Service "eltm" (PID 24239)
```

```

hasn't caught signal 9 (no core).
2013 May 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 .
2013 May 17 16:31:14 dc3-test %SYSMGR-2-SERVICE_CRASHED: Service "eltm" (PID 24401)
hasn't caught signal 9 (no core).
2013 May 17 16:31:23 dc3-test %CALLHOME-2-EVENT: SW_CRASH alert for service: eltm
2013 May 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 .
2013 May 17 16:31:23 dc3-test %SYSMGR-2-SERVICE_CRASHED: Service "eltm" (PID 24407)
hasn't caught signal 9 (no core).
2013 May 17 16:31:24 dc3-test vsh[24532]: CLIC-3-FAILED_EXEC: Can not exec command
<more> return code <14>
2013 May 17 16:31:24 dc3-test vsh[24548]: CLIC-3-FAILED_EXEC: Can not exec command
<more> return code <14>
2013 May 17 16:31:24 dc3-test vsh[24535]: CLIC-3-FAILED_EXEC: Can not exec command
<more> return code <14>
2013 May 17 16:31:33 dc3-test %NETSTACK-3-INTERNAL_ERROR: netstack [4336] (null)
2013 May 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
type:text
data:

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 Ethernet3/29 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

end attachment
start attachment
type:text
data:
end attachment
start attachment
name:show license usage
type:text
data:
Feature Ins Lic Status Expiry Date Comments
Count
-----
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:TX12345678:478F82E6</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>2013-05-17 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:TX12345678:478F82E6</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>2013-05-17 16:31:33 GMT+0000</ch:EventTime>
<ch:MessageDescription>SYSLOG_ALERT 2013 May 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>Nexus9000</ch:Series> </ch:Event> <ch:CustomerData> <ch:UserData>
<ch:Email>contact@example.com</ch:Email>
</ch:UserData>
<ch:ContractData>
<ch:DeviceId>N9K-C9508@C@TX12345678</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>N9K-C9508</rme:Model>
<rme:HardwareVersion>0.405</rme:HardwareVersion>
<rme:SerialNumber>TX12345678</rme:SerialNumber>
</rme:Chassis>
</ch:Device>
</ch:CallHome>
</aml-block:Content>
<aml-block:Attachments>
<aml-block:Attachment type="inline">
<aml-block:Name>show logging logfile | tail -n 200</aml-block:Name> <aml-block:Data
encoding="plain">
<![CDATA[2013 May 17 10:57:51 dc3-test %SYSLOG-1-SYSTEM_MSG : Logging logfile (messages)
cleared by user
2013 May 17 10:57:53 dc3-test %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configuring console from
/dev/ttyS0 /dev/ttyS0_console
2013 May 17 10:58:35 dc3-test %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configuring console from

```

```

/dev/ttyS0 /dev/ttyS0_console
2013 May 17 10:59:00 dc3-test %DAEMON-3-SYSTEM_MSG: error: setsockopt IP_TOS 16: Invalid
argument: - sshd[14484]
2013 May 17 10:59:05 dc3-test %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configuring console from
/dev/ttyS0 /dev/ttyS0_console
2013 May 17 12:11:18 dc3-test %SYSMGR-STANDBY-5-SUBPROC_TERMINATED: \"System Manager
(gsync controller)\" (PID 12000) has finished with error code
SYSMGR_EXITCODE_GSYNCFIILED_NONFATAL (12).
2013 May 17 16:28:03 dc3-test %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configuring console from
/dev/ttyS0 /dev/ttyS0_console
2013 May 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 .
2013 May 17 16:28:44 dc3-test %SYSMGR-2-SERVICE_CRASHED: Service \"\"elmt\"\" (PID 3504)
hasn't caught signal 9 (no core).
2013 May 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 .
2013 May 17 16:29:08 dc3-test %SYSMGR-2-SERVICE_CRASHED: Service \"\"elmt\"\" (PID 23210)
hasn't caught signal 9 (no core).
2013 May 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 .
2013 May 17 16:29:17 dc3-test %SYSMGR-2-SERVICE_CRASHED: Service \"\"elmt\"\" (PID 23294)
hasn't caught signal 9 (no core).
2013 May 17 16:29:25 dc3-test %SYSMGR-2-HASWITCHOVER_PRE_START: This supervisor is
becoming active (pre-start phase).
2013 May 17 16:29:25 dc3-test %SYSMGR-2-HASWITCHOVER_START: This supervisor is becoming
active.
2013 May 17 16:29:26 dc3-test %USER-3-SYSTEM_MSG: crdcfg_get_srvinf: mts_send failed -
device_test
2013 May 17 16:29:27 dc3-test %NETSTACK-3-IP_UNK_MSG_MAJOR: netstack [4336] Unrecognized
message from MRIB. Major type 1807
2013 May 17 16:29:27 dc3-test %IM-5-IM_INTF_STATE: mgmt0 is DOWN
2013 May 17 16:29:28 dc3-test %SYSMGR-2-SWITCHOVER_OVER: Switchover completed.
2013 May 17 16:29:28 dc3-test %DAEMON-3-SYSTEM_MSG: ntp:socket family : 2 - ntpd[19045]
2013 May 17 16:29:28 dc3-test %DAEMON-3-SYSTEM_MSG: ntp:socket family : 10 - ntpd[19045]
2013 May 17 16:29:28 dc3-test %DAEMON-3-SYSTEM_MSG: ntp:ipv6 only defined - ntpd[19045]
2013 May 17 16:29:28 dc3-test %DAEMON-3-SYSTEM_MSG: ntp:bindv6 only defined - ntpd[19045]
2013 May 17 16:29:28 dc3-test %DAEMON-3-SYSTEM_MSG: ntp:socket family : 2 - ntpd[19045]
2013 May 17 16:29:28 dc3-test %DAEMON-3-SYSTEM_MSG: ntp:socket family : 0 - ntpd[19045]
2013 May 17 16:29:28 dc3-test %DAEMON-3-SYSTEM_MSG: ntp:socket family : 0 - ntpd[19045]
2013 May 17 16:29:28 dc3-test %NETSTACK-3-CLIENT_GET: netstack [4336] HA client filter
recovery failed (0)
2013 May 17 16:29:28 dc3-test %NETSTACK-3-CLIENT_GET: netstack [4336] HA client filter
recovery failed (0)
2013 May 17 16:29:29 dc3-test %DAEMON-3-SYSTEM_MSG: ssh disabled, removing -
dcos-xinetd[19072]
2013 May 17 16:29:29 dc3-test %DAEMON-3-SYSTEM_MSG: Telnet disabled, removing -
dcos-xinetd[19072]
2013 May 17 16:29:31 dc3-test %DAEMON-3-SYSTEM_MSG: Telnet disabled, removing -
dcos-xinetd[19073]
2013 May 17 16:29:32 dc3-test %DAEMON-3-SYSTEM_MSG: ssh disabled, removing -
dcos-xinetd[19079]
2013 May 17 16:29:32 dc3-test %DAEMON-3-SYSTEM_MSG: Telnet disabled, removing -
dcos-xinetd[19079]
2013 May 17 16:29:34 dc3-test %IM-5-IM_INTF_STATE: mgmt0 is UP
2013 May 17 16:29:34 dc3-test %DAEMON-3-SYSTEM_MSG: ssh disabled, removing -
dcos-xinetd[19105]
2013 May 17 16:29:34 dc3-test %DAEMON-3-SYSTEM_MSG: Telnet disabled, removing -
dcos-xinetd[19105]
2013 May 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
2013 May 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
2013 May 17 16:29:38 dc3-test %CALLHOME-2-EVENT: SUP_FAILURE
2013 May 17 16:29:46 dc3-test vsh[19166]: CLIC-3-FAILED_EXEC: Can not exec command <more>

```

```

return code <14>
2013 May 17 16:30:24 dc3-test vsh[23810]: CLIC-3-FAILED_EXEC: Can not exec command <more>
return code <14>
2013 May 17 16:30:24 dc3-test vsh[23803]: CLIC-3-FAILED_EXEC: Can not exec command <more>
return code <14>
2013 May 17 16:30:24 dc3-test vsh[23818]: CLIC-3-FAILED_EXEC: Can not exec command <more>
return code <14>
2013 May 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 .
2013 May 17 16:30:47 dc3-test %SYSMGR-2-SERVICE_CRASHED: Service \"eltm\" (PID 4820)
hasn't caught signal 9 (no core).
2013 May 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 .
2013 May 17 16:31:02 dc3-test %SYSMGR-2-SERVICE_CRASHED: Service \"eltm\" (PID 24239)
hasn't caught signal 9 (no core).
2013 May 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 .
2013 May 17 16:31:14 dc3-test %SYSMGR-2-SERVICE_CRASHED: Service \"eltm\" (PID 24401)
hasn't caught signal 9 (no core).
2013 May 17 16:31:23 dc3-test %CALLHOME-2-EVENT: SW_CRASH alert for service: eltm
2013 May 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 .
2013 May 17 16:31:23 dc3-test %SYSMGR-2-SERVICE_CRASHED: Service \"eltm\" (PID 24407)
hasn't caught signal 9 (no core).
2013 May 17 16:31:24 dc3-test vsh[24532]: CLIC-3-FAILED_EXEC: Can not exec command <more>
return code <14>
2013 May 17 16:31:24 dc3-test vsh[24548]: CLIC-3-FAILED_EXEC: Can not exec command <more>
return code <14>
2013 May 17 16:31:24 dc3-test vsh[24535]: CLIC-3-FAILED_EXEC: Can not exec command <more>
return code <14>
2013 May 17 16:31:33 dc3-test %NETSTACK-3-INTERNAL_ERROR: netstack [4336] (null)
2013 May 17 16:31:33 dc3-test %ETHERPORT-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> <aml-block:Data encoding="plain"> <![CDATA[
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

]]>
</aml-block:Data>
</aml-block:Attachment>
<aml-block:Attachment type="inline">
<aml-block:Name> <aml-block:Data encoding="plain"> <!--> </aml-block:Data>
</aml-block:Attachment> <aml-block:Attachment type="inline"> <aml-block:Name>show license
usage</aml-block:Name> <aml-block:Data encoding="plain">
<![CDATA[Feature Ins Lic Status Expiry Date Comments
Count
-----

```

```
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>
```

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/nexus9000/Nexus9000MIBSupportList.html



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。

この章は、次の内容で構成されています。

- [セッション マネージャについて, on page 157](#)
- [セッション マネージャの前提条件 \(158 ページ\)](#)
- [Session Manager の注意事項および制約事項 \(158 ページ\)](#)
- [Session Manager の設定 \(158 ページ\)](#)
- [Session Manager 設定の確認, on page 161](#)
- [Session Manager のコンフィギュレーション例, on page 161](#)
- [その他の参考資料 \(162 ページ\)](#)

セッション マネージャについて

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クス検査を行います。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。エラーが発生すると、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。

高可用性

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。

セッション マネージャの前提条件

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。

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。

- 1 つのセッションを使用して実行できるサービス アクセス ポイント (SAP) は 1 つだけです。
- 設定セッションは、リロード後に保持されません。
- 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。
- 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 (例えば 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) 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、セッション マネージャがコマンドを受け取るようになります。

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。

Procedure

	Command or Action	Purpose
ステップ 1	configure session name Example: <pre>switch# configure session myACLs switch(config-s)#</pre>	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	(Optional) show configuration session [name] Example: <pre>switch(config-s)# show configuration session myACLs</pre>	セッションの内容を表示します。
ステップ 3	(Optional) save location Example: <pre>switch(config-s)# save bootflash:sessions/myACLs</pre>	セッションをファイルに保存します。保管場所には <code>bootflash:</code> 、 <code>slot0:</code> 、または <code>volatile:</code> 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。

Procedure

	Command or Action	Purpose
ステップ 1	configure session name Example: <pre>switch# configure session myacl switch(config-s)#</pre>	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 Example: <pre>switch(config-s)# ip access-list acl switch(config-s-acl)#</pre>	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	(Optional) permit protocol source destination Example:	ACL に許可文を追加します。

	Command or Action	Purpose
	<code>switch(config-s-acl)# permit tcp any any</code>	
ステップ 4	interface <i>interface-type number</i> Example: <code>switch(config-s-acl)# interface ethernet 2/1</code> <code>switch(config-s-if)#</code>	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 <i>name {in out}</i> Example: <code>switch(config-s-if)# ip access-group acl1 in</code>	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	(Optional) show configuration session [<i>name</i>] Example: <code>switch(config-s-if)# show configuration session myacls</code>	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: <code>switch(config-s)# verify</code>	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: <code>switch(config-s)# commit</code>	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: <pre>switch(config-s)# save bootflash:sessions/myACLs</pre>	(任意) セッションをファイルに保存します。保管場所には <code>bootflash:</code> 、 <code>slot0:</code> 、または <code>volatile:</code> 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: <pre>switch(config-s)# abort switch#</pre>	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
コンフィギュレーション ファイル	『Cisco Nexus 9000 Series NX-OS Fundamentals Configuration Guide』



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。

- [スケジューラについて \(163 ページ\)](#)
- [スケジューラ的前提条件 \(164 ページ\)](#)
- [スケジューラの注意事項および制約事項 \(165 ページ\)](#)
- [スケジューラのデフォルト設定 \(165 ページ\)](#)
- [スケジューラの設定 \(165 ページ\)](#)
- [スケジューラの設定確認 \(172 ページ\)](#)
- [スケジューラの設定例 \(172 ページ\)](#)

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。
- 1回限定モード：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。

高可用性

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

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。
- スケジュールリングされたジョブを設定するには、`network-admin` のユーザ権限が必要です。

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。
 - 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。
- スケジューラは、スケジュールモード設定で **time** コマンドの繰り返しオプションを使用して、任意のスケジュールの過去の `start_time` を承認します。次に、入力された開始時刻が過去であることを示す警告がスローされます。任意のスケジュールの `start_time` は、リポート後、および以前に保存された設定を再適用した後でも、最初と同じままです。

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

スケジューラの有効化または無効化

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有効にすることができ、または、スケジューラを有効にした後にスケジューラ機能を無効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	configure terminal 例：	グローバル設定モードを開始します。

	コマンドまたはアクション	目的
	switch# configure terminal switch(config)#	
ステップ 2	[no] feature scheduler 例： switch(config)# feature scheduler	スケジューラを有効または無効にします。
ステップ 3	(任意) show scheduler config 例： switch(config)# show scheduler config config terminal feature scheduler scheduler logfile size 16 end	スケジューラ設定を表示します。
ステップ 4	(任意) copy running-config startup-config 例： switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

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	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	scheduler logfile size value 例： switch(config)# scheduler logfile size 1024	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。

	コマンドまたはアクション	目的
ステップ 3	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	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ルリングを行うユーザにリモート認証を使用するように、スケジュールを設定できます。



- (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	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	scheduler aaa-authentication password [0 7] password 例 : <pre>switch(config)# scheduler aaa-authentication password X12y34Z56a</pre>	現在ログインしているユーザのクリアテキストパスワードを設定します。
ステップ 3	scheduler aaa-authentication username name password [0 7] password 例 : <pre>switch(config)# scheduler aaa-authentication username newuser password Z98y76X54b</pre>	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。

	コマンドまたはアクション	目的
ステップ 4	(任意) show running-config include "scheduler aaa-authentication" 例： <pre>switch(config)# show running-config include "scheduler aaa-authentication"</pre>	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	(任意) copy running-config startup-config 例： <pre>switch(config)# copy running-config startup-config</pre>	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	configure terminal 例： <pre>switch# configure terminal switch(config)#</pre>	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	scheduler job name string 例： <pre>switch(config)# scheduler job name backup-cfg switch(config-job)</pre>	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	command1 ;[command2 ;command3 ;...] 例： <pre>switch(config-job)# copy running-config tftp://1.2.3.4/\$(SWITCHNAME)-cfg.\$(TIMESTAMP) vrf management switch(config-job)#</pre>	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（「;」のように）区切る必要があります。 この例では、実行コンフィギュレーションをブートフラッシュ内のファイルに保存するスケジューラジョブを作成しています。その後ジョブはブートフラッシュ

	コマンドまたはアクション	目的
		シュから TFTP サーバにファイルをコピーし、現在のタイムスタンプとスイッチ名を使用してファイル名を作成します。
ステップ 4	(任意) show scheduler job [name name] 例： switch(config-job)# show scheduler job	ジョブ情報を表示します。
ステップ 5	(任意) copy running-config startup-config 例： switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

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	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 scheduler job name string 例： switch(config)# no scheduler job name configsave switch(config-job)	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	(任意) show scheduler job [name name] 例： switch(config-job)# show scheduler job name configsave	ジョブ情報を表示します。
ステップ 4	(任意) copy running-config startup-config 例： switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

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	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	scheduler schedule name string 例： switch(config)# scheduler schedule name weekendbackupqos switch(config-schedule)#	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	job name string 例： switch(config-schedule)# job name offpeakZoning	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	time daily time 例：	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。

	コマンドまたはアクション	目的
	<code>switch(config-schedule)# time daily 23:00</code>	
ステップ 5	<p>time weekly <i>[[dow:]HH:]MM</i></p> <p>例 :</p> <pre>switch(config-schedule)# time weekly Sun:23:00</pre>	<p>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。</p> <p>曜日 (dow) は次のいずれかの方法で指定されます。</p> <ul style="list-style-type: none"> • 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。 <p>引数全体の最大長は 10 です。</p>
ステップ 6	<p>time monthly <i>[[dm:]HH:]MM</i></p> <p>例 :</p> <pre>switch(config-schedule)# time monthly 28:23:00</pre>	<p>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。</p>
ステップ 7	<p>time start {now repeat <i>repeat-interval</i> <i>delta-time</i> [repeat <i>repeat-interval</i>]}</p> <p>例 :</p> <pre>switch(config-schedule)# time start now repeat 48:00</pre>	<p>ジョブが定期的に開始することを意味します。</p> <p>start-time の形式は <code>[[[yyy:]mmm:]dd:]HH:]MM</code> です。</p> <ul style="list-style-type: none"> • <i>delta-time</i> : 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よう指定します。 • repeat repeat-interval : ジョブを反復する回数を指定します。 <p>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。</p>
ステップ 8	<p>(任意) show scheduler config</p> <p>例 :</p> <pre>switch(config)# show scheduler config</pre>	<p>スケジューラ設定を表示します。</p>
ステップ 9	<p>(任意) copy running-config startup-config</p> <p>例 :</p>	<p>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。</p>

	コマンドまたはアクション	目的
	switch(config)# copy running-config startup-config	

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	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	clear scheduler logfile 例： switch(config)# clear scheduler logfile	スケジューラ ログ ファイルを消去します。

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

この例では、実行コンフィギュレーションをブートフラッシュ内のファイルに保存するスケジュールジョブを作成する方法を示します。このジョブは、その後で、ブートフラッシュから

TFTP サーバにファイルをコピーします（現在のタイムスタンプとスイッチ名を使用してファイル名を作成します）。

```
switch# configure terminal
switch(config)# scheduler job name backup-cfg
switch(config-job)# copy running-config
tftp://1.2.3.4/${SWITCHNAME}-cfg.${TIMESTAMP} vrf management
switch(config-job)# end
switch(config)#
```

スケジュール ジョブのスケジュールリング

次に、backup-cfg という名前のスケジュール ジョブを、毎日午前1時に実行するようスケジュール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#
```

スケジュール ジョブの実行結果の表示

次に、スケジュールによって実行されたスケジュール 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#
```



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。

この章は、次の内容で構成されています。

- [SNMP について, on page 175](#)
- [SNMP の注意事項および制約事項 \(182 ページ\)](#)
- [SNMP のデフォルト設定 \(183 ページ\)](#)
- [SNMP の設定 \(183 ページ\)](#)
- [SNMP ローカル エンジン ID の設定, on page 209](#)
- [SNMP の設定の確認, on page 210](#)
- [SNMP の設定例 \(211 ページ\)](#)
- [その他の参考資料 \(212 ページ\)](#)

SNMP について

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。

- MIB (Management Information Base; 管理情報ベース) : SNMP エージェントの管理対象オブジェクトの集まり

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。インフォームは、SNMP エージェントから SNMP マネージャに送信される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び送信できます。

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、デフォルトで有効になっている SNMP トラップを示します。

Trap Type	説明
全体	: coldStart
エンティティ	: entity_fan_status_change
エンティティ	: entity_mib_change
エンティティ	: entity_module_status_change
エンティティ	: entity_module_inserted
エンティティ	: entity_module_removed
エンティティ	: entity_power_out_change
エンティティ	: entity_power_status_change
エンティティ	: entity_unrecognised_module
リンク	: cErrDisableInterfaceEventRev1

Trap Type	説明
リンク	: cieLinkDown
リンク	: cieLinkUp
リンク	: cmn-mac-move-notification
リンク	: delayed-link-state-change
リンク	: extended-linkDown
リンク	: extended-linkUp
リンク	: linkDown
リンク	: linkUp
rf	: redundancy_framework
ライセンス	: notify-license-expiry
ライセンス	: notify-no-license-for-feature
ライセンス	: notify-licensefile-missing
ライセンス	: notify-license-expiry-warning
upgrade	: UpgradeOpNotifyOnCompletion
upgrade	: UpgradeJobStatusNotify
エンティティ	: entity_sensor
rmon	: fallingAlarm
rmon	: hcRisingAlarm
rmon	: hcFallingAlarm
rmon	: risingAlarm

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。このレベルは、SNMPv3 ではサポートされていません。
- **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。

Table 14: 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	なし	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	なし	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	authNoPriv	HMAC-MD5、または HMAC-SHA	未対応	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。

モデル	レベル	認証	暗号化	結果
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、SNMPv3 に 3 つの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。



Note 外部の AAA サーバを使用して SNMPv3 を使う場合、外部 AAA サーバのユーザー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ワードは、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ワードになります。
- 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。



Note 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。

グループベースの SNMP アクセス



Note グループが業界全体で使用されている標準 SNMP 用語なので、この SNMP の項では、ロールのことをグループと言います。

SNMP アクセス権は、グループ別に編成されます。SNMP 内の各グループは、CLI を使用する場合のロールに似ています。各グループは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 Embedded Event Manager

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、SNMP のインスタンスを 1 つサポートします。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。

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。

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/nexus9000/Nexus9000MIBSupportList.html>
- Cisco NX-OS は、SNMPv3 noAuthNoPriv セキュリティ レベルをサポートしていません。
- Cisco Nexus 9000 シリーズ スイッチと、Cisco Nexus 3164Q、31128PQ、3232C、3264Q スイッチは、SNMP ローカル エンジン ID の設定をサポートしています。
- 以前のリリースへの無停止ダウングレードパスを行う場合、ローカル エンジン ID を設定していたなら、ローカル エンジン ID の設定を戻してから、SNMP ユーザとコミュニティ文字列を再設定する必要があります。
- デフォルトの SNMP PDU 値は 1500 バイトです。SNMP エージェントは、1500 バイトを超える応答 PDU をドロップするので、SNMP リクエストは失敗します。1500 バイトを超える MIB データ値を受信するには、`snmp-server packetsize <byte-count>` コマンドを使用して、パケット サイズを再設定します。有効なバイト数の範囲は 484 ~ 17382 です。GETBULK 応答がパケット サイズを超えると、データが切り捨てられることがあります。
- スイッチの機能を設定するには、CLI または SNMP を使用する必要があります。スイッチに、両方のインターフェイスを使用して機能を設定しないでください。
- シャーシにファンが装着されていない個々のファン OID ツリーで `cefcFanTrayOperStatus snmpwalk` を使用すると、ツリー内の次の OID エントリに対する応答が返されることがあります。この動作を防ぐには、`snmpwalk` で `-CI` オプションを使用します。
この動作は、親 OID をポーリングする場合、または `getmany` を使用する場合には見られません。
- SNMP トラップが完全に適切な機能動作を実行するには、少なくとも 1 つの実行中の BGP インスタンスが必要です。`snmp-server traps` 関連のコマンドを設定する前に、BGP ルーティングインスタンスを設定します。

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	有効 (Enabled)

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りますので注意してください。

SNMP ユーザの設定

SNMP ユーザを設定できます。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: 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	switch(config)# snmp-server user name [auth {md5 sha} <i>passphrase</i> [auto] [priv [aes-128] <i>passphrase</i>] [engineID id] [localizedkey]] Example: 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。 パスワードには最大 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、パスワード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	(Optional) show snmp user Example:	1 人または複数の SNMP ユーザに関する情報を表示します。

	Command or Action	Purpose
	<code>switch(config)# show snmp user</code>	
ステップ 4	(Optional) copy running-config startup-config Example: <code>switch(config)# copy running-config startup-config</code>	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するすべての 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： <code>switch# configure terminal</code> <code>switch(config)#</code>	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： <code>switch(config)# snmp-server user Admin enforcePriv</code>	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： <code>switch(config)# snmp-server globalEnforcePriv</code>	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	(任意) copy running-config startup-config 例： <code>switch(config)# copy running-config startup-config</code>	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
ステップ 2	snmp-server user name group 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	(任意) copy running-config startup-config 例： switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

SNMP 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tring を作成します。

	コマンドまたはアクション	目的
ステップ 3	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	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 SNMPv2 コミュニティまたは SNMPv3 ユーザに割り当てて、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 : <pre>switch# configure terminal switch(config)#</pre>	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 [use-ipv4acl acl-name use-ipv6acl acl-name] 例 : <pre>switch(config)# snmp-server community public use-ipv4acl myacl</pre>	SNMP コミュニティに IPv4 ACL または IPv6 ACL を割り当てて SNMPv2 要求をフィルタします。 (注) IPv6 ACL は、Cisco NX-OS リリース 7.0(3)I4(1) 以降、SNMPv2 コミュニティでサポートされます。

	コマンドまたはアクション	目的
		(注) Cisco NX-OS リリース 7.0(3)I4(1) より前のリリースでは、この CLI コマンドには use-ipv4acl ではなく use-acl が含まれています。
ステップ 3	snmp-server user <i>username</i> [use-ipv4acl <i>acl-name</i> use-ipv6acl <i>acl-name</i>] 例 : <pre>switch(config)# snmp-server user user1 use-ipv4acl myacl</pre>	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) IPv6 ACL は、Cisco NX-OS リリース 7.0(3)I4(1) 以降、SNMPv3 ユーザでサポートされます。 (注) Cisco NX-OS リリース 7.0(3)I4(1) より前のリリースでは、この CLI コマンドには use-ipv4acl ではなく use-acl が含まれています。
ステップ 4	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	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 通知レシーバの設定

複数のホスト レシーバに対して 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 : <pre>switch# configure terminal switch(config)#</pre>	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 <i>ip-address</i> traps version 1 <i>community</i> [udp_port number] 例 :	SNMPv1 トラップのホスト レシーバを設定します。 <i>ip-address</i> は IPv4 または IPv6 アドレスを使用できます。コミュニティは、最大 255 文字の英数字で指定

	コマンドまたはアクション	目的
	switch(config)# snmp-server host 192.0.2.1 traps version 1 public	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。 <i>ip-address</i> は IPv4 または IPv6 アドレス を使用できます。コミュニティは、最大 255 文字の英数字で指定できます。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。 <i>ip-address</i> は IPv4 または IPv6 アドレスを使用できま す。ユーザ名は、最大 255 文字の英数字 で指定できます。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解読す るために、Cisco NX-OS デバ イスの SNMP engineID 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	(任意) copy running-config startup-config 例： switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スター トアップ コンフィギュレーションにコ ピーします。

SNMP 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 : <pre>switch# configure terminal switch(config)#</pre>	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 traps version 2c name 例 : <pre>snmp-server host 192.0.2.1 source-interface ethernet 2/1 traps version 2c public</pre>	(任意) このホストにトラップメッセージを送信します。 トラップのバージョンには、通知メッセージに使用する SNMP バージョンを指定します。2c は、SNMPv2c が使用されることを示します。
ステップ 3	snmp-server host ip-address source-interface if-type if-number use-vrf vrf-name 例 : <pre>snmp-server host 192.0.2.1 source-interface ethernet 2/1 use-vrf default</pre>	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 アドレスにできます。VRF 名は、最大 32 文字の英数字で指定できます。 (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 4	snmp-server host ip-address source-interface if-type if-number [udp_port number] 例 : <pre>switch(config)# snmp-server host 192.0.2.1 source-interface ethernet 2/1</pre>	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。サポートされているインターフェイス タイプを特定するために「?」を使用します。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。

	コマンドまたはアクション	目的
ステップ 5	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。サポートされているインターフェイスタイプを特定するために「?」を使用します。
ステップ 6	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。

通知ターゲット 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アルを使用して、設定された通知ホスト レシーバへの SNMPv3 応答要求通知メッセージを暗号化します。



(注) 受信した INFORM PDU を認証して解読する場合、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 クレデンシアルが通知ホスト 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 sha-256} 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	(任意) copy running-config startup-config 例：	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。

	コマンドまたはアクション	目的
	switch(config)# copy running-config startup-config	

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 : <pre>switch# configure terminal switch(config)#</pre>	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 : <pre>switch(config)# snmp-server host 192.0.2.1 use-vrf Blue</pre>	<p>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。<i>ip-address</i> を IPv4 または IPv6 アドレスにできます。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。</p> <p>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。</p> <p>(注) このコマンドによってホスト設定は削除されません。</p>

	コマンドまたはアクション	目的
ステップ 3	<p>[no] snmp-server host ip-address filter-vrf vrf-name [udp_port number]</p> <p>例 :</p> <pre>switch(config)# snmp-server host 192.0.2.1 filter-vrf Red</pre>	<p>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。<i>ip-address</i> 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。</p> <p>このコマンドによって、 CISCO-SNMP-TARGET-EXT-MB の ExtSnmTargetVrfTable にエンタリが追 加されます。</p> <p>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 ExtSnmTargetVrfTable からエンタリを 削除します。</p> <p>(注) このコマンドによってホスト 設定は削除されません。</p>
ステップ 4	<p>(任意) copy running-config startup-config</p> <p>例 :</p> <pre>switch(config)# copy running-config startup-config</pre>	<p>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。</p>

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	<p>configure terminal</p> <p>例 :</p> <pre>switch# configure terminal switch(config)#</pre>	<p>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</p>
ステップ 2	<p>snmp-server source-interface traps if-type if-number</p> <p>例 :</p>	<p>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。サポートされているインターフェ</p>

	コマンドまたはアクション	目的
	<pre>switch(config)# snmp-server source-interface traps ethernet 1/2</pre>	<p>イスタップを特定するために「?」を使用します。</p> <p>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。</p> <p>(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。</p>
ステップ 3	<p>(任意) show snmp source-interface</p> <p>例 :</p> <pre>switch(config)# show snmp source-interface</pre>	<p>設定した発信元インターフェイスの情報を表示します。</p>
ステップ 4	<p>snmp-server host ip-address use-vrf vrf-name [udp_port number]</p> <p>例 :</p> <pre>switch(config)# snmp-server host 171.71.48.164 use-vrf default</pre>	<p>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。<i>ip-address</i> 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。</p> <p>(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。</p>
ステップ 5	<p>(任意) show snmp host</p> <p>例 :</p> <pre>switch(config)# show snmp host</pre>	<p>設定した SNMP ホストの情報を表示します。</p>

	コマンドまたはアクション	目的
ステップ 6	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	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。通知名を指定しなかった場合、Cisco NX-OS は、BGP、EIGRP、および OSPF の通知を除き、通知をすべてイネーブルにします。



Note **snmp-server enable traps** コマンドを使用すると、設定通知ホストレシーバによっては、トラップとインフォームの両方をイネーブルにできます。

次の表に、Cisco NX-OS MIB の通知を有効にするコマンドを示します。

Table 15: SNMP 通知のイネーブル化

MIB	関連コマンド
すべての通知 (BGP、EIGRP、および OSPF を除く)	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-CALLHOME-MIB	snmp-server enable traps callhome snmp-server enable traps callhome event-notify snmp-server enable traps callhome smtp-send-fail
CISCO-CONFIG-MAN-MIB	snmp-server enable traps config snmp-server enable traps config ccmCLIRunningConfigChanged
CISCO-EIGRP-MIB	snmp-server enable traps eigrp [<i>tag</i>]
CISCO-ERR-DISABLE-MIB	snmp-server enable traps link cerrDisableInterfaceEventRev1

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

MIB	関連コマンド
IF-MIB	<pre>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</pre>
OSPF-MIB, OSPF-TRAP-MIB	<pre>snmp-server enable traps ospf [tag] snmp-server enable traps ospf lsa snmp-server enable traps ospf rate-limit rate</pre>
CISCO-RF-MIB	<pre>snmp-server enable traps rf snmp-server enable traps rf redundancy_framework</pre>
CISCO-RMON-MIB	<pre>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</pre>
SNMPv2-MIB	<pre>snmp-server enable traps snmp snmp-server enable traps snmp authentication</pre>
CISCO-MAC-NOTIFICATION-MIB	<pre>snmp-server enable trap link cmn-mac-move-notification</pre>
CISCO-PORT-STORM-CONTROL-MIB	<pre>storm-control action trap</pre>
CISCO-STP-EXTENSIONS-MIB	<pre>snmp-server enable traps stpx stpxMstInconsistencyUpdate</pre>
CISCO-STP-BRIDGE-MIB	<pre>snmp-server enable traps bridge snmp-server enable traps bridge newroot snmp-server enable traps bridge topologychange</pre>

MIB	関連コマンド
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
VTP-MIB	snmp-server enable traps vtp snmp-server enable traps vtp notifs snmp-server enable traps vtp vlancreate snmp-server enable traps vtp vlandelete

指定した通知を有効にするには、示しているように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 例: <pre>switch(config)# snmp-server enable traps</pre>	すべての SNMP 通知をイネーブルにします。
snmp-server enable traps aaa [server-state-change] 例: <pre>switch(config)# snmp-server enable traps aaa</pre>	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。 <ul style="list-style-type: none"> • server-state-change : AAA サーバの状態変化通知を有効にします。
snmp-server enable traps bgp 例: <pre>switch(config)# snmp-server enable traps bgp</pre>	ボーダー ゲートウェイ プロトコル (BGP) SNMP 通知を有効にします。

コマンド	目的
<p>snmp-server enable traps bridge [newroot] [topologychange]</p> <p>例:</p> <pre>switch(config)# snmp-server enable traps bridge</pre>	<p>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。</p> <ul style="list-style-type: none"> • newroot : STP の新しいルートブリッジ通知を有効にします。 • topologychange : STP ブリッジのトポロジ変更通知を有効にします。
<p>snmp-server enable traps callhome [event-notify] [smtp-send-fail]</p> <p>例:</p> <pre>switch(config)# snmp-server enable traps callhome</pre>	<p>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。</p> <ul style="list-style-type: none"> • event-notify : Call Home の外部イベント通知を有効にします。 • 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有効にします。
<p>snmp-server enable traps config [ccmCLIRunningConfigChanged]</p> <p>例:</p> <pre>switch(config)# snmp-server enable traps config</pre>	<p>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。</p> <ul style="list-style-type: none"> • 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 通知を有効にします。
<p>snmp-server enable traps eigrp [tag]</p> <p>例:</p> <pre>switch(config)# snmp-server enable traps eigrp</pre>	<p>CISCO-EIGRP-MIB SNMP 通知をイネーブルにします。</p>

コマンド	目的
<p>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]</p> <p>例:</p> <pre>switch(config)# snmp-server enable traps entity</pre>	<p>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。</p> <ul style="list-style-type: none"> • entity_fan_status_change : エンティティファンの状態変化通知を有効にします。 • entity_mib_change : エンティティ MIB 変更通知を有効にします。 • entity_module_inserted : エンティティモジュール挿入通知を有効にします。 • entity_module_removed : エンティティモジュール削除通知を有効にします。 • 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有効にします。 • entity_power_out_change : エンティティの出力パワー変更通知を有効にします。 • entity_power_status_change : エンティティのパワーステータス変更通知を有効にします。 • entity_unrecognised_module : エンティティの未確認モジュール通知を有効にします。
<p>snmp-server enable traps feature-control [FeatureOpStatusChange]</p> <p>例:</p> <pre>switch(config)# snmp-server enable traps feature-control</pre>	<p>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。</p> <ul style="list-style-type: none"> • FeatureOpStatusChange : 機能操作の状態変化通知を有効にします。
<p>snmp-server enable traps hsrp state-change</p> <p>例:</p> <pre>switch(config)# snmp-server enable traps hsrp</pre>	<p>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。</p> <ul style="list-style-type: none"> • state-change : HSRP の状態変化通知を有効にします。

コマンド	目的
<p>snmp-server enable traps license [notify-license-expiry] [notify-license-expiry-warning] [notify-licensefile-missing] [notify-no-license-for-feature]</p> <p>例:</p> <pre>switch(config)# snmp-server enable traps license</pre>	<p>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。</p> <ul style="list-style-type: none"> • notify-license-expiry : ライセンス失効通知を有効にします。 • notify-license-expiry-warning : ライセンス失効の警告通知を有効にします。 • notify-licensefile-missing : ライセンスファイル不明通知を有効にします。 • notify-no-license-for-feature : no-license-installed-for-feature 通知を有効にします。
<p>snmp-server enable traps link [cieLinkDown] [cieLinkUp] [cmn-mac-move-notification] [IETF-extended-linkDown] [IETF-extended-linkUp] [cisco-extended-linkDown] [cisco-extended-linkUp][linkDown] [linkUp]</p> <p>例:</p> <pre>switch(config)# snmp-server enable traps link</pre>	<p>IF-MIB リンク通知をイネーブルにします。任意で、以下の特定の通知をイネーブルにします。</p> <ul style="list-style-type: none"> • IETF-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。 • IETF-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。 • cmn-mac-move-notification : MACアドレス移動通知をイネーブルにします。 • cisco-extended-linkDown : Internet Engineering Task Force (インターネットエンジニアリングタスクフォース、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。 • cisco-extended-linkUP : Internet Engineering Task Force (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。 • linkDown : IETF リンクステートダウン通知を有効にします。 • linkUp : IETF リンクステートアップ通知を有効にします。

コマンド	目的
<p>snmp-server enable traps ospf [<i>tag</i>] [<i>lsa</i>]</p> <p>例:</p> <pre>switch(config)# snmp-server enable traps ospf</pre>	<p>Open Shortest Path First (OSPF) 通知を有効にします。任意で、次の特定の通知をイネーブルにします。</p> <ul style="list-style-type: none"> • lsa : OSPF リンク ステート アドバタイズメント (LSA) 通知を有効にします。
<p>snmp-server enable traps rf [redundancy-framework]</p> <p>例:</p> <pre>switch(config)# snmp-server enable traps rf</pre>	<p>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。</p> <ul style="list-style-type: none"> • redundancy-framework : RF スーパーバイザ スイッチオーバー MIB 通知を有効にします。
<p>snmp-server enable traps rmon [fallingAlarm] [hcFallingAlarm] [hcRisingAlarm] [risingAlarm]</p> <p>例:</p> <pre>switch(config)# snmp-server enable traps rmon</pre>	<p>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。</p> <ul style="list-style-type: none"> • fallingAlarm : RMON 下限アラーム通知を有効にします。 • hcFallingAlarm : RMON high-capacity 下限アラーム通知を有効にします。 • hcRisingAlarm : RMON high-capacity 上限アラーム通知を有効にします。 • risingAlarm : RMON 上限アラーム通知を有効にします。
<p>snmp-server enable traps snmp [authentication]</p> <p>例:</p> <pre>switch(config)# snmp-server enable traps snmp</pre>	<p>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。</p> <ul style="list-style-type: none"> • authentication : SNMP 認証通知を有効にします。

コマンド	目的
<p>snmp-server enable traps stpx[inconsistency] [loop-inconsistency] [root-inconsistency]</p> <p>例:</p> <pre>switch(config)# snmp-server enable traps stpx</pre>	<p>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。</p> <ul style="list-style-type: none"> • inconsistency : SNMP STPX MIB 不一致アップデート通知を有効にします。 • loop-inconsistency : SNMP STPX MIB ループ不一致アップデート通知を有効にします。 • root-inconsistency : SNMP STPX MIB ルート不一致アップデート通知を有効にします。
<p>snmp-server enable traps syslog [message-generated]</p> <p>例:</p> <pre>switch(config)# snmp-server enable traps syslog</pre>	<p>定義された SNMP ホストに syslog メッセージをトラップとして送信します。任意で、次の特定の通知をイネーブルにします。</p> <ul style="list-style-type: none"> • message-generate : ソフトウェア ログメッセージ生成通知を有効にします。
<p>snmp-server enable traps sysmgr [cseFailSwCoreNotifyExtended]</p> <p>例:</p> <pre>switch(config)# snmp-server enable traps sysmgr</pre>	<p>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。</p> <ul style="list-style-type: none"> • cseFailSwCoreNotifyExtended : ソフトウェア コア通知を有効にします。
<p>snmp-server enable traps upgrade [UpgradeJobStatusNotify] [UpgradeOpNotifyOnCompletion]</p> <p>例:</p> <pre>switch(config)# snmp-server enable traps upgrade</pre>	<p>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。</p> <ul style="list-style-type: none"> • UpgradeJobStatusNotify : アップグレードジョブ ステータス通知を有効にします。 • UpgradeOpNotifyOnCompletion : アップグレードグローバルステータス通知を有効にします。

コマンド	目的
snmp-server enable traps vtp[notifs] [vlancreate] [vlandelete] 例: <pre>switch(config)# snmp-server enable traps vtp</pre>	VTP 通知を有効にします。任意で、次の特定の通知をイネーブルにします。 <ul style="list-style-type: none"> • notifs : VTP 通知を有効にします。 • vlancreate : VLAN 作成の通知を有効にします。 • vlandelete : VLAN 削除の通知を有効にします。
storm-control action traps 例: <pre>switch(config-if)# storm-control action traps</pre>	トラフィック ストーム制御の制限に達した場合のトラフィック ストーム制御通知を有効にします。

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 : <pre>switch# configure terminal switch(config)#</pre>	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 : <pre>switch(config)# interface ethernet 2/2</pre>	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 : <pre>switch(config-if)# no snmp trap link-status</pre>	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	(任意) copy running-config startup-config 例 :	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。

	コマンドまたはアクション	目的
	<code>switch(config-if)# copy running-config startup-config</code>	

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 : <pre>switch# show interface snmp-ifindex grep -i Eth12/1 Eth12/1 441974784 (0x1a580000)</pre>	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有効化

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 : <pre>switch# configure terminal switch(config)#</pre>	グローバル設定モードを開始します。
ステップ 2	snmp-server tcp-session [auth] 例 : <pre>switch(config)# snmp-server tcp-session</pre>	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	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	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 スイッチのコンタクト（連絡先）およびロケーション情報の指定

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。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: 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 Example: 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 Example: 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	(Optional) show snmp Example: switch(config)# show snmp	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	(Optional) copy running-config startup-config Example: switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

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。

Before you begin

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 9000 シリーズ NX-OS ユニキャストルーティング設定ガイド](#)』または『[Cisco Nexus 9000 シリーズ NX-OS マルチキャストルーティング設定ガイド](#)』を参照してください。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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] Example: <pre>switch(config)# snmp-server context public1 vrf red</pre>	<p>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。名前には最大 32 の英数字を使用できます。</p> <p>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。</p> <p>Note 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。インスタンス、vrf、またはトポロジ 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。</p>
ステップ 3	(Optional) snmp-server mib community-map community-name context context-name Example: <pre>switch(config)# snmp-server mib community-map public context public1</pre>	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	(Optional) show snmp context Example: <pre>switch(config)# show snmp context</pre>	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。
ステップ 5	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	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 を無効にできます。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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 : <pre>switch(config)# no snmp-server protocol enable</pre>	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。 (注) SNMPv2 を無効にせずに SNMPv1 を無効にすることはできません。SNMPv1 を無効にする場合は、SNMPv3 のみを設定するか、SNMP を完全に無効にします。

SNMP サーバ カウンタ キャッシュ更新タイマーの管理

Cisco NX-OS がキャッシュ ポートの状態を保持する時間は、秒単位で変更できます。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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 counter cache timeout seconds 例 : <pre>switch(config)# snmp-server counter cache timeout 1200</pre>	ポートの状態がローカル キャッシュに保持される時間を秒単位で定義します。カウンタ キャッシュはデフォルトで有効になっており、デフォルトのキャッシュ タイムアウト値は 10 秒です。無効にすると、デフォルトのキャッシュ タイムアウト値は 50 秒になります。範囲は 1 ~ 3600 です。

	コマンドまたはアクション	目的
		(注) End of Row (EoR) スイッチングの場合、範囲は 10 ~ 3600 です。
ステップ 3	(任意) show running-config snmp all i cac 例： switch(config)# copy running-config snmp all i cac	設定された SNMP サーバカウンタ キャッシュ更新タイムアウト値を表示します。
ステップ 4	no snmp-server counter cache enable 例： switch(config)# no snmp-server counter cache enable	カウンタ キャッシュの更新を無効にします。 (注) カウンタ キャッシュの更新が無効になっている場合、 timeout パラメータに設定された値によって、ポートの状態がカウンタ キャッシュに保持される時間が決まります。

AAA 同期時間の変更

同期したユーザ設定を Cisco NX-OS に維持させる時間の長さを変更できます。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	snmp-server aaa-user cache-timeout seconds 例： switch(config)# snmp-server aaa-user cache-timeout 1200	ローカル キャッシュで AAA 同期ユーザ設定を維持する時間を設定します。値の範囲は 1 ~ 86400 秒です。デフォルトは 3600 です。
ステップ 3	(任意) copy running-config startup-config 例： switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

SNMP ローカル エンジン ID の設定

Cisco NX-OS リリース 7.0(3)I6(1)以降では、ローカルデバイスにエンジン ID を設定できます。



Note SNMP ローカル エンジン ID を設定すると、すべての SNMP ユーザ、V3 ユーザに設定されたホスト、およびコミュニティストリングを再設定する必要があります。Cisco NX-OS リリース 7.0(3)I7(1)以降では、SNMP ユーザとコミュニティストリングのみを再設定する必要があります。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: 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 engineID local engineid-string Example: switch(config)# snmp-server engineID local AA:BB:CC:1A:2C:10	ローカルデバイスの SNMP エンジン ID を変更します。 ローカルエンジン ID は、コロンで指定された 16 進数オクテットのリストとして設定する必要があります。ここでは 10 ~ 64 の範囲の偶数 16 進数文字が使用され、2 つの 16 進数文字ごとにコロンで区切られます。たとえば、80:00:02:b8:04:61:62:63 です。
ステップ 3	show snmp engineID Example: switch(config)# show snmp engineID	設定されている SNMP エンジンの ID を表示します。
ステップ 4	[no] snmp-server engineID local engineid-string Example: switch(config)# no snmp-server engineID local AA:BB:CC:1A:2C:10	ローカルエンジン ID を無効にし、自動生成されたデフォルトのエンジン ID を設定します。
ステップ 5	Required: copy running-config startup-config Example: switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

SNMP の設定の確認

SNMP 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。 9.3(8) リリース以降、show run の SNMPv3 ユーザは、ハッシュではなく SALT 形式で表示されます。
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。 Note snmp-server mib community-map コマンドの SNMP コンテキストの名前が 11 文字を超える場合、 show snmp community コマンドの出力は表形式ではなく垂直形式で表示されます。
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。
show snmp session	SNMP セッションを表示します。

コマンド	目的
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tring 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tring 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

```

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
IP ACL と AAA	『Cisco Nexus 9000 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	シンプル ネットワーク管理プロトコル (SNMPv3) バージョン 3 向けユーザベースセキュリティ モデル (USM)
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/nexus9000/Nexus9000MIBSupportList.html



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。

この章は、次の内容で構成されています。

- [RMON について, on page 215](#)
- [RMON の注意事項と制約事項 \(217 ページ\)](#)
- [RMON のデフォルト設定 \(217 ページ\)](#)
- [RMON の設定 \(218 ページ\)](#)
- [RMON 設定の確認, on page 220](#)
- [RMON の設定例 \(220 ページ\)](#)
- [その他の参考資料 \(221 ページ\)](#)

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で使用し、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 はデフォルトで有効ですが、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。指定されたオブジェクトは、標準のドット付き表記（たとえば、1.3.6.1.2.1.2.2.1.14 は ifInOctets.14 を表します）の既存の SNMP MIB オブジェクトでなければなりません。

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。
- サンプル間隔：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ときの値
- 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ときの値
- 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



Note 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。



Note 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。



Note 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、RMON アラームのみを設定できます。
- 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 cpmCPUCPUTotal5minRev に対応し、.1 は cpmCPUCPUIndex 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	有効
アラーム	未設定
イベント	設定済み (ただし、トリガーされたイベントは何も引き起こしません)

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ります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。

Before you begin

SNMP ユーザーが設定され、SNMP 通知が有効であることを確認します。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: 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] Example:	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。

	Command or Action	Purpose
	<pre>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</pre>	
ステップ 3	<p>rmon hcalarm <i>index mib-object</i> <i>sample-interval {absolute delta}</i> rising-threshold-high <i>value</i> rising-threshold-low <i>value [event-index]</i> falling-threshold-high <i>value</i> falling-threshold-low <i>value [event-index]</i> [owner name] [storagetype type]</p> <p>Example:</p> <pre>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</pre>	<p>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。</p> <p>ストレージタイプの範囲は 1 ~ 5 です。</p>
ステップ 4	<p>(Optional) show rmon {alarms hcalarms}</p> <p>Example:</p> <pre>switch(config)# show rmon alarms</pre>	<p>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。</p>
ステップ 5	<p>(Optional) copy running-config startup-config</p> <p>Example:</p> <pre>switch(config)# copy running-config startup-config</pre>	<p>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。</p>

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。

Before you begin

SNMP ユーザが設定され、SNMP 通知が有効であることを確認します。

Procedure

	Command or Action	Purpose
ステップ 1	<p>configure terminal</p> <p>Example:</p> <pre>switch# configure terminal switch(config)#</pre>	<p>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</p>

	Command or Action	Purpose
ステップ 2	rmon event <i>index</i> [<i>description string</i>] [log] [<i>trap string</i>] [<i>owner name</i>] Example: switch(config)# rmon event 1 trap trap1	RMON イベントを設定します。説明の文字列、トラップの文字列、およびオーナー名は、任意の英数字文字列です。
ステップ 3	(Optional) show rmon events Example: switch(config)# show rmon events	RMON イベントに関する情報を表示します。
ステップ 4	(Optional) copy running-config startup-config Example: switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

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

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/nexus9000/Nexus9000MIBSupportList.html



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。

- [オンライン診断について, on page 223](#)
- [オンライン診断の注意事項と制約事項 \(234 ページ\)](#)
- [オンライン診断のデフォルト設定 \(235 ページ\)](#)
- [オンライン診断の設定 \(236 ページ\)](#)
- [オンライン診断設定の確認, on page 240](#)
- [オンライン診断のコンフィギュレーション例 \(240 ページ\)](#)

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、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マonitoring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マonitoring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、ヘルスマonitoring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。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。

Table 16: ブートアップ診断

診断	説明
OBFL	オンボード障害ロギングフラッシュ (Cisco NX-OS) の整合性を確認します。
BootupPortLoopback	モジュールの起動時にのみ実行されます。スーパーバイザ CPU から ASIC の各物理前面パネルポートへのパケットパスをテストします。
MacSecPortLoopback (Cisco Nexus 9736C-FX および 9736Q-FX ラインカードのみ)	<p>スーパーバイザから ASIC の各物理前面パネルポートへのパケットパス、各ポートの MACSEC 機能、および Cisco Nexus 9736C-FX および 9736Q-FX ラインカードの暗号化機能と復号化機能をテストします。 diagnostic bootup level が complete に設定されている場合、ブート時に MacSecPortLoopback テストが実行されます。</p> <p>MacSecPortLoopback テストは、Cisco Nexus 9736C-FX および 9736Q-FX ラインカードの 36 個の前面ポートのすべてのポートで実行されます。MAC sec ハードウェアは、使用可能な 4 つの暗号スイートアルゴリズム (GCM-AES-128、GCM-AES-256、GCM-AES-XPN-128、および GCM-AES-XPN-256) でテストされます。</p> <p>Note MacSecPortLoopback テストが失敗すると、テストは SYSLOG または OBFL の形式でレポートします。テスト障害が発生すると、ポートがダウンし、show interface CLI 出力に MACsec 障害が表示されます。MACsec テストをスキップするには、diagnostic bootup level を minimal または bypass に設定します。</p>
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
ManagementPortLoopback	中断を伴うテスト、非オンデマンド型テスト。モジュールの管理ポートでループバックをテスト
EOBCPortLoopback	中断を伴うテスト、非オンデマンド型テスト。イーサネット帯域外。

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。

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ヘルス モニタリング診断テストは、中断を伴わず、バックグラウンドで実行されます。ヘルス モニタリングテストはイネーブルまたはディセーブルにできます。また、ランタイムインターバルの変更が可能です。

次の表に、モジュールおよびスーパーバイザのヘルス モニタリング診断とテスト ID を示します。



- (注) モジュールの機能に応じて、テストが存在する場合と存在しない場合があります。モジュールで使用可能なテストのリストは、CLI コマンド、**show diagnostic content module <module>** を使用して確認できます。

表 17:ヘルス モニタリングの無停止での診断

診断	デフォルトのインターバル	デフォルト設定	説明	改善処置
モジュール				
ACT2	30 分	アクティブ	モジュール上のセキュリティ デバイスの整合性を確認します。	GOLD "ACT2" テストに 20 回連続で失敗した場合は、CallHome を実行し、エラーを記録し、その後 HM テストをディセーブルにします。

診断	デフォルト のインター バル	デフォルト 設定	説明	改善処置
ASICRegisterCheck	モジュラ スイッチ： 1分 非モジュラ スイッチ： 20秒、最 小設定のデ フォルト シミュレー ション間隔 は10秒	アクティ ブ	モジュール上の ASIC への読み取 り/書き込みアク セスを検証しま す。	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。
PrimaryBootROM	24 時間 1	アクティ ブ	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。	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。
SecondaryBootROM	24 時間 1	アクティ ブ	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。	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。

診断	デフォルト のインター バル	デフォルト 設定	説明	改善処置
BootupPortLoopback	起動時のみ	起動時のみ：アクティブ	スーパーバイザから前面パネルのポート（および背面）パスが動作しているかどうかを確認します。すべてのフロントポートについて、テストはアクティブスーパーバイザでパケットを生成し、ターゲットポートにパケットを送信し、フロントポート内の内部ループバックを使用して、パケットをアクティブスーパーバイザにリダイレクトします。	GOLD "BootupPortLoopback" テストに1回連続で失敗した場合は、CallHome を実行し、影響があるポートのエラーを無効にして、影響を受けたポートでのエラーテストを記録します。
PortLoopback	30 分	アクティブ	すべての管理ダウンポートでポート単位で診断をチェックします。	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	1分	アクティブ	1 エンジン ASIC デバイスまでのすべてのポートの無停止ループバックの整合性を確認します。	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。

診断	デフォルト のインター バル	デフォルト 設定	説明	改善処置
AsicMemory	起動時のみ	起動時のみ：非アクティブ	ASIC の Mbist ビットを使用して AsicMemory の整合性をチェックします。	GOLD "AsicMemory" テストに失敗した場合には、CallHome を実行し、エラーを記録します。テストの失敗の原因となる問題は一時的なものである可能性があるため、カーネルパニックによるリカバリ リロードを試行します。 (注) テストが失敗したときにカーネルパニックを回避するには、EEM システムポリシーを上書します。
FpgaRegTest	30 秒	ヘルスモニタリングテスト：30 秒ごと：アクティブ	FPGA への読み取り/書き込みによって FPGA のステータスをテストします。	GOLD "FpgaRegTest" テストに 20 回連続で失敗した場合は、CallHome を実行し、エラーを記録し、その後 HM テストをディセーブルにします。テストの失敗の原因となる問題は一時的なものである可能性があるため、カーネルパニックによるリカバリ リロードを試行します。 (注) テストが失敗したときにカーネルパニックを回避するには、EEM システムポリシーを上書します。

診断	デフォルト のインター バル	デフォルト 設定	説明	改善処置
L2ACLRedirect	1分	ヘルスモ ニタリン グ テス ト : 30 分 : アク ティブ	アクティブ ノー ドが動作している かどうかを確認し ます。テストで は、アクティブ ファブリックモ ジュールを介して アクティブスー パーバイザでパ ケットを生成しま す。次に、パケッ トを前面パネルに 送信し、ACL エ ントリを使用し て、パケットをア クティブスー パーバイザにリダ イレクトします。	L2ACLRedirect テストを 10 回連続で失敗した場合は、 CallHome を実行し、エ ラーを記録し、その後 HM テストをディセーブルにし ます。テストの失敗の原因 となる問題は一時的なもの である可能性があるため、 カーネルパニックによるリ カバリ リロードを試行し ます。 (注) テストが失敗し たときにカーネ ルパニックを回 避するには、 EEM システム ポリシーを上書 します。
OBFL	30 分	アクティ ブ	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、デバ イスの利用可能な ストレージをモニ タリングします。	

診断	デフォルト のインター バル	デフォル ト設定	説明	改善処置
FabricConnectivityTest	1分	アクティ ブ	<p>ファブリック/ラ インカードのリン ク ステータスを 確認します。</p> <p>ファブリック リ ンクが機能してい ることを検証しま す。</p> <p>(注) Cisco Nexus 9500-R シリー ズライ ンカー ドでの み使用 できま す。</p>	

診断	デフォルト のインター バル	デフォルト 設定	説明	改善処置
FabricReachabilityTest	1分	アクティ ブ	<p>ファブリック/ライ ンカードの到 達可能性ステータ スを確認します。</p> <p>各ファブリック コンポーネント に、システム内の 他のすべてのファ ブリック コン ポーネントへの有 効なパスがあるこ とを検証します。</p> <p>(注) Cisco Nexus 9500-R シリー ズライ ンカー ドでの み使用 できま す。</p>	
スーパーバイザ (Supervisor)				
バックプレーン	30分	アクティ ブ	バックプレーン SPROM デバイス の整合性を確認し ます。	
NVRAM	5分	アクティ ブ	スーパーバイザの NVRAMブロック の健全性を確認し ます。	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。

診断	デフォルト のインター バル	デフォルト 設定	説明	改善処置
RealTimeClock	5 分	アクティ ブ	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。	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。
PrimaryBootROM	30 分	アクティ ブ	スーパーバイザ上 のプライマリ ブート デバイス の完全性を確認し ます。	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。
SecondaryBootROM	30 分	アクティ ブ	スーパーバイザ上 のセカンダリ ブート デバイス の完全性を確認し ます。	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。
ブートフラッシュ	30 分	アクティ ブ	ブートフラッシュ デバイスへのアク セスを確認しま す。	GOLD "CryptoDevice" テス トに失敗したら、 CallHome を実行し、エ ラーを記録します。
USB	30 分	アクティ ブ	USB デバイスへの アクセスを確認し ます。	Call Home を実行し、 GOLD "USB" テストに失 敗するとエラーを記録し ます。
SystemMgmtBus	30 秒	アクティ ブ	システム管理バス の使用可能性を確 認します。	Call Home 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 テストを無効にし ます。

診断	デフォルト のインター バル	デフォルト 設定	説明	改善処置
MCE	30 分	ヘルスモ ニタリン グ テス ト : 30 分 : アク ティブ	このテストは mcd_dameon を使 用し、カーネルに よって報告された マシンチェック エラーを報告しま す。	GOLD "ACT2" テストに 20 回連続で失敗した場合は、 CallHome を実行し、エ ラーを記録し、その後 HM テストをディセーブルにし ます。
Pcie	起動時のみ	起動時の み : 非ア クティブ	PCIe ステータス レジスタを読み取 り、PCIe デバイ スのエラーを チェックします。	GOLD "Pcie" テストに失敗 したら、CallHome を実行 し、エラーを記録します。
コンソール	起動時のみ	起動時の み : 非ア クティブ	これにより、起動 時に管理ポートで ポートループ バックテストが 実行され、整合性 が確認されます。	GOLD "Cosole" テストに 20 回連続で失敗した場合 は、CallHome を実行し、 エラーを記録し、その後 HM テストをディセーブル にします。
FpgaRegTest	30 秒	ヘルスモ ニタリン グ テス ト : 30 秒 ごと : ア クティブ	FPGA への読み取 り/書き込みに よって FPGA のス テータスをテスト します。	GOLD "FpgaRegTest" テス トに 20 回連続で失敗した 場合は、CallHome を実行 し、エラーを記録し、その 後 HM テストをディセー ブルにします。テストの失 敗の原因となる問題は一時 的なものである可能性がある ため、カーネルパニック によるリカバリ リロード を試行します。 (注) テストが失敗し たときにカーネ ルパニックを回 避するには、 EEM システム ポリシーを上書 します。

¹ 設定可能な最小テスト間隔は 6 時間です。

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、次のような状況が必要です。

- 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ルリングできます。

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。

高可用性

ハイアベイラビリティの重要な機能は、アクティブなネットワークでデバイスが稼働している状態のままハードウェア障害を検出して、対処することです。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。リポ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

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。

- 次の Cisco Nexus プラットフォーム スイッチおよびラインカードは、ランタイム PortLoopback テストをサポートしていませんが、BootupPortLoopback テストをサポートしています。

スイッチ

- Cisco Nexus 92160YC-X
- Cisco Nexus 92304QC
- Cisco Nexus 9264PQ
- Cisco Nexus 9272Q
- Cisco Nexus 9232C

- Cisco Nexus 9236C
- Cisco Nexus 9256PV
- Cisco Nexus 92300YC
- Cisco Nexus 93108TC-EX
- Cisco Nexus 93108TC-EX-24
- Cisco Nexus 93180LC-EX
- Cisco Nexus 93180YC-EX
- Cisco Nexus 93180YC-EXU
- Cisco Nexus 93180YC-EX-24

ラインカード

- Cisco Nexus 9736C-EX
 - Cisco Nexus 97160YC-EX
 - Cisco Nexus 9732C-EX
 - Cisco Nexus 9732C-EXM
- 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。
 - インターフェイス Rx および Tx パケット カウンタは、シャットダウン状態のポートで増えます（およそ 15 分ごとに 4 パケット）。
 - PortLoopback テストは定期的に行われるため、パケット カウンタは管理ダウン ポートで 30 分ごとに追加されます。テストは管理ダウン ポートでのみ実行されます。ポートが閉じられている場合は、カウンタは影響を受けません。
 - ポートごとの BootupPortLoopback テストでポートが失敗すると、ポートは errdisable ステータスになります。（この状態を削除するには、ポートで **shutdown** および **no shutdown** およびコマンドを入力します）。

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	アクティブ

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時診断を設定することも、またはモジュールが短時間で起動するように、すべての起動時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。

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	diagnostic bootup level {complete bypass} 例： switch(config)# diagnostic bootup level complete	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。 <ul style="list-style-type: none"> • 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 : 起動診断テストをまったく実行しません。
ステップ 3	(任意) show diagnostic bootup level 例： switch(config)# show diagnostic bootup level	デバイスに現在設定されている起動診断レベル (bypass または complete) を表示します。

	コマンドまたはアクション	目的
ステップ 4	<p>(任意) copy running-config startup-config</p> <p>例 :</p> <pre>switch(config)# copy running-config startup-config</pre>	<p>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。</p>

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。

手順

	コマンドまたはアクション	目的
ステップ 1	<p>configure terminal</p> <p>例 :</p> <pre>switch# configure terminal switch(config)#</pre>	<p>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</p>
ステップ 2	<p>diagnostic monitor interval module slot test [<i>test-id</i> <i>name</i> all] hour <i>hour</i> min <i>minute</i> second <i>second</i></p> <p>例 :</p> <pre>switch(config)# diagnostic monitor interval module 6 test 3 hour 1 min 0 second 0</pre>	<p>指定されたテストを実行する間隔を設定します。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。</p> <p>引数の範囲は次のとおりです。</p> <ul style="list-style-type: none"> • <i>slot</i> : 範囲は 1 ~ 10 です。 • <i>test-id</i> : 範囲は 1 ~ 14 です。 • <i>name</i> : 32 文字以内の英数字のストリング（大文字と小文字を区別）で指定します。 • <i>hour</i> : 範囲は 0 ~ 23 時間です。 • <i>minute</i> : 範囲は 0 ~ 59 分です。 • <i>second</i> : 範囲は 0 ~ 59 秒
ステップ 3	<p>[no] diagnostic monitor module slot test [<i>test-id</i> <i>name</i> all]</p> <p>例 :</p> <pre>switch(config)# diagnostic monitor interval module 6 test 3</pre>	<p>指定されたテストをアクティブにします。</p> <p>引数の範囲は次のとおりです。</p> <ul style="list-style-type: none"> • <i>slot</i> : 範囲は 1 ~ 10 です。 • <i>test-id</i> : 範囲は 1 ~ 14 です。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • <i>name</i> : 32 文字以内の英数字のストリング（大文字と小文字を区別）で指定します。 <p>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、スケジュール上の間隔ではテストは実行されません。</p>
ステップ 4	（任意） show diagnostic content module <i>{slot all}</i> 例： <pre>switch(config)# show diagnostic content module 6</pre>	診断テストおよび対応する属性の情報を表示します。

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。

手順

	コマンドまたはアクション	目的
ステップ 1	（任意） diagnostic ondemand iteration <i>number</i> 例： <pre>switch# diagnostic ondemand iteration 5</pre>	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	（任意） diagnostic ondemand action-on-failure <i>{continue failure-count num-fails stop}</i> 例： <pre>switch# diagnostic ondemand action-on-failure stop</pre>	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。 <i>num-fails</i> の範囲は 1～999 です。デフォルトは 1 です。
ステップ 3	必須: diagnostic start module <i>slot test</i> [<i>test-id name all non-disruptive</i>] [<i>port port-number all</i>] 例：	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。 <i>test-id</i> の範囲は 1～14 です。テスト名は大文字と小

	コマンドまたはアクション	目的
	<code>switch# diagnostic start module 6 test all</code>	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	<p>必須: diagnostic stop module slot test [<i>test-id</i> <i>name</i> all]</p> <p>例 :</p> <pre>switch# diagnostic stop module 6 test all</pre>	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。 <i>test-id</i> 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	<p>(任意) show diagnostic status module slot</p> <p>例 :</p> <pre>switch# show diagnostic status module 6</pre>	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。

診断結果のシミュレーション

診断テスト結果のシミュレーションが可能です。

手順

	コマンドまたはアクション	目的
ステップ 1	<p>diagnostic test simulation module slot test <i>test-id</i> {fail random-fail success} [port number all]</p> <p>例 :</p> <pre>switch# diagnostic test simulation module 2 test 2 fail</pre>	テスト結果のシミュレーションを行います。 <i>test-id</i> の範囲は 1 ~ 14 です。ポート範囲は 1 ~ 48 です。

診断結果の消去

診断テスト結果を消去できます。

手順

	コマンドまたはアクション	目的
ステップ 1	<p>diagnostic clear result module [<i>slot</i> all] test {<i>test-id</i> all}</p> <p>例 :</p> <pre>switch# diagnostic clear result module 2 test all</pre>	<p>指定されたテストのテスト結果を消去します。</p> <p>引数の範囲は次のとおりです。</p> <ul style="list-style-type: none"> • <i>slot</i> : 範囲は 1 ~ 10 です。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • <i>test-id</i> : 範囲は 1 ~ 14 です。
ステップ 2	diagnostic test simulation module slot test <i>test-id clear</i> 例 : <pre>switch# diagnostic test simulation module 2 test 2 clear</pre>	シミュレーションしたテスト結果を消去します。 <i>test-id</i> の範囲は 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 [<i>test-name</i> all]	診断テストの説明を表示します。
show diagnostic events [error info]	診断イベントをエラーおよび情報イベントタイプ別に表示します。
show diagnostic ondemand setting	オンデマンド診断に関する情報を表示します。
show diagnostic result module slot [test [<i>test-name</i> 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 hardware capacity [eobe 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
```




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。

- [EEM について \(243 ページ\)](#)
- [EEM の前提条件 \(248 ページ\)](#)
- [EEM の注意事項と制約事項 \(248 ページ\)](#)
- [EEM のデフォルト設定 \(249 ページ\)](#)
- [EEM の設定 \(250 ページ\)](#)
- [EEM の設定確認 \(265 ページ\)](#)
- [EEM の設定例 \(266 ページ\)](#)
- [イベント ログの自動収集とバックアップ \(267 ページ\)](#)

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。

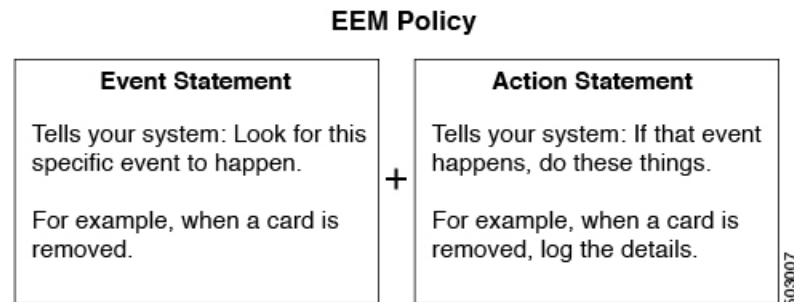
- イベント文：別の Cisco NX-OS コンポーネントからモニタし、アクション、回避策、または通知が必要になる可能性のあるイベント。
- アクション文：CLI コマンドの実行、Smart Call Home 機能を使用した電子メールの送信、インターフェイスの無効化など、イベントから回復するために EEM が実行できるアクション。
- ポリシー：イベントのトラブルシューティングまたはイベントからの回復を目的とした 1 つまたは複数のアクションとペアになったイベント。

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 3: 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。

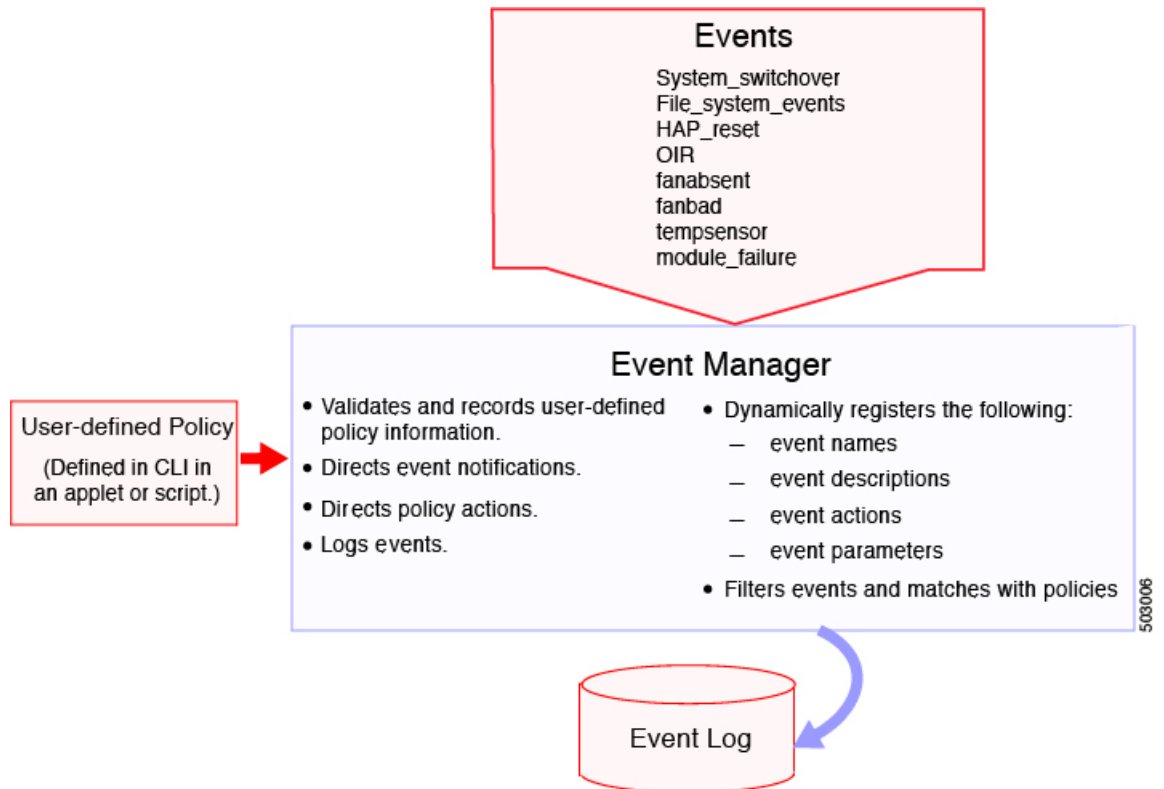
イベント文

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 4: 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。

アクション文

アクション文では、ポリシーによって実行されるアクションを記述します。各ポリシーに複数のアクション文を設定できます。ポリシーにアクションを関連付けなかった場合、EEM はイベント観察を続けますが、アクションは実行されません。

EEM がアクション文でサポートするアクションは、次のとおりです。

- CLI コマンドの実行。
- カウンタのアップデート。
- 例外の記録。
- モジュールの強制的シャットダウン
- デバイスをリロードします。
- 電力のバジェット超過による特定モジュールのシャットダウン。
- Syslog メッセージの生成。
- Call Home イベントの生成。
- SNMP 通知の生成。
- システム ポリシー用デフォルトアクションの使用。



(注) EEM は、合計 1024 文字までの、完全なアクション CLI リストのみを処理できます。さらにアクションが必要な場合は、同じトリガーを持つ新しい冗長アプレットとして定義する必要があります。



(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、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 ポリシーの作成後、そのポリシーをデバイスにコピーしてアクティブにします。

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 イベント関連

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。

高可用性

Cisco NX-OS は、EEM のステートレス リスタートをサポートします。リブートまたはスーパーバイザ スイッチオーバーの後、Cisco NX-OS は実行コンフィギュレーションを適用します。

仮想化のサポート

アクションまたはイベントがすべて表示されるわけではありません。ポリシーを設定するには、`network-admin` の権限が必要です。

EEM の前提条件

EEM の前提条件は、次のとおりです。

- EEM を設定するには、`network-admin` のユーザ権限が必要です。

EEM の注意事項と制約事項

EEM 設定時の注意事項と制約事項は次のとおりです。

- 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には、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 ログの自動収集とバックアップには、次の注意事項があります。
 - デフォルトでは、スイッチのログ収集を有効にすると、サイズ、規模、コンポーネントのアクティビティに応じて、15分から数時間のイベントログが利用できるようになります。
 - 長期間にわたる関連ログを収集できるようにするには、必要な特定のサービス/機能に対してのみイベントログの保持を有効にします。「単一サービスの拡張ログファイル保持の有効化」を参照してください。内部イベントログをエクスポートすることもできます。「外部ログ ファイルストレージ」を参照してください。
 - トラブルシューティングを行うときは、内部イベントログのスナップショットを手動によりリアルタイムで収集することをお勧めします。「最近のログファイルのローカルコピーの生成」を参照してください。
- `show tech` コマンドを収集するように EEM ポリシーアクションを設定する場合は、同じアクションが再度呼び出される前に、`show tech` コマンドが完了するのに十分な時間を割り当ててください。
- オーバーライドポリシーについては、次の点に注意してください。

- イベント文が指定されていても、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。
- 正規コマンド式には、次のルールが適用されます。
 - すべての正規表現は、Portable Operating System Interface for uniX (POSIX) 拡張標準に準拠している必要があります。
 - すべてのキーワードを展開する必要があります。
 - 引数の置換には * 記号のみを使用できます。
- EEM イベント関連については、次の点に注意してください。
 - EEM イベント関連はスーパーバイザ モジュールだけでサポートされます。
 - EEM イベント関連は、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 イベント関連は 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。
 - EEM イベント関連はシステムのデフォルト ポリシーを上書きしません。
- 複数のイベント文が EEM ポリシーに存在する場合は、各イベント文に **tag** キーワードと一意な tag 引数が必要です。
- デフォルトアクション実行は、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 9000 シリーズ NX-OS プログラマビリティ ガイド](#)』を参照してください。

EEM のデフォルト設定

この表では、EEM のデフォルト設定を一覧にしています。

パラメータ	デフォルト
システム ポリシー	アクティブ

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： <pre>switch# configure terminal switch(config)#</pre>	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 <i>variable-name</i> <i>variable-value</i> 例： <pre>switch(config)# event manager environment emailto "admin@anyplace.com"</pre>	EEM 用の環境変数を作成します。 <i>variable-name</i> 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。 <i>variable-value</i> 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	(任意) show event manager environment { <i>variable-name</i> all } 例： <pre>switch(config)# show event manager environment all</pre>	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	(任意) copy running-config startup-config 例： <pre>switch(config)# copy running-config startup-config</pre>	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 <i>applet-name</i> 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。 <i>applet-name</i> 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	(任意) description <i>policy-description</i> 例： switch(config-applet)# description "Monitors interface shutdown."	ポリシーの説明になるストリングを設定します。 <i>string</i> 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 <i>event-statement</i> 例： switch(config-applet)# event cli match "conf t ; interface * ; 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 (252 ページ) 」を参照してください。
ステップ 5	(任意) tag <i>tag</i> {and andnot or} <i>tag</i> [and andnot or {<i>tag</i>}] {happens occurs in seconds} 例： switch(config-applet)# tag one or two happens 1 in 10000	ポリシー内の複数のイベントを相互に関連付けます。 <i>occurs</i> 引数の範囲は 1 ~ 4294967295 です。 <i>seconds</i> 引数の範囲は 0 ~ 4294967295 秒です。
ステップ 6	action <i>number</i> [<i>number2</i>] <i>action-statement</i> 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 (258 ページ) 」を参照してください。
ステップ 7	(任意) show event manager policy-state <i>name</i> [<i>module module-id</i>] 例： switch(config-applet)# show event manager policy-state monitorShutdown	設定したポリシーの状態に関する情報を表示します。
ステップ 8	(任意) copy running-config startup-config 例：	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。

コマンドまたはアクション	目的
switch(config)# copy running-config startup-config	

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
<p>event application [<i>tag tag</i>] sub-system <i>sub-system-id</i> type <i>event-type</i></p> <p>例:</p> <pre>switch(config-applet)# event application sub-system 798 type 1</pre>	<p>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。</p> <p><i>sub-system-id</i> と <i>event-type</i> の範囲は 1 ~ 4294967295 です。</p> <p>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。</p> <p>(注) このコマンドを使用するには、まず feature evmed コマンドを有効にして一般的なイベントディテクタを有効にする必要があります。</p>
<p>event cli [<i>tag tag</i>] match <i>expression</i> [<i>count repeats</i> <i>time seconds</i>]</p> <p>例:</p> <pre>switch(config-applet)# event cli match "conf t ; interface * ; shutdown"</pre>	<p>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。</p> <p>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。</p> <p><i>repeats</i> の範囲は 1 ~ 65000 です。<i>time</i> の範囲は 0 ~ 4294967295 秒です。0 は無制限を示します。</p>

コマンド	目的
<p>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}]</p> <p>例:</p> <pre>switch(config-applet)# event counter name mycounter entry-val 20 gt</pre>	<p>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。</p> <p>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。</p> <p>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。</p>
<p>event fanabsent [fan number] time seconds</p> <p>例:</p> <pre>switch(config-applet)# event fanabsent time 300</pre>	<p>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。 seconds の範囲は 10 ~ 64000 です。</p>
<p>event fanbad [fan number] time seconds</p> <p>例:</p> <pre>switch(config-applet)# event fanbad time 3000</pre>	<p>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。 seconds の範囲は 10 ~ 64000 です。</p>
<p>event fib {adjacency extra resource tcam usage route {extra inconsistent missing}}</p> <p>例:</p> <pre>switch(config-applet)# event fib adjacency extra</pre>	<p>次のいずれかに対するイベントを発生させます。</p> <ul style="list-style-type: none"> • 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。
<p>event gold module {slot all} test test-name [severity {major minor moderate}] testing-type {bootup monitoring ondemand scheduled} consecutive-failure count</p> <p>例:</p> <pre>switch(config-applet)# event gold module 2 test ASICRegisterCheck testing-type ondemand consecutive-failure 2</pre>	<p>名前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。 slot の範囲は 1 ~ 10 です。 test-name は設定されたオンライン診断テストの名前です。 count の範囲は 1 ~ 1000 です。</p>

コマンド	目的
<p>event interface [<i>tag tag</i>] {<i>name interface slot/port parameter</i>}</p> <p>例:</p> <pre>switch(config-applet)# event interface ethernet 2/2 parameter</pre>	<p>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。</p> <p>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。</p> <p>(注) このコマンドを使用するには、まず feature evmed コマンドを有効にして一般的なイベントディテクタを有効にする必要があります。</p>
<p>event memory {<i>critical minor severe</i>}</p> <p>例:</p> <pre>switch(config-applet)# event memory critical</pre>	<p>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 (262 ページ) も参照してください。</p>
<p>event module [<i>tag tag</i>] status {<i>online offline any</i>} module {<i>all module-num</i>}</p> <p>例:</p> <pre>switch(config-applet)# event module status offline module all</pre>	<p>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。</p> <p>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。</p>
<p>event module-failure [<i>tag tag</i>] type <i>failure-type module</i> {<i>slot all</i>} count <i>repeats</i> [<i>time seconds</i>]</p> <p>例:</p> <pre>switch(config-applet)# event module-failure type lc-failed module 3 count 1</pre>	<p>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。</p> <p>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。</p> <p><i>repeats</i> 範囲は 0 ~ 4294967295 です。<i>seconds</i> の範囲は 0 ~ 4294967295 秒です。0 は無制限を示します。</p>
<p>event none</p> <p>例:</p> <pre>switch(config-applet)# event none</pre>	<p>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。</p> <p>(注) このコマンドを使用するには、まず feature evmed コマンドを有効にして一般的なイベントディテクタを有効にする必要があります。</p>

コマンド	目的
<p>event oir [tag tag] {fan module powersupply} {anyoir insert remove} [<i>number</i>]</p> <p>例:</p> <pre>switch(config-applet)# event oir fan remove 4</pre>	<p>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。</p> <p>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。</p> <p>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。 <i>number</i> の範囲は次のとおりです。</p> <ul style="list-style-type: none"> • 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
<p>event policy-default count <i>repeats</i> [time seconds]</p> <p>例:</p> <pre>switch(config-applet)# event policy-default count 3</pre>	<p>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。</p> <p><i>repeats</i> の範囲は 1～65000 です。<i>seconds</i> の範囲は 0～4294967295 秒です。0 は無制限を示します。</p>
<p>event poweroverbudget</p> <p>例:</p> <pre>switch(config-applet)# event poweroverbudget</pre>	<p>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。</p>

コマンド	目的
<p>event snmp [<i>tag tag</i>] oid <i>oid</i> get-type {<i>exact</i> <i>next</i>} entry-op {<i>eq</i> <i>ge</i> <i>gt</i> <i>le</i> <i>lt</i> <i>ne</i>} entry-val <i>entry</i> [exit-comb {<i>and</i> <i>or</i>}] exit-op {<i>eq</i> <i>ge</i> <i>gt</i> <i>le</i> <i>lt</i> <i>ne</i>} exit-val <i>exit</i> exit-time <i>time</i> polling-interval <i>interval</i></p> <p>例:</p> <pre>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</pre>	<p>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。</p> <p>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。</p> <p><i>entry</i> および <i>exit</i> の値の範囲は 0 ~ 18446744073709551615 です。 <i>time</i> の範囲は 0 ~ 2147483647 秒です。 <i>interval</i> の範囲は 1 ~ 2147483647 秒です。</p>
<p>event storm-control</p> <p>例:</p> <pre>switch(config-applet)# event storm-control</pre>	<p>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。</p>
<p>event syslog [occurs <i>count</i>] [pattern <i>string</i> period <i>time</i> priority <i>level</i> tag <i>tag</i>]</p> <p>例:</p> <pre>switch(config-applet)# event syslog period 500</pre>	<p>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。</p> <p>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。</p>
<p>event sysmgr memory [module <i>module-num</i>] major <i>major-percent</i> minor <i>minor-percent</i> clear <i>clear-percent</i></p> <p>例:</p> <pre>switch(config-applet)# event sysmgr memory minor 80</pre>	<p>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。</p>
<p>event sysmgr switchover count <i>count</i> time <i>interval</i></p> <p>例:</p> <pre>switch(config-applet)# event sysmgr switchover count 10 time 1000</pre>	<p>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。</p>

コマンド	目的
<p>event temperature [module slot] [sensor-number] threshold {any major minor}</p> <p>例:</p> <pre>switch(config-applet)# event temperature module 2 threshold any</pre>	<p>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。</p>
<p>event timer {absolute time time name name countdown time time name name cron cronentry string tag tag watchdog time time name name}</p> <p>例:</p> <pre>switch(config-applet)# event timer absolute time 100 name abtimer</pre>	<p>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。</p> <ul style="list-style-type: none"> • 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。 <p>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。</p> <p>(注) このコマンドを使用するには、まず feature evmed コマンドを有効にして一般的なイベントディテクタを有効にする必要があります。</p>
<p>event track [tag tag] object-number state {any down up}</p> <p>例:</p> <pre>switch(config-applet)# event track 1 state down</pre>	<p>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。</p> <p>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。</p> <p>指定できる object-number の範囲は 1 ~ 500 です。</p>

アクション文の設定

アクション文を設定するには、EEM コンフィギュレーション モードで次のいずれかのコマンドを使用します。

コマンド	目的
<p>action <i>number</i>[.<i>number2</i>] cli <i>command1</i> [<i>command2</i>...] [local]</p> <p>例:</p> <pre>switch(config-applet)# action 1.0 cli "show interface e 3/1"</pre>	<p>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 <i>number1.number2</i> です。</p> <p><i>number</i> は 16 桁までの任意の数値にできます。<i>number2</i> の範囲は 0 ~ 9 です。</p>
<p>action <i>number</i>[.<i>number2</i>] counter <i>name</i> <i>counter value val op</i> {dec inc nop set}</p> <p>例:</p> <pre>switch(config-applet)# action 2.0 counter name mycounter value 20 op inc</pre>	<p>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 <i>number1.number2</i> です。</p> <p><i>number</i> は 16 桁までの任意の数値にできます。<i>number2</i> の範囲は 0 ~ 9 です。</p> <p><i>counter name</i> 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。<i>val</i> には 0 ~ 2147483647 の整数または置換パラメータを指定できます。</p>
<p>action <i>number</i>[.<i>number2</i>] event-default</p> <p>例:</p> <pre>switch(config-applet)# action 1.0 event-default</pre>	<p>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 <i>number1.number2</i> です。</p> <p><i>number</i> は 16 桁までの任意の数値にできます。<i>number2</i> の範囲は 0 ~ 9 です。</p>
<p>action <i>number</i>[.<i>number2</i>] forceshut [module slot xbar xbar-number] reset-reason <i>seconds</i></p> <p>例:</p> <pre>switch(config-applet)# action 1.0 forceshut module 2 reset-reason "flapping links"</pre>	<p>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 <i>number1.number2</i> です。</p> <p><i>number</i> は 16 桁までの任意の数値にできます。<i>number2</i> の範囲は 0 ~ 9 です。</p> <p>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。</p>
<p>action <i>number</i>[.<i>number2</i>] overbudgetshut [module slot[-<i>slot</i>]]</p> <p>例:</p> <pre>switch(config-applet)# action 1.0 overbudgetshut module 3-5</pre>	<p>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。</p> <p><i>number</i> は 16 桁までの任意の数値にできます。<i>number2</i> の範囲は 0 ~ 9 です。</p>

コマンド	目的
action number[.number2] policy-default 例: <pre>switch(config-applet)# action 1.0 policy-default</pre>	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 <code>number1.number2</code> です。 <i>number</i> は 16 桁までの任意の数値にできます。 <i>number2</i> の範囲は 0 ~ 9 です。
action number[.number2] publish-event 例: <pre>switch(config-applet)# action 1.0 publish-event</pre>	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 <code>number1.number2</code> です。 <i>number</i> は 16 桁までの任意の数値にできます。 <i>number2</i> の範囲は 0 ~ 9 です。
action number[.number2] reload [module slot[-slot]] 例: <pre>switch(config-applet)# action 1.0 reload module 3-5</pre>	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。 <i>number</i> は 16 桁までの任意の数値にできます。 <i>number2</i> の範囲は 0 ~ 9 です。
action number[.number2] snmp-trap {[intdata1 data [intdata2 data]] [strdata string]} 例: <pre>switch(config-applet)# action 1.0 snmp-trap strdata "temperature problem"</pre>	設定されたデータとともに SNMP トラップを送信します。 <i>number</i> には、最大 16 桁の任意の数値を指定できます。 <i>number2</i> の範囲は 0 ~ 9 です。 <i>data</i> 引数には、最大 80 桁の任意の数を指定できます。 <i>string</i> には最大 80 文字の英数字を使用できます。
action number[.number2] syslog [priority prio-val] msg error-message 例: <pre>switch(config-applet)# action 1.0 syslog priority notifications msg "cpu high"</pre>	設定されている優先度で、カスタマイズされた Syslog メッセージが送信されます。数値は 16 桁までの任意の数値にできます。 <i>number2</i> の範囲は 0 ~ 9 です。 <i>error-message</i> 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。



- (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 manager bypass** コマンドを使用して、CLI でのすべての EEM ポリシーを、CLI コマンドの実行と一致させることができます。

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。

始める前に

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： <pre>switch# configure terminal switch(config)#</pre>	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 <i>policy-script</i> 例： <pre>switch(config)# event manager policy moduleScript</pre>	EEM スクリプト ポリシーを登録してアクティブにします。 <i>policy-script</i> 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	(任意) copy running-config startup-config 例： <pre>switch(config)# copy running-config startup-config</pre>	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	(任意) 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	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 イベントおよび設定例 (495 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。 <i>applet-name</i> 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。 <i>system-policy</i> は、システムポリシーの1つにする必要があります。
ステップ 4	(任意) description policy-description 例： description "Overrides link flap policy."	ポリシーの説明になるストリングを設定します。 <i>string</i> 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	必須: 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	必須: 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	(任意) show event manager policy-state name 例： switch(config-applet)# show event manager policy-state ethport	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	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	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。

始める前に

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 : <pre>switch# configure terminal switch(config)#</pre>	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 : <pre>switch(config)# system memory-thresholds minor 60 severe 70 critical 80</pre>	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。 <ul style="list-style-type: none"> • マイナー - 85 • 深刻 - 90 • 重大 - 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。 <ul style="list-style-type: none"> • 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
		<ul style="list-style-type: none"> • 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	(任意) system memory-thresholds threshold critical no-process-kill 例 : <pre>switch(config)# system memory-thresholds threshold critical no-process-kill</pre>	メモリを割り当てられない場合もプロセスを終了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	(任意) show running-config include "system memory" 例 : <pre>switch(config-applet)# show running-config include "system memory"</pre>	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	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	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。

始める前に

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 : <pre>switch# configure terminal switch(config)#</pre>	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 <i>applet-name</i> 例 : <pre>switch(config)# event manager applet abc switch(config-applet)#</pre>	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 [<i>tag tag</i>] {<i>occurs number</i> <i>period seconds</i> <i>pattern msg-text</i> <i>priority priority</i>} 例 : <pre>switch(config-applet)# event syslog occurs 10</pre>	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。 <ul style="list-style-type: none"> • tag <i>tag</i> 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 <i>number</i> 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 <i>seconds</i> のキーワードと引数のペアは、発生回数を指定します。値の範囲は 1 ~ 4294967295 です。 • pattern <i>msg-text</i> のキーワードと引数のペアは、マッチさせ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 <i>priority</i> 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

	コマンドまたはアクション	目的
		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。
ステップ 4	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	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 の設定確認

EEM 設定情報を表示するには、次のいずれかの作業を実行します。

コマンド	目的
show event manager environment [<i>variable-name</i> 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 [<i>event</i> all <i>module slot</i>]	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] [<i>maximum num-events</i>] [<i>severity</i> { 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-state <i>policy-name</i>	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 [<i>policy-name</i> all]	スクリプト ポリシーに関する情報を表示します。
show event manager system-policy [all]	定義済みシステム ポリシーに関する情報を表示します。
show running-config eem	EEM の実行コンフィギュレーションに関する情報を表示します。
show startup-config eem	EEM のスタートアップコンフィギュレーションに関する情報を表示します。

EEM の設定例

モジュール 3 の中断のないアップグレードエラーのしきい値だけを変更することによって、`__lcm_module_failure` システムポリシーを上書きする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
```

最大障害しきい値に達すると、AsicMemory、FpgaRegTest、および L2ACLRedirect システムポリシーによってスイッチのリロードが強制されます。次に、これらのポリシーのいずれかのデフォルトアクションを上書きし、代わりに syslog を発行する例を示します。

```
event manager applet gold override __fpgareg
action 1 syslog priority emergencies msg FpgaRegTest_override
```

次に、デフォルト ポリシーを上書きし、デフォルト アクションを実行する例を示します。

```
event manager applet gold_fpga_ovrd override __fpgareg
  action 1 policy-default
  action 2 syslog priority emergencies msg FpgaRegTest_override
```



(注) その他の設定例については、「[Embedded Event Manager システム イベントおよび設定例 \(495 ページ\)](#)」を参照してください。

イベント ログの自動収集とバックアップ

自動的に収集されたイベントログは、スイッチのメモリにローカルに保存されます。イベント ログ ファイル ストレージは、一定期間ファイルを保存する一時バッファです。時間が経過すると、バッファのロールオーバーによって次のファイルのためのスペースが確保されます。ロールオーバーでは、先入れ先出し方式が使用されます。

Cisco NX-OS リリース 9.3(3)以降、EEM は以下の収集およびバックアップ方法を使用します。

- 拡張ログ ファイルの保持
- トリガーベースのイベント ログの自動収集

拡張ログ ファイルの保持

Cisco NX-OS リリース 9.3 (3) 以降、すべての Cisco Nexus プラットフォーム スイッチは、少なくとも 8 GB のシステムメモリを備え、イベント ロギング ファイルの拡張保持をサポートします。ログ ファイルをスイッチにローカルに保存するか、外部コンテナを介してリモートに保存すると、ロールオーバーによるイベント ログの損失を削減できます。

すべてのサービスの拡張ログ ファイル保持のイネーブル化

拡張ログファイル保持は、スイッチで実行されているすべてのサービスに対してデフォルトで有効になっています。スイッチでログファイル保持機能がイネーブルになっていない場合 (**no bloggerd log-dump** が設定されている場合)、次の手順を使用してイネーブルにします。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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

すべてのサービスの拡張ログ ファイル保持の無効化

	コマンドまたはアクション	目的
ステップ 2	bloggerd log-dump all 例： switch(config)# bloggerd log-dump all switch(config)#	すべてのサービスのログ ファイル保持機能をイネーブルにします。

例

```
switch# configure terminal
switch(config)# bloggerd log-dump all
Sending Enable Request to Bloggerd
Bloggerd Log Dump Successfully enabled
switch(config)#
```

すべてのサービスの拡張ログ ファイル保持の無効化

拡張ログファイル保持は、スイッチ上のすべてのサービスに対してデフォルトで有効になっています。スイッチのログファイル保持機能がすべてのサービスに対して有効になっている場合は、次の手順を実行します。

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 bloggerd log-dump all 例： switch(config)# no bloggerd log-dump all switch(config)#	スイッチ上のすべてのサービスのログ ファイル保持機能を無効にします。

例

```
switch# configure terminal
switch(config)# no bloggerd log-dump all
Sending Disable Request to Bloggerd
Bloggerd Log Dump Successfully disabled
switch(config)#
```

単一サービスの拡張ログファイル保持の有効化

拡張ログファイル保持は、スイッチで実行されているすべてのサービスに対してデフォルトで有効になっています。スイッチで (**no bloggerd log-dump**が設定されていて) ログ ファイル保

持機能が有効になっていない場合、次の手順を使用して単一のサービスに対して有効にします。

手順

	コマンドまたはアクション	目的
ステップ 1	show system internal sysmgr service name <i>service-type</i> 例 : <pre>switch# show system internal sysmgr service name aclmgr</pre>	サービス SAP 番号を含む ACL Manager に関する情報を表示します。
ステップ 2	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	bloggerd log-dump sap number 例 : <pre>switch(config)# bloggerd log-dump sap 351</pre>	ACL Manager サービスのログ ファイル 保持機能をイネーブルにします。
ステップ 4	show system internal bloggerd info log-dump-info 例 : <pre>switch(config)# show system internal bloggerd info log-dump-info</pre>	スイッチ上のログ ファイル保持機能に関する情報を表示します。

例

```
switch# show system internal sysmgr service name aclmgr
Service "aclmgr" ("aclmgr", 80):
  UUID = 0x182, PID = 653, SAP = 351
  State: SRV_STATE_HANDSHAKED (entered at time Mon Nov  4 11:10:41 2019).
  Restart count: 1
  Time of last restart: Mon Nov  4 11:10:39 2019.
  The service never crashed since the last reboot.
  Tag = N/A
  Plugin ID: 0
switch(config)# configure terminal
switch(config)# bloggerd log-dump sap 351
Sending Enable Request to Bloggerd
Bloggerd Log Dump Successfully enabled
switch(config)# show system internal bloggerd info log-dump-info
-----
Log Dump config is READY
Log Dump is DISABLED for ALL application services in the switch
Exceptions to the above rule (if any) are as follows:
-----
Module      | VDC      | SAP      | Enabled?
-----
```

```

1          | 1          | 351 (MTS_SAP_ACLMGR      ) | Enabled
-----
Log Dump Throttle Switch-Wide Config:
-----
Log Dump Throttle                               : ENABLED
Minimum buffer rollover count (before throttling) : 5
Maximum allowed rollover count per minute       : 1
-----

switch(config)#

```

拡張ログ ファイルの表示

スイッチに現在保存されているイベント ログ ファイルを表示するには、次の作業を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	dir debug:log-dump/ 例： switch# dir debug:log-dump/	スイッチに現在保存されているイベント ログ ファイルを表示します。

例

```

switch# dir debug:log-dump/

3676160 Dec 05 02:43:01 2019 20191205023755_evtlog_archive.tar
3553280 Dec 05 06:05:06 2019 20191205060005_evtlog_archive.tar

Usage for debug://sup-local
913408 bytes used
4329472 bytes free
5242880 bytes total

```

単一サービスに対する拡張ログファイル保持の無効化

拡張ログファイル保持は、スイッチ上のすべてのサービスに対してデフォルトで有効になっています。スイッチで単一またはすべてのサービス（Cisco NX-OSリリース9.3(5)ではデフォルト）に対してログファイル保持機能が有効になっている場合に、特定のサービスを無効にするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	show system internal sysmgr service name <i>service-type</i> 例：	サービス SA P番号を含む ACL Manager 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
	switch# show system internal sysmgr service name aclmgr	
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 bloggerd log-dump sap number 例 : switch(config)# no bloggerd log-dump sap 351	ACL Manager サービスのログ ファイル 保持機能を無効にします。
ステップ 4	show system internal bloggerd info log-dump-info 例 : switch(config)# show system internal bloggerd info log-dump-info	スイッチ上のログ ファイル保持機能に 関する情報を表示します。

例

次に、「aclmgr」という名前のサービスの拡張ログ ファイル保持を無効にする例を示 します。

```
switch# show system internal sysmgr service name aclmgr
Service "aclmgr" ("aclmgr", 80):
  UUID = 0x182, PID = 653, SAP = 351
  State: SRV_STATE_HANDSHAKED (entered at time Mon Nov  4 11:10:41 2019).
  Restart count: 1
  Time of last restart: Mon Nov  4 11:10:39 2019.
  The service never crashed since the last reboot.
  Tag = N/A
  Plugin ID: 0
switch(config)# configure terminal
switch(config)# no bloggerd log-dump sap 351
Sending Disable Request to Bloggerd
Bloggerd Log Dump Successfully disabled
switch(config)# show system internal bloggerd info log-dump-info
-----
Log Dump config is READY
Log Dump is DISABLED for ALL application services in the switch
Exceptions to the above rule (if any) are as follows:
-----
Module      | VDC      | SAP              | Enabled?
-----
1           | 1        | 351 (MTS_SAP_ACLMGR) | Disabled
-----
Log Dump Throttle Switch-Wide Config:
-----
Log Dump Throttle                               : ENABLED
Minimum buffer rollover count (before throttling) : 5
Maximum allowed rollover count per minute         : 1
```

```
switch(config)#
```

トリガーベースのイベント ログの自動収集

トリガーベースのログ収集機能：

- 問題発生時に関連データを自動的に収集します。
- コントロールプレーンへの影響なし
- カスタマイズ可能な設定ですか：
 - シスコが入力するデフォルト
 - 収集対象は、ネットワーク管理者または Cisco TACによって、選択的に上書きされません。
 - イメージのアップグレード時は新しいトリガーを自動的に更新します。
- ログをスイッチにローカルに保存するか、外部サーバにリモートで保存します。
- 重大度 0、1、および 2 の syslog をサポートします：
- アドホック イベントのカスタム syslog (syslog と接続する自動収集コマンド)

トリガーベースのログ ファイルの自動収集の有効化

ログ ファイルのトリガーベースの自動作成を有効にするには、`__syslog_trigger_default` システム ポリシーのオーバーライドポリシーをカスタム YAML ファイルで作成し、情報を収集する特定のログを定義する必要があります。

ログ ファイルの自動収集を有効にするカスタム YAML ファイルの作成の詳細については、[自動収集 YAML ファイルの設定 \(273 ページ\)](#) を参照してください。

自動収集 YAML ファイル

EEM 機能の **action** コマンドで指定される自動収集 YAML ファイルは、さまざまなシステムまたは機能コンポーネントのアクションを定義します。このファイルは、スイッチ ディレクトリ `/bootflash/scripts` にあります。デフォルトの YAML ファイルに加えて、コンポーネント固有の YAML ファイルを作成し、同じディレクトリに配置できます。コンポーネント固有の YAML ファイルの命名規則は **component-name.yaml** です。コンポーネント固有のファイルが同じディレクトリに存在する場合は、**action** コマンドで指定されたファイルよりも優先されます。たとえば、アクションファイル **bootflash/scripts/platform.yaml** がデフォルトのアクションファイル `/bootflash/scripts` とともに **bootflash/scripts/test.yaml** ディレクトリにある場合、**platform.yaml** ファイルで定義された命令がデフォルトの **test.yaml** ファイルに存在するプラットフォーム コンポーネントの手順よりも優先します。

コンポーネントの例としては、ARP、BGP、IS-ISなどがあります。すべてのコンポーネント名に精通していない場合は、シスコカスタマーサポートに連絡して、コンポーネント固有のアクション（およびデフォルトの **test.yaml** ファイル）の YAML ファイルを定義してください。

例：

```
event manager applet test_1 override __syslog_trigger_default
  action 1.0 collect test.yaml $_syslog_msg
```

自動収集 YAML ファイルの設定

YAML ファイルの内容によって、トリガーベースの自動収集時に収集されるデータが決まります。スイッチには YAML ファイルが 1 つだけ存在しますが、任意の数のスイッチ コンポーネントとメッセージの自動収集メタデータを含めることができます。

スイッチの次のディレクトリで YAML ファイルを見つけます。

```
/bootflash/scripts
```

次の例を使用して、トリガーベース収集の YAML ファイルを呼び出します。この例は、ユーザ定義の YAML ファイルを使用してトリガーベース収集を実行するために最低限必要な設定を示しています。

```
switch# show running-config eem
!Command: show running-config eem
!Running configuration last done at: Mon Sep 30 19:34:54 2019
!Time: Mon Sep 30 22:24:55 2019
version 9.3(3) Bios:version 07.59
event manager applet test_1 override __syslog_trigger_default
  action 1.0 collect test.yaml $_syslog_msg
```

上記の例では、「test_1」がアプレットの名前で、「test.yaml」が /bootflash/scripts ディレクトリにあるユーザ設定の YAML ファイルの名前です。

YAML ファイルの例

次に、トリガーベースのイベント ログ自動収集機能をサポートする基本的な YAML ファイルの例を示します。ファイル内のキー/値の定義を次の表に示します。



- (注) YAML ファイルに適切なインデントがあることを確認します。ベストプラクティスとして、スイッチで使用する前に任意の「オンライン YAML 検証」を実行します。

```
bash-4.3$ cat /bootflash/scripts/test.yaml
version: 1
components:
  securityd:
    default:
      tech-sup: port
      commands: show module
  platform:
    default:
      tech-sup: port
      commands: show module
```

キー : 値	説明
バージョン : 1	1 に設定します。他の番号を使用すると、自動収集スクリプトに互換性がなくなります。
コンポーネント :	以下がスイッチ コンポーネントであることを指定するキーワード。
securityd :	syslog コンポーネントの名前 (securityd は syslog のファシリティ名)。
デフォルト :	コンポーネントに属するすべてのメッセージを識別します。
tech-sup : port	securityd syslog コンポーネントのポート モジュールのテクニカル サポートを収集します。
コマンド : show module	securityd syslog コンポーネントの show module コマンド出力を収集します。
プラットフォーム :	syslog コンポーネントの名前 (platform は syslog のファシリティ名)。
tech-sup : port	platform syslog コンポーネントのポート モジュールのテクニカル サポートを収集します。
コマンド : show module	platform syslog コンポーネントの show module コマンド出力を収集します。

特定のログにのみ自動収集メタデータを関連付けるには、次の例を使用します。たとえば、SECURITYD-2-FEATURE_ENABLE_DISABLE

```
securityd:
  feature_enable_disable:
    tech-sup: security
    commands: show module
```

キー : 値	説明
securityd :	syslog コンポーネントの名前 (securityd は syslog のファシリティ名)。
feature_enable_disable :	syslog メッセージのメッセージ ID。
tech-sup : security	securityd syslog コンポーネントのセキュリティモジュールのテクニカル サポートを収集します。
コマンド : show module	セキュリティ syslog コンポーネントの show module コマンド出力を収集します。

上記の YAML エントリの syslog 出力の例 :

```
2019 Dec 4 12:41:01 n9k-c93108tc-fx %SECURITYD-2-FEATURE_ENABLE_DISABLE: User
has enabled the feature bash-shell
```

複数の値を指定するには、次の例を使用します。

```
version: 1
components:
  securityd:
    default:
      commands: show module;show version;show module
      tech-sup: port;lldp
```



- (注) 複数の show コマンドとテクニカルサポートキーの値を区切るには、セミコロンを使用します (前の例を参照)。

コンポーネントあたりの自動収集の量の制限

自動収集の場合、コンポーネントイベントあたりのバンドル数の制限はデフォルトで3に設定されています。1つのコンポーネントで3つ以上のイベントが発生すると、イベントはドロップされ、ステータスメッセージ **EVENTLOGLIMITREACHED** が表示されます。イベントログがロールオーバーすると、コンポーネントイベントの自動収集が再開されます。

例：

```
switch# show system internal event-logs auto-collect history
DateTime          Snapshot ID  Syslog                               Status/Secs/Logsize (Bytes)
2020-Jun-27 07:20:03 1140276903 ACLMGR-0-TEST_SYSLOG                EVENTLOGLIMITREACHED
2020-Jun-27 07:15:14 1026359228 ACLMGR-0-TEST_SYSLOG                RATELIMITED
2020-Jun-27 07:15:09 384952880  ACLMGR-0-TEST_SYSLOG                RATELIMITED
2020-Jun-27 07:13:55 1679333688 ACLMGR-0-TEST_SYSLOG                PROCESSED:2:9332278
2020-Jun-27 07:13:52 1679333688 ACLMGR-0-TEST_SYSLOG                PROCESSING
2020-Jun-27 07:12:55 502545693  ACLMGR-0-TEST_SYSLOG                RATELIMITED
2020-Jun-27 07:12:25 1718497217 ACLMGR-0-TEST_SYSLOG                RATELIMITED
2020-Jun-27 07:08:25 1432687513 ACLMGR-0-TEST_SYSLOG                PROCESSED:2:10453823
2020-Jun-27 07:08:22 1432687513 ACLMGR-0-TEST_SYSLOG                PROCESSING
2020-Jun-27 07:06:16 90042807   ACLMGR-0-TEST_SYSLOG                RATELIMITED
2020-Jun-27 07:03:26 1737578642 ACLMGR-0-TEST_SYSLOG                RATELIMITED
2020-Jun-27 07:02:56 40101277  ACLMGR-0-TEST_SYSLOG                PROCESSED:3:10542045
2020-Jun-27 07:02:52 40101277  ACLMGR-0-TEST_SYSLOG                PROCESSING
```

自動収集ログ ファイル

自動収集ログ ファイルについて

YAML ファイルの設定によって、自動収集ログ ファイルの内容が決まります。収集ログ ファイルで使用されるメモリの量は設定できません。保存後のファイルが消去される頻度は設定できます。

自動収集ログ ファイルは、次のディレクトリに保存されます。

```
switch# dir bootflash:eem_snapshots
 44205843   Sep 25 11:08:04 2019
1480625546_SECURITYD_2_FEATURE_ENABLE_DISABLE_eem_snapshot.tar.gz
  Usage for bootflash://sup-local
 6940545024 bytes used
44829761536 bytes free
51770306560 bytes total
```

ログファイルへのアクセス

コマンドキーワード「debug」を使用してログを検索します。

```
switch# dir debug:///
...
      26   Oct 22 10:46:31 2019  log-dump
      24   Oct 22 10:46:31 2019  log-snapshot-auto
      26   Oct 22 10:46:31 2019  log-snapshot-user
```

次の表に、ログの場所と保存されるログの種類を示します。

場所	説明
log-dump	このフォルダには、ログロールオーバー時にイベントログが保存されます。
log-snapshot-auto	このフォルダには、syslogイベント0、1、2の自動収集ログが含まれます。
log-snapshot-user	このフォルダには、bloggerd log-snapshot の実行時に収集されたログが保存されます。

ログロールオーバーで生成されたログファイルを表示するには、次の例を参考にしてください。

```
switch# dir debug:log-dump/
debug:log-dump/20191022104656_evtlog_archive.tar
debug:log-dump/20191022111241_evtlog_archive.tar
debug:log-dump/20191022111841_evtlog_archive.tar
debug:log-dump/20191022112431_evtlog_archive.tar
debug:log-dump/20191022113042_evtlog_archive.tar
debug:log-dump/20191022113603_evtlog_archive.tar
```

ログ tar ファイルの解析

tar ファイル内のログを解析するには、次の例を参考にしてください。

```
switch# show system internal event-logs parse
debug:log-dump/20191022104656_evtlog_archive.tar
-----LOGS:/tmp/BLOGGERD0.991453012199/tmp/1-191022104658-191022110741-device_test-M27-V1-I1:0-P884.gz-----
2019 Oct 22 11:07:41.597864 E_DEBUG Oct 22 11:07:41 2019(diag_test_start):Data Space
Limits(bytes): Soft: -1 Ha rd: -1
2019 Oct 22 11:07:41.597857 E_DEBUG Oct 22 11:07:41 2019(diag_test_start):Stack Space
Limits(bytes): Soft: 500000 Hard: 500000
2019 Oct 22 11:07:41.597850 E_DEBUG Oct 22 11:07:41 2019(diag_test_start):AS: 1005952076
-1
2019 Oct 22 11:07:41.597406 E_DEBUG Oct 22 11:07:41 2019(device_test_process_events):Sdwrap
msg unknown
2019 Oct 22 11:07:41.597398 E_DEBUG Oct 22 11:07:41 2019(diag_test_start):Going back to
select
2019 Oct 22 11:07:41.597395 E_DEBUG Oct 22 11:07:41 2019(nvram_test):TestNvram examine
27 blocks
2019 Oct 22 11:07:41.597371 E_DEBUG Oct 22 11:07:41 2019(diag_test_start):Parent: Thread
created test index:4 thread_id:-707265728
2019 Oct 22 11:07:41.597333 E_DEBUG Oct 22 11:07:41 2019(diag_test_start):Node inserted
2019 Oct 22 11:07:41.597328 E_DEBUG Oct 22 11:07:41 2019(diag_test_start):The test index
in diag is 4
2019 Oct 22 11:07:41.597322 E_DEBUG Oct 22 11:07:41 2019(diag_test_start):result severity
level
2019 Oct 22 11:07:41.597316 E_DEBUG Oct 22 11:07:41 2019(diag_test_start):callhome alert
level
```


次の表に、特定の tar ファイルの解析に使用できる追加のキーワードを示します。

キーワード	説明
component	プロセス名で識別されるコンポーネントに属するログをデコードします。
from-datetime	yy [mm [dd [HH [MM [SS]]]]] 形式で指定した、特定の日時のログをデコードします。
instance	デコードする SDWRAP バッファ インスタンスのリスト (カンマ区切り)。
module	SUP や LC などのモジュールからのログをデコードします (モジュール ID を使用)。
to-datetime	yy [mm [dd [HH [MM [SS]]]]] 形式で指定した、特定の日時までのログをデコードします。

別の場所へログをコピーする

リモートサーバなどの別の場所にログをコピーするには、次の例を参考にしてください。

```
switch# copy debug:log-dump/20191022104656_evtlog_archive.tar
scp://<ip-address>/nobackup/<user> vrf management use-kstack
Enter username: user@<ip-address>'s password:
20191022104656_evtlog_archive.tar                               100% 130KB
 130.0KB/s   00:00
Copy complete, now saving to disk (please wait)...
Copy complete.
```

自動収集ログファイルの消去

生成されるトリガーベースの自動収集ログには、EventHistory と EventBundle の 2 種類があります。

EventHistory ログの消去ロジック

イベント履歴の場合は、/var/sysmgr/srv_logs/xport フォルダで消去が行われます。250 MB のパーティション RAM が、/var/sysmgr/srv_logs ディレクトリにマウントされます。

/var/sysmgr/srv_logs のメモリ使用率が、割り当てられた 250 MB の 65% 未満の場合、ファイルは消去されません。メモリ使用率が 65% の制限レベルに達すると、新しいログの保存を続行するのに十分なメモリが使用可能になるまで、最も古いファイルから消去されます。

EventBundle ログの消去ロジック

イベントバンドルの場合、消去ロジックは /bootflash/eem_snapshots フォルダでの状態に基づいて実行されます。自動収集されたスナップショットを保存するために、EEM 自動収集スクリプトは、ブートフラッシュストレージの 5% を割り当てます。ブートフラッシュ容量の 5% が使用されると、ログは消去されます。

新しい自動収集ログが利用可能になっているものの、ブートフラッシュに保存するスペースがない場合 (すでに 5% の容量に達している)、システムは次のことを確認します。

1. 12時間以上経過した既存の自動収集ファイルがある場合、システムはファイルを削除し、新しいログをコピーします。
2. 既存の自動収集ファイルが12時間未満の場合、新しく収集されたログは保存されずに廃棄されます。

デフォルトページ時間である12時間は、次のコマンドを使用して変更できます。コマンドで指定する時間は分単位です。

```
switch(config)# event manager applet test override __syslog_trigger_default
switch(config-applet)# action 1.0 collect test.yaml purge-time 300 $_syslog_msg
```

event manager command: *test* は、ポリシー例の名前です。**__syslog_trigger_default** は、オーバーライドする必要があるシステムポリシーの名前です。この名前は、二重アンダースコア (__) で始まる必要があります。

action command: **1.0** は、アクションの実行順番を示している例となっています。**collect** は、データがYAMUファイルを使用して収集されることを示しています。*test.yaml* は、YAMLファイルの名前の例です。**\$_syslog_msg** は、コンポーネントの名前です。



- (注) どの時点でも、進行中のトリガーベースの自動収集イベントは1つだけです。自動収集がすでに発生しているときに別の新しいログ イベントを保存しようとする、新しいログ イベントは破棄されます。

デフォルトでは、トリガーベースのバンドルは5分(300秒)ごとに1つだけ収集されます。このレート制限は、次のコマンドでも設定できます。コマンドで指定する時間は秒単位です。

```
switch(config)# event manager applet test override __syslog_trigger_default
switch(config-applet)# action 1.0 collect test.yaml rate-limit 600 $_syslog_msg
```

event manager command: *test* はポリシーの名前の例です。**__syslog_trigger_default** は、オーバーライドするシステムポリシーの名前の例です。この名前は、二重アンダースコア (__) で始まる必要があります。

action command: **1.0** は、アクションの実行順番を示している例となっています。**collect** は、データがYAMUファイルを使用して収集されることを示しています。*test.yaml* は、YAMLファイルの名前の例です。**\$_syslog_msg** は、コンポーネントの名前です。

自動収集の統計情報と履歴

トリガーベースの収集統計情報の例を次に示します。

```
switch# show system internal event-logs auto-collect statistics
-----EEM Auto Collection Statistics-----
Syslog Parse Successful :88 Syslog Parse Failure :0
Syslog Ratelimited :0 Rate Limit Check Failed :0
Syslog Dropped(Last Action In Prog) :53 Storage Limit Reached :0
User Yaml Action File Unavailable :0 User Yaml Parse Successful :35
User Yaml Parse Error :0 Sys Yaml Action File Unavailable :11
Sys Yaml Parse Successful :3 Sys Yaml Parse Error :0
Yaml Action Not Defined :0 Syslog Processing Initiated :24
Log Collection Failed :0 Tar Creation Error :0
```

```
Signal Interrupt :0 Script Exception :0
Syslog Processed Successfully :24 Logfiles Purged :0
```

次の例は、CLI コマンドを使用して取得されたトリガーベースの収集履歴（処理された syslog 数、処理時間、収集されたデータのサイズ）を示しています。

```
switch# show system internal event-logs auto-collect history
DateTime Snapshot ID Syslog Status/Secs/Logsize(Bytes)
2019-Dec-04 05:30:32 1310232084 VPC-0-TEST_SYSLOG PROCESSED:9:22312929
2019-Dec-04 05:30:22 1310232084 VPC-0-TEST_SYSLOG PROCESSING
2019-Dec-04 04:30:13 1618762270 ACLMGR-0-TEST_SYSLOG PROCESSED:173:33194665
2019-Dec-04 04:28:47 897805674 SYSLOG-1-SYSTEM_MSG DROPPED-LASTACTIONINPROG
2019-Dec-04 04:28:47 947981421 SYSLOG-1-SYSTEM_MSG DROPPED-LASTACTIONINPROG
2019-Dec-04 04:27:19 1618762270 ACLMGR-0-TEST_SYSLOG PROCESSING
2019-Dec-04 02:17:16 1957148102 CARDCLIENT-2-FPGA_BOOT_GOLDEN NOYAMLFILEFOUND
```

トリガーベースのログ収集の確認

次の例のように **show event manager system-policy | i trigger** コマンドを入力して、トリガーベースのログ収集機能が有効になっていることを確認します。

```
switch# show event manager system-policy | i trigger n 2
Name : __syslog_trigger_default
Description : Default policy for trigger based logging
Overridable : Yes
Event type : 0x2101
```

トリガーベースのログ ファイル生成の確認

トリガーベースの自動収集機能によってイベント ログ ファイルが生成されたかどうかを確認できます。次の例のいずれかのコマンドを入力します。

```
switch# dir bootflash:eem_snapshots
9162547 Nov 12 22:33:15 2019
1006309316_SECURITYD_2_FEATURE_ENABLE_DISABLE_eem_snapshot.tar.gz

Usage for bootflash://sup-local
8911929344 bytes used
3555950592 bytes free
12467879936 bytes total

switch# dir debug:log-snapshot-auto/
63435992 Dec 03 06:28:52 2019
20191203062841_1394408030_PLATFORM_2_MOD_PWRDN_eem_snapshot.tar.gz

Usage for debug://sup-local
544768 bytes used
4698112 bytes free
5242880 bytes total
```

ローカル ログ ファイルのストレージ

ローカル ログ ファイルのストレージ機能：

- ローカルデータストレージ時間の量は、導入の規模とタイプによって異なります。モジュラスイッチと非モジュラスイッチの両方で、ストレージ時間は15分から数時間のデータです。長期間にわたる関連ログを収集するには、次の手順を実行します。

- 必要な特定のサービス/機能に対してのみイベント ログの保持を有効にします。「[単一サービスの拡張ログファイル保持の有効化 \(268 ページ\)](#)」を参照してください。
- スイッチから内部イベント ログをエクスポートします。「[外部ログ ファイルのストレージ \(282 ページ\)](#)」を参照してください。
- 圧縮されたログは RAM に保存されます。
- 250MB のメモリは、ログ ファイル ストレージ用に予約されています。
- ログ ファイルは tar 形式で最適化されます (5 分ごとに 1 ファイルまたは 10 MB のいずれか早い方)。
- スナップショット収集を許可します。

最近のログ ファイルのローカル コピーの生成

拡張ログファイル保持は、スイッチで実行されているすべてのサービスに対してデフォルトで有効になっています。ログ ファイルは、フラッシュ メモリにローカルに保存されます。次の手順を使用して、最新のイベント ログ ファイルを最大 10 個生成します。

手順

	コマンドまたはアクション	目的
ステップ 1	<p>bloggerd log-snapshot [<i>file-name</i>] [bootflash: <i>file-path</i> logflash: <i>file-path</i> usb1:] [size <i>file-size</i>] [time <i>minutes</i>]</p> <p>例 :</p> <pre>switch# bloggerd log-snapshot snapshot1</pre>	<p>スイッチに保存されている最新の 10 個のイベント ログのスナップショットバンドル ファイルを作成します。この操作のデフォルトのストレージは logflash です。</p> <p><i>file-name</i> : 生成されたスナップショット ログ ファイル バンドルのファイル名。 <i>file-name</i> には最大 64 文字を使用します。</p> <p>(注) この変数はオプションです。設定されていない場合、システムはタイムスタンプと「_snapshot_bundle.tar」をファイル名として適用します。</p> <p>例 :</p> <pre>20200605161704_snapshot_bundle.tar</pre> <p>bootflash: <i>file-path</i> : スナップショット ログ ファイル バンドルがブートフラッシュに保存されているファイルパス。次の初期パスのいずれかを選択します。</p> <ul style="list-style-type: none"> • bootflash:///

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • bootflash://module-1/ • bootflash://sup-1/ • bootflash://sup-active/ • bootflash://sup-local/ <p>logflash: file-path : スナップショット ログ ファイルバンドルがログ フラッシュ に保存されるファイルパス。次の初期パスのいずれかを選択します。</p> <ul style="list-style-type: none"> • logflash:// • logflash://module-1/ • logflash://sup-1/ • logflash://sup-active/ • logflash://sup-local/ <p>usb1 : USB デバイス上のスナップ ショット ログ ファイルバンドルが保存 されているファイルパス。</p> <p>size file-size : メガバイト (MB) 単位の サイズに基づくスナップショット ログ ファイルバンドル。範囲は 5MB〜 250MB です。</p> <p>time minutes : 最後の x 時間 (分) に基 づくスナップショット ログ ファイルバ ンドル。範囲は 1 ~ 30 分です。</p>

例

```
switch# bloggerd log-snapshot snapshot1
Snapshot generated at logflash:evt_log_snapshot/snapshot1_snapshot_bundle.tar Please
cleanup once done.
switch#
switch# dir logflash:evt_log_snapshot
159098880 Dec 05 06:40:24 2019 snapshot1_snapshot_bundle.tar
159354880 Dec 05 06:40:40 2019 snapshot2_snapshot_bundle.tar

Usage for logflash://sup-local
759865344 bytes used
5697142784 bytes free
6457008128 bytes total
```

次の例のコマンドを使用して、同じファイルを表示します。

```
switch# dir debug:log-snapshot-user/  
159098880 Dec 05 06:40:24 2019 snapshot1_snapshot_bundle.tar  
159354880 Dec 05 06:40:40 2019 snapshot2_snapshot_bundle.tar  
  
Usage for debug://sup-local  
929792 bytes used  
4313088 bytes free  
5242880 bytes total
```



(注) 例の最後のファイル名に注意してください。個々のログファイルは、生成された日時によっても識別されます。

外部ログ ファイルのストレージ

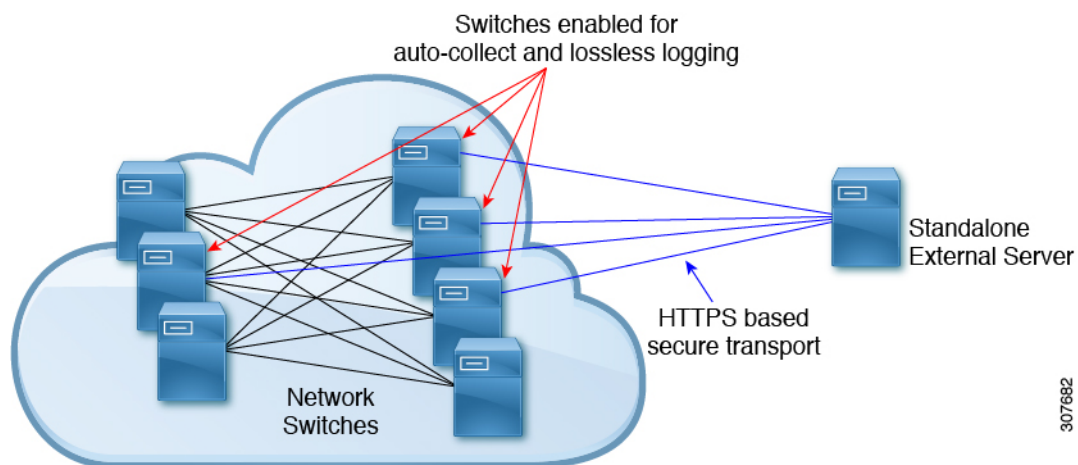
外部サーバソリューションは、ログを安全な方法でオフスイッチに保存する機能を提供します。



(注) 外部ストレージ機能を作成するため、Cisco Technical Assistance Center (TAC) に連絡して、外部サーバソリューションの展開をサポートを求めてください。

次に、外部ログ ファイルの保存機能を示します。

- オンデマンドで有効
- HTTPS ベースの転送
- ストレージ要件 :
 - 非モジュラ スイッチ : 300 MB
 - モジュラ スイッチ : 12 GB (1 日あたり、スイッチあたり)
- 通常、外部サーバには 10 台のスイッチのログが保存されます。ただし、外部サーバでサポートされるスイッチの数に厳密な制限はありません。



307682

外部サーバソリューションには、次の特性があります。

- コントローラレス環境
- セキュリティ証明書の手動管理
- サポートされている 3 つの使用例：
 - 選択したスイッチからのログの継続的な収集
 - TAC のサポートによる、シスコ サーバへのログの展開とアップロード。
 - 限定的なオンプレミス処理



(注) 外部サーバでのログファイルの設定と収集については、Cisco TAC にお問い合わせください。



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。

- [OBFL の概要 \(285 ページ\)](#)
- [OBFL の前提条件 \(286 ページ\)](#)
- [OBFL の注意事項と制約事項 \(286 ページ\)](#)
- [OBFL のデフォルト設定 \(286 ページ\)](#)
- [OBFL の設定 \(286 ページ\)](#)
- [OBFL 設定の確認 \(289 ページ\)](#)
- [OBFL のコンフィギュレーション例 \(290 ページ\)](#)
- [その他の参考資料 \(291 ページ\)](#)

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。このオンボード障害ロギング (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

OBFL の前提条件

network-admin ユーザ権限が必要です。

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りますので注意してください。

OBFL のデフォルト設定

次の表に、VACL 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。

始める前に

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 : <pre>switch# configure terminal switch(config)#</pre>	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 : <pre>switch(config)# hw-module logging onboard Module: 7 Enabling ... was successful. Module: 10 Enabling ... was successful. Module: 12 Enabling ... was successful.</pre>	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 : <pre>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.</pre>	OBFL カウンタ統計情報を有効にします。
ステップ 4	hw-module logging onboard cpuhog 例 : <pre>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.</pre>	OBFL CPU hog イベントを有効にします。
ステップ 5	hw-module logging onboard environmental-history 例 : <pre>switch(config)# hw-module logging onboard environmental-history Module: 7 Enabling environmental-history ... was successful. Module: 10 Enabling</pre>	OBFL 環境履歴をイネーブルにします。

	コマンドまたはアクション	目的
	<pre>environmental-history ... was successful. Module: 12 Enabling environmental-history ... was successful.</pre>	
ステップ 6	<p>hw-module logging onboard error-stats</p> <p>例 :</p> <pre>switch(config)# hw-module logging onboard error-stats Module: 7 Enabling error-stats ... was successful. Module: 10 Enabling error-stats ... was successful. Module: 12 Enabling error-stats ... was successful.</pre>	OBFL エラー統計をイネーブルにします。
ステップ 7	<p>hw-module logging onboard interrupt-stats</p> <p>例 :</p> <pre>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.</pre>	OBFL 割り込み統計をイネーブルにします。
ステップ 8	<p>hw-module logging onboard module slot</p> <p>例 :</p> <pre>switch(config)# hw-module logging onboard module 7 Module: 7 Enabling ... was successful.</pre>	モジュールの OBFL 情報をイネーブルにします。
ステップ 9	<p>hw-module logging onboard obfl-logs</p> <p>例 :</p> <pre>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.</pre>	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。

	コマンドまたはアクション	目的
ステップ 10	(任意) show logging onboard 例： <pre>switch(config)# show logging onboard</pre>	OBFL に関する情報を表示します。 (注) 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、 OBFL 設定の確認 (289 ページ) を参照してください。
ステップ 11	(任意) copy running-config startup-config 例： <pre>switch(config)# copy running-config startup-config</pre>	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 設定の確認

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 スロット	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。

コマンド	目的
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 を有効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
コンフィギュレーション ファイル	『Cisco Nexus 9000 Series NX-OS Fundamentals Configuration Guide』



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。

- [SPAN の概要, on page 293](#)
- [SPAN の前提条件 \(297 ページ\)](#)
- [SPAN の注意事項および制約事項 \(297 ページ\)](#)
- [SPAN のデフォルト設定 \(307 ページ\)](#)
- [SPAN の設定 \(307 ページ\)](#)
- [SPAN 設定の確認 \(317 ページ\)](#)
- [SPAN のコンフィギュレーション例 \(318 ページ\)](#)
- [その他の参考資料 \(322 ページ\)](#)

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（Rx）、出力（Tx）、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（ただしサブインターフェイスではない）
- コントロールプレーン CPU への帯域内インターフェイス。



Note 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 CPU により送信されたすべてのパケットをモニタします。

- VLAN

- VLAN を SPAN 送信元として指定する場合は、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 ソースになります。
- VLAN は、入力方向にのみ SPAN 送信元となることができます。



Note これは、Cisco Nexus 9300-EX/-FX/-FX2/-GX プラットフォームスイッチ、および -EX/-FX ラインカードを搭載する Cisco Nexus 9500 シリーズプラットフォームスイッチを除くすべてのスイッチに適用されます。

- Cisco Nexus 2000 シリーズファブリックエクステンダ (FEX) 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アクセスモードおよびレイヤ2トランクモードでサポートされます。レイヤ3モードではサポートされず、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 Nexus 9300 および 9500 プラットフォームスイッチは、FEX ポートを SPAN 送信元としてサポートします。この場合、入力方向については、すべてのトラフィックを対象としますが、出力方向については、スイッチと FEX を通る既知のレイヤ2ユニキャストトラフィックフローに限られます。ルーティングされたトラフィックは FEX HIF 出力 SPAN で表示されないことがあります。



Note 1つの SPAN セッションに、上述の送信元を組み合わせ使用できます。

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。
- スーパーバイザインバンドインターフェイスを SPAN 送信元として使用する場合、スーパーバイザハードウェア（出力）によって生成されたすべてのパケットがモニタされます。



Note Rx は ASIC の観点から見たものです（トラフィックはインバンドを介してスーパーバイザから出力され、ASIC / SPAN で受信されます）。

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。SPAN 宛先には、次のものが含まれます。

- 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
- アクセスモードまたはトランクモードのポートチャンネル
- Cisco Nexus 9300 シリーズスイッチのアップリンクポート



Note FEX ポートは SPAN 宛先ポートとしてサポートされません。

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。

- 宛先ポートとして設定されたポートは、送信元ポートとして設定できません。
- 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 パケットを含みます。

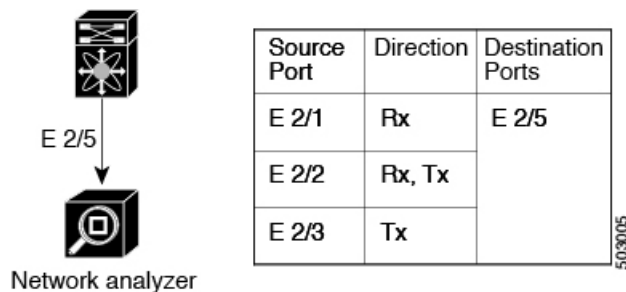
SPAN セッション

SPAN セッションを作成し、送信元と宛先をモニタに指定できます。

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 9000 シリーズ NX-OS 検証済みスケーラビリティガイド』を参照してください。

この図では、SPAN 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 5: SPAN の設定



ローカライズされた SPAN セッション

すべての送信元インターフェイスが同じラインカード上にある場合、SPANセッションはローカライズされます。セッション宛先インターフェイスは、任意のラインカードに配置できます。



(注) VLAN 送信元との SPAN セッションはローカライズされません。

SPAN 切り捨て

Cisco NX-OS Release 7.0(3)I7(1) 以降では、MTU のサイズに基づいて各 SPAN セッションの送信元パケットの切り捨てを設定できます。切り捨てにより、モニタするパケットのサイズを減らすことで、SPAN の帯域幅を効果的に軽減できます。設定された MTU 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。たとえば、MTU を 300 バイトに設定すると、300 バイトを超えるパケットは 300 バイトに切り捨てられます。

SPAN 切り捨てはデフォルトでディセーブルです。切り捨てを使用するには、個々の SPAN セッションで有効にしておく必要があります。

ACL TCAM リージョン

ハードウェアの ACL Ternary Content Addressable Memory (TCAM) リージョンのサイズを変更できます。SPANセッションで使用される TCAM リージョンの詳細については、『Cisco Nexus 9000 シリーズ NX-OS セキュリティ設定ガイド』の「IP ACL の設定」のセクションを参照してください。

高可用性

SPAN 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 9000 シリーズ NX-OS ハイアベイラビリティおよび冗長性ガイド』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 9000 シリーズ NX-OS インターフェイス設定ガイド』を参照してください。

SPAN の注意事項および制約事項



- (注) スケールの情報については、リリース特定の『Cisco Nexus 9000 Series NX-OS Verified Scalability Guide』を参照してください。

SPAN 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。

- ACL によって拒否されたトラフィックは、SPAN 宛先ポートに到達する可能性があります。これは、SPAN 複製が ACL の適用 (ACL ドロップ トラフィック) の前に入力側で実行されるためです。
- SPAN セッションの制限については、『Cisco Nexus 9000 シリーズ NX-OS 検証スケーラビリティガイド』を参照してください。
- すべての SPAN 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。
- 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。
- 同じ送信元インターフェイスで 2 つの SPAN または ERSPAN セッションを 1 つのフィルタだけで設定することはできません。同じ送信元が複数の SPAN または ERSPAN セッションで使用されている場合は、すべてのセッションに異なるフィルタを設定するか、セッションにフィルタを設定しないでください。
- VLAN フィルタが構成されている場合、複数のスパンセッションで同じソースを構成することはできません。
- アクセスポート dot1q ヘッダーの SPAN コピーには、次のガイドラインが適用されます。
 - トラフィックがトランクポートから入力され、アクセスポートに出力される場合、スイッチインターフェイス上のアクセスポートの出力 SPAN コピーには常に dot1q ヘッダーがあります。
 - トラフィックがアクセスポートから入り、トランクポートに出る場合、スイッチインターフェイスのアクセスポートの入力 SPAN コピーには dot1q ヘッダーがありません。

- トラフィックがアクセスポートから入力され、アクセスポートに出力される場合、スイッチインターフェイス上のアクセスポートの入力/出力 SPAN コピーには dot1q ヘッダーがありません。
- FCS エラーがあるパケットは、SPAN セッションでミラーリングされません。
- SPAN セッションで 1 つの宛先ポートはのみ設定できます。
- 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。
- ポートを送信元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。
- SPAN 送信元ポートと宛先ポートでの単方向リンク検出 (UDLD) の同時イネーブル化はサポートされていません。UDLD フレームがこのような SPAN セッションの送信元ポートでキャプチャされることが予想される場合は、SPAN セッションの宛先ポートで UDLD をディセーブルにします。
- SPAN は、管理ポートではサポートされません。
- フィルタ アクセス グループの統計情報はサポートされていません。
- SPAN はレイヤ 3 モードでサポートされます。ただし、SPAN はレイヤ 3 サブインターフェイスまたはレイヤ 3 ポートチャンネル サブインターフェイスではサポートされません。
- 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、これらのポートを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。送信元ポート上でのこの動作の例を、次に示します。
 - フラ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
- 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。
- VLAN SPAN がモニタするのは、VLAN のレイヤ 2 ポートを出入りするトラフィックだけです。
- VLAN は、SPAN 送信元またはフィルタとして使用される場合、属することができるのは 1 つのセッションだけです。
- 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。
- VLAN ACL を使用して SPAN をフィルタリングする場合、**action forward** のみがサポートされます。**action drop** および **action redirect** はサポートされていません。

- VLAN 送信元セッションおよびポート送信元セッションの組み合わせはサポートされていません。トラフィック ストリームが VLAN 送信元セッションとポート送信元セッションと一致する場合、2 つの宛先ポートで 2 つのコピーが必要です。ハードウェアの制限により、VLAN 送信元 SPAN と特定の宛先ポートのみが SPAN パケットを受信します。この制限は、次のシスコ デバイスにのみ適用されます。

表 18: Cisco Nexus 9000 シリーズ スイッチ

Cisco Nexus 93120TX	Cisco Nexus 93128TX	Cisco Nexus 9332PQ
Cisco Nexus 9372PX	Cisco Nexus 9372PX-E	Cisco Nexus 9372TX
Cisco Nexus 9396PX	Cisco Nexus 9372TX-E	Cisco Nexus 9396TX

表 19: Cisco Nexus 9000 シリーズ ラインカード、ファブリック モジュールおよび GEM モジュール

N9K-X9408PC-CFP2	N9K-X9536PQ	N9K-C9508-FM
N9K-X9432PQ	N9K-X9564PX	N9K-C9504-FM
N9K-X9464PX	N9K-X9564TX	N9K-C9516-FM
N9K-X9464TX	N9K-X9636PQ	N9K-M4PC-CFP2

- ラインカードごとの SPAN セッションの数は、同じインターフェイスが複数セッションの双方向送信元として設定されている場合は、2 に減少します。このガイドラインは、9636C-R および 9636Q-R ラインカードを搭載した Cisco Nexus 9508 スイッチには適用されません。
- SPAN セッションのアクセス グループ フィルタは、vlan-accessmap として設定する必要があります。このガイドラインは、9636C-R および 9636Q-R ラインカードを搭載した Cisco Nexus 9508 スイッチには適用されません。
- スーパーバイザ生成の Stream Of Bytes Module Header (SOBMH) パケットには、インターフェイスから出力されるための情報がすべて含まれており、SPAN および ERSPAN を含めた、ハードウェア内部でのフォワーディング ルックアップはすべてバイパス可能です。レイヤ 3 インターフェイスの CPU 生成フレームおよびパケットのブリッジプロトコル データ ユニット (BPDU) クラスは、SOBMH を使用して送信されます。このガイドラインは、9636C-R および 9636Q-R ラインカードを搭載した Cisco Nexus 9508 スイッチには適用されません。Cisco Nexus 9636C-R と 9636Q-R は両方とも、インバンド SPAN とローカル SPAN をサポートします。
- Cisco NX-OS は、送信元インターフェイスがホスト インターフェイス ポート チャネルでないときは、リンク層検出プロトコル (LLDP) またはリンク集約制御プロトコル (LACP) パケットをスパンしません。
- マルチキャスト パケットの SPAN コピーは、書き換え前に作成されます。したがって、TTL、VLAN ID、出力ポリシーによる再マーキングなどは、SPAN コピーにキャプチャされません。

- SPAN が ASIC インスタンスのインターフェイスに入力され、別の ASIC インスタンスのレイヤ 3 インターフェイス（SPAN 送信元）に出力されるトラフィックをミラーリングしている場合、Tx ミラーリング パッケージは Cisco Nexus 9300 プラットフォーム スイッチ（-EX、-FX、または -FX2 を除く）および非 EX または非 FX ラインカードを使用する Cisco Nexus 9500 プラットフォーム モジュラー スイッチで 4095 の VLAN ID をもちます。ただし、FM を通過する Cisco Nexus X97160YC-EX スパン Tx フロースルー トラフィックは、VLAN 4095 でタグ付けされます。
- スイッチ インターフェイスのアクセス ポートの出力 SPAN コピーには、常に dot1q ヘッダーがあります。このガイドラインは、9636C-R および 9636Q-R ラインカードを搭載した Cisco Nexus 9508 プラットフォーム スイッチには適用されません。
- 不明ユニキャストでフラグgingされたパケットのルーティング後のフローは SPAN セッションに置かれますが、これはフローが転送されるポートをモニタしないよう SPAN セッションが設定されている場合であっても同様です。この制限は、ネットワーク フォワーディング エンジン（NFE）と NFE2 対応 EOR スイッチおよび SPAN セッションで Tx ポートの送信元を持つものに適用されます。
- VLAN 送信元は、Rx 方向にのみスパンされます。この制限は、両方向の VLAN スパニングをサポートする次のスイッチ プラットフォームには適用されません。
 - Cisco Nexus 9300-EX プラットフォーム スイッチ
 - Cisco Nexus 9300-FX プラットフォーム スイッチ
 - Cisco Nexus 9300-FX2 プラットフォーム スイッチ
 - Cisco Nexus 9300-GX プラットフォーム スイッチ
 - 97160YC-EX ラインカードを搭載した Cisco Nexus 9504、9508 および 9516 スイッチ。
 - 9636C-R および 9636Q-R ラインカードを搭載した Cisco Nexus 9508 スイッチ。
- VLAN 送信元が 1 つのセッションで両方向として設定され、物理インターフェイス送信元が他の 2 つのセッションで設定されている場合、物理インターフェイス送信元セッションでは Rx SPAN はサポートされません。この制限は、Cisco Nexus 97160YC-EX ラインカードに適用されます。
- セッション フィルタリング機能（VLAN または ACL フィルタ）は、Rx 送信元でのみサポートされます。このガイドラインは、9636C-R および 9636Q-R ラインカードを搭載した Cisco Nexus 9508 スイッチには適用されません。
- FEX NIF インターフェイスまたはポート チャネルは、SPAN 送信元または SPAN 宛先として使用できません。FEX NIF インターフェイスまたはポート チャネルが SPAN 送信元または SPAN 宛先として指定されている場合、ソフトウェアではサポートされていないエラーが表示されます。
- SPAN / ERSPAN を使用して FEX HIF ポートで Rx トラフィックをキャプチャすると、キャプチャされたトラフィックに追加の VNTAG および 802.1Q タグが存在します。
- VLAN および ACL フィルタは FEX ポートではサポートされません。

- 双方向 SPAN セッションで使用される送信元が同じ FEX からのものである場合、ハードウェア リソースは 2 つの SPAN セッションに制限されます。
- 切り捨てはローカルおよび ERSPAN 送信元セッションでのみサポートされます。それは、ERSPAN 宛先セッションではサポートされません。
- SPAN セッションで MTU を設定すると、（そのセッションの）SPAN 宛先で出力されるすべてのパケットが、指定した MTU 値に切り捨てられます。
 - 切り捨てられたパケットの巡回冗長検査（CRC）が再計算されます。
 - 指定されたバイトは、パケットのヘッダーから保持されます。パケットが MTU より長い場合、残りは切り捨てられます。

Cisco Nexus 3000 プラットフォーム スイッチの SPAN の制限

次の注意事項と制約事項は、Cisco Nexus 9000 コードを実行する Nexus 3000 シリーズ スイッチにのみ適用されます。

- Cisco Nexus 3232C および 3264Q スイッチは、宛先として CPU で SPAN をサポートしていません。

Cisco Nexus 9200 プラットフォーム スイッチの SPAN の制限事項



- (注) スケールの情報については、リリース特定の『*Cisco Nexus 9000 Series NX-OS Verified Scalability Guide*』を参照してください。

次の注意事項と制約事項は、Cisco Nexus 9200 プラットフォーム スイッチにのみ適用されます。

- Cisco Nexus 9200 プラットフォーム スイッチの場合、Rx SPAN は、SPAN 宛先ポートと同じスライス上に転送インターフェイスがないマルチキャストではサポートされません。
- Cisco Nexus 9200 プラットフォーム スイッチでは、マルチキャスト、未知のマルチキャスト、およびブロードキャストトラフィックに対する Tx SPAN はサポートされません。
- CPU 生成パケットの Tx SPAN は、Cisco Nexus 9200 プラットフォーム スイッチではサポートされません。
- UDF ベースの SPAN は、Cisco Nexus 9200 プラットフォーム スイッチでサポートされません。
- Cisco Nexus 9200 プラットフォーム スイッチは、同じ送信元での複数の ACL フィルタをサポートしていません。
- VLAN Tx SPAN は、Cisco Nexus 9200 プラットフォーム スイッチでサポートされます。

- 同じスライスにある複数の出力ポートで、出力 SPAN トラフィックのために輻輳が発生すると、Cisco Nexus 9200 プラットフォームスイッチ上のこれらの出力ポートでは、ラインレートを取得できません。
- ACL フィルタを使用した、親インターフェイスでのサブインターフェイス トラフィックのSPANは、Cisco Nexus 9200 プラットフォームスイッチではサポートされません。
- Cisco Nexus 9200 プラットフォームスイッチでは、CPU SPAN ソースはRx 方向（CPU からの SPAN パケット）でのみ追加できます。
- Cisco Nexus 9200 プラットフォームスイッチでは、CPU への SPAN パケットはレート制限され、インバンドパスでドロップされます。レート制限の変更は、**hardware rate-limiter span** コマンドで行えます。スーパーバイザの SPAN コピーの分析は、**ethanalyzer local interface inband mirror detail** コマンドで行えます。

Cisco Nexus 9300 プラットフォームスイッチの SPAN の制限事項



- (注) スケールの情報については、リリース特定の『*Cisco Nexus 9000 Series NX-OS Verified Scalability Guide*』を参照してください。

次の注意事項と制約事項は、Cisco Nexus 9300 プラットフォームスイッチにのみ適用されます。

- 次のフィルタリング制限は、すべての Cisco Nexus 9300-EX/FX/FX2/GX プラットフォームスイッチの出力 (Tx) SPAN に適用されます。
 - ACL フィルタリングはサポートされていません（ユニキャストおよびブロードキャスト、不明なユニキャストおよびマルチキャスト (BUM) トラフィックの両方に適用されます)
 - VLAN フィルタリングはサポートされますが、ユニキャスト トラフィックのみ
 - VLAN フィルタリングは BUM トラフィックではサポートされません。
- Cisco Nexus 9300-EX/FX プラットフォームスイッチでは、SPAN と sFlow の両方を同時に有効にすることはできません。一方がアクティブな場合、もう一方は有効にできません。ただし、Cisco Nexus 9300-EX/FX/FX2 プラットフォームスイッチでは、NetFlow と SPAN を同時に有効にすることができるので、sFlow と SPAN を併用する代わりに使用できます。



- (注) Cisco Nexus 9300-FX2 スイッチは、sFlow と SPAN の共存をサポートしません。

- VLAN Tx SPAN は、Cisco Nexus 9300-EX および FX プラットフォームスイッチでサポートされます。

- Cisco Nexus 9300 プラットフォーム スイッチは、同じソースに対する複数の ACL フィルタをサポートします。
- 1つのフォワーディング エンジン インスタンスで4つの SPAN セッションがサポートされます。Cisco Nexus 9300 シリーズ スイッチの場合は、最初の3つのセッションに双方向のソースが含まれていると、4番目のセッションのハードウェア リソースは Rx ソース専用になります。
- Cisco Nexus 9300-EX/FX/FX2/FX3/FXP プラットフォーム スイッチは、入力方向の SPAN ソースとしてのみ FEX ポートをサポートします。
- Cisco Nexus 9300 プラットフォーム スイッチ (Cisco Nexus 9300-EX/FX/FX2/FX3/FXP スイッチを除く) は、FEX ポートを SPAN ソースとしてサポートします。この場合、入力方向については、すべてのトラフィックを対象としますが、出力方向については、スイッチと FEX を通る既知のレイヤ2ユニキャストトラフィックフローに限られます。ルーティングされたトラフィックは FEX HIF 出力 SPAN で表示されないことがあります。
- Cisco Nexus 9300 シリーズ スイッチは、Tx SPAN を 40G アップリンク ポートでサポートしません



(注) この制限は、100G インターフェイスを持つ Nexus 9300-EX/FX/FX2 スイッチには適用されません。

- CPU 生成パケットの Tx SPAN は、Cisco Nexus 9300-EX/FX/FXP プラットフォーム スイッチではサポートされません。
- 異なるスライス間でマルチキャスト Tx トラフィックの SPAN をサポートするのは、Cisco Nexus 9300-EX プラットフォーム スイッチだけです。スライスは同じリーフ スパイン エンジン (LSE) 上にある必要があります。
- Cisco Nexus 9300-EX/FX/FX2/GX プラットフォーム スイッチのレイヤ2 スイッチ ポートおよびポートチャネルソースを使用する Tx インターフェイス SPAN の場合、同じ VLAN でストリームを受信しているレイヤ2 メンバーの数に関係なく、レシーバユニットごとに1つのコピーのみが作成されます。たとえば、e1/1~8がすべて Tx 方向の SPAN ソースであり、すべてが同じグループに参加している場合、SPAN ディスティネーションポートは、8つのコピーではなく、書き換え前のストリームの1つのコピーを認識します。さらに、何らかの理由で、これらのポートの1つ以上が出力でパケットをドロップした場合でも (輻輳など)、パケットは SPAN ディスティネーションポートに到達できます。Cisco Nexus 9732C-EX ラインカードの場合、メンバーを持つユニットごとに1つのコピーが作成されます。ポートチャネルソースの場合、SPAN を実行するレイヤ2 メンバーが最初のポートチャネルメンバーになります。
- SPAN Tx ブロードキャストおよび SPAN Tx マルチキャストは、Cisco Nexus 9300-EX/FX/FX2/GX プラットフォーム スイッチおよびCisco Nexus 9732C-EX ラインカードのスライス全体のレイヤ2ポートおよびポートチャネルソースでサポートされます。ただし IGMP スヌーピングがディセーブルの場合に限られます。(それ以外の場合は、スライスの制限が適用されます)。これらの機能は、レイヤ3ポートソース、FEX ポート (ユ

ニキャストまたはマルチキャストトラフィック)、および VLAN ソースではサポートされません。

- Cisco Nexus 9300 シリーズスイッチ 40G アップリンク インターフェイスの SPAN コピーは、Rx 方向にスパンする際に、dot1q 情報を取り逃がします。



(注) この制限は、100G インターフェイスを持つ Nexus 9300-EX/FX/FX2 プラットフォームスイッチには適用されません。

- UDF ベースの SPAN は、Cisco Nexus 9300-EX/-FX/-FX2/GX プラットフォームスイッチでサポートされます。
- UDF-SPAN の ACL フィルタリングはソースインターフェイス rx のみをサポートします。この制限は、次のスイッチに適用されます。
 - Cisco Nexus 9332PQ
 - Cisco Nexus 9372PX
 - Cisco Nexus 9372PX-E
 - Cisco Nexus 9372TX
 - Cisco Nexus 9372TX-E
 - Cisco Nexus 93120TX
- Cisco Nexus 9300-EX/FX/FX2/GX プラットフォームスイッチは、同じソースの複数の ACL フィルタをサポートしていません。
- 同じスライスにある複数の出力ポートで、出力 SPAN トラフィックのために輻輳が発生すると、Cisco Nexus 9300-EX/FX/FX2/GX プラットフォームスイッチ上のこれらの出力ポートでは、ライン レートを取得できません。
- ACL フィルタを使用した、親インターフェイスでのサブインターフェイストラフィックのスパンは、Cisco Nexus 9300-EX/FX/FX2/GX プラットフォームスイッチではサポートされません。
- Cisco Nexus 9300-EX/FX/FX2/GX プラットフォームスイッチでは、CPU SPAN ソースは Rx 方向 (CPU からの SPAN パケット) でのみ追加できます。
- Cisco Nexus 9300-EX/FX/FX2/GX プラットフォームスイッチでは、CPU への SPAN パケットはレート制限され、インバンドパスでドロップされます。レート制限の変更は、**hardware rate-limiter span** コマンドで行えます。スーパーバイザの SPAN コピーの分析は、**ethanalyzer local interface inband mirror detail** コマンドで行えます。
- 次の Cisco Nexus スイッチは、sFlow と SPAN を同時にサポートします。
 - Cisco Nexus 9336C-FX2
 - Cisco Nexus 93240YC-FX2

- Cisco Nexus 93360YC-FX2
- Cisco NX-OS リリース 9.3(3) 以降、Cisco Nexus 9300-GX プラットフォーム スイッチは、sFlow と SPAN の両方をサポートしています。

Cisco Nexus 9500 プラットフォーム スイッチの SPAN の制限事項



(注) スケールの情報については、リリース特定の『Cisco Nexus 9000 Series NX-OS Verified Scalability Guide』を参照してください。

次の注意事項と制約事項は、Cisco Nexus 9500 プラットフォーム スイッチにのみ適用されます。

- 次のフィルタリング制限は、EX または FX ラインカードを搭載した 9500 プラットフォーム スイッチの出力 (Tx) SPAN に適用されます。
 - ACL フィルタリングはサポートされていません (ユニキャストおよびブロードキャスト、不明なユニキャストおよびマルチキャスト (BUM) トラフィックの両方に適用されます)
 - VLAN フィルタリングはサポートされますが、ユニキャスト トラフィックのみ
 - VLAN フィルタリングは BUM トラフィックではサポートされません。
- FEX および SPAN ポート チャンネルの宛先は、EX または FX ラインカードを備えた Cisco Nexus 9500 プラットフォーム スイッチではサポートされません。
- EX/FX モジュールを搭載した Cisco Nexus 9500 プラットフォーム スイッチでは、SPAN と sFlow の両方を同時に有効にすることはできません。一方がアクティブな場合、もう一方は有効にできません。ただし、EX または FX ラインカードを備えた Cisco Nexus 9500 プラットフォーム スイッチでは、NetFlow と SPAN の両方を同時に有効にすることができ、sFlow と SPAN を使用する代わりに実行可能です。
- Cisco Nexus 9500 プラットフォーム スイッチは、次のラインカードを備えた VLAN Tx SPAN をサポートします。
 - Cisco Nexus 97160YC-EX
 - Cisco Nexus 9732C-EX
 - Cisco Nexus 9732C-FX
 - Cisco Nexus 9736C-EX
 - Cisco Nexus 9736C-FX
 - Cisco Nexus 9736Q-FX
 - Cisco Nexus 9788TC-FX

- Cisco Nexus 9500 プラットフォーム スイッチは、同じソースに対する複数の ACL フィルタをサポートします。
- CPU で生成されたパケットの Tx SPAN は、EX ベースのライン カードを搭載した Cisco Nexus 9500 プラットフォーム スイッチではサポートされません。
- TCAM カービングは、次のライン カードの SPAN/ERSPAN には必要ありません。
 - Cisco Nexus 9636C-R
 - Cisco Nexus 9636Q-R
 - Cisco Nexus 9636C-RX
 - Cisco Nexus 96136YC-R



(注) SPAN/ERSPAN をサポートする他のすべてのスイッチは、TCAM カービングを使用する必要があります。

- Cisco Nexus 9500 プラットフォーム スイッチでは、SPAN 送信元の転送エンジン インスタンス マッピングに応じて、単一の転送エンジン インスタンスが 4 つの SPAN セッションをサポートする場合があります。このガイドラインは、9636C-R および 9636Q-R ライン カードを搭載した Cisco Nexus 9508 スイッチには適用されません。
- 複数の ACL フィルタは、同じ送信元ではサポートされません。
- Cisco Nexus 9500 プラットフォーム スイッチは、スイッチと FEX を通過する既知のレイヤ 2 ユニキャストトラフィックフローに対してのみ、すべてのトラフィックの入力方向と出力方向の SPAN 送信元として FEX ポートをサポートします。ルーティングされたトラフィックが FEX HIF 出力 SPAN で表示されないことがあります。
- SPAN は、Cisco Nexus 9408PC-CFP2 ライン カード ポートの宛先をサポートしません。
- 切り捨ては、9700-EX または 9700-FX ライン カードを搭載した Cisco Nexus 9500 プラットフォーム スイッチでサポートされます。
- VLAN は、9636C-R および 9636Q-R ライン カードを備えた Cisco Nexus 9508 スイッチの入力および出力方向の SPAN 送信元にできます。
- UDF-SPAN acl-filtering は送信元インターフェイス rx のみをサポートします。この制限は、次のライン カードに適用されます。
 - Cisco Nexus 9564PX
 - Cisco Nexus 9464TX2
 - Cisco Nexus 9464TX
 - Cisco Nexus 9464TX2
 - Cisco Nexus 9564TX
 - Cisco Nexus 9464PX

- Cisco Nexus 9536PQ
- Cisco Nexus 9636PQ
- Cisco Nexus 9432PQ

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

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。



Note 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せん。

Before you begin

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する必要があります。詳細については、『Cisco Nexus 9000 シリーズ NX-OS インターフェイス設定ガイド』を参照してください。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: 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

	Command or Action	Purpose
ステップ 2	interface <i>ethernet slot/port</i> Example: 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 Example: 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	switchport monitor Example: 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。
ステップ 5	(Optional) ステップ 2 ~ 4 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。	—
ステップ 6	no monitor session <i>session-number</i> Example: 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 7	monitor session <i>session-number</i> [rx tx] [shut] Example: switch(config) # monitor session 3 rx switch(config-monitor) # Example: switch(config) # monitor session 3 tx switch(config-monitor) # Example: 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 8	description <i>description</i> Example: 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 9	source { interface <i>type</i> [rx tx both] [vlan { <i>number</i> <i>range</i> } [rx]] [vsan { <i>number</i> <i>range</i> } [rx]] } Example:	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。一定範囲のイーサネットポート、ポートチャネル、インバンドインターフェイス

	Command or Action	Purpose
	<pre>switch(config-monitor)# source interface ethernet 2/1-3, ethernet 3/1 rx</pre> <p>Example:</p> <pre>switch(config-monitor)# source interface port-channel 2</pre> <p>Example:</p> <pre>switch(config-monitor)# source interface sup-eth 0 rx</pre> <p>Example:</p> <pre>switch(config-monitor)# source vlan 3, 6-8 rx</pre> <p>Example:</p> <pre>switch(config-monitor)# source interface ethernet 101/1/1-3</pre>	<p>ス、一定範囲の VLAN、または Cisco Nexus 2000 シリーズファブリック エクステンダ (FEX) 上のサテライトポートまたはホストインターフェイスポートチャンネルを入力できます。</p> <p>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。</p> <p>コピーするトラフィックの方向は、受信 (rx)、送信 (tx)、または両方 (both) を設定できます。</p> <p>Note 送信元 VLAN は、入力方向でのみサポートされます。送信元 FEX ポートは、すべてのトラフィックに対して入力方向でサポートされ、既知のレイヤ 2 ユニキャストトラフィックには出力方向のみがサポートされます。</p> <p>この注意事項は、Cisco Nexus EX/-FX/-FX2/-GX シリーズプラットフォームスイッチ、および -EX/-FX ラインカードを備えた Cisco Nexus 9500 シリーズプラットフォームスイッチには適用されません。</p> <p>送信元としてのスーパーバイザは、Rx 方向でのみサポートされます。</p> <p>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。</p>
ステップ 10	(Optional) ステップ 9 を繰り返して、すべての SPAN 送信元を設定します。	
ステップ 11	<p>filter vlan {<i>number</i> <i>range</i>}</p> <p>Example:</p> <pre>switch(config-monitor)# filter vlan 3-5, 7</pre>	<p>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</p>

	Command or Action	Purpose
		<p>として、複数設定することもできます。</p> <p>Note SPAN 送信元として設定された FEX ポートは VLAN フィルタをサポートしません。</p>
ステップ 12	(Optional) ステップ 11 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。	
ステップ 13	<p>(Optional) filter access-group <i>acl-filter</i></p> <p>Example:</p> <pre>switch(config-monitor)# filter access-group ACL1</pre>	ACL を SPAN セッションにアソシエートします。
ステップ 14	<p>Required: destination interface <i>type slot/port</i></p> <p>Example:</p> <pre>switch(config-monitor)# destination interface ethernet 2/5</pre> <p>Example:</p> <pre>switch(config-monitor)# destination interface sup-eth 0</pre>	<p>コピーする送信元パケットの宛先を設定します。</p> <p>Note 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。</p> <p>Note 宛先ポートでモニタモードを有効にする必要があります。</p> <p>次のプラットフォーム スイッチの SPAN 宛先として CPU を設定できます。</p> <ul style="list-style-type: none"> • Cisco Nexus 9200 シリーズ スイッチ (Cisco NX-OS リリース 7.0(3)I4(1) 以降) • Cisco Nexus 9300-EX シリーズ スイッチ (Cisco NX-OS リリース 7.0(3)I4(2) 以降) • Cisco Nexus 9300-FX シリーズ スイッチ (Cisco NX-OS リリース 7.0(3)I7(1) 以降) • Cisco Nexus 9300-FX2 シリーズ スイッチ (Cisco NX-OS リリース 7.0(3)I7(3) 以降)

	Command or Action	Purpose
		<ul style="list-style-type: none"> • Cisco Nexus 9300-GX シリーズ スイッチ (Cisco NX-OS リリース 9.3(3) 以降) • -EX/FX ライン カード搭載の Cisco Nexus 9500-EX シリーズ スイッチ <p>これを行うには、インターフェイス タイプに sup-eth 0 を入力します。</p>
ステップ 15	<p>Required: no shut</p> <p>Example:</p> <pre>switch(config-monitor)# no shut</pre>	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 16	<p>(Optional) show monitor session {all session-number range session-range} [brief]</p> <p>Example:</p> <pre>switch(config-monitor)# show monitor session 3</pre>	SPAN 設定を表示します。
ステップ 17	<p>(Optional) copy running-config startup-config</p> <p>Example:</p> <pre>switch(config)# copy running-config startup-config</pre>	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。

UDF ベース SPAN の設定

外部または内部パケット フィールド (ヘッダまたはペイロード) のユーザ定義フィールド (UDF) で照合し、一致するパケットを SPAN 宛先に送信するようにデバイスを設定できます。そのように設定することで、ネットワークのパケットドロップを分析して、分離することができます。

始める前に

UDF ベース SPAN をイネーブルにするのに十分な空き領域を確保するために、**hardware access-list tcam region** コマンドを使用して適切な TCAM リージョン (racl、ifacl、または vacl) 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 9000 Series NX-OS Security Configuration Guide』の「Configuring ACL TCAM Region Sizes」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	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	udf udf-name offset-base offset length 例 : <pre>switch(config)# udf udf-x packet-start 12 1 switch(config)# udf udf-y header outer 13 20 2</pre>	次のように UDF を定義します。 <ul style="list-style-type: none"> • udf-name : UDF の名前を指定します。名前には最大 16 文字の英数字を入力できます。 • offset-base : UDF オフセットベースを以下のように指定します。ここで header は、オフセットのために考慮に入れるべきパケット ヘッダーです : packet-start header {outer inner {13 14}}. • オフセット : オフセット ベースからのオフセット バイト数を指定します。オフセット ベース (レイヤ 3/レイヤ 4 ヘッダー) の最初のバイトを照合するには、オフセットを 0 に設定します。 • 長さ : オフセット からバイトの数を指定します。1 または 2 バイトのみがサポートされています。追加のバイトに一致させるためには、複数の UDF を定義する必要があります。 複数の UDF を定義できますが、シスコは必要な UDF のみ定義することを推奨します。
ステップ 3	hardware access-list tcam region {racl ifacl vacl } qualify qualifier-name 例 : <pre>switch(config)# hardware access-list tcam region racl qualify ing-13-span-filter</pre>	次のいずれかの TCAM リージョンに UDF を付加します。 <ul style="list-style-type: none"> • racl : レイヤ 3 ポートに適用されます。 • ifacl : レイヤ 2 ポートに適用します。 • vacl : 送信元 VLAN に適用します。

	コマンドまたはアクション	目的
		<p>UDF は TCAM リージョンに最大 8 個まで付加できます。</p> <p>(注) UDF 修飾子が追加されると、TCAM リージョンはシングル幅から倍幅に拡大します。十分な空きスペースがあることを確認してください。それ以外の場合このコマンドは拒否されます。必要な場合、未使用のリージョンから TCAM スペースが減りますので、このコマンドを再入力します。詳細については『Cisco Nexus 9000 Series NX-OS Security Configuration Guide』の「Configuring ACL TCAM Region Sizes」の項を参照してください。</p> <p>(注) このコマンドの no 形式は、UDF を TCAM リージョンから切り離し、リージョンをシングル幅に戻します。</p>
ステップ 4	<p>必須: copy running-config startup-config</p> <p>例 :</p> <pre>switch(config)# copy running-config startup-config</pre>	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。
ステップ 5	<p>必須: reload</p> <p>例 :</p> <pre>switch(config)# reload</pre>	<p>デバイスがリロードされます。</p> <p>(注) UDF 設定は copy running-config startup-config + reload を入力した後のみ有効になります。</p>
ステップ 6	<p>ip access-list span-acl</p> <p>例 :</p> <pre>switch(config)# ip access-list span-acl-udf-only switch(config-acl)#</pre>	IPv4 アクセス コントロール リスト (ACL) を作成して、IP アクセス リスト コンフィギュレーション モードを開始します。
ステップ 7	<p>次のいずれかのコマンドを入力します。</p> <ul style="list-style-type: none"> • permit udf udf-name value mask 	ACL を設定し、UDF (例 1) でのみ、または外部パケット フィールドについて

	コマンドまたはアクション	目的
	<ul style="list-style-type: none"> • permit ip source destination udf udf-name value mask 例 : <pre>switch(config-acl)# permit udf udf-x 0x40 0xF0 udf-y 0x1001 0xF00F</pre> 例 : <pre>switch(config-acl)# permit ip 10.0.0./24 any udf udf-x 0x02 0x0F udf-y 0x1001 0xF00F</pre>	現在のアクセス コントロール エントリ (ACE) と併せて UDF で一致させるように設定します (例 2) シングル ACL は、UDFがある場合とない場合の両方とも、ACE を有することができます。各 ACE には一致する異なる UDF フィールドがあるか、すべての ACE を UDF の同じリストに一致させることができます。
ステップ 8	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	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 切り捨ての設定

切り捨ては、ローカルおよび SPAN 送信元セッションに対してのみ設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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 : <pre>switch(config)# monitor session 5 switch(config-monitor)#</pre>	指定した SPAN セッションのモニタ コンフィギュレーション モードを開始します。
ステップ 3	source interface type slot/port [rx tx both] 例 : <pre>switch(config-monitor)# source interface ethernet 1/5 both</pre>	送信元インターフェイスを設定します。
ステップ 4	mtu size 例 : <pre>switch(config-monitor)# mtu 320</pre> 例 :	MTU の切り捨てサイズを設定します。設定された MTU 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。SPAN パケッ

	コマンドまたはアクション	目的
	<pre>switch(config-monitor)# mtu ? <320-1518> Enter the value of MTU truncation size for SPAN packets</pre>	<p>ト切り捨ての MTU 範囲は次のとおりです。</p> <ul style="list-style-type: none"> • Cisco Nexus 9300-EX プラットフォームスイッチの MTU サイズの範囲は、320～1518 バイトです。 • Cisco Nexus 9300-FX プラットフォームスイッチの MTU サイズの範囲は 64～1518 バイトです。 • 9700-EX および 9700-FX ラインカードを搭載した Cisco Nexus 9500 プラットフォームスイッチの場合、MTU サイズの範囲は 320～1518 バイトです。
ステップ 5	<p>destination interface type slot/port</p> <p>例 :</p> <pre>switch(config-monitor)# destination interface Ethernet 1/39</pre>	イーサネット SPAN 宛先ポートを設定します。
ステップ 6	<p>no shut</p> <p>例 :</p> <pre>switch(config-monitor)# no shut</pre>	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	<p>(任意) show monitor session session</p> <p>例 :</p> <pre>switch(config-monitor)# show monitor session 5</pre>	SPAN 設定を表示します。
ステップ 8	<p>copy running-config startup-config</p> <p>例 :</p> <pre>switch(config-monitor)# copy running-config startup-config</pre>	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。

異なる LSE スライス間のマルチキャスト Tx トラフィックの SPAN の設定

Cisco NX-OS Release 7.0(3)I7(1) 以降では、Cisco Nexus 9300-EX プラットフォームスイッチ上の異なるリーフスパインエンジン (LSE) スライス間で、マルチキャスト Tx トラフィックの SPAN 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)#	グローバル設定モードを開始します。
ステップ 2	[no] hardware multicast global-tx-span 例： switch(config)# hardware multicast global-tx-span	異なるリーフスパインエンジン (LSE) スライス間のマルチキャスト Tx トラフィックの SPAN を設定します。
ステップ 3	copy running-config startup-config 例： switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。
ステップ 4	reload 例： switch(config)# reload	デバイスがリロードされます。

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、別のセッションを有効にできます。デフォルトでは、SPAN セッションはシャット状態で作成されます。

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状態およびイネーブル状態は、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。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: 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

	Command or Action	Purpose
ステップ 2	<p>[no] monitor session {session-range all} shut</p> <p>Example:</p> <pre>switch(config)# monitor session 3 shut</pre>	<p>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状態で作成されます。</p> <p>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状態で作成されます。</p> <p>Note モニタセッションが有効で動作状況がダウンの場合、セッションを有効にするには、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。</p>
ステップ 3	<p>monitor session session-number</p> <p>Example:</p> <pre>switch(config)# monitor session 3 switch(config-monitor)#</pre>	<p>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。</p>
ステップ 4	<p>[no] shut</p> <p>Example:</p> <pre>switch(config-monitor)# shut</pre>	<p>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状態で作成されます。</p> <p>コマンドの no 形式は SPAN セッションを有効にします。デフォルトでは、セッションはシャット状態で作成されます。</p>
ステップ 5	<p>(Optional) show monitor</p> <p>Example:</p> <pre>switch(config-monitor)# show monitor</pre>	<p>SPAN セッションのステータスを表示します。</p>
ステップ 6	<p>(Optional) copy running-config startup-config</p> <p>Example:</p> <pre>switch(config)# copy running-config startup-config</pre>	<p>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。</p>

SPAN 設定の確認

SPAN 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
<code>show monitor session {all session-number range session-range} [brief]</code>	SPAN セッション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
```

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
```

SPAN ACL の設定例

次に、SPAN 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 span_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 span_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
switch(config-erspan-src)# filter access_group span_filter
```

UDF ベース SPAN の設定例

次に、以下の一致基準を使用して、カプセル化された IP-in-IP パケットの内部 TCP フラグで照合する UDF ベース SPAN を設定する例を示します。

- 外部送信元 IP アドレス : 10.0.0.2
- 内部 TCP フラグ : 緊急 TCP フラグを設定
- バイト : Eth Hdr (14) + 外部 IP (20) + 内部 IP (20) + 内部 TCP (20、ただし、13 番目のバイトの TCP フラグ)
- パケットの先頭からのオフセット : $14 + 20 + 20 + 13 = 67$
- UDF の照合値 : 0x20
- UDF マスク : 0xFF

```

udf udf_tcpflags packet-start 67 1
hardware access-list tcam region racl qualify ing-13-span-filter
copy running-config startup-config
reload
ip access-list acl-udf
permit ip 10.0.0.2/32 any udf udf_tcpflags 0x20 0xff
monitor session 1
source interface Ethernet 1/1
filter access-group acl-udf

```

次に、以下の一致基準を使用して、レイヤ 4 ヘッダーの先頭から 6 バイト目のパケット署名 (DEADBEEF) と通常の IP パケットを照合する UDF ベース SPAN を設定する例を示します。

- 外部送信元 IP アドレス : 10.0.0.2
- 内部 TCP フラグ : 緊急 TCP フラグを設定
- バイト : Eth Hdr (14) + IP (20) + TCP (20) + ペイロード : 112233445566DEADBEEF7788
- レイヤ 4 ヘッダーの先頭からのオフセット : $20 + 6 = 26$
- UDF の照合値 : 0xDEADBEEF (2 バイトのチャンクおよび 2 つの UDF に分割)
- UDF マスク : 0xFFFFFFFF

```

udf udf_pktsig_msb header outer 14 26 2
udf udf_pktsig_lsb header outer 14 28 2
hardware access-list tcam region racl qualify ing-13-span-filter
copy running-config startup-config
reload
ip access-list acl-udf-pktsig
permit udf udf_pktsig_msb 0xDEAD 0xFFFF udf udf_pktsig_lsb 0xBEEF 0xFFFF
monitor session 1
source interface Ethernet 1/1
filter access-group acl-udf-pktsig

```

SPAN 切り捨ての設定例

この例では、MPLS ストリッピングで使用する SPAN 切り捨てを設定する方法を示します。

```

mpls strip
ip access-list mpls
statistics per-entry
20 permit ip any any redirect Ethernet1/5
interface Ethernet1/5

```

```

switchport
switchport mode trunk
mtu 9216
no shutdown
monitor session 1
source interface Ethernet1/5 tx
mtu 64
destination interface Ethernet1/6
no shut

```

LSE スライス間のマルチキャスト Tx SPAN の設定例

次に、Cisco Nexus 9300-EX プラットフォームスイッチの LSE スライス間でマルチキャスト Tx SPAN を設定する例を示します。また、マルチキャスト Tx SPAN の設定前後の出力例を示します。

マルチキャスト Tx SPAN の設定前

```
switch# show interface eth1/15-16, ethernet 1/27 counters
```

```

-----
Port                InOctets           InUcastPkts
-----
Eth1/15              580928              0
Eth1/16                239                 0
Eth1/27                0                   0

```

```

-----
Port                InMcastPkts        InBcastPkts
-----
Eth1/15              9077                0
Eth1/16                1                   0
Eth1/27                0                   0

```

```

-----
Port                OutOctets           OutUcastPkts
-----
Eth1/15              453                  0
Eth1/16             581317                0
Eth1/27                0                   0

```

```

-----
Port                OutMcastPkts        OutBcastPkts
-----
Eth1/15                4                   0
Eth1/16             9080                   0
Eth1/27                0                   0

```

マルチキャスト Tx SPAN の設定

```

switch(config)# hardware multicast global-tx-span
Warning: Global Tx SPAN setting changed, please save config and reload
switch(config)# copy running-config start-up config
[#####] 100%
Copy complete.
switch(config)# reload
This command will reboot the system. (y/n)? [n] y

```

マルチキャスト Tx SPAN の設定後

```
switch# show interface eth1/15-16, eth1/27 counters
```

```
-----
Port           InOctets      InUcastPkts
-----
Eth1/15        392576        0
Eth1/16         0             0
Eth1/27         0             0
-----
Port           InMcastPkts   InBcastPkts
-----
Eth1/15         6134          0
Eth1/16         0             0
Eth1/27         0             0
-----
Port           OutOctets      OutUcastPkts
-----
Eth1/15         0             0
Eth1/16        392644        0
Eth1/27        417112        0
-----
Port           OutMcastPkts   OutBcastPkts
-----
Eth1/15         0             0
Eth1/16         6135          0
Eth1/27         6134          0
```

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
ACL TCAM リージョン	『Cisco Nexus 9000 Series NX-OS Security Configuration Guide』
FEX	『Cisco Nexus 2000 Series NX-OS Fabric Extender Software Configuration Guide for Cisco Nexus 9000 Series Switches』



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。

- [ERSPAN について \(323 ページ\)](#)
- [ERSPAN の前提条件 \(325 ページ\)](#)
- [ERSPAN の注意事項および制約事項 \(325 ページ\)](#)
- [デフォルト設定 \(329 ページ\)](#)
- [ERSPAN の設定 \(329 ページ\)](#)
- [ERSPAN 設定の確認 \(345 ページ\)](#)
- [ERSPAN の設定例 \(346 ページ\)](#)

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。もう 1 つの方法は、パケットを解析して内部 (SPAN コピー) フレームにアクセスするために、ERSPAN カプセル化形式を理解する必要があるアナライザ自体を宛先とする方法です。

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 (ただしサブインターフェイスではない)
- 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。



- (注) 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 CPU により送信されたすべてのパケットをモニタします。



- (注) スーパーバイザインバンドインターフェイスを SPAN 送信元として使用する場合、スーパーバイザハードウェア（出力）によって生成されたすべてのパケットがモニタされます。

Rx は ASIC の観点から見たものです（トラフィックはインバンドを介してスーパーバイザから出力され、ASIC / SPAN で受信されます）。

• VLAN

- 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。
- VLAN は、Cisco Nexus 9300-EX/-FX/-FX2/-GX シリーズプラットフォームスイッチおよび -EX/-FX ラインカードを備えた Cisco Nexus 9500 シリーズプラットフォームスイッチを除き、入力方向でのみ ERSPAN 送信元にすることができます。



- (注) 1 つの ERSPAN セッションに、上述の送信元を組み合わせで使用できます。

ERSPAN の宛先

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。宛先ポートは、リモートモニタリング (RMON) プロンプなどのデバイス、あるいはコピーされたパケットを 1 つまたは複数の送信元ポートから受信したり、解析することができるセキュリティデバイスに接続されたポートです。宛先ポートはスパン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。

Cisco Nexus 9200、9300-EX、9300-FX、および 9300-FX2 プラットフォームスイッチは、GRE ヘッダートラフィックフローを使用して、スイッチポートモードの物理インターフェイスまたはポートチャンネルインターフェイスで設定された ERSPAN 宛先セッションをサポートします。送信元 IP アドレスは、デフォルト VRF で設定する必要があります。複数の ERSPAN 宛先セッションを同じ送信元 IP アドレスで設定する必要があります。

ERSPAN セッション

モニタする送信元を指定する ERSPAN セッションを作成できます。

ローカライズされた ERSPAN セッション

すべての送信元インターフェイスが同じラインカード上にある場合、ERSPAN セッションはローカライズされます。



(注) VLAN 送信元の ERSPAN セッションはローカライズされません

ERSPAN の切り捨て

Cisco NX-OS Release 7.0(3)I7(1) 以降では、MTU のサイズに基づいて各 ERSPAN セッションの送信元パケットの切り捨てを設定できます。切り捨てにより、モニタするパケットのサイズを減らすことで、ERSPAN の帯域幅を効果的に軽減できます。設定された MTU 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。ERSPAN では、ERSPAN ヘッダータイプに応じて、切り捨てられたパケットに 54 – 166 バイトの ERSPAN ヘッダーが追加されます。たとえば、MTU を 300 バイトに設定すると、ERSPAN ヘッダータイプの設定に応じて、パケットは 354 – 466 バイトの ERSPAN ヘッダーサイズで複製されません。

ERSPAN 切り捨てはデフォルトでは無効です。切り捨てを使用するには、個々の ERSPAN セッションで有効にしておく必要があります。

ERSPAN の前提条件

ERSPAN 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 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 9000 シリーズ NX-OS インターフェイス設定ガイド』を参照してください。

ERSPAN の注意事項および制約事項



(注) スケールの情報については、リリース特定の『Cisco Nexus 9000 Series NX-OS Verified Scalability Guide』を参照してください。

ERSPAN 設定時の注意事項と制限事項は次のとおりです。

- ERSPAN 宛先は、プラットフォームに基づいて MTU のジャンボフレームを異なる方法で処理します。次の Cisco Nexus 9300 プラットフォームスイッチおよびサポートラインカードを備えた Cisco Nexus 9500 プラットフォームスイッチの場合、ERSPAN 宛先はジャンボフレームをドロップします。

- Cisco Nexus 9332PQ
- Cisco Nexus 9372PX
- Cisco Nexus 9372PX-E
- Cisco Nexus 9372TX
- Cisco Nexus 9372TX-E
- Cisco Nexus 93120TX
- 次のライン カードを備えた Cisco Nexus 9500 プラットフォーム スイッチ
 - Cisco Nexus 9564PX
 - Cisco Nexus 9464TX
 - Cisco Nexus 9464TX2
 - Cisco Nexus 9564TX
 - Cisco Nexus 9464PX
 - Cisco Nexus 9536PQ
 - Cisco Nexus 9636PQ
 - Cisco Nexus 9432PQ

次の Cisco Nexus 9200 プラットフォーム スイッチおよびサポート ライン カードを備えた Cisco Nexus 9500 プラットフォーム スイッチの場合、ERSPAN はポート MTU でパケットを切り捨て、TX 出力エラーを発行します。

- Cisco Nexus 92160YC-X
- Cisco Nexus 92304QC
- Cisco Nexus 9272Q
- Cisco Nexus 9232C
- Cisco Nexus 9236C
- Cisco Nexus 92300YC
- Cisco Nexus 93108TC-EX
- Cisco Nexus 93180LC-EX
- Cisco Nexus 93180YC-EX
- 次のライン カードを備えた Cisco Nexus 9500 プラットフォーム スイッチ
 - Cisco Nexus 9736C-EX
 - Cisco Nexus 97160YC-EX
 - Cisco Nexus 9732C-EX
 - Cisco Nexus 9732C-EXM

- タイプ 3 ヘッダをもつ ERSPAN は、Cisco NX-OS リリース 9.3(3) ではサポートされません。
- ERSPAN セッションの制限については、『Cisco Nexus 9000 シリーズ NX-OS 検証スケーラビリティ ガイド』を参照してください。
- ラインカードごとの ERSPAN セッションの数は、同じインターフェイスが複数セッションの双方向送信元として設定されている場合は、2 に減少します。
- 同じ送信元インターフェイスで 2 つの SPAN または ERSPAN セッションを 1 つのフィルタだけで設定することはできません。同じ送信元が複数の SPAN または ERSPAN セッションで使用されている場合は、すべてのセッションに異なるフィルタを設定するか、セッションにフィルタを設定しないでください。
- FCS エラーがあるパケットは、ERSPAN セッションでミラーリングされません。
- TCAM カービングは、次のライン カードの SPAN/ERSPAN には必要ありません。
 - Cisco Nexus 9636C-R
 - Cisco Nexus 9636Q-R
 - Cisco Nexus 9636C-RX
 - Cisco Nexus 96136YC-R



(注) SPAN/ERSPAN をサポートする他のすべてのスイッチは、TCAM カービングを使用する必要があります。

- フィルタ アクセス グループの統計情報はサポートされていません。
- ERSPAN セッションのアクセス グループフィルタは、vlan-accessmap として設定する必要があります。
- スーパーバイザによって生成されたコントロールプレーン パケットは、ERSPAN カプセル化または ERSPAN アクセス コントロール リスト (ACL) によるフィルタ処理をすることはできません。
- ERSPAN は、管理ポートではサポートされません。
- ERSPAN は、レイヤ 3 ポート チャネル サブインターフェイスの宛先をサポートしません。
- 送信元としての VLAN は、R シリーズ ライン カードおよび N3K-C36180YC-R、N3KC36480LD-R2、および N3K-C3636C-R プラットフォーム スイッチの ERSPAN 設定ではサポートされません。
- VLAN は、ERSPAN 送信元またはフィルタとして使用される場合、属することができるのは 1 つのセッションだけです。
- VLAN ERSPAN がモニタするのは、VLAN のレイヤ 2 ポートを出入りするトラフィックだけです。

- 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されなければならない場合は、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。
- ERSPAN は、VXLAN オーバーレイではサポートされません。
- マルチキャストパケットの ERSPAN コピーは、書き換え前に作成されます。したがって、TTL、VLANID、出力ポリシーによる再マーキングなどは ERSPAN コピーにキャプチャされません。
- ERSPAN タイプ III セッションのタイムスタンプの粒度は、CLI では設定できません。100 ピコ秒で、PTP を介して駆動されます。
- ERSPAN はデフォルトおよびデフォルト以外の VRF で動作しますが、ERSPAN マーカーパケットはデフォルト VRF でのみ動作します。
- 同じ送信元は、複数のセッションの一部にすることができます。

次の注意事項と制約事項が (Tx) ERSPAN に適用されます。

- 不明ユニキャストでフラッディングされたパケットのルーティング後のフローは ERSPAN セッションに置かれますが、これはフローが転送されるポートをモニタしないよう ERSPAN セッションが設定されている場合であっても同様です。この制限は、ネットワーク フォワーディング エンジン (NFE) と NFE2 対応 EOR スイッチおよび ERSPAN セッションで Tx ポートの送信元を持つものに適用されます。
- 次の注意事項と制約事項が (Rx) ERSPAN に適用されます。
 - VLAN 送信元は Rx 方向のみがサポートされます。
 - セッションフィルタリング機能 (VLAN または ACL フィルタ) は、Rx 送信元でのみサポートされます。
 - VLAN は、ERSPAN 送信元として入力方向でのみサポートされます。
- 次の注意事項および制約事項が FEX ポートに適用されます。
 - 双方向 ERSPAN セッションで使用される送信元が同じ FEX からのものである場合、ハードウェア リソースは 2 つの ERSPAN セッションに制限されます。
 - FEX ポートは、ERSPAN としてすべてのトラフィックに対して入力方向でサポートされ、既知のレイヤ 2 ユニキャスト トラフィックには出力方向のみがサポートされます。
 - Cisco Nexus 9300 プラットフォーム スイッチは、FEX インターフェイスに接続されている ERSPAN 宛先をサポートしていません。ERSPAN 宛先は、前面パネル ポートに接続する必要があります。
 - VLAN および ACL フィルタは FEX ポートではサポートされません。フィルタとは共存できません。
- プライオリティフロー制御 (PFC) ERSPAN には、次の制約事項と制約事項があります。

- フィルタとは共存できません。
- 物理または port-channel インターフェイスの Rx 方向でのみサポートされています。VLAN インターフェイスの Rx 方向、または Tx 方向ではサポートされていません。
- ERSPAN 宛先には、次の注意事項と制約事項が適用されます。
 - Cisco Nexus 9200、9300-EX、9300-FX、および 9300-FX2 プラットフォーム スイッチは、GRE ヘッダー トラフィック フローを使用して、スイッチポートモードの物理インターフェイスまたはポートチャネルインターフェイスで設定された ERSPAN 宛先セッションをサポートします。
 - ERSPAN 宛先は、Cisco Nexus 9200、9300、9300-EX、9300-FX、および 9300-FX2 プラットフォーム スイッチの MPLS や VXLAN などの他のトンネル機能と共存できません。
 - ERSPAN 宛先セッションは、デフォルトの VRF のみをサポートします。
 - Cisco Nexus 9300-EX/FX スイッチは、Cisco Nexus 3000 および非 EX/FX Cisco Nexus 9000 スイッチの ERSPAN 宛先として機能できません。

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 20: デフォルトの **ERSPAN** パラメータ

パラメータ	デフォルト
ERSPAN セッション	シャット ステートで作成されます
ERSPAN マーカー パケット間隔	100 ミリ秒
ERSPAN タイプ III セッションのタイムスタンプの粒度	100 ピコ秒

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。



(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	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 erspan origin ip-address ip-address global 例： switch(config)# monitor erspan origin ip-address 10.0.0.1 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	no monitor session {session-number all} 例： switch(config)# no monitor session 3	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	monitor session {session-number all} type erspan-source [shut] 例： switch(config)# monitor session 3 type erspan-source switch(config-erspan-src)#	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	description description 例： switch(config-erspan-src)# description erspan_src_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 6	source {interface type [tx rx both] vlan {number range} [rx]} 例：	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。一定範囲のイーサネットポート、ポートチャネル、インバンドインターフェイ

	コマンドまたはアクション	目的
	<pre>switch(config-erspan-src)# source interface ethernet 2/1-3, ethernet 3/1 rx</pre> <p>例 :</p> <pre>switch(config-erspan-src)# source interface port-channel 2</pre> <p>例 :</p> <pre>switch(config-erspan-src)# source interface sup-eth 0 rx</pre> <p>例 :</p> <pre>switch(config-erspan-src)# source vlan 3, 6-8 rx</pre> <p>例 :</p> <pre>switch(config-erspan-src)# source interface ethernet 101/1/1-3</pre>	<p>ス、または一定範囲の VLAN、または Cisco Nexus 2000 シリーズ ファブリック エクステンダ (FEX) 上のサテライトポートまたはホストインターフェイスポートチャンネルを入力できます。</p> <p>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。</p> <p>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。</p> <p>(注) 送信元 VLAN は、入力方向でのみサポートされます。送信元 FEX ポートは、すべてのトラフィックに対して入力方向でサポートされ、既知のレイヤ 2 ユニキャストトラフィックには出力方向のみがサポートされます。</p> <p>送信元としてのスーパーバイザは、Rx 方向でのみサポートされます。</p>
ステップ 7	(任意) ステップ 7 を繰り返して、すべての ERSPAN 送信元を設定します。	—
ステップ 8	<pre>filter vlan {number range}</pre> <p>例 :</p> <pre>switch(config-erspan-src)# filter vlan 3-5, 7</pre>	<p>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 9000 シリーズ NX-OS レイヤ 2 スイッチング設定ガイド』を参照してください。</p> <p>(注) ERSPAN 送信元として設定された FEX ポートは VLAN フィルタをサポートしません。</p>

	コマンドまたはアクション	目的
ステップ 9	(任意) ステップ 9 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。	—
ステップ 10	filter access-group <i>acl-filter</i> 例： switch(config-erspan-src)# filter access-group ACL1 例：	ACL を ERSPAN セッションにアソシエートします。(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 9000 シリーズ NX-OS セキュリティ設定ガイド』を参照してください)。
ステップ 11	destination ip <i>ip-address</i> 例： switch(config-erspan-src)# destination ip 10.1.1.1	ERSPAN セッションの宛先 IP アドレスを設定します。 (注) 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	erspan-id <i>erspan-id</i> 例： switch(config-erspan-src)# erspan-id 5	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	vrf <i>vrf-name</i> 例： switch(config-erspan-src)# vrf default	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 名は、32 文字以内の英数字のストリング (大文字と小文字を区別) で指定します。
ステップ 14	(任意) ip ttl <i>ttl-number</i> 例： switch(config-erspan-src)# ip ttl 25	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	(任意) ip dscp <i>dscp-number</i> 例： switch(config-erspan-src)# ip dscp 42	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	(任意) [no] marker-packet <i>milliseconds</i> 例： switch(config-erspan-src)# marker-packet 100	ERSPAN タイムスタンプの実際の値を回復するために、セッションの ERSPAN マーカーパケットを有効にします。この間隔の範囲には、100 ~ 1000 マイクロ秒を設定できます。このコマンドの no 形式を使用すると、セッ

	コマンドまたはアクション	目的
		セッションのマーカークラッシュが無効になります。 (注) ERSPAN マーカークラッシュはタイプ3セッションにのみ適用されます。
ステップ 17	no shut 例： 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状態で作成されます。
ステップ 18	exit 例： switch(config-erspan-src)# exit switch(config)#	モニタ設定モードを閉じます。
ステップ 19	(任意) show monitor session {all session-number range session-range} [brief] 例： switch(config)# show monitor session 3	ERSPAN セッション設定を表示します。
ステップ 20	(任意) show running-config monitor 例： switch(config)# 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。
ステップ 21	(任意) show startup-config monitor 例： switch(config)# 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。
ステップ 22	(任意) copy running-config startup-config 例： switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

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

を有効にできます。デフォルトでは、ERSPAN セッションはシャット状態で作成されます。

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	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-range all} shut 例： switch(config)# monitor session 3 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状態で作成されます。
ステップ 3	no monitor session {session-range all} shut 例： switch(config)# no monitor session 3 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状態で作成されます。 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	monitor session session-number type erspan-source 例： switch(config)# monitor session 3 type erspan-source switch(config-erspan-src)#	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	shut 例： 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状態で作成されます。

	コマンドまたはアクション	目的
ステップ 6	no shut 例： 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	exit 例： switch(config-erspan-src)# exit switch(config)#	モニタ設定モードを閉じます。
ステップ 8	(任意) show monitor session all 例： switch(config)# show monitor session all	ERSPAN セッションのステータスを表示します。
ステップ 9	(任意) show running-config monitor 例： switch(config)# 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。
ステップ 10	(任意) show startup-config monitor 例： switch(config)# 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。
ステップ 11	(任意) copy running-config startup-config 例： switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

ERSPAN ACL の設定

デバイスに IPv4 ERSPAN ACL を作成して、ルールを追加できます。

始める前に

DSCP 値または GRE プロトコルを変更するには、新しい宛先モニタセッションを割り当てる必要があります。最大 4 つの宛先モニタセッションがサポートされます。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	ip access-list <i>acl-name</i> 例 : <pre>switch(config)# ip access-list erspan-acl switch(config-acl)#</pre>	ERSPAN ACL を作成して、IP ACL コンフィギュレーション モードを開始します。 <i>acl-name</i> 引数は 64 文字以内で指定します。
ステップ 3	[<i>sequence-number</i>] {permit deny} <i>protocol source destination</i> [set-erspan-dscp <i>dscp-value</i>] [set-erspan-gre-PROTO <i>protocol-value</i>] 例 : <pre>switch(config-acl)# permit ip 192.168.2.0/24 any set-erspan-dscp 40 set-erspan-gre-PROTO 5555</pre>	<p>ERSPAN ACL 内にルールを作成します。多数のルールを作成できます。<i>sequence-number</i> 引数には、1 ~ 4294967295 の整数を指定します。</p> <p>permit コマンドと deny コマンドには、トラフィックを識別するための多くの方法が用意されています。</p> <p>set-erspan-dscp オプションは、ERSPAN 外部 IP ヘッダーに DSCP 値を設定します。DSCP 値の範囲は 0 ~ 63 です。ERSPAN ACL に設定された DSCP 値で、モニタセッションに設定されている値が上書きされます。ERSPAN ACL にこのオプションを含めない場合、0 またはモニタセッションで設定されている DSCP 値が設定されます。</p> <p>set-erspan-gre-PROTO オプションは、ERSPAN GRE ヘッダーにプロトコル値を設定します。プロトコル値の範囲は 0 ~ 65535 です。ERSPAN ACL にこのオプションを含めない場合、ERSPAN カプセル化パケットの GRE ヘッダーのプロトコルとしてデフォルト値の 0x88be が設定されます。</p> <p>et-erspan-gre-PROTO または set-erspan-dscp アクションが設定されている各アクセス コントロール エントリ (ACE) は、1つの宛先モニタセッションを使用します。ERSPAN ACL ごとに、これらのアクションのいずれかが設定さ</p>

	コマンドまたはアクション	目的
		<p>れている最大3つの ACE がサポートされます。たとえば、次のいずれかを設定できます。</p> <ul style="list-style-type: none"> • set-erspan-gre-proto または set-erspan-dscp アクションが設定された最大3つの ACE を持つ ACL が設定されている、1つの ERSPAN セッション • set-erspan-gre-proto または set-erspan-dscp アクションが設定され、1つの追加のローカルまたは ERSPAN セッションが設定された2つの ACE を持つ ACL が設定されている、1つの ERSPAN セッション • set-erspan-gre-proto または set-erspan-dscp アクションが設定された1つの ACE を持つ ACL が設定されている、1つの ERSPAN セッション
ステップ 4	<p>(任意) show ip access-lists name</p> <p>例 :</p> <pre>switch(config-acl)# show ip access-lists erspan-acl</pre>	ERSPAN ACL の設定を表示します。
ステップ 5	<p>(任意) show monitor session {all session-number range session-range} [brief]</p> <p>例 :</p> <pre>switch(config-acl)# show monitor session 1</pre>	ERSPAN セッション設定を表示します。
ステップ 6	<p>(任意) copy running-config startup-config</p> <p>例 :</p> <pre>switch(config-acl)# copy running-config startup-config</pre>	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。

UDF ベース ERSPAN の設定

外部または内部パケット フィールド（ヘッダまたはペイロード）のユーザ定義フィールド（UDF）で照合し、一致するパケットを ERSPAN 宛先に送信するようにデバイスを設定できます。そのように設定することで、ネットワークのパケットドロップを分析して、分離することができます。

始める前に

UDF ベース ERSPAN をイネーブルにするのに十分な空き領域を確保するために、**hardware access-list tcam region** コマンドを使用して適切な TCAM リージョン（`racl`、`ifacl`、または `vacl`）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 9000 シリーズ NX-OS セキュリティ設定ガイドの『ACL TCAM リージョンサイズの設定』セクション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 : <pre>switch# configure terminal switch(config)#</pre>	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	udf udf-name offset-base offset length 例 : <pre>switch(config)# udf udf-x packet-start 12 1 switch(config)# udf udf-y header outer 13 20 2</pre>	次のように UDF を定義します。 <ul style="list-style-type: none"> • udf-name : UDF の名前を指定します。名前には最大 16 文字の英数字を入力できます。 • offset-base : UDF オフセットベースを以下のように指定します。ここで header は、オフセットのために考慮に入れるべきパケット ヘッダーです : packet-start header {outer inner {13 14}}. • オフセット : オフセットベースからのオフセット バイト数を指定します。オフセットベース（レイヤ 3/レイヤ 4 ヘッダー）の最初のバイトを照合するには、オフセットを 0 に設定します。 • 長さ : オフセット からバイトの数を指定します。1 または 2 バイトのみがサポートされています。追加のバイトに一致させるためには、複数

	コマンドまたはアクション	目的
		<p>の UDF を定義する必要があります。</p> <p>複数の UDF を定義できますが、シスコは必要な UDF のみ定義することを推奨します。</p>
<p>ステップ 3</p>	<p>hardware access-list tcam region {racl ifacl vacl } qualify udf udf-names</p> <p>例 :</p> <pre>switch(config)# hardware access-list tcam region racl qualify udf udf-x udf-y</pre>	<p>次のいずれかの TCAM リージョンに UDF を付加します。</p> <ul style="list-style-type: none"> • racl : レイヤ 3 ポートに適用します : レイヤ 2 および レイヤ 3 ポートに適用します。 • ifacl : レイヤ 2 ポートに適用します。 • vacl : 送信元 VLAN に適用します。 <p>UDF は TCAM リージョンに最大 8 個まで付加できます。</p> <p>(注) UDF 修飾子が追加されると、TCAM リージョンはシングル幅から倍幅に拡大します。十分な空きスペースがあることを確認してください。それ以外の場合このコマンドは拒否されます。必要な場合、未使用のリージョンから TCAM スペースが減りますので、このコマンドを再入力します。詳細については、Cisco Nexus 9000 シリーズ NX-OS セキュリティ設定ガイドの『ACL TCAM リージョンサイズの設定』セクションを参照してください。</p> <p>(注) このコマンドの no 形式は、UDF を TCAM リージョンから切り離し、リージョンをシングル幅に戻します。</p>
<p>ステップ 4</p>	<p>必須: copy running-config startup-config</p> <p>例 :</p>	<p>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</p>

	コマンドまたはアクション	目的
	<pre>switch(config)# copy running-config startup-config</pre>	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。
ステップ 5	<p>必須: reload</p> <p>例 :</p> <pre>switch(config)# reload</pre>	<p>デバイスがリロードされます。</p> <p>(注) UDF 設定は copy running-config startup-config + reload を入力した後のみ有効になります。</p>
ステップ 6	<p>ip access-list erspan-acl</p> <p>例 :</p> <pre>switch(config)# ip access-list erspan-acl-udf-only switch(config-acl)#</pre>	IPv4 アクセス コントロール リスト (ACL) を作成して、IP アクセス リスト コンフィギュレーション モードを開始します。
ステップ 7	<p>次のいずれかのコマンドを入力します。</p> <ul style="list-style-type: none"> • permit udf udf-name value mask • permit ip source destination udf udf-name value mask <p>例 :</p> <pre>switch(config-acl)# permit udf udf-x 0x40 0xF0 udf-y 0x1001 0xF00F</pre> <p>例 :</p> <pre>switch(config-acl)# permit ip 10.0.0./24 any udf udf-x 0x02 0x0F udf-y 0x1001 0xF00F</pre>	<p>ACL を設定し、UDF (例 1) でのみ、または外部パケット フィールドについて現在のアクセス コントロール エントリ (ACE) と併せて UDF で一致させるように設定します (例 2)</p> <p>シングル ACL は、UDF がある場合とない場合の両方とも、ACE を有することができます。各 ACE には一致する異なる UDF フィールドがあるか、すべての ACE を UDF の同じリストに一致させることができます。</p>
ステップ 8	<p>(任意) copy running-config startup-config</p> <p>例 :</p> <pre>switch(config)# copy running-config startup-config</pre>	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 切り捨ての設定

切り捨ては、ローカルおよび ERSPAN 送信元セッションに対してのみ設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	<p>configure terminal</p> <p>例 :</p>	グローバル設定モードを開始します。

	コマンドまたはアクション	目的
	switch# configure terminal switch(config)#	
ステップ 2	monitor session session-number type erspan-source 例： switch(config)# monitor session 10 type erspan-source switch(config-erspan-src)#	指定された ERSPAN セッションのモニタ設定モードに入ります。
ステップ 3	source interface type slot/port [rx tx both] 例： switch(config-erspan-src)# source interface ethernet 1/5 both	送信元インターフェイスを設定します。
ステップ 4	mtu size 例： switch(config-erspan-src)# mtu 512 例： switch(config-erspan-src)# mtu ? <512-1518> Enter the value of MTU truncation size for ERSPAN packets (erspan header + truncated original packet)	MTU の切り捨てサイズを設定します。 設定された MTU 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。ERSPAN パケットの切り捨ての MTU 範囲は次のとおりです。 <ul style="list-style-type: none"> • Cisco Nexus 9300-EX シリーズ スイッチの MTU サイズの範囲は 512～1518 バイトです。 • Cisco Nexus 9300-FX シリーズ スイッチの MTU サイズの範囲は 64～1518 バイトです。 • 9700-EX および 9700-FX ラインカードを搭載した Cisco Nexus 9500 プラットフォーム スイッチの場合、MTU サイズの範囲は 512～1518 バイトです。
ステップ 5	destination interface type slot/port 例： switch(config-erspan-src)# destination interface Ethernet 1/39	イーサネット ERSPAN 宛先ポートを設定します。
ステップ 6	no shut 例： 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状態で作成されます。
ステップ 7	(任意) show monitor session session 例：	ERSPAN の設定を表示します。

	コマンドまたはアクション	目的
	<code>switch(config-erspan-src)# show monitor session 5</code>	
ステップ 8	copy running-config startup-config 例 : <code>switch(config-erspan-src)# copy running-config startup-config</code>	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。

始める前に

スイッチポート 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。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <code>switch# configure terminal</code> <code>switch(config)#</code>	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 slot/port[-port] 例 : <code>switch(config)# interface ethernet 2/5</code> <code>switch(config-if)#</code>	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	switchport 例 : <code>switch(config-if)# switchport</code>	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] 例 : <code>switch(config-if)# switchport mode trunk</code>	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。 <ul style="list-style-type: none"> • アクセス • トランク

	コマンドまたはアクション	目的
ステップ 5	switchport monitor 例： 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。	—
ステップ 7	no monitor session {session-number all} 例： switch(config-if)# no monitor session 3	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	monitor session {session-number all} type erspan-destination 例： switch(config-if)# monitor session 3 type erspan-destination switch(config-erspan-dst)#	ERSPAN 宛先セッションを設定します。
ステップ 9	description description 例： switch(config-erspan-dst)# description erspan_dst_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 10	source ip ip-address 例： switch(config-erspan-dst)# source ip 10.1.1.1	ERSPAN セッションの宛先 IP アドレスを構成します。送信元 IP アドレスは、ローカルに構成された IP アドレスです。ERSPAN 宛先セッションの送信元 IP アドレスは、カプセル化されたデータの受信元である ERSPAN 送信元セッションで構成された宛先 IP アドレスと一致する必要があります。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 11	destination {[interface [type slot/port[-port]]] [port-channel channel-number]} 例： switch(config-erspan-dst)# destination interface ethernet 2/5	コピーする送信元パケットの宛先を設定します。宛先インターフェイスを設定できます。 (注) 宛先ポートをトランクポートとして設定できます。

	コマンドまたはアクション	目的
ステップ 12	(任意) ステップ 11 を繰り返して、すべての ERSPAN 宛先を設定します。	—
ステップ 13	erspan-id <i>erspan-id</i> 例： switch(config-erspan-dst)# erspan-id 5	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	no shut 例： switch(config-erspan-dst)# no shut	ERSPAN 宛先セッションを有効にします。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 15	exit 例： switch(config-erspan-dst)# exit	モニタ設定モードを閉じます。
ステップ 16	exit 例： 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 17	(任意) show monitor session {all session-number range session-range} 例： switch(config)# show monitor session 3	ERSPAN セッション設定を表示します。
ステップ 18	(任意) show running-config monitor 例： switch(config-erspan-src)# 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。
ステップ 19	(任意) show startup-config monitor 例： switch(config-erspan-src)# 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。
ステップ 20	(任意) copy running-config startup-config 例： switch(config-erspan-src)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

ERSPAN 設定の確認

ERSPAN 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
<code>show ip access-lists name</code>	ERSPAN ACL の設定を表示します。
<code>show monitor session {all session-number range session-range} [brief]</code>	ERSPAN セッション設定を表示します。 出力には、ERSPAN パケットの送信に使用される出力インターフェイスが含まれます。出力内容は、使用された出力インターフェイスのタイプによって異なります。 <ul style="list-style-type: none"> • 物理レイヤ3インターフェイス：インターフェイス名を表示します。 • SVI インターフェイス：ルートを学習したメンバー インターフェイスを表示します。 • レイヤ3 ポート チャネル：port-channel インターフェイス名を表示します。 • レイヤ3 サブインターフェイス：親インターフェイス名を表示します。 • ECMP パス：いずれかの等コスト マルチパス (ECMP) メンバー インターフェイスの名前を表示します。ルートが ECMP の場合でも、表示されているインターフェイスだけがトラフィックのミラーリングに使用されます。 • PFC on interfaces：インターフェイスのプライオリティフロー制御 (PFC) ステータスを表示します。
<code>show running-config monitor</code>	ERSPAN の実行コンフィギュレーションを表示します。
<code>show startup-config monitor</code>	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。

ERSPAN の設定例

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 rxswitch(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 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)# filter access_group erspan_filter
```

定義済みの ACL フィルタに基づいて対象トラフィックが選択されるさまざまな ERSPAN 接続先の場合、最後に設定されたセッションが常に高い優先順位を持ちます。

たとえば、モニターセッション 1 が構成されているとします。次に、モニターセッション 2 が構成されます。この場合、ERSPAN トラフィックフィルタは意図したとおりに機能します。ただし、ユーザーがモニターセッション 1 に戻り、既存の構成行の 1 つを再適用した場合 (構成に新しい変更はありません)。その後、スパンされたトラフィックはモニターセッション 1 に戻ります。

マーカー パケットの設定例

次に、2 秒間隔で ERSPAN マーカー パケットを有効にする例を示します。

```
switch# configure terminal
switch(config)# monitor erspan origin ip-address 172.28.15.250 global
switch(config)# monitor session 1 type erspan-source
switch(config-erspan-src)# header-type 3
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)# source interface ethernet 1/15 both
switch(config-erspan-src)# marker-packet 100
switch(config-erspan-src)# no shut
switch(config-erspan-src)# show monitor session 1
session 1
-----
type           : erspan-source
state          : up
granularity    : nanoseconds
erspan-id      : 1
vrf-name       : default
destination-ip : 9.1.1.2
ip-ttl         : 16
ip-dscp        : 5
header-type    : 3
origin-ip      : 172.28.15.250 (global)
source intf    :
  rx           : Eth1/15
  tx           : Eth1/15
  both         : Eth1/15
  rx           :
marker-packet  : enabled
packet interval : 100
packet sent     : 25
packet failed   : 0
egress-intf    :
```

UDF ベース ERSPAN の設定例

次に、以下の一致基準を使用して、カプセル化された IP-in-IP パケットの内部 TCP フラグで照合する UDF ベース ERSPAN を設定する例を示します。

- 外部送信元 IP アドレス : 10.0.0.2
- 内部 TCP フラグ : 緊急 TCP フラグを設定
- バイト : Eth Hdr (14) + 外部 IP (20) + 内部 IP (20) + 内部 TCP (20、ただし、13 番目のバイトの TCP フラグ)
- パケットの先頭からのオフセット : $14 + 20 + 20 + 13 = 67$
- UDF の照合値 : 0x20
- UDF マスク : 0xFF

```

udf udf_tcpflags packet-start 67 1
hardware access-list tcam region racl qualify udf udf_tcpflags
copy running-config startup-config
reload
ip access-list acl-udf
permit ip 10.0.0.2/32 any udf udf_tcpflags 0x20 0xff
monitor session 1 type erspan-source
source interface Ethernet 1/1
filter access-group acl-udf

```

次に、以下の一致基準を使用して、レイヤ 4 ヘッダーの先頭から 6 バイト目のパケット署名 (DEADBEEF) と通常の IP パケットを照合する UDF ベース ERSPAN を設定する例を示します。

- 外部送信元 IP アドレス : 10.0.0.2
- 内部 TCP フラグ : 緊急 TCP フラグを設定
- バイト : EthHdr (14) + IP (20) + TCP (20) + ペイロード : 112233445566DEADBEEF7788
- レイヤ 4 ヘッダーの先頭からのオフセット : $20 + 6 = 26$
- UDF の照合値 : 0xDEADBEEF (2 バイトのチャンクおよび 2 つの UDF に分割)
- UDF マスク : 0xFFFFFFFF

```

udf udf_pktsig_msb header outer 13 26 2
udf udf_pktsig_lsb header outer 13 28 2
hardware access-list tcam region racl qualify udf udf_pktsig_msb udf_pktsig_lsb
copy running-config startup-config
reload
ip access-list acl-udf-pktsig
permit udf udf_pktsig_msb 0xDEAD 0xFFFF udf udf_pktsig_lsb 0xBEEF 0xFFFF
monitor session 1 type erspan-source
source interface Ethernet 1/1
filter access-group acl-udf-pktsig

```

ERSPAN 切り捨ての設定例

次に、MPLS ストリッピングで使用する ERSPAN 切り捨てを設定する例を示します。

```

mpls strip
ip access-list mpls
  statistics per-entry
  20 permit ip any any redirect Ethernet1/5

interface Ethernet1/5
  switchport
  switchport mode trunk
  mtu 9216
  no shutdown

monitor session 1
  source interface Ethernet1/5 tx
  mtu 64
  destination interface Ethernet1/6
  no shut
monitor session 21 type erspan-source
  description "ERSPAN Session 21"

```



```
header-type 3
erspan-id 21
vrf default
destination ip 19.1.1.2
source interface Ethernet1/5 tx
mtu 64
no shut
monitor session 22 type erspan-source
description "ERSPAN Session 22"
erspan-id 22
vrf default
destination ip 19.2.1.2
source interface Ethernet1/5 tx
mtu 750
no shut
monitor session 23 type erspan-source
description "ERSPAN Session 23"
header-type 3
marker-packet 1000
erspan-id 23
vrf default
destination ip 19.3.1.2
source interface Ethernet1/5 tx
mtu 1000
no shut
```

IPv4 上の構成例

次に、ERSPAN 接続先セッションを構成する例を示します。

destination interface eth1/1 はスイッチポート モニタ モードです。このインターフェイスは、mpls strip、tunnel、nv Overlay、vn-segment-vlan-based、mpls segment-routing、mpls evpn、mpls static、mpls oam、mpls l3vpn、mpls ldp、および nv overlay evpn 機能と共存できません。

```
switch# monitor session 1 the erspan-destination
switch(config)# erspan-id 1
switch(config-erspan-dst)# source ip 1.2.3.4
switch(config-erspan-dst)# destination interface eth1/1
switch(config-erspan-dst)# no shut
switch(config-erspan-dst)# exit
```




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、次の内容で構成されています。

- [LLDP について \(351 ページ\)](#)
- [LLDP に関する注意事項および制約事項 \(353 ページ\)](#)
- [LLDP のデフォルト設定 \(354 ページ\)](#)
- [LLDP の設定 \(354 ページ\)](#)
- [LLDP 設定の確認 \(364 ページ\)](#)
- [LLDP の設定例 \(365 ページ\)](#)

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。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 Link Layer Discovery Protocol (LLDP) もサポートしています。LLDP を使用すると、ネットワーク デバイスはそれ自体の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をアドバタイズします。

- DCBXP
- 管理用アドレス
- ポートの説明
- ポートVLAN
- システム機能
- システムの説明
- 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。このプロトコルは、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、LLDPパケットのDCBXP TLVとしてパッケージ化されます。CEEを使用する場合、DCBXPはLLDP経由の確認応答メカニズムを使用します。ポートが起動すると、DCBX TLVが送信され、受信したDCBX TLVが処理されます。デフォルトでは、DCBXプロトコルは自動検出に設定され、両方のピアでサポートされている最新のプロトコルバージョンが使用されます。

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機能は次のとおりです。

- 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有効にします。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有効にすることで、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。
- 強化された転送選択 (ETS) : ETSは、仮想リンクの最適帯域幅管理を可能にします。ETS (Enhanced Transmission Selection) は、優先度グルーピングとも呼ばれます。PFCの同じ優先度クラス内の処理の区別を有効にします。帯域幅割り当て、低遅延、またはベストエフォートに基づいて処理の優先順位が付けられるため、結果としてグループごとのトラフィッククラス割り当てが可能になります。たとえば、イーサネットトラフィッククラスに高優先度を指定し、その同じクラスの中でベストエフォートを指定する場合があります。ETSによって、同じ優先度クラスの中でトラフィックを差別化する、つまり優先度グループを作成することが可能になります。

- アプリケーションプライオリティ構成：特定のプロトコルに割り当てられたプライオリティに関する情報を伝送します。
- DSCP マッピングへのプライオリティ：QoS ポリシーで構成された DSCP 値と COS 値のマッピングは、アプリケーションプライオリティ TLV で送信されます。



(注) Quality of Service (QoS) 機能の詳細については、『Cisco Nexus 9000 シリーズ NX-OS Quality of Service 設定ガイド』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 が有効な場合、DCBXP は `[no] lldp tlv-select dcbxp` コマンドお使用して有効または無効にできます。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。

高可用性

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 9000 シリーズ NX-OS ハイ アベイラビリティおよび冗長性ガイド』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 に関する注意事項および制約事項

LLDP の設定のガイドラインおよび制限事項は、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。
- DCBXP は次のプラットフォームでサポートされます。
 - Cisco Nexus 9200、9300-EX、9300-FX、および 9300-FX2 シリーズ スイッチ
 - Cisco Nexus 9332C、9332PQ、9364C、9372PX、9372PX-E、および 9396PX スイッチ
 - Cisco Nexus 9504 および 9508 スイッチで、X9432PQ、X9564PX、X9636PQ、X9732C-EX、および X9736C-FX ラインカードを搭載したもの

- Cisco Nexus 3232C および 3264Q スイッチは、DCBXP をサポートしていません。
- 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。
- DCBX TLV は、入力キューイングが設定され、システム レベルで適用されている場合にのみ送信されます。
- PFC TLV は、ネットワーク QoS ポリシーで少なくとも 1 つの COS 値に対して一時停止が有効になっており、インターフェイス レベルで priority-flow-control モードが auto である場合に送信されます。

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	無効
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	[有効 (Enabled)]
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	有効 (提供された LLDP が有効になります)
DCBXP のバージョン	自動検出

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 をグローバルに有効化または無効化する

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	configure terminal 例： switch# configure terminal switch(config)#	グローバル設定モードを開始します。
ステップ 2	[no] feature lldp 例： switch(config)# 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。
ステップ 3	(任意) show running-config lldp 例： switch(config)# 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。LLDP が有効の場合、「feature lldp」と表示されます。LLDP が無効の場合、「Invalid command」エラーが表示されます。
ステップ 4	(任意) copy running-config startup-config 例： switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

インターフェイス上での LLDP の有効化または無効化

LLDP をグローバルに有効にすると、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で有効になります。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。

始める前に

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	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 7/1 switch(config-if)#	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	[no] lldp transmit 例： switch(config-if)# 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 をグローバルに有効にすると、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で有効になります。
ステップ 4	[no] lldp receive 例： switch(config-if)# 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 をグローバルに有効にすると、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で有効になります。
ステップ 5	(任意) show lldp interface interface slot/port 例： switch(config-if)# show lldp interface ethernet 7/1	インターフェイス上で LLDP の設定を表示します。
ステップ 6	(任意) copy running-config startup-config 例： switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

DCBXP プロトコルバージョンの設定

DCBX TLV が送信されるプロトコルバージョンを指定できます。



- (注) ピアが同じバージョンを実行していない場合、リンクの DCBX パラメータが収束しない可能性があります。新しいプロトコルバージョンを有効にするには、リンクをリセットする必要があります。

始める前に

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	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 1/25 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	lldp dcbx version cee/ieee/auto 例 : switch(config-if)#lldp dcbx version cee	Specifies the protocol version mode sent. 送信されるプロトコルバージョン モードを指定します。 <ul style="list-style-type: none"> • <i>cee</i> 変数は、Converged Enhanced Ethernet (CEE) プロトコルバージョンの TLV のみを送信するようにポートを設定します。 • <i>ieee</i> 変数は、IEEE 802.1Qaz プロトコルバージョンの TLV のみを送信するようにポートを設定します。 • <i>auto</i> 変数は、両方のピアでサポートされている最新のプロトコルバージョンで TLV を送信するようにポートを設定します。 デフォルトは <i>auto</i> に設定されています。

	コマンドまたはアクション	目的
		(注) IEEE 802.1Qaz をサポートしていないデバイスは、自動ネゴシエーションの試行に適切に応答せず、 <code>lldp dcbx version cee</code> 用にインターフェイスを手動で設定する必要があります。

物理インターフェイスごとの複数の LLDP ネイバー

多くの場合、ネットワーク デバイスは複数の LLDP パケットを送信しますが、そのうちの1つは実際のホストからのものです。Cisco Nexus スイッチがデバイスと通信しているが、インターフェイスごとに1つの LLDP ネイバーしか管理できない場合は、実際に必要なホストとのネイバーになることが失敗する可能性があります。これを最小限に抑えるために、Cisco Nexus スイッチ インターフェイスは複数の LLDP ネイバーをサポートできるため、正しいデバイスで LLDP ネイバーになる可能性が高くなります。

同じインターフェイスで複数の LLDP ネイバーをサポートするには、LLDP マルチネイバー サポートをグローバルに設定する必要があります。



(注) LLDP マルチネイバー サポートを設定する前に、DCBX をグローバルに無効にする必要があります。これを行わないと、エラー メッセージが表示されます。

LLDP マルチネイバー サポートのイネーブル化またはディセーブル化

始める前に

インターフェイスで LLDP マルチネイバー サポートを有効にする前に、次の点を考慮してください。

- 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 (グローバル設定コマンド `feature lldp`) 。



(注) LLDP をグローバルに有効にすると、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で有効になります。

- 1 つのインターフェイスで最大 3 つのネイバーがサポートされます。
- LLDP マルチネイバーは、FEX インターフェイスではサポートされません。

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	必須: no lldp tlv-select dcbxp 例： switch(config)# no lldp tlv-select dcbxp switch(config)#	DCBXP TLV をグローバルに無効にします。 (注) LLDP マルチネイバー サポートが設定された後にエラーメッセージが表示されないようにするには、このコマンドを入力する必要があります。
ステップ 3	必須: [no] lldp multi-neighbor 例： switch(config)# lldp multi-neighbor switch(config)#	すべてのインターフェイスの LLDP マルチネイバーサポートをグローバルに有効または無効にします。
ステップ 4	interface port / slot 例： switch(config)# interface 1/1 switch(config-if)#	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 5	(任意) [no] lldp transmit 例： switch(config-if)# lldp transmit	インターフェイスでの LLDP パケットの送信をディセーブル (またはイネーブル) にします。 (注) このインターフェイスでの LLDP パケットの送信は、グローバル feature lldp コマンドを使用してイネーブルにされました。このオプションは、この特定のインターフェイスの機能を無効にします。
ステップ 6	(任意) [no] lldp receive 例： switch(config-if)# lldp receive	インターフェイスでの LLDP パケットの受信をディセーブル (またはイネーブル) にします。

	コマンドまたはアクション	目的
		(注) このインターフェイスでの LLDP パケットの受信は、グローバル feature lldp コマンドを使用してイネーブルになりました。このオプションは、この特定のインターフェイスの機能を無効にします。
ステップ 7	(任意) show lldp interface port / slot 例： switch(config-if)# show lldp interface 1/1	インターフェイス上で LLDP の設定を表示します。
ステップ 8	(任意) copy running-config startup-config 例： switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

ポートチャネルインターフェイスでの LLDP サポートの有効化または無効化

始める前に

ポートチャネルで LLDP サポートを有効にする前に、次の点を考慮してください。

- 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（グローバル設定コマンド **feature lldp**）。



(注) LLDP をグローバルに有効にすると、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で有効になります。

- ポートチャネルに **lldp transmit** および **lldp receive** コンフィギュレーションコマンドを適用しても、ポートチャネルのメンバーの設定には影響しません。
- LLDP ネイバーは、LLDP 送受信がポートチャネルの両側で設定されている場合にのみ、ポートチャネル間で形成されます。
- LLDP の送受信コマンドは、MCT、VPC、FEX ファブリック、FEX ポートチャネル、およびポートチャネルサブインターフェイスでは機能しません。



- (注) LLDP ポートチャネル機能をグローバルに有効にすると、LLDP 設定はこれらのポートタイプのいずれにも適用されません。ポートチャネルから設定が削除された場合、またはポートタイプ機能がグローバルに無効になった場合は、**lldp port-channel** コマンドを使用して新しくサポートされたポートチャネルで有効にすることはできません。コマンドはすでに発行されています。問題のポートチャネルで LLDP ポートチャネルを有効にするには、**lldp transmit** および **lldp receive** を各ポートチャネルに対して設定します（次の手順のステップ 4、5、および 6 を参照）。

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	必須: no lldp tlv-select dcbxp 例： switch(config)# no lldp tlv-select dcbxp switch(config)#	DCBXP TLV をグローバルに無効にします。ポートチャネルで LLDP を設定する前に、このコマンドを入力する必要があります。
ステップ 3	必須: [no] lldp port-channel 例： switch(config)# lldp port-channel switch(config)#	すべてのポートチャネルの LLDP 送信をグローバルに有効または無効にします。
ステップ 4	interface port-channel <i>[port-channel-number port-channel-range]</i> 例： switch(config)# interface port-channel 3 switch(config-if)# 例： 複数のポートチャネルで LLDP を設定する場合は、ポートチャネル番号の範囲を入力します。 switch(config)# interface port-channel 1-3 switch(config-if-range)#	LLDP を有効にするインターフェイスポートチャネルを指定し、インターフェイス設定モードを開始します。 LLDP を有効にするインターフェイスポートチャネル範囲を指定し、インターフェイス範囲設定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 5	(任意) [no] lldp transmit 例： <pre>switch(config-if)# lldp transmit</pre>	ポートチャネルまたはポートチャネルの範囲で LLDP パケットの送信を無効（または有効）にします。 (注) このポートチャネルでの LLDP パケットの送信は、ステップ 3 の lldp port-channel コマンドを使用して有効になりました。このオプションは、この特定のポートチャネルの機能を無効にします。
ステップ 6	(任意) [no] lldp receive 例： <pre>switch(config-if)# lldp receive</pre>	ポートチャネルまたはポートチャネルの範囲での LLDP パケットの受信を無効（または有効）にします。 (注) このポートチャネルでの LLDP パケットの受信は、ステップ 3 の lldp port-channel コマンドを使用して有効になりました。このオプションは、この特定のポートチャネルの機能を無効にします。
ステップ 7	(任意) show lldp interface port-channel port-channel-number 例： <pre>switch(config-if)# show lldp interface port-channel 3</pre>	ポートチャネル上の LLDP 設定を表示します。
ステップ 8	(任意) copy running-config startup-config 例： <pre>switch(config)# copy running-config startup-config</pre>	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	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	(任意) [no] lldp holdtime seconds 例： switch(config)# lldp holdtime 200	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	(任意) [no] lldp reinit seconds 例： switch(config)# lldp reinit 5	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	(任意) [no] lldp timer seconds 例： switch(config)# lldp timer 50	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。
ステップ 5	(任意) show lldp timers 例： switch(config)# 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。
ステップ 6	(任意) [no] lldp tlv-select tlv 例： switch(config)# lldp tlv-select system-name	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	(任意) show lldp tlv-select 例： switch(config)# show lldp tlv-select	LLDP TVL コンフィギュレーションを表示します。
ステップ 8	(任意) copy running-config startup-config 例：	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。

	コマンドまたはアクション	目的
	<code>switch(config)# copy running-config startup-config</code>	

LLDP 設定の確認

LLDP 設定を表示するには、次のタスクのうちのいずれかを実行します。

コマンド	目的
<code>show running-config lldp</code>	LLDP のグローバル コンフィギュレーションを表示します。
<code>show lldp all</code>	LLDP DCBXP を表示し、すべてのインターフェイスの設定を送信および受信します。
<code>show lldp interface interface slot/port</code>	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。
<code>show lldp timers</code>	LLDP の保持時間、遅延時間、更新頻度の設定を表示します。
<code>show lldp tlv-select</code>	LLDP TVL コンフィギュレーションを表示します。
<code>show lldp dcxb interface interface slot/port</code>	特定のインターフェイスの DCBXP TLV 情報を表示します。
<code>show lldp neighbors {detail interface interface slot/port}</code>	LLDP ネイバーのデバイス ステータスを表示します。
<code>show lldp traffic</code>	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。
<code>show lldp traffic interface interface slot/port</code>	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。
<code>show qos dcxbp interface slot/port</code>	特定のインターフェイスの DCBXP 情報を表示します。

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 の設定例

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
```




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。

この章は、次の内容で構成されています。

- [NetFlow について \(367 ページ\)](#)
- [NetFlow の前提条件 \(371 ページ\)](#)
- [NetFlow に関する注意事項および制約事項 \(371 ページ\)](#)
- [NetFlow の設定 \(375 ページ\)](#)
- [NetFlow 設定の確認 \(385 ページ\)](#)
- [NetFlow のモニタリング \(386 ページ\)](#)
- [NetFlow の表示例 \(386 ページ\)](#)
- [NetFlow のコンフィギュレーション例 \(386 ページ\)](#)

NetFlow について

NetFlow は入力 IP パケット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クデバイスを変更する必要はありません。

NetFlow ではフローを使用して、アカウントリング、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（VLAN 向け）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有効にする Flexible NetFlow 機能をサポートします。フレキシブル 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 エクスポートを使用し、このデータを Cisco Stealthwatch などのリモート 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。

- フローはフロータイムアウト値に従って定期的にエクスポートされます。設定されていない場合、デフォルトは 10 秒です。
- 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。フローモニター、フローレコードおよびフローエクスポートを NetFlow キャッシュ情報と結合します。

Cisco NX-OS は NetFlow 統計を集計し、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。

デュアルレイヤ NetFlow の実装

他の Cisco Nexus プラットフォームとは異なり、Cisco Nexus 9000 シリーズスイッチは、NetFlow 処理を次の 2 つのレイヤに分離します。

- 第 1 レイヤは、ラインレートトラフィックのパケット単位の可視性をサポートします。パケットをサンプリングして統計的に分析する必要はありません。代わりに、パケットをラインレートで処理および集約できます。
- 2 番目のレイヤは、大規模なフローの収集を可能にします。フローを失うことなく何十万ものフローを維持でき、定期的に外部コレクタにエクスポートします。

フローレコード

フローレコードでは、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 **collect** 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 flow direction

フロー エクスポート

フローエクスポートでは、NetFlow エクスポート パッケージに関して、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 エクスポート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 (NetFlow コレクタが NetFlow パッケージをリスニングするところ) : デフォルト値は 9995 です。



(注) NetFlow エクスポート パッケージでは、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を設定しない場合、フローエクスポートはエクスポートする予定のフローをドロップします。

Cisco NX-OS は、タイムアウトが発生するたびにデータを NetFlow コレクタへエクスポートします。キャッシュをフラッシュし、フローを強制的にエクスポートするには、フラッシュキャッシュ タイムアウトを設定できます (**flow timeout** コマンドを使用)。

エクスポート形式

Cisco NX-OS は、バージョン 9 のエクスポート形式をサポートします。この形式は、古いバージョン 5 のエクスポート形式よりも効率的なネットワーク使用率をサポートし、IPv6 およびレイヤ 2 フィールドをサポートします。さらに、バージョン 9 エクスポート形式は、NetFlow コレクタで完全な 32 ビット SNMP ifIndex 値をサポートします。

レイヤ 2 NetFlow キー

フレキシブル 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 チャンネル



- (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。

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 エクスポートを参照します。フロー モニタはインターフェイスに適用します。

NetFlow 出カインターフェイス

FM-E および FM-E2 モジュールを搭載した Cisco Nexus 9300-FX および Cisco Nexus 9500 プラットフォーム スイッチの NetFlow 出カインターフェイスには、次の機能があります。

- **show flow cache** コマンドの NetFlow は `output_if_id` を表示し、出カインターフェイスを 9700-EX ラインカードを備えた Cisco Nexus 9300-FX および 9500 プラットフォーム スイッチのコレクタにエクスポートします。
- Cisco Nexus 9300-FX プラットフォーム スイッチの NetFlow 出カインターフェイスは、IPv4 と IPv6 の両方のトラフィック フローをサポートします。Cisco Nexus 9500 プラットフォーム スイッチの NetFlow 出カインターフェイスは、IPv4 トラフィック フローでのみサポートされ、IPv6 トラフィック フローではサポートされません。**show flow cache** コマンドは、`output_if_id` を `0x0` として表示します。またこの機能は、コントロールプレーントラフィックや ICMP 要求/応答メッセージなど、スイッチ宛でのトラフィック以外のトラフィックでもサポートされます。
- NetFlow は、宛先インターフェイスとしてネクストホップを持つ IPv4/IPv6 着信トラフィック フローのコレクタへの出カインターフェイスのエクスポートをサポートします。InputInt および OutputInt の NetFlow エクスポート形式は、NetFlow コレクタで完全な 32 ビット SNMP ifIndex 値をサポートします。
- NetFlow 出カインターフェイスは、MPLS、VXLAN、GRE などのトンネルトラフィック フローではサポートされません。
- NetFlow 出カインターフェイスの例の詳細については、[NetFlow の表示例 \(386 ページ\)](#) を参照してください。

高可用性

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ません。

NetFlow の前提条件

NetFlow の前提条件は、次のとおりです。

- 使用しているデバイスで必要とされるリソースを正しく理解していること。NetFlow はメモリと CPU リソースを消費するからです。

NetFlow に関する注意事項および制約事項



- (注) スケールの情報については、リリース特定の『Cisco Nexus 9000 Series NX-OS Verified Scalability Guide』を参照してください。

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。

- 次の注意事項は、EX および FX ライン カード搭載のすべての Cisco Nexus 9500 プラットフォーム スイッチに適用されます。

FX ポートがすでに適用されている NetFlow 設定のトランクである場合、EX ポートをトランクとして設定しても、サポートされていない EX NetFlow 設定は FX ポート トランクから削除されません。たとえば、3 つ以上の異なる IPv4 フロー モニタを FX ポート トランクに適用し、EX ポートが同じトランクに追加された場合、EX ポートの制限のみであるため、2 つのモニタを超えるトランクの設定は自動的に削除されません。この設定では、EX トランク ポートの 2 つのモニタを超えるフローはレポートされないため、EX ポートと FX ポートの両方が同じトランクに存在する可能性があるモジュラスイッチでは、プロトコルごとに 2 つのモニタ (v4/v6/CE) のみを使用することを推奨します。

- Cisco NX-OS リリース 9.3 (4) 以降では、次の RTP / NetFlow モニタリング制限が存在します。

RTP モニタリング機能は、スイッチのすべてのインターフェイスで RTP フローのモニタをイネーブルにし、**show flow rtp detail** コマンド出力で報告します。RTP フローは、16384～32767 の範囲内の送信元ポートを持つ UDP フローです。RTP モニタリングがイネーブルになっているスイッチ インターフェイスに NetFlow モニタが接続されている場合、そのインターフェイス上のすべてのトラフィック/フロー (RTP フローを含む) が **show flow cache** コマンドの出力で報告されます。RTP フローは、**show flow rtp detail** コマンドの出力に表示されなくなります。接続されたモニタが削除されると、RTP フローが **show flow rtp detail** コマンド出力で再度報告されます。

この制限は、次のスイッチに影響します。

- Cisco Nexus 9336C-FX2
- Cisco Nexus 93240YC-FX2

- Cisco Nexus 9348GC-FXP
 - Cisco Nexus 93180YC-FX
 - Cisco Nexus 93108TC-FX
 - Cisco Nexus 9316D-GX
 - Cisco Nexus 93600CD-GX
 - Cisco Nexus 9364C-GX
 - 9636C-RX ラインカードを搭載した Cisco Nexus 9504、9508 および 9516 スイッチ
- Cisco NX-OS リリース 9.3(3) 以降、NetFlow に関する次の無停止インサーブिस ソフトウェア アップグレード (ND ISSU) の制限がすべての Cisco Nexus 9000 シリーズスイッチに適用されます。
 - ND ISSU の実行中、2 分間のエクスポート損失が予想されます。
 - ND ISSU 中は、管理インターフェイスの送信元ポートを持つエクスポートはサポートされません。エクスポート損失は、管理インターフェイスが起動するまで予想されません。
 - **record netflow ipv4 original-input**、**record netflow ipv4 original-output**、および **record netflow layer2-switched input** コマンドは、Cisco NX-OS リリース 9.3(1) ではサポートされていません。
 - Cisco NX-OS リリース 9.2(2) 以降、Cisco Nexus 9300-FX スイッチは NetFlow データエクスポート (NDE) の OUTPUT_SNMP フィールドの収集をサポートしています。他の Cisco Nexus 9000 プラットフォームスイッチまたは Cisco Nexus ラインカードは、OUTPUT_SNMP フィールドの収集をサポートしていません。
 - Cisco Nexus 9300-FX プラットフォームスイッチに対して、レイヤ 2 NetFlow に対してすでに設定されているポートチャンネルにメンバを追加すると、NetFlow の設定が削除され、ポートチャンネルのレイヤ 2 設定が追加されます。
 - NetFlow はトンネル インターフェイスではサポートされていません。
 - NetFlow は、CPU で送信されるパケットではサポートされません。
 - 入力 NetFlow のみがサポートされます。出力 NetFlow はサポートされていません。
 - フローキャッシュは、レイヤ 2、IPv4、IPv6 などのフロータイプごとにクリアできます。フロー モニタごとにクリアすることはできません。
 - フロー収集は ARP トラフィックに対して実行されません。
 - NetFlow データエクスポート (NDE) 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い場合、フローエクスポートはエクスポートする予定のフローをドロップします。

- レイヤ 2 スイッチドフロー モニタは、レイヤ 2 インターフェイスにのみ適用されます。IP および IPv6 フロー モニタは、VLAN、SVI、レイヤ 3 ルーテッド インターフェイス、またはサブインターフェイスに適用できます。
- 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か、レイヤ 3 インターフェイスをレイヤ 2 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。
- 同じフロー モニタを VLAN およびレイヤ 3 インターフェイス（物理レイヤ 3 インターフェイス、SVI インターフェイス、またはレイヤ 3 サブインターフェイスなど）と共有することはできません。ACL は異なるため共有できないため、VLAN とレイヤ 3 インターフェイスを区別する必要があります。これらは 2 つの異なるプロファイルとして扱う必要があります。
- 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、ロールバックは失敗します。
- Cisco NX-OS リリース 9.2(1) 以降：
 - FEX レイヤ 3 ポートの NetFlow は Cisco Nexus 9300 EX と 9300 FX プラットフォームスイッチでサポートされています。
 - Cisco Nexus 9300-EX プラットフォームスイッチで NetFlow CE がサポートされています。



(注) すべての EX タイプのプラットフォームスイッチ（Cisco Nexus 9700-EX ラインカードを含む）では、CE NetFlow は非 IPv4 および IPv6 トラフィック フローの CE フローレコードのみをキャプチャします。FX および FX2 タイプのプラットフォームスイッチとラインカードでは、**mac packet-classify** がインターフェイスに適用されている限り、IP フローの CE フローデータをキャプチャできます。

- Cisco Nexus 9300-EX プラットフォームスイッチの場合、VLAN または SVI に適用されたフロー モニタは、スイッチドトラフィックとルーテッドトラフィックの両方のフローを収集できます。Cisco Nexus 9300-FX プラットフォームスイッチの場合、NetFlow VLAN はスイッチドトラフィックに対してのみサポートされ、NetFlow SVI はルーテッドトラフィックに対してのみサポートされます。
- Cisco Nexus 9300-EX プラットフォームスイッチは、同じインターフェイスで NetFlow と SPAN を同時にサポートします。この機能は、SPAN および sFlow の代わりに使用できます。
- Cisco Nexus 9300-EX/FX プラットフォームスイッチ、および EX/FX モジュールを搭載した Cisco Nexus 9500 プラットフォームスイッチでは、SPAN と sFlow の両方を同時に有効にすることはできません。一方がアクティブな場合、もう一方は有効にできません。ただし、Cisco Nexus 9300-EX/FX/FX2 および EX モジュールを搭載した Cisco Nexus 9500 プラ

トフォームスイッチでは、NetFlow と SPAN の両方を同時に有効にすることができ、sFlow と SPAN を使用する代わりに実行可能です。



(注) Cisco Nexus 9300-FX2 プラットフォーム スイッチは、sFlow と SPAN の共存をサポートします。

- Cisco Nexus 9300-EX プラットフォーム スイッチでは、同じフロー モニタを VLAN と SVI に同時に接続することはできません。
- Cisco Nexus 9300-EX プラットフォーム スイッチには専用の TCAM があり、カービングは必要ありません。
- ing-netflow リージョンの TCAM カービング設定は、FX ラインカードでは実行できます。EX ラインカードでは、デフォルトの ing-netflow リージョン TCAM カービングが 1024 であり、それ以外の場合は設定できません。EX および FX ラインカードのポートの場合、ing-netflow リージョンの推奨最大値は 1024 です。
- ToS フィールドは、Cisco Nexus 9300-EX プラットフォーム スイッチではエクスポートされません。
- IP ToS に基づくレコード一致は、IPv6 フローモニタではサポートされません。ToS 値は、トラフィックが保持する値に関係なく、コレクタで 0x0 として収集されます。

この制限は、次のプラットフォーム スイッチ ファミリに適用されます。

- Cisco Nexus 9300-EX
- Cisco Nexus 9300-FX
- Cisco Nexus 9300-FX2
- Cisco Nexus 9300-GX
- EX または FX ラインカード搭載の Cisco Nexus 9500
- Cisco Nexus 3232C および 3264Q スイッチは、NetFlow をサポートしていません。
- Cisco NX-OS リリース 10.1(2) 以降、Netflow は N9K-X9716D-GX ラインカードでサポートされます。
- この機能をサポートするプラットフォームでのみ NetFlow を有効にします。



(注) 確認済みの NetFlow のスケール数については、『[Cisco Nexus 9000 Series NX-OS Verified Scalability Guide](#)』を参照してください。

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 機能を有効にします。
- 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 エクスポートを定義します。
- ステップ 4 フロー レコードおよびフロー エクスポートに基づいて、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、または VLAN インターフェイスにフロー モニタを適用します。

NetFlow 機能の有効化

フローを設定するには、先に NetFlow をグローバルで有効しておく必要があります。

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)#	グローバル設定モードを開始します。
ステップ 2	[no] feature netflow 例： switch(config)# feature netflow	NetFlow 機能を有効にします。デフォルトではディセーブルになっています。 (注) N9K-T2 EoR を搭載した Cisco Nexus 9500 プラットフォームスイッチは、NetFlow をサポートしていません。
ステップ 3	(任意) copy running-config startup-config 例： switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

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。

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 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。フローレコード名には最大 63 文字の英数字を入力できます。
ステップ 3	(任意) description string 例： switch(config-flow-record)# description IPv4Flow	最大 63 文字で、フローレコードの説明を示します。
ステップ 4	(任意) match type 例： switch(config-flow-record)# match transport destination-port	一致キーを指定します。詳細については、 match パラメータの指定 (377 ページ) を参照してください。 (注) レイヤ4ポート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	(任意) collect type 例： switch(config-flow-record)# collect counter packets	コレクションフィールドを指定します。詳細については、 collect パラメータの指定 (378 ページ) を参照してください。
ステップ 6	(任意) show flow record [name] [record-name] {netflow-original netflow protocol-port netflow {ipv4 ipv6} {original-input original-output}} 例： switch(config-flow-record)# show flow record netflow protocol-port	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 7	(任意) copy running-config startup-config 例 : <pre>switch(config-flow-record)# copy running-config startup-config</pre>	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。

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 datalink {mac source-address mac destination-address ethertype vlan} 例: <pre>switch(config-flow-record)# match datalink ethertype</pre>	レイヤ 2 属性をキーとして指定します。
match ip {protocol tos} 例: <pre>switch(config-flow-record)# match ip protocol</pre>	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。 データは show hardware flow ip コマンドの出力に収集されて表示されますが、両方のコマンドを設定するまで収集とエクスポートは行われません。
match ipv4 {destination address source address} 例: <pre>switch(config-flow-record)# match ipv4 destination address</pre>	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 options} 例: <pre>switch(config-flow-record)# match ipv6 flow-label</pre>	IPv6 キーを指定します。

コマンド	目的
<p>match transport {destination-port source-port}</p> <p>例:</p> <pre>switch(config-flow-record)# match transport destination-port</pre>	<p>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。</p> <p>(注) レイヤ 4 ポート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。</p> <p>データは show hardware flow ip コマンドの出力に収集されて表示されますが、両方のコマンドを設定するまで収集とエクスポートは行われません。</p>

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
<p>collect counter {bytes packets} [long]</p> <p>例:</p> <pre>switch(config-flow-record)# collect counter packets</pre>	<p>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。</p>
<p>collect ip version</p> <p>例:</p> <pre>switch(config-flow-record)# collect ip version</pre>	<p>フローの IP バージョンを収集します。</p>
<p>collect timestamp sys-uptime {first last}</p> <p>例:</p> <pre>switch(config-flow-record)# collect timestamp sys-uptime last</pre>	<p>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。</p>
<p>collect transport tcp flags</p> <p>例:</p> <pre>switch(config-flow-record)# collect transport tcp flags</pre>	<p>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。</p>

フロー エクスポートの作成

フロー エクスポートの設定では、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 Collector 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 switch(config-flow-exporter)#	フローエクスポートを作成し、フローエクスポートコンフィギュレーションモードを開始します。フローエクスポート名を最大 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トの宛先 IPv4 または IPv6 アドレスを設定します。任意で、NetFlow Collector 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	source interface-type name/port 例： switch(config-flow-exporter)# source ethernet 2/1	設定された宛先で NetFlow Collector 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	(任意) description string 例： switch(config-flow-exporter)# description exportversion9	このフローエクスポート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 6	(任意) dscp value 例： switch(config-flow-exporter)# dscp 0	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	(任意) transport udp port 例： switch(config-flow-exporter)# transport udp 200	NetFlow Collector 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。

	コマンドまたはアクション	目的
ステップ 8	version 9 例 : <pre>switch(config-flow-exporter)# version 9 switch(config-flow-exporter-version-9)#</pre>	NetFlow エクスポートバージョンを指定します。フローエクスポートのバージョン 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	(任意) option {exporter-stats interface-table} timeout seconds 例 : <pre>switch(config-flow-exporter-version-9)# option exporter-stats timeout 1200</pre>	フローエクスポート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	(任意) template data timeout seconds 例 : <pre>switch(config-flow-exporter-version-9)# template data timeout 1200</pre>	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	(任意) copy running-config startup-config 例 : <pre>switch(config-flow-exporter-version-9)# copy running-config startup-config</pre>	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 エクスポート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ト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 : <pre>switch# configure terminal switch(config)#</pre>	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 : <pre>switch(config)# flow monitor flow-monitor-one switch(config-flow-monitor)#</pre>	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。

	コマンドまたはアクション	目的
ステップ 3	(任意) description string 例： <pre>switch(config-flow-monitor) # description IPv4Monitor</pre>	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	(任意) exporter name 例： <pre>switch(config-flow-monitor) # export v9</pre>	フロー エクスポートとこのフロー モニタを関連付けます。エクスポート名には最大 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： <pre>switch(config-flow-monitor) # record IPv4Flow</pre>	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。 (注) record netflow ipv4 original-input 、 record netflow ipv4 original-output 、 record netflow layer2-switched input は、Cisco NX-OS リリース 9.3(1) ではサポートされていません。
ステップ 6	(任意) copy running-config startup-config 例： <pre>switch(config-flow-monitor) # copy running-config startup-config</pre>	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。

インターフェイスへのフロー モニタの適用

フロー モニタは入力インターフェイスに適用できます。出力 NetFlow はサポートされていません。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： <pre>switch# configure terminal switch(config)#</pre>	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 vlan <i>vlan-id</i> 例： switch(config)# interface vlan 10 switch(config-if)#	VLAN インターフェイスを設定し、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	ip flow monitor {ipv4 ipv6 layer-2-switched} input 例： switch(config-if)# ip flow monitor ipv4 input	入力パケットのインターフェイスに、IPv4、IPv6、またはレイヤ 2 スイッチ フロー モニタを関連付けます。
ステップ 4	(任意) copy running-config startup-config 例： switch(config-if)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

VLAN 上でのブリッジ型 NetFlow の設定

VLAN のレイヤ 2 スイッチド パケットでレイヤ 3 データを収集するために、VLAN にフロー モニタを適用できます。

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 <i>vlan-id</i> 例： switch(config)# vlan configuration 30 switch(config-vlan-config)#	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	{ip ipv6} flow monitor <i>name</i> 例： switch(config-vlan-config)# ip flow monitor testmonitor	入力パケットのフロー モニタを VLAN に関連付けます。フロー モニタ名を最大 63 文字の英数字で入力できます。

	コマンドまたはアクション	目的
ステップ 4	(任意) copy running-config startup-config 例 : <pre>switch(config-vlan-config)# copy running-config startup-config</pre>	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。

レイヤ 2 NetFlow キーの設定

フレキシブル 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。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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 : <pre>switch(config)# flow record L2_record switch(config-flow-record)#</pre>	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の詳細については、 フローレコードの作成 (376 ページ) を参照してください。
ステップ 3	match datalink {mac source-address mac destination-address ethertype vlan} 例 : <pre>switch(config-flow-record)# match datalink ethertype</pre>	レイヤ 2 属性をキーとして指定します。
ステップ 4	exit 例 : <pre>switch(config-flow-record)# exit switch(config)#</pre>	フローレコード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	interface {ethernet slot/port port-channel number} 例 : <pre>switch(config)# interface Ethernet 6/3 switch(config-if#)</pre>	インターフェイス設定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。

	コマンドまたはアクション	目的
ステップ 6	switchport 例： <code>switch(config-if)# switchport</code>	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に関する詳細については、「 Cisco Nexus 9000 シリーズ NX-OS レイヤ 2 スイッチング設定ガイド 」を参照してください。
ステップ 7	mac packet-classify 例： <code>switch(config-if)# mac packet-classify</code>	パケットの MAC 分類を強制します。 このコマンドの使用に関する詳細については、「 Cisco Nexus 9000 シリーズ NX-OS セキュリティ設定ガイド 」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 8	layer2-switched flow monitor <i>flow-name</i> input 例： <code>switch(config-if)# layer2-switched flow monitor L2_monitor input</code>	フローモニタをスイッチポートの入力パケットに関連付けます。フローモニタ名を最大 63 文字の英数字で入力できます。
ステップ 9	(任意) show flow record netflow layer2-switched input 例： <code>switch(config-if)# show flow record netflow layer2-switched input</code>	レイヤ 2 NetFlow のデフォルト レコードの情報を表示します。
ステップ 10	(任意) copy running-config startup-config 例： <code>switch(config-if)# copy running-config startup-config</code>	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。

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。デフォルト値は 10 秒です。
ステップ 3	(任意) copy running-config startup-config 例： switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

NetFlow 設定の確認

NetFlow 設定を表示するには、次のタスクのうちのいずれかを実行します。

コマンド	目的
show flow cache [ipv4 ipv6 ce]	NetFlow IP フローに関する情報を表示します。
show flow exporter [name]	NetFlow のフロー エクスポート情報と統計情報を表示します。フロー エクスポート名を最大 63 文字の英数字で入力できます。
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。フローレコード名には最大 63 文字の英数字を入力できます。
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 running-config netflow	現在デバイスにある 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 エクスポート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 の表示例

IPv4 の **show flow cache** コマンドの出力には、次のように表示されます。

```
show flow cache
IPV4 Entries
SIP          DIP          BD ID  S-Port  D-Port  Protocol  Byte Count  Packet Count  TCP
FLAGS  TOS  if_id      output_if_id  flowStart  flowEnd
10.10.30.4  30.33.1.2  1480   30000   17998    17         683751850   471553         0x0
          0x0  0x90105c8  0x1a005000    14096494  14153835
30.33.1.2   10.10.39.4  4145   30000   18998    17         43858456   30164          0x0
          0x0  0x1a005000 0x1a006600    14096477  14099491
10.10.29.4  30.33.1.2  1479   30000   17998    17         683751850   471553         0x0
          0x0  0x90105c7  0x1a005000    14096476  14153817
10.10.7.4   30.33.1.2  1457   30000   17998    17         683753300   471554         0x0
          0x0  0x90105b1  0x1a005000    14096481  14153822
30.33.1.2   10.10.42.4  4145   30000   18998    17         95289344   65536          0x0
          0x0  0x1a005000 0x1a006600    14112551  14119151
10.10.49.4  30.33.1.2  1499   30000   17998    17         683753300   471554         0x0
          0x0  0x90105db  0x1a005000    14096486  14153827
```

NetFlow のコンフィギュレーション例

この例では、IPv4 に対して NetFlow エクスポートを設定する方法を示します。

```
feature netflow
flow exporter ee
 destination 171.70.242.48 use-vrf management
 source mgmt0
 version 9
  template data timeout 20
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
```



第 21 章

sFlow の設定

この章では、Cisco NX-OS デバイスで sFlow 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。

- [sFlow について \(387 ページ\)](#)
- [sFlow の前提条件 \(388 ページ\)](#)
- [sFlow の注意事項および制約事項 \(388 ページ\)](#)
- [sFlow のデフォルト設定 \(389 ページ\)](#)
- [sFlow の設定 \(390 ページ\)](#)
- [sFlow 設定の確認 \(397 ページ\)](#)
- [sFlow 統計情報のモニタリングとクリア \(398 ページ\)](#)
- [sFlow の設定例 \(398 ページ\)](#)
- [その他の参考資料 \(399 ページ\)](#)

sFlow について

サンプリングされた Flow (sFlow) を使用すると、スイッチやルータを含むデータネットワーク内のリアルタイムトラフィックをモニターできます。sFlow では、トラフィックをモニターするためにスイッチとルータ上の sFlow エージェント ソフトウェアでサンプリングメカニズムを使用して、サンプルデータを中央のデータコレクタに転送します。

sFlow の詳細については、[RFC 3176](#) を参照してください。

sFlow エージェント

Cisco NX-OS ソフトウェアに組み込まれている sFlow エージェントは、サンプリングされるパケットのデータソースに関連付けられたインターフェイスカウンタを定期的にサンプリングまたはポーリングします。このデータソースは、イーサネットインターフェイス、EtherChannel インターフェイス、ある範囲に属するイーサネットインターフェイスのいずれかです。sFlow エージェントは、イーサネットポートマネージャにクエリーを送信して対応する EtherChannel メンバーシップ情報を確認するほか、イーサネットポートマネージャからもメンバーシップの変更の通知を受信します。

sFlow サンプルングをイネーブルにすると、サンプルングレートとハードウェア内部の乱数に基づいて、入力パケットと出力パケットが sFlow でサンプルングされたパケットとして CPU に送信されます。sFlow エージェントはサンプルングされたパケットを処理し、sFlow アナライザに sFlow データグラムを送信します。sFlow データグラムには、元のサンプルングされたパケットに加えて、入力ポート、出力ポート、および元のパケット長に関する情報が含まれます。sFlow データグラムには、複数の sFlow サンプルを含めることができます。

sFlow の前提条件

sFlow には、次の前提条件があります。

- Cisco Nexus 9332PQ、9372PX、9372TX、93120TX スイッチ、および N9K-M6PQ 汎用拡張モジュール (GEM) 搭載の Cisco Nexus 9396PX、9396TX、93128TX スイッチについては、sFlow データ ソースとして設定するすべてのアップリンク ポート用の sFlow および SPAN ACL TCAM リージョン サイズを設定する必要があります。これを行うには、**hardware access-list tcam region sflow** および **hardware access-list tcam region span** コマンドを使用します。詳細については、『[ACL TCAM リージョン サイズの設定](#)』を参照してください。



(注) デフォルトでは、sflow リージョンサイズはゼロで、span リージョンサイズはゼロ以外です。ポートを sFlow データソースとして設定するには、sflow リージョンを 256 に設定し、十分なエントリを span リージョンに割り当てる必要があります。

- マルチキャストトラフィックの出力 sFlow には、ハードウェアマルチキャストグローバル TX スパン設定が必要です

sFlow の注意事項および制約事項



(注) スケールの情報については、リリース特定の『[Cisco Nexus 9000 Series NX-OS Verified Scalability Guide](#)』を参照してください。

sFlow には、次の注意事項と制限事項があります。

- 少なくとも 1 つの sFlow データソースが設定されている場合、SPAN セッションは起動できません。
 - 少なくとも 1 つの SPAN セッションが **no shut** として設定されている場合、sFlow データソースは追加できません。
 - sFlow に使用されるサンプルングモードは、LFSR と呼ばれるアルゴリズムに基づいています。LFSR を使用するため、数個のパケットごとに 1 個がサンプルングレート

n でサンプリングされることは保証されません。ただし、サンプリングされるパケットの数は、一定期間の合計パケット数と同じです。

- sFlow と SPAN が同じインターフェイスに設定されており、ハードウェア レートリミッタが sFlow 用に設定されている場合、**show hardware rate-limiter** コマンドの出力の Rate-Limiter Drops カウンタは予想よりも多くのドロップを表示します。
- sFlow はソフトウェア駆動型の機能で、ハードウェアは sFlow 送信元インターフェイスから CPU にトラフィックのコピーを送信するだけです。高い CPU 使用率が予想されます。ハードウェアによって CPU に送信される sFlow トラフィックは、CPU を保護するためにレート制限されます。
- インターフェイスの sFlow をイネーブルにすると、入力と出力の両方に対してイネーブルになります。入力だけまたは出力だけの sFlow をイネーブルにできません。
- sFlow は SVI ではサポートされません。
- サブインターフェイスは sFlow ではサポートされていません。
- システムの sFlow の設定およびトラフィックに基づいてサンプリングレートを設定することをお勧めします。
- スイッチは 1 つのみの sFlow コレクタをサポートします。
- sFlow とネットワーク アドレス変換 (NAT) は、同じポートではサポートされません。
- sFlow は、IPv4 コレクタ ポートでのみ IPv6 トラフィックのサンプリングをサポートしません。
- sFlow カウンタは、sFlow データ送信元インターフェイスに入力される制御パケットに対しても増加します。これらのパケットはサンプリングされ、sFlow データグラムとして送信されます (データ プレーン トラフィックと同様) 。
- 次の Cisco Nexus スイッチは、sFlow と SPAN を同時にサポートします。
 - N9336C-FX2
 - N93240YC-FX2
 - N93360YC-FX2
- Cisco NX-OS リリース 9.3(3) 以降、Cisco Nexus 9300-GX プラットフォーム スイッチは、sFlow と SPAN の両方をサポートしています。
- Cisco Nexus 9300-EX および 9300-FX プラットフォーム スイッチでは、FEX、HIF、および NIF ポートを sFlow データ ソース インターフェイスとして設定できません。

sFlow のデフォルト設定

次の表に、sFlow パラメータのデフォルト設定を示します。

表 21: デフォルトの sFlow パラメータ

パラメータ	デフォルト
sFlow のサンプリング レート	4096
sFlow のサンプリング サイズ	128
sFlow カウンタのポーリング間隔	20
sFlow の最大データグラム サイズ	1400
sFlow コレクタの IP アドレス	0.0.0.0
sFlow のコレクタ ポート	6343
sFlow エージェントの IP アドレス	0.0.0.0

sFlow の設定

sFlow の有効化

スイッチの sFlow を設定する前に sFlow 機能を有効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	configure terminal 例： switch# configure terminal switch(config)#	グローバル設定モードを開始します。
ステップ 2	[no] feature sflow 例： switch(config)# feature sflow	sFlow を有効または無効にします。
ステップ 3	(任意) show feature 例： switch(config)# show feature	有効および無効にされた機能を表示します。
ステップ 4	(任意) copy running-config startup-config 例： switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

サンプリングレートの設定

sFlow のサンプリングレートを設定できます。

始める前に

sFlow が有効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	[no] sflow sampling-rate sampling-rate 例： switch(config)# sflow sampling-rate 50000	パケットの sFlow のサンプリングレートを設定します。 <i>sampling-rate</i> には 4096 ~ 1000000000 の整数を指定できます。
ステップ 3	(任意) show sflow 例： switch(config)# show sflow	sFlow 設定を表示します。
ステップ 4	(任意) copy running-config startup-config 例： switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

最大サンプリングサイズの設定

サンプリングされたパケットからコピーする最大バイト数を設定できます。

始める前に

sFlow が有効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：	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
	switch# configure terminal switch(config)#	
ステップ 2	[no] sflow max-sampled-size <i>sampling-size</i> 例： switch(config)# sflow max-sampled-size 200	sFlow の最大サンプリングサイズを設定 します。 <i>sampling-size</i> の範囲は 64～256 バイトで す。
ステップ 3	(任意) show sflow 例： switch(config)# show sflow	sFlow 設定を表示します。
ステップ 4	(任意) copy running-config startup-config 例： switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スター トアップ コンフィギュレーションにコ ピーします。

カウンタのポーリング間隔の設定

データソースに関連するカウンタの継続的なサンプル間の最大秒数を設定できます。サンプリング間隔 0 は、カウンタのサンプリングをディセーブルにします。

始める前に

sFlow が有効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	[no] sflow counter-poll-interval <i>poll-interval</i> 例： switch(config)# sflow counter-poll-interval 100	インターフェイスの sFlow のポーリング 間隔を設定します。 <i>poll-interval</i> の範囲は 0～2147483647 秒 です。
ステップ 3	(任意) show sflow 例： switch(config)# show sflow	sFlow 設定を表示します。

	コマンドまたはアクション	目的
ステップ 4	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	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。

最大データグラム サイズの設定

1 つのサンプル データグラムで送信できるデータの最大バイト数を設定できます。

始める前に

sFlow が有効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 : <pre>switch# configure terminal switch(config)#</pre>	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] sflow max-datagram-size datagram-size 例 : <pre>switch(config)# sflow max-datagram-size 2000</pre>	sFlow の最大データグラム サイズを設定します。 <i>datagram-size</i> の範囲は 200~9000 バイトです。
ステップ 3	(任意) show sflow 例 : <pre>switch(config)# show sflow</pre>	sFlow 設定を表示します。
ステップ 4	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	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。

sFlow コレクタ アドレスの設定

管理ポートに接続されている sFlow データ コレクタの IPv4 アドレスを設定できます。

始める前に

sFlow が有効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 : <pre>switch# configure terminal switch(config)#</pre>	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] sflow collector-ip ip-address vrf vrf [source ip-address] 例 : <pre>switch(config)# sflow collector-ip 192.0.2.5 vrf management</pre>	<p>sFlow コレクタの IPv4 アドレスを設定します。IP アドレスを 0.0.0.0 に設定すると、すべてのサンプリングが無効になります。</p> <p>vrf は次のいずれかになります。</p> <ul style="list-style-type: none"> • ユーザ定義の VRF 名：最大 32 文字の英数字を指定できます。 • vrf 管理：sFlow データ コレクタが管理ポートに接続されたネットワークに存在する場合は、このオプションを使用する必要があります。 • vrf デフォルト：sFlow データ コレクタが前面パネルのポートに接続されたネットワークに存在する場合は、このオプションを使用する必要があります。 <p>source ip-address オプションを指定すると、送信される sFlow データグラムで送信元 IP アドレスが IP パケットの送信元アドレスとして使用されるようになります。送信元 IP アドレスは、スイッチのローカル インターフェイスの 1 つです。すでに設定されている必要があります。それ以外の場合は、エラー メッセージが表示されます。このオプションの設定後に送信元 IP アドレスを持つインターフェイスが変更または削除されると、sFlow データグラムは送信されなくなり、イベント履歴エラーと syslog エラーがログに記録されます。source ip-address オプションが未設定の場合、Cisco NX-OS は</p>

	コマンドまたはアクション	目的
		送信される sFlow データグラムに対して、IP パケットの送信元アドレスを自動的に選択します。
ステップ 3	(任意) show sflow 例： switch(config)# show sflow	sFlow 設定を表示します。
ステップ 4	(任意) copy running-config startup-config 例： switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

sFlow コレクタ ポート の設定

sFlow データグラムの宛先ポートを設定できます。

始める前に

sFlow が有効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	[no] sflow collector-port collector-port 例： switch(config)# sflow collector-port 7000	sFlow コレクタの UDP ポートを設定します。 <i>collector-port</i> の範囲は 1~65535 です。
ステップ 3	(任意) show sflow 例： switch(config)# show sflow	sFlow 設定を表示します。
ステップ 4	(任意) copy running-config startup-config 例： switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

sFlow エージェントアドレスの設定

sFlow エージェントの IPv4 アドレスを設定します。

始める前に

sFlow を有効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	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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] sflow agent-ip ip-address 例 : <pre>switch(config)# sflow agent-ip 192.0.2.3</pre>	<p>sFlow エージェントの IPv4 アドレスを設定します。</p> <p>デフォルトの IP アドレスは 0.0.0.0 です。つまり、すべてのサンプリングがスイッチで無効であることを示します。sFlow 機能をイネーブルにするには、有効な IP アドレスを指定する必要があります。</p> <p>(注) この IP アドレスは、コレクタに sFlow データグラムを送信するための送信元 IP アドレスとは限りません。</p>
ステップ 3	(任意) show sflow 例 : <pre>switch(config)# show sflow</pre>	sFlow 設定を表示します。
ステップ 4	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	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。

sFlow サンプリング データ ソースの設定

sFlow のサンプリングデータソースには、イーサネットポート、イーサネットポートの範囲、またはポート チャンネルとして設定できます。

始める前に

sFlow を有効にしていることを確認します。

データ ソースとしてポート チャネルを使用する場合は、すでにポート チャネルを設定して、ポート チャネル番号がわかっていることを確認してください。

Cisco Nexus 9332PQ、9372PX、9372TX、93120TX スイッチ、および N9K-M6PQ または N9K-M12PQ 汎用拡張モジュール (GEM) 搭載の Cisco Nexus 9396PX、9396TX、93128TX スイッチについて、これらのデバイスで sFlow データ ソースとして設定されているすべてのアップリンク ポート用の sFlow および SPAN ACL TCAM リージョン サイズが設定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	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] sflow data-source interface [ethernet slot/port[-port] port-channel channel-number] 例 : switch(config)# sflow data-source interface ethernet 1/5-12	sFlow のサンプリング データ ソースを設定します。 イーサネットのデータ ソースの場合、 <i>slot</i> はスロット番号、 <i>port</i> は 1 つのポート番号または <i>port-port</i> で指定されたポートの範囲です。
ステップ 3	(任意) show sflow 例 : switch(config)# show sflow	sFlow 設定を表示します。
ステップ 4	(任意) copy running-config startup-config 例 : switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

sFlow 設定の確認

sFlow 設定を表示するには、次のコマンドを使用します。

表 22: sFlow Show コマンド

コマンド	目的
show sflow	sFlow サンプラーおよびsFlow エージェント設定のすべてのデータ ソースを表示します。
show process	sFlow プロセスが実行されているかどうかを確認します。
show running-config sflow [all]	現在実行中の sFlow コンフィギュレーションを表示します。

sFlow 統計情報のモニタリングとクリア

sFlow 統計情報を表示するには、**show sflow statistics** コマンドを使用します。

sFlow 統計情報をクリアするには、次のコマンドを使用します。

コマンド	説明
clear sflow statistics	show sflow statistics コマンドから sFlow 統計情報のほとんどをクリアします。
clear counters interface all	show sflow statistics コマンドの [トータル パケット (Total Packets)] フィールドをクリアします。
clear hardware rate-limiter sflow	show sflow statistics コマンドの [トータル サンプル (Total Samples)] フィールドをクリアします。

sFlow の設定例

次に sFlow を設定する例を示します。

```
feature sflow
sflow sampling-rate 5000
sflow max-sampled-size 200
sflow counter-poll-interval 100
sflow max-datagram-size 2000
sflow collector-ip 192.0.2.5 vrf management
sflow collector-port 7000
sflow agent-ip 192.0.2.3
sflow data-source interface ethernet 1/5
```

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
ACL TCAM リージョン	IP ACL の設定



第 22 章

『Configuring TAP Aggregation and MPLS Stripping』

この章では、Cisco NX-OS デバイスで TAP アグリゲーションおよび MPLS ストリッピング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。

- [TAP アグリゲーションについて \(401 ページ\)](#)
- [MPLS ストリッピングについて \(404 ページ\)](#)
- [TAP アグリゲーションの設定 \(406 ページ\)](#)
- [TAP アグリゲーションの設定の確認 \(410 ページ\)](#)
- [TAP アグリゲーションの設定例 \(410 ページ\)](#)
- [MPLS ストリッピングの設定 \(411 ページ\)](#)
- [MPLS ストリッピング設定の確認 \(416 ページ\)](#)
- [MPLS ストリッピングカウンタおよびラベルエントリのクリア \(417 ページ\)](#)
- [MPLS ストリッピングの設定例 \(418 ページ\)](#)
- [その他の参考資料 \(418 ページ\)](#)

TAP アグリゲーションについて

ネットワーク TAP

さまざまなメソッドを使用して、パケットをモニタできます。1つのメソッドでは、物理ハードウェアテストアクセスポイント (TAP) が使用されます。

ネットワーク タップは、ネットワークを通過するデータへの直接インラインアクセスが可能なので、トラフィックのモニターリングに非常に役立ちます。多くの場合、サードパーティがネットワーク内の 2 ポイント間のトラフィックをモニタします。ポイント A と B の間のネットワークが物理ケーブルで構成されている場合、ネットワーク TAP がこのモニターリングを実現する最良の方法になります。ネットワーク TAP には、少なくとも 3 つのポート (A ポート、B ポート、およびモニタポート) があります。A ポートと B ポートの間に挿入される TAP は、

すべてのトラフィックをスムーズに通過させますが、同じデータをそのモニタ ポートにもコピーするため、サードパーティがリスンできるようになります。

TAP には次の利点があります。

- 全二重データ伝送を処理可能。
- 目立たず、ネットワークによって検出されることがなく、物理または論理アドレッシングが不要
- 一部の TAP は、分散 TAP を構築する機能のあるフル インライン パワーをサポート

ネットワークのエッジまたは仮想エッジにおけるサーバー間データ通信に対する可視性を確保しようとする場合、またはネットワークのインターネット エッジで侵入防御システム (IPS) アプライアンスにトラフィックのコピーを提供する場合でも、ネットワーク TAP は、環境内のほぼすべての場所で使用できます。ただし、大規模環境にネットワーク タップを導入する場合、多くのコストがかかり、運用の複雑さが増し、ケーブル配線の問題が生じます。

TAP アグリゲーション

TAP アグリゲーションは、データ センターのタスクのモニタリングとトラブルシューティングに役立つ代替ソリューションです。複数のテスト アクセス ポイント (TAP) の集約を許可し、複数のモニタリング システムに接続するようにデバイスを指定することで機能します。タップアグリゲーションスイッチは、監視する必要があるパケットを処理するネットワーク ファブリック内の特定のポイントにすべてのモニターリング デバイスをリンクします。

タップアグリゲーションスイッチソリューションでは、Cisco Nexus 9000 シリーズスイッチは、パケットのモニターリングに都合の良い、ネットワーク内のさまざまなポイントに接続されます。各ネットワーク要素から、スイッチドポートアナライザ (SPAN) または光 TAP を使用して、この TAP アグリゲーションスイッチにトラフィックフローを直接送信できます。TAP アグリゲーションスイッチ自体は、ネットワーク ファブリック内のイベントをモニタするために使用されるすべての分析ツールに直接接続されます。これらのモニターリングデバイスには、リモートモニターリング (RMON) プロンプ、アプリケーションファイアウォール、IPS デバイス、およびパケット スニファ ツールが含まれます。

特定のトラフィックをフィルタリングして1つ以上のツールにリダイレクトするように TAP アグリゲーションスイッチを設定できます。トラフィックを複数のインターフェイスにリダイレクトするために、マルチキャスト グループがスイッチの内部で作成され、リダイレクト リストの一部であるインターフェイスがメンバー ポートとして追加されます。リダイレクト アクションを持つアクセス コントロール リスト (ACL) ポリシーがインターフェイスに適用されると、作成された内部マルチキャスト グループに ACL ルールに一致するトラフィックがリダイレクトされます。

TAP 集約の注意事項と制約事項



(注) スケールの情報については、リリース特定の『Cisco Nexus 9000 Series NX-OS Verified Scalability Guide』を参照してください。

TAP アグリゲーションに関する注意事項と制約事項は次のとおりです。

- TAP アグリゲーション：
 - すべての Cisco Nexus 9300 シリーズ スイッチおよび 3164Q、31128PQ、3232C と 3264Q スイッチでサポートされます。
 - 100G ポートでサポートされます。
 - スイッチ ポートおよび入力方向でのみサポートされます。
 - Cisco Nexus 9200、9300、および 9300-EX シリーズ スイッチの UDF ベースの一致で IPv4 ACL をサポートします。
 - Cisco Nexus 9300-FX、9300-FX2、9300-FX3、9300-GX、9300-GX2、9500-EX、および 9500-FX プラットフォーム スイッチでサポートされます。
 - サポートされるリダイレクト ポートの最大数は 32 インターフェイスです。
- Cisco NX-OS リリース 9.2(1) 以降、MPLS タグに基づく TAP アグリゲーション フィルタは、次の Cisco Nexus プラットフォーム スイッチでサポートされています。
 - 9700-EX および 9700-FX ラインカードを搭載した Cisco Nexus 9000 プラットフォーム スイッチ。
 - Cisco Nexus 9200 プラットフォーム スイッチ。
 - Cisco Nexus 9300 プラットフォーム スイッチ。
 - Cisco Nexus 9500 スイッチ。
- 次の Cisco Nexus シリーズ スイッチ、ラインカードおよびファブリック モジュールでは、MPLS タグでの TAP アグリゲーション フィルタはサポートされていません。

表 23: Cisco Nexus 9000 シリーズ スイッチ

Cisco Nexus 3164Q-40GE	Cisco Nexus 9372PX	Cisco Nexus 9372PX-E
Cisco Nexus 9372TX	Cisco Nexus 9372TX-E	Cisco Nexus 9332PQ
Cisco Nexus 3232C	Cisco Nexus 93120TX	Cisco Nexus 31128PQ
Cisco Nexus 3264Q-S	—	—

表 24: Cisco Nexus 9500 シリーズ ラインカードおよびファブリック モジュール

N9K-X9564PX	N9K-X9564TX	N9K-X9536PQ
N9K-M12PQ	N9K-C93128TX	N9K-C9396PX
N9K-C9396TX	N9K-X9408PC-CFP2	N9K-M4PC-CFP2
N9K-X9432PQ	N9K-X9464PX	N9K-X9464TX
N9K-X9464TX2	N9K-X9632PC-QSFP100	N9K-S X9432C
N9K-M6PQ	N9K-M6PQ-E	—

- Cisco Nexus 9700-EX および 9700-FX ラインカードは、IPv4、IPv6、および MAC ACL による TAP アグリゲーションをサポートします。
- レイヤ 2 インターフェイスのみが TAP アグリゲーション ポリシーをサポートします。レイヤ 3 インターフェイスにポリシーを設定できますが、そのポリシーは機能しなくなります。
- リダイレクトポートは、送信元 (TAP) ポートと同じ VLAN の一部である必要があります。
- 各ルールは、1 つの固有の一致基準とのみ関連付ける必要があります。
- TAP アグリゲーション ポリシー用インターフェイスのリストを入力する場合は、スペースではなくカンマでエントリを区切る必要があります。たとえば、`port-channel50`、`ethernet1/12`、`port-channel20` などです。
- ポリシーにターゲット インターフェイスを指定する場合、簡略版ではなく、完全なインターフェイスタイプを入力する必要があります。たとえば、`eth1/1` の代わりに `ethernet1/1` を入力し、`po50` の代わりに `port-channel50` を入力します。
- `tcp-option-length` と `VLAN ID` フィルタを同時に使用する HTTP 要求はサポートされていません。両方のフィルタを同時に設定すると、ACE に対するトラフィック照合が機能しない場合があります。
- まだ設定されていないポートチャネルへのリダイレクトを使用して ACL エントリを設定する場合、ユーザーは指定されたポートチャネルを後で設定するように注意する必要があります。

MPLS ストリッピングについて

Cisco Nexus 9000 シリーズ スイッチの入力ポートは、さまざまなマルチプロトコル ラベル スイッチング (MPLS) パケットタイプを受信します。MPLS ネットワークの各データパケットには、1 つ以上のラベルヘッダーがあります。これらのパケットはリダイレクトアクセスコントロール リスト (ACL) に基づいてリダイレクトされます。

ラベルは、Forwarding Equivalence Class (FEC) を特定するために使用される短い4バイトの固定長のローカルで有効な識別子です。特定の packets に設定されているラベルは、その packets が割り当てられている FEC を表します。次のコンポーネントがあります。

- Label : ラベルの値 (非構造化)、20 ビット
- Exp : 試験的使用、3 ビット、現在、サービス クラス (CoS) フィールドとして使用
- S : スタックの一番下、1 ビット
- TTL : 存続可能時間、8 ビット

一部の MPLS ラベルは、レイヤ 2 ヘッダとレイヤ 3 ヘッダの間に適用されます。これらのラベルの場合、ヘッダとデータは標準バイト オフセットに配置されません。標準のネットワーク モニタリング ツールでは、このトラフィックのモニタリングと分析はできません。単一ラベルの packets は、MPLS ラベルヘッダーから取り除かれ、T キャッシュ デバイスにリダイレクトされます。

複数のラベルヘッダーがある MPLS packets は、MPLS ヘッダーが削除されずに、ディープ packets インスペクション (DPI) デバイスに送信されます。

Cisco NX-OS リリース 7.0(3)I7(3) 以降、Cisco Nexus 9300-EX スイッチでは、リダイレクトポートから送信される packets に VLAN タグを適用できます。MPLS ストリップで 1~5 個のラベルをポップできます。

MPLS ストリッピングに関する注意事項と制限事項



- (注) スケールの情報については、リリース特定の『Cisco Nexus 9000 Series NX-OS Verified Scalability Guide』を参照してください。

MPLS ストリッピングに関する注意事項と制約事項は次のとおりです。

- Cisco Nexus 9700-EX および 9700-FX ラインカードは、MPLS ストリッピングをサポートしていません。
- Cisco Nexus 9000-FX2 スイッチ (N9K-C93216TC-FX2、N9K-C93240YC-FX2、N9K-C93360YC-FX2、N9K-C9336C-FX2) は、EoMPLS カプセル化タイプの MPLS ストリッピングをサポートしていません。ただし、IPoMPLS ストリップはサポートされています。
- MPLS ストリッピングを有効にする前に、すべてのレイヤ 3 および vPC 機能を無効にします。
- スタティック MPLS、MPLS セグメントルーティング、および MPLS ストリッピングを同時に有効にすることはできません。
- MPLS ストリッピングに関係する入力インターフェイスで、TAP 集約が有効になっている必要があります。

- 目的の宛先にパケットを転送するためには、入力インターフェイスのリダイレクトアクションを使用してタップアグリゲーション ACL を設定する必要があります。
- システムでは 1 つのタップ ACL のみサポートされます。
- MPLS ストリップ後、SMAC はスイッチ mac (`show vdc`) に変更され、DMAC は **00:00:00:ab:cd:ef** に設定されます。
- 削除されたパケットが出力される出力インターフェイスは、許可 VLAN としての VLAN 1 が存在するインターフェイスである必要があります。出力インターフェイスは、デフォルトですべての VLAN が許可されるトランクとして設定することを推奨します。
- ストリッピングは IP PACL に基づいており、ストリッピングに MAC-ACL を使用することはできません。
- MPLS ストリッピングは、IPv4 トラフィックに対してのみサポートされます。
- MPLS ストリッピング パケットの場合、ポートチャネルロードバランシングがサポートされます。
- レイヤ 3 ヘッダー ベースのハッシュおよびレイヤ 4 ヘッダー ベースのハッシュはサポートされていますが、レイヤ 2 ヘッダー ベースのハッシュはサポートされていません。
- MPLS ストリッピング中、着信 VLAN は維持されません。
- Cisco Nexus 9200、9300-EX、および 9300-FX プラットフォーム スイッチは、リダイレクトポートから送信されるパケットへの VLAN のタグgingをサポートします。入力/出力ポートは、イーサネットまたはポート チャネルのいずれかです。VLAN タグは、着信ポート設定から取得されます。入力インターフェイスの新しい ACL を、インターフェイス VLAN 値とは異なる VLAN 値に関連付けないでください。
- 一意のリダイレクトポートリストを持つすべての ACE (特定の VLAN に関連付けられた ACL の下) に対して、ハードウェア エントリを割り当てます。現在の ACE 数のハードウェア制限は 50 で、50 を超える ACE を設定することはできません。
- MPLS ストリップは、MPLS ラベル スタックのレイヤ 3 パケットでのみサポートされます。
- MPLS ストリップは、疑似回線または VPLS ではサポートされません。

TAP アグリゲーションの設定

ラインカードの TAP 集約のイネーブル化

Cisco NX-OS リリース 7.0(3)I7(2) 以降では、9700-EX および 9700-FX ラインカードを備えた Cisco Nexus 9500 プラットフォーム スイッチの TAP 集約を有効にできます。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル設定モードを開始します。
ステップ 2	[no] hardware acl tap-agg 例： switch(config)# hardware acl tap-agg	Cisco Nexus 9700-EX および 9700-FX ラインカードの TAP 集約を有効にします。 このコマンドは、Cisco Nexus 9300-GX プラットフォーム スイッチでも必要であり、リロードが必要になる場合があります。
ステップ 3	(任意) copy running-config startup-config 例： switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

TAP 集約ポリシーの設定

IP アクセス コントロール リスト (ACL) または MAC ACL で、TAP アグリゲーション ポリシーを設定できます。

始める前に

IPv4 ポート ACL または MAC ポート ACL 用の ACL TCAM のリージョンサイズは、**hardware access-list tcam region {ifacl | mac-ifacl}** コマンドを使用して設定する必要があります。**hardware access-list team region ipv6-ifcal** コマンドを使用して、IPv6 ポート ACL の ACL TCAM リージョンサイズを設定します。

詳細については、『Cisco Nexus 9000 シリーズ NX-OS セキュリティの設定ガイド』の「ACL TCAM リージョンサイズの設定」を参照してください。



- (注) デフォルトでは、ifacl と mac-ifacl の両方の領域サイズはゼロです。TAP 集約をサポートするには、ifacl または mac-ifacl リージョンに十分なエントリを割り当てる必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	次のいずれかのコマンドを入力します。 <ul style="list-style-type: none"> • ip access-list access-list-name • mac access-list access-list-name 例 : <pre>switch(config)# ip access-list test switch(config-acl)# switch(config)# mac access-list mactapl switch(config-mac-acl)# switch(config)# ipv6 access-list testv6 switch# sh running-config aclmgr !Command: show running-config aclmgr !Time: Thu Aug 11 18:19:50 2016 version 7.0(3)I5(1) ipv6 access-list testv6 10 permit ipv6 any any redirect Ethernet2/1 interface Ethernet6/6 ipv6 port traffic-filter testv6 in</pre>	(注) Cisco NX-OS リリース 7.0(3)I5(2) 以降、IPv6 ACL のサポートが Cisco Nexus 9000 シリーズ スイッチに追加されました。IPv6 ACL ではリダイレクトアクションがサポートされます。リダイレクトアクションでは、現在 IPv6 PACL でサポートされているすべての match オプションがサポートされています。 IP ACL を作成して IP アクセス リスト コンフィギュレーション モードを開始するか、あるいは MAC ACL を作成して MAC アクセス リスト 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	(任意) statistics per-entry 例 : <pre>switch(config-acl)# statistics per-entry</pre>	各エントリで許可または拒否されるパケット数の統計情報の記録を開始します。
ステップ 4	[no] permit protocol source destination redirect interfaces 例 : <pre>switch(config-acl)# permit ip any any redirect ethernet1/8</pre>	条件ごとにトラフィックのリダイレクトを許可する IP または MAC ACL ルールを作成します。このコマンドの いずれのバージョンも 、ポリシーからのパーミッションを削除することはありません。

	コマンドまたはアクション	目的
		(注) TAP 集約ポリシーのインターフェイスを入力するときは、それを省略しないでください。インターフェイスのリストを入力するときは、コンマで区切り、スペースを入れしないでください。
ステップ 5	<p>(任意) 次のいずれかのコマンドを入力します。</p> <ul style="list-style-type: none"> • show ip access-lists [<i>access-list-name</i>] • show mac access-lists [<i>access-list-name</i>] <p>例 :</p> <pre>switch(config-acl)# show ip access-lists test switch(config-mac-acl)# show mac access-lists mactap1</pre>	すべての IPv4 または MAC ACL、あるいは特定の IPv4 または MAC ACL を表示します。
ステップ 6	<p>(任意) copy running-config startup-config</p> <p>例 :</p> <pre>switch(config-acl)# copy running-config startup-config</pre>	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。

TAP アグリゲーションポリシーのインターフェイスへのアタッチ

TAP アグリゲーションで設定された ACL をレイヤ 2 インターフェイスに適用できます。

手順

	コマンドまたはアクション	目的
ステップ 1	<p>configure terminal</p> <p>例 :</p> <pre>switch# configure terminal switch(config)#</pre>	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	<p>interface type slot/port</p> <p>例 :</p> <pre>switch(config)# interface ethernet 2/2 switch(config-if)#</pre>	指定したインターフェイスに対してインターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	switchport 例： <pre>switch(config-if)# switchport</pre>	レイヤ3インターフェイスをレイヤ2インターフェイスに変更します。 (注) インターフェイスがレイヤ2インターフェイスであることを確認します。
ステップ 4	次のいずれかのコマンドを入力します。 <ul style="list-style-type: none"> • [no] ip port access-group access-list-name in • [no] mac port access-group access-list-name in 例： <pre>switch(config-if)# ip port access-group test in</pre> <pre>switch(config-if)# mac port access-group test in</pre>	TAP 集約で設定された IPv4 または MAC ACL をインターフェイスに適用します。このコマンドの no 形式を使用すると、インターフェイスから ACL を削除します。
ステップ 5	(任意) copy running-config startup-config 例： <pre>switch(config-if)# copy running-config startup-config</pre>	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。

TAP アグリゲーションの設定の確認

TAP アグリゲーション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 ip access-lists [<i>access-list-name</i>]	すべての IPv4 ACL または特定の IPv4 ACL を表示します。
show mac access-lists [<i>access-list-name</i>]	すべての MAC ACL または特定の MAC ACL を表示します。

TAP アグリゲーションの設定例

次に、IPv4 ACL で TAP アグリゲーションポリシーを設定する例を示します。

```
switch# configure terminal
switch(config)# ip access-list test
```

```

switch(config-acl)# 10 deny ip 100.1.1/24 any
switch(config-acl)# 20 permit tcp any eq www any redirect port-channel4
switch(config-acl)# 30 permit ip any any redirect
Ethernet1/1,Ethernet1/2,port-channel7,port-channel8,Ethernet1/12,Ethernet1/13
switch(config-acl)# show ip access-lists test
IP access list test
    10 deny ip 100.1.1/24 any
    20 permit tcp any eq www any redirect port-channel4
    30 permit ip any any redirect
Ethernet1/1,Ethernet1/2,port-channel7,port-channel8,Ethernet1/12,Ethernet1/13

```

次に、UDF ベースの一致を使用して IPv4 ACL に TAP 集約ポリシーを適用する例を示します。

```

switch# configure terminal

switch(config)# ip access-list tap_agg
switch(config-acl)# statistics per-entry
switch(config-acl)# 10 permit ip any any redirect Ethernet1/1
switch(config-acl)# 20 deny ip any any
switch# configure terminal
switch(config)# interface Ethernet1/4
switch(config-if)# ip port access-group tap_agg in
switch(config-if)# switchport
switch(config-if)# no shutdown

```

次に、MAC ACL で TAP アグリゲーション ポリシーを設定する例を示します。

```

switch# configure terminal

switch(config)# mac access-list mactap1
switch(config-mac-acl)# 10 permit any any 0x86dd redirect port-channel1
switch(config-mac-acl)# show mac access-lists mactap1
MAC access list mactap1
    10 permit any any 0x86dd redirect port-channel1

```

次に、TAP アグリゲーション ポリシーをレイヤ 2 インターフェイスにアタッチする例を示します。

```

switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# ip port access-group test in
switch(config-if)#

```

MPLS ストリッピングの設定

MPLS ストリッピングの有効化

MPLS ストリッピングをグローバルに有効にできます。

始める前に

MPLS ストリッピングを有効にする前に、すべてのレイヤ 3 および vPC 機能を無効にします。

mode tap-aggregation コマンドを使用して、TAP アグリゲーション ポリシーを含む ACL をレイヤ 2 インターフェイスまたはポート チャネルにアタッチします。詳細については、[TAP アグリゲーション ポリシーのインターフェイスへのアタッチ \(409 ページ\)](#) 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	configure terminal 例： switch# configure terminal switch(config)#	グローバル設定モードを開始します。
ステップ 2	[no] mpls strip 例： switch(config)# mpls strip	MPLS ストリッピングをグローバルに有効にします。このコマンドの no 形式を使用すると、MPLS ストリッピングが無効化されます。
ステップ 3	[no] mpls strip mode dot1q 例： switch(config)# mpls strip mode dot1q	リダイレクトポートからのパケットの VLAN タギングを有効にします。タグ付けする必要がある VLAN は、入力ポートで指定する必要があります。
ステップ 4	必須: copy running-config startup-config 例： switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

VLAN タグの着信ポートの設定

VLAN タグは、着信ポート設定から取得されます。入力/出力ポートは、イーサネットまたはポート チャネルのいずれかです。

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	interface type slot/port 例： switch(config)# interface ethernet 1/26 switch(config-if)#	指定したインターフェイスに対してインターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	switchport 例 : <pre>switch(config-if)# switchport</pre>	レイヤ3インターフェイスをレイヤ2インターフェイスに変更します。 (注) インターフェイスがレイヤ2インターフェイスであることを確認します。
ステップ 4	次のいずれかのコマンドを入力します。 <ul style="list-style-type: none"> • [no] ip port access-group access-list-name in • [no] mac port access-group access-list-name in 例 : <pre>switch(config-if)# ip port access-group test in</pre> <pre>switch(config-if)# mac port access-group test in</pre>	TAP 集約で設定された IPv4 または MAC ACL をインターフェイスに適用します。このコマンドの no 形式を使用すると、インターフェイスから ACL を削除します。
ステップ 5	次のいずれかのコマンドを入力します。 <ul style="list-style-type: none"> • [no] ip port access-group access-list-name in • [no] mac port access-group access-list-name in 例 : <pre>switch(config-if)# ip port access-group test in</pre> <pre>switch(config-if)# mac port access-group test in</pre>	TAP 集約で設定された IPv4 または MAC ACL をインターフェイスに適用します。このコマンドの no 形式を使用すると、インターフェイスから ACL を削除します。
ステップ 6	必須: mode tap-aggregation vlan vlan_id 例 : <pre>switch(config-if)# mode tap-aggregation vlan 26</pre>	リダイレクトポートからのパケットにタグ付けされる VLAN の値を設定します。
ステップ 7	(任意) copy running-config startup-config 例 : <pre>switch(config-if)# copy running-config startup-config</pre>	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。

MPLS ラベルの追加と削除

デバイスは、フレームが TAP インターフェイスで不明なラベルを受信するたびにラベルを動的に学習できます。また、スタティック MPLS ラベルを追加または削除できます。

始める前に

TAP アグリゲーションポリシーを設定してインターフェイスへアタッチする詳細については、『Cisco Nexus 9000 Series NX-OS System Management Configuration Guide』を参照してください。

目的の宛先にパケットを転送するためには、入力インターフェイスのリダイレクトアクションを使用してタップアグリゲーション ACL を設定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	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	mpls strip label ラベル 例 : <pre>switch(config)# mpls strip label 100</pre>	指定したスタティック MPLS ラベルを追加します。ラベルの 20 ビット値の範囲は 1 ~ 1048575 です。 (注) この CLI は、次のクラウドスケールプラットフォームスイッチを除き、「注意事項と制限事項」の項で MPLS ストリッピング機能に指定されたすべてのプラットフォームスイッチで使用できます。 <ul style="list-style-type: none"> • N9K-C93180YC-EX • N9K-C93180YC-FX • N9K-C93240YC-FX2 • N9K-C93180YC-FX3 [no] mpls strip label {label all} コマンドは、指定したスタティック MPLS ラベルを削除します。 all オプションは、すべてのスタティック MPLS ラベルを削除します。

	コマンドまたはアクション	目的
ステップ 3	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	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。

宛先 MAC アドレスの設定

削除された出力フレームの宛先 MAC 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	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	mpls strip dest-mac mac-address 例 : <pre>switch(config)# mpls strip dest-mac 1.1.1</pre>	ヘッダーが削除された出力フレームの宛先 MAC アドレスを指定します。 MAC アドレスは、次の 4 つのいずれかの形式で指定できます。 <ul style="list-style-type: none"> • E.E.E • EE-EE-EE-EE-EE-EE • EE:EE:EE:EE:EE:EE • EEEE.EEEE.EEEE
ステップ 3	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	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。

MPLS ラベル エージングの設定

使用されていないダイナミック MPLS ラベルがエージアウトする時間を定義できます。

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	mpls strip label-age 経過期間 例： switch(config)# mpls strip label-age 300	ダイナミック MPLS ラベルがエージアウトする時間を指定します (秒)。範囲は 61～31622400 です。
ステップ 3	(任意) copy running-config startup-config 例： switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

MPLS ストリッピング設定の確認

MPLS ストリッピング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 mpls strip labels [<i>label</i> all dynamic static]	MPLS ラベルに関する情報を表示します。次のオプションを指定できます。 <ul style="list-style-type: none"> • label : 表示するラベル • all : すべてのラベルを表示することを指定します。これがデフォルトのオプションです。 • dynamic : ダイナミック ラベルのみ表示することを指定します。 • static : スタティック ラベルのみ表示することを指定します。

次に、すべての MPLS ラベルを表示する例を示します。

```
switch# show mpls strip labels
MPLS Strip Labels:
  Total      : 3005
  Static     : 5
Legend:      * - Static Label
             Interface - where label was first learned
             Idle-Age - Seconds since last use
```

```

SW-Counter- Packets received in Software
HW-Counter- Packets switched in Hardware
-----
Label      Interface      Idle-Age      SW-Counter      HW-Counter
-----
4096      Eth1/53/1      15            1                210
4097      Eth1/53/1      15            1                210
4098      Eth1/53/1      15            1                210
4099      Eth1/53/1      7             2                219
4100      Eth1/53/1      7             2                219
4101      Eth1/53/1      7             2                219
4102      Eth1/53/1      39            1                206
4103      Eth1/53/1      39            1                206
4104      Eth1/53/1      39            1                206
4105      Eth1/53/1      1             1                217
4106      Eth1/53/1      1             1                217
4107      Eth1/53/1      1             1                217
4108      Eth1/53/1      15            1                210
* 25000   None <User>    39            1                206
* 20000   None <User>    39            1                206
* 21000   None <User>    1             1                217

```

次に、スタティック MPLS ラベルのみ表示する例を示します。

```

switch(config)# show mpls strip labels static
MPLS Strip Labels:
  Total      : 3005
  Static     : 5
Legend:      * - Static Label
  Interface - where label was first learned
  Idle-Age  - Seconds since last use
  SW-Counter- Packets received in Software
  HW-Counter- Packets switched in Hardware
-----
Label      Interface      Idle-Age      SW-Counter      HW-Counter
-----
* 300      None <User>    403            0                0
* 100      None <User>    416            0                0
* 25000    None <User>    869            0                0
* 20000    None <User>    869            0                0
* 21000    None <User>    869            0                0

```

MPLS ストリッピング カウンタおよびラベル エントリのクリア

MPLS ストリッピング カウンタとラベル エントリをクリアするには、次の作業を行います。

コマンド	目的
clear mpls strip label dynamic	MPLS ラベル テーブルからダイナミック ラベル エントリをクリアします。
clear counters mpls strip	すべての MPLS ストリッピング カウンタをクリアします。

次に、すべての MPLS ストリッピング カウンタをクリアする例を示します。

```

switch# clear counters mpls strip
switch# show mpls strip labels
MPLS Strip Labels:
  Total      : 15000
  Static     : 2
Legend:      * - Static Label
  Interface - where label was first learned
  Idle-Age  - Seconds since last use
  SW-Counter- Packets received in Software
  HW-Counter- Packets switched in Hardware
-----
      Label      Interface      Idle-Age      SW-Counter      HW-Counter
-----
      4096      Eth1/44          15              0              0
      8192      Eth1/44          17              0              0
     12288      Eth1/44          15              0              0
     16384      Eth1/44          39              0              0
     20480      Eth1/44          47              0              0
     24576      Eth1/44          7               0              0
     28672      Eth1/44          5               0              0
     36864      Eth1/44          7               0              0
     40960      Eth1/44          19              0              0
     45056      Eth1/44          9               0              0
     49152      Eth1/44          45              0              0
     53248      Eth1/44          9               0              0

```

MPLS ストリッピングの設定例

次に、スタティック MPLS ラベルを追加する例を示します。

```

switch# configure terminal
switch(config)# mpls strip label 100
switch(config)# mpls strip label 200
switch(config)# mpls strip label 300

```

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
IP ACL	『Cisco Nexus 9000 Series NX-OS Security Configuration Guide』
MAC ACL	『Cisco Nexus 9000 Series NX-OS Security Configuration Guide』
ポートチャネル対称ハッシュ	『Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide』
リモート モニタリング (RMON)	RMON の設定 (218 ページ)

関連項目	マニュアルタイトル
スイッチドポートアナライザ (SPAN)	SPAN の設定 (293 ページ)
トラブルシューティング	『Cisco Nexus 9000 Series NX-OS Troubleshooting Guide』



第 23 章

MPLS アクセス リストの構成

- [MPLS アクセス リストの構成 \(421 ページ\)](#)
- [MPLS アクセス リスト構成の検証 \(422 ページ\)](#)
- [MPLS アクセス リストの構成例 \(422 ページ\)](#)

MPLS アクセス リストの構成

MPLS アクセス リストを使用すると、MPLS ラベルに基づいて MPLS パケットをフィルタリングし、フィルタリングされたパケットを構成済みのリダイレクトインターフェイスに送信できます。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル設定モードを開始します。
ステップ 2	[no]install feature-set mpls 例 : <pre>switch(config)# install feature-set mpls switch(config)# feature-set mpls switch(config)# feature mpls segment-routing</pre>	MPLS パケットの解析を有効にします。 これは、MPLS ラベルに基づいて MPLS パケットをフィルタリングするために必須です。
ステップ 3	mpls access list mpls-acl 例 : <pre>switch(config)# mpls access list mpls-acl switch(config-mpls-acl)# 10 permit mpls 1600 any redirect Ethernet1/15</pre>	着信外部 MPLS ラベルに基づくフィルタリングを使用して、mpls-access リストを構成します。 この例では、着信ラベル 1600 と MPLS パケットが一致し、Ethernet1/15 にリダイレクトされます。

	コマンドまたはアクション	目的
ステップ 4	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	(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。

MPLS アクセス リスト構成の検証

MPLS アクセス リスト構成を表示するには、の作業を実行します。

コマンド	目的
show mpls access lists	MPLS アクセス リストの情報を表示します。

MPLS アクセス リストの構成例

次の例は、MPLS アクセス リストを構成する方法を示しています。

```
switch# configure terminal
switch(config)# install feature-set mpls
switch(config)# feature-set mpls
switch(config)# feature mpls segment-routing
switch(config)# mpls access list mpls-acl
switch(config-mpls-acl)# 10 permit mpls 1600 any redirect Ethernet1/15
switch(config)# copy running-config startup-config
```



第 24 章

グレースフル挿入と削除の設定

この章では、Cisco Nexus 9000 シリーズ スイッチでグレースフル挿入と削除（GIR）を設定する方法について説明します。

この章は、次の内容で構成されています。

- [グレースフル挿入と削除について](#) (423 ページ)
- [GIR の注意事項と制限事項](#) (426 ページ)
- [GIR ワークフロー](#) (427 ページ)
- [メンテナンス モード プロファイルの設定](#) (427 ページ)
- [通常モード プロファイルの設定](#) (429 ページ)
- [スナップショットの作成](#) (430 ページ)
- [スナップショットへの show コマンドの追加](#) (432 ページ)
- [グレースフル削除のトリガー](#) (434 ページ)
- [グレースフル挿入のトリガー](#) (437 ページ)
- [メンテナンス モードの強化](#) (438 ページ)
- [GIR 設定の確認](#) (439 ページ)
- [GIR の設定例](#) (441 ページ)

グレースフル挿入と削除について

グレースフル挿入と削除を使用してスイッチを正常に取り出し、そのスイッチをネットワークから分離して、デバッグ操作やアップグレード操作を実行することができます。スイッチは、最小限のトラフィックの中断だけで、通常の転送パスから取り外されます。デバッグ操作やアップグレード操作の実行が終了したら、グレースフル挿入を使用して、そのスイッチを完全な運用（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、すべての設定済みのレイヤ 3 コントロールプレーンがネットワークから分離されます。この状態では、直接接続されたルートは取り消されたり変更されたりしません。通常モードが復元されると、すべてのルートのアドバタイズメントが復元されます。

グレースフル削除では、すべてのプロトコルと vPC ドメインが正常に停止し、スイッチはネットワークから分離されます。グレースフル挿入では、すべてのプロトコルと vPC ドメインが復元されます。

次のプロトコルは、IPv4 と IPv6 両方のアドレス ファミリでサポートされます。

- Border Gateway Protocol (BGP)
- Enhanced Interior Gateway Routing Protocol (EIGRP)
- Intermediate System-to-Intermediate System (ISIS)
- Open Shortest Path First (OSPF)
- Protocol Independent Multicast (PIM)
- Routing Information Protocol (RIP)



(注) グレースフル挿入と削除の場合、PIM プロトコルは vPC 環境にのみ適用できます。グレースフル削除の間、vPC 転送ロールがマルチキャストトラフィックのすべてのノースバウンド送信元に対する vPC ピアに転送されます。

プロファイル

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。

プロトコルを個別に分離、シャットダウン、または復元する（あるいは追加の設定を実施する）場合は、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、プロファイルを作成できます。ただし、プロトコルの順序が正しいことを確認し、すべての依存関係を考慮する必要があります。

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。

プロファイルでは、次のコマンド（および任意の設定コマンド）がサポートされています。



(注) ルーティング プロトコル インスタンスまたはメンテナンスモード プロファイルで **shutdown** と **isolate** の両方が設定されている場合、**shutdown** コマンドが優先されます。

コマンド	説明
isolate	プロトコルをスイッチから分離し、プロトコルをメンテナンスモードにします。
no isolate	プロトコルを復元し、プロトコルを通常モードにします。
shutdown	プロトコルまたは vPC ドメインをシャットダウンします。
no shutdown	プロトコルまたは vPC ドメインを起動します。
system interface shutdown [exclude fex-fabric]	システム インターフェイスをシャットダウンします (管理 インターフェイスを除く)。
no system interface shutdown [exclude fex-fabric]	システム インターフェイスを起動します。
sleep instance <i>instance-number seconds</i>	指定の秒数だけコマンドの実行を遅延させます。コマンドの複数のインスタンスを遅延できます。 <i>instance-number</i> および <i>seconds</i> 引数の範囲は、0 ~ 2177483647 です。
python instance <i>instance-number uri [python-arguments]</i> 例 : python instance 1 bootflash://script1.py	Python スクリプトの呼び出しをプロファイルに設定します。コマンドの複数の呼び出しをプロファイルに追加できます。 Python 引数には最大 32 文字の英数字を入力できます。



(注) Cisco NX-OS リリース 9.3(5) 以降、**isolate** コマンドは **include-local** オプションとともに提供されます。これは、**router bgp** にのみ適用されます。

このオプションを使用すると、BGP はピアからすべてのルートを取り消します。このオプションを使用しない場合、BGP はリモートで学習したルートのみを撤回し、集約、注入、ネットワーク、再頒布などのローカルで生成されたルートは、eBGP ピアへの最大の Multi-Exit Discriminator (MED) と iBGP ピアへの最小のローカルプリファレンスで引き続きアドバタイズされます。

スナップショット

Cisco NX-OS では、スナップショットは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するプロセスです。

スナップショットは、グレースフル削除前とグレースフル挿入後のスイッチの状態を比較する場合に役立ちます。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て、機能間の相違を表示する

GIR の注意事項と制限事項

グレースフル挿入と置換 (GIR) には、設定に関し、次の注意事項と制約事項があります。

- Cisco NX-OS リリース 9.2(1) 以降では、L2 グレースフル挿入および置換がサポートされています。通常モードからメンテナンスモードに移行すると、MCT がダウンし、垂直型トラフィックが収束します。ゼロ パケット損失はサポートされていません。次の表に、各 VPC ポートに 2 ポート メンバー、60k MAC スケールを持つ 10 の vPC でのトラフィックコンバージェンスの例を示します。

表 25:

トリガー	ロール	垂直型トラフィック	逆垂直型トラフィック
通常からメンテナンスモードへ	プライマリ	760 ms	1320 ms
メンテナンスモードから通常モードへ	プライマリ	13155 ms	27980 ms
通常からメンテナンスモードへ	セカンダリ	300 ミリ秒	1375 ms
メンテナンスモードから通常モードへ	セカンダリ	15905 ms	23350 ms

- Cisco NX-OS リリース 9.2(1) 以降では、OSPF の分離オプションを設定すると、直接ルートとスタブルートが最大メトリックルートとしてアドバタイズされます。その結果、1つの vPC スイッチだけが分離されている場合、SVI ホストへの垂直型トラフィックは vPC ピアを通過します。

- 通常モードとメンテナンス モードの新しいカスタム プロファイルを作成する前に、すべての既存のカスタムプロファイルを削除してください。
- Cisco NX-OS リリース 9.3(5) 以降、**include-local** オプションが既存の **isolate** コマンドに追加されています。ただし、**include-local** オプションは **router bgp** のみに適用されます。

GIR ワークフロー

グレースフル挿入と削除 (GIR) のワークフローを完了する手順は、次のとおりです。

1. (任意) メンテナンス モードプロ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の設定 (427 ページ) を参照)。
2. (任意) 通常モードプロファイルを作成します (通常モードプロファイルの設定 (429 ページ) を参照)。
3. グレースフル削除をトリガーする前のスナップショットを取得します (スナップショットの作成 (430 ページ) を参照)。
4. グレースフル削除をトリガーして、スイッチをメンテナンスモードにします (グレースフル削除のトリガー (434 ページ) を参照)。
5. グレースフル挿入をトリガーして、スイッチを通常モードに戻します (グレースフル挿入のトリガー (437 ページ) を参照)。
6. グレースフル挿入をトリガーした後のスナップショットを取得します (スナップショットの作成 (430 ページ) を参照)。
7. `show snapshots compare` コマンドを使用して、グレースフル削除と挿入の前後のスイッチの運用データを比較して、すべてが想定どおりに動作していることを確認します (GIR 設定の確認 (439 ページ) を参照)。

メンテナンス 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	<p>[no] configure maintenance profile maintenance-mode</p> <p>例 :</p> <pre>switch# configure maintenance profile maintenance-mode Enter configuration commands, one per</pre>	<p>メンテナンス モードプロファイルのコンフィギュレーションセッションを開始します。 no オプションは、メンテナンス プロファイルのメンテナンス モードを削除します。</p>

	コマンドまたはアクション	目的
	<pre>line. End with CNTL/Z. switch(config-mm-profile) #</pre>	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。サポートされるコマンドの一覧については、 プロファイル (424 ページ) を参照してください。
ステップ 2	end 例 : <pre>switch(config-mm-profile) # end switch#</pre>	メンテナンス モード プロファイルを終了します。
ステップ 3	show maintenance profile maintenance-mode 例 : <pre>switch# show maintenance profile maintenance-mode</pre>	メンテナンス モード プロファイルの詳細を表示します。

例

次に、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
Enter configuration commands, one per line. End with CNTL/Z.
switch(config-mm-profile) # ip pim isolate
switch(config-mm-profile) # vpc domain 10
switch(config-mm-profile-config-vpc-domain) # shutdown
switch(config-mm-profile) # router bgp 100
switch(config-mm-profile-router) # shutdown
switch(config-mm-profile) # router eigrp 10
switch(config-mm-profile-router) # shutdown
switch(config-mm-profile-router) # address-family ipv6 unicast
switch(config-mm-profile-router-af) # shutdown
switch(config-mm-profile) # system interface shutdown
switch(config-mm-profile) # end
Exit maintenance profile mode.
switch# show maintenance profile maintenance-mode
[Maintenance Mode]
ip pim isolate
vpc domain 10
  shutdown
router bgp 100
  shutdown
router eigrp 10
  shutdown
  address-family ipv6 unicast
    shutdown
system interface shutdown
```

次に、カスタムプロファイルでスリープインスタンスを設定して、次のプロトコル変更までの遅延を追加する例を示します。


```

switch# configure maintenance profile maintenance-mode
Enter configuration commands, one per line. End with CNTL/Z.
switch(config-mm-profile)# router bgp 65001
switch(config-mm-profile-router)# isolate
switch(config-mm-profile-router)# sleep instance 1 10
switch(config-mm-profile)# router eigrp 200
switch(config-mm-profile-router)# isolate
switch(config-mm-profile-router)# sleep instance 2 15
switch(config-mm-profile)# router ospf 100
switch(config-mm-profile-router)# isolate
switch(config-mm-profile-router)# sleep instance 3 20
switch(config-mm-profile)# router ospfv3 300
switch(config-mm-profile-router)# isolate
switch(config-mm-profile-router)# sleep instance 4 5
switch(config-mm-profile)# router isis 400
switch(config-mm-profile-router)# isolate
switch(config-mm-profile)#end
Exit maintenance profile mode.
switch#
    
```



- (注) メンテナンス モード プロファイルの適用中に `exec` コマンドを実行するか、動的遅延を追加する必要がある場合は、`python instance instance-number uri [python-arguments]` スクリプトを使用します。

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、通常モード プロファイルを作成できます。

手順

	コマンドまたはアクション	目的
ステップ 1	<p>[no] configure maintenance profile normal-mode</p> <p>例 :</p> <pre> switch# configure maintenance profile normal-mode Enter configuration commands, one per line. End with CNTL/Z. switch(config-mm-profile)# </pre>	<p>通常モードプロファイルのコンフィギュレーションセッションを開始します。</p> <p>no バージョンは、メンテナンス プロファイルの normal-mode を削除します。</p> <p>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。サポートされるコマンドの一覧については、プロファイル (424 ページ) を参照してください。</p>
ステップ 2	<p>end</p> <p>例 :</p> <pre> switch(config-mm-profile)# end switch# </pre>	<p>通常モードプロファイルを終了します。</p>

	コマンドまたはアクション	目的
ステップ 3	show maintenance profile normal-mode 例 : <pre>switch# show maintenance profile normal-mode</pre>	通常モードプロファイルの詳細を表示します。

例

次に、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 normal-mode
switch(config-mm-profile)# no system interface shutdown
switch(config-mm-profile)# router eigrp 10
switch(config-mm-profile-router)# no shutdown
switch(config-mm-profile-router)# address-family ipv6 unicast
switch(config-mm-profile-router-af)# no shutdown
switch(config-mm-profile)# router bgp 100
switch(config-mm-profile-router)# no shutdown
switch(config-mm-profile)# vpc domain 10
switch(config-mm-profile-config-vpc-domain)# no shutdown
switch(config-mm-profile)# no ip pim isolate
switch(config-mm-profile)# end
Exit maintenance profile mode.
switch# show maintenance profile normal-mode
[Normal Mode]
no system interface shutdown
router eigrp 10
  no shutdown
  address-family ipv6 unicast
    no shutdown
router bgp 100
  no shutdown
vpc domain 10
  no shutdown
no ip pim isolate
```

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と、事前定義された一連の **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	snapshot create snapshot-name description 例 : <pre>switch# snapshot create snap_before_maintenance Taken before</pre>	選択した機能の実行状態または運用データをキャプチャし、データを永続ストレージメディアに保存します。

	<p>コマンドまたはアクション</p> <pre> maintenance 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 Feature 'vpc' not enabled, skipping... Executing 'show ip ospf vrf all'... Done Feature 'ospfv3' not enabled, skipping... Feature 'isis' not enabled, skipping... Feature 'rip' not enabled, skipping... Snapshot 'snap_before_maintenance' created </pre>	<p>目的</p> <p>最大 64 文字の英数字のスナップショット名と最大 254 文字の英数字の説明を入力できます。</p> <p>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。</p>
<p>ステップ 2</p>	<p>show snapshots</p> <p>例 :</p> <pre> switch# show snapshots Snapshot Name Time Description ----- snap_before_maintenance Wed Aug 19 13:53:28 2015 Taken before maintenance </pre>	<p>スイッチ上に存在するスナップショットを表示します。</p>
<p>ステップ 3</p>	<p>show snapshots compare snapshot-name-1 snapshot-name-2 [summary ipv4routes ipv6routes]</p> <p>例 :</p> <pre> switch# show snapshots compare snap_before_maintenance snap_after_maintenance </pre>	<p>2つのスナップショットの比較を表示します。</p> <p>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。</p> <p>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。</p>

例

次に、2つのスナップショット間の変更の概要の例を示します。

```

switch# show snapshots compare snapshot1 snapshot2 summary
feature                snapshot1    snapshot2    changed
basic summary
  # of interfaces       16          12          *
  # of vlans            10          4           *
  # of ipv4 routes      33          3           *
  .....
interfaces
                    
```

```

# of eth interfaces          3          0          *
# of eth interfaces up      2          0          *
# of eth interfaces down    1          0          *
# of eth interfaces other   0          0
.....

# of vlan interfaces        3          1          *
# of vlan interfaces up     3          1          *
# of vlan interfaces down   0          0
# of vlan interfaces other  0          1          *
.....

```

次に、2つのスナップショット間のIPv4ルートの変更の例を示します。

```

switch# show snapshots compare snapshot1 snapshot2 ipv4routes
metric                snapshot1    snapshot2    changed
# of routes            33          3            *
# of adjacencies      10          4            *

Prefix                Changed Attribute
-----
23.0.0.0/8            not in snapshot2
10.10.10.1/32         not in snapshot2
21.1.2.3/8            adjacency index has changed from 29 (snapshot1) to 38 (snapshot2)
.....

There were 28 attribute changes detected

```

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	<p>snapshot section add section <i>"show-command" row-id element-key1</i> <i>[element-key2]</i></p> <p>例 :</p> <pre>switch# snapshot section add myshow "show ip interface brief" ROW_intf intf-name</pre>	<p>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。<i>section</i> 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。</p> <p>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。</p> <p><i>row-id</i> 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。<i>element-key1</i> および <i>element-key2</i> 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</p>

	コマンドまたはアクション	目的
		<p>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 <i>element-key1</i> 引数だけです。</p> <p>(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 コマンドを使用します。</p>
ステップ 2	<p>show snapshots sections</p> <p>例 :</p> <pre>switch# show snapshots sections</pre>	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。
ステップ 3	<p>show snapshots compare snapshot-name-1 snapshot-name-2 [summary ipv4routes ipv6routes]</p> <p>例 :</p> <pre>switch# show snapshots compare snap1 snap2</pre>	<p>2つのスナップショットの比較を表示します。</p> <p>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。</p> <p>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。</p>

例

次に、**show ip interface brief** コマンドを myshow スナップショットセクションに追加する例を示します。この例では、2つのスナップショット (snap1 および snap2) が比較され、両方のスナップショットにユーザ指定のセクションが表示されます。

```
switch# snapshot section add myshow "show ip interface brief" ROW_intf intf-name
switch# show snapshots sections
user-specified snapshot sections
-----
[myshow]
  cmd: show ip interface brief
  row: ROW_intf
  key1: intf-name
  key2: -

[sect2]
  cmd: show ip ospf vrf all
  row: ROW_ctx
  key1: instance_number
  key2: cname

switch# show snapshots compare snap1 snap2
=====
Feature          Tag          snap1          snap2
=====
```

```
[bgp]
-----
.....

[interface]
-----

      [interface:mgmt0]
          vdc_lvl_in_pkts          692310          **692317**
          vdc_lvl_in_mcast        575281          **575287**
          vdc_lvl_in_bcast        77209           **77210**
          vdc_lvl_in_bytes        63293252         **63293714**
          vdc_lvl_out_pkts        41197           **41198**
          vdc_lvl_out_ucast       33966           **33967**
          vdc_lvl_out_bytes       6419714         **6419788**
.....

[ospf]
-----
.....

[myshow]
-----

      [interface:Ethernet1/1]
          state                    up                **down**
          admin_state              up                **down**
.....
```

グレースフル削除のトリガー

デバッグ操作やアップグレード操作を実行するために、スイッチのグレースフル削除をトリガーして、スイッチを取り出し、ネットワークからそのスイッチを分離できます。

始める前に

作成したメンテナンスモードプロファイルを使用するシステムの場合は、[メンテナンスモードプロファイルの設定 \(427 ページ\)](#) 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	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 mode maintenance [dont-generate-profile timeout value shutdown on-reload reset-reason reason] 例：	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)。

コマンドまたはアクション	目的
<pre> switch(config)# system mode maintenance Following configuration will be applied: ip pim isolate router bgp 65502 isolate router ospf p1 isolate router ospfv3 p1 isolate Do you want to continue (y/n)? [no] y Generating a snapshot before going into maintenance mode Starting to apply commands... Applying : ip pim isolate Applying : router bgp 65502 Applying : isolate Applying : router ospf p1 Applying : isolate Applying : router ospfv3 p1 Applying : isolate Maintenance mode operation successful. </pre>	<p>次のオプションを使用できます。</p> <ul style="list-style-type: none"> • 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。作成したメンテナンス モード プロファイルをシステムに使用させる場合は、このオプションを使用します。 • 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。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。 • shutdown : すべてのプロトコル、vPC ドメイン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。 • 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 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。 <p>メンテナンス モードのリセット理由は次のとおりです。</p> <ul style="list-style-type: none"> • HW_ERROR : ハードウェアエラー • SVC_FAILURE : 重大なサービス障害

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • 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 • LC_FAILURE : ラインカード障害 • MATCH_ANY : 上記のいずれかの理由 <p>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。</p>
ステップ 3	(任意) show system mode 例 : <pre>switch(config)# show system mode System Mode: Maintenance</pre>	<p>現在のシステム モードを表示します。</p> <p>スイッチはメンテナンス モードになっています。スイッチに対する目的のデバッグ操作やアップグレード操作を実行できます。</p>
ステップ 4	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	<p>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。このコマンドは、再起動後にメンテナンス モードを維持する場合に必要です。</p>

例

次に、スイッチのすべてのプロトコル、vPC ドメイン、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(config)# system mode maintenance shutdown
```

Following configuration will be applied:

```
vpc domain 10
 shutdown
router bgp 65502
 shutdown
router ospf p1
 shutdown
router ospfv3 p1
 shutdown
system interface shutdown
```



```

Do you want to continue (y/n)? [no] y

Generating a snapshot before going into maintenance mode

Starting to apply commands...

Applying : vpc domain 10
Applying : shutdown
Applying : router bgp 65502
Applying : shutdown
Applying : router ospf p1
Applying : shutdown
Applying : router ospfv3 p1
Applying : shutdown

Maintenance mode operation successful.
    
```

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(config)# system mode maintenance on-reload reset-reason fatal_error
```

グレースフル挿入のトリガー

デバッグ操作やアップグレード操作の実行が終了したら、グレースフル挿入をトリガーして、すべてのプロトコルを復元できます。

始める前に

作成する通常モードプロファイルをシステムに使用させる場合は、[メンテナンスモードプロファイルの設定 \(427 ページ\)](#) 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	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル設定モードを開始します。
ステップ 2	no system mode maintenance [dont-generate-profile] 例 : <pre>switch(config)# no system mode maintenance dont-generate-profile Following configuration will be applied: no ip pim isolate</pre>	すべての有効なプロトコルを通常モードにします (no isolate コマンドを使用)。 dont-generate-profile オプションを指定すると、有効なプロトコルの動的な検索が回避され、通常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せん。作成した通常モードプロファイル

	コマンドまたはアクション	目的
	<pre>router bgp 65502 no isolate router ospf p1 no isolate router ospfv3 p1 no isolate Do you want to continue (y/n)? [no] y Starting to apply commands... Applying : no ip pim isolate Applying : router bgp 65502 Applying : no isolate Applying : router ospf p1 Applying : no isolate Applying : router ospfv3 p1 Applying : no isolate Maintenance mode operation successful. Generating Current Snapshot</pre>	<p>をシステムに使用させる場合は、このオプションを使用します。</p> <p>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。</p>
ステップ 3	<p>(任意) show system mode</p> <p>例 :</p> <pre>switch(config)# show system mode System Mode: Normal</pre>	<p>現在のシステム モードを表示します。スイッチは通常モードになっていて、完全に機能しています。</p>

メンテナンス モードの強化

リリース 7.0(3)I5(1) 以降、メンテナンス モードの次の機能拡張が Cisco Nexus 9000 シリーズ スイッチに追加されました。

- システム メンテナンス シャットダウン モードで次のメッセージが追加されます。

```
NOTE: The command system interface shutdown will shutdown all interfaces excluding mgmt 0.
```

- CLI コマンドを入力すると、**system mode maintenance** によって孤立ポートがチェックされ、アラートが送信されます。
- 隔離モードで vPC が設定されると、次のメッセージが追加されます。

```
NOTE: If you have vPC orphan interfaces, please ensure vpc orphan-port suspend is configured under them, before proceeding further.
```

- カスタム プロファイル設定 : 新しい CLI コマンド、**system mode maintenance always-use-custom-profile** がカスタム プロファイル設定に追加されます。新しい CLI コマンド、**system mode maintenance non-interactive** は Cisco Nexus 9000 シリーズ スイッチのみに追加されます。これにより、確認を行わずに、または CLI セッションに各ステップを出力することなく、メンテナンスモードまたは通常モードへの移行を容易に行うことができます。

ループバック インターフェイスがデバイス上の IP アドレスで設定され、このデバイスがピアデバイスにアダプタイズされると、デバイス（ループバック インターフェイスを含む）はメンテナンス モードに移行します。このような場合、**system interface shutdown** がデバイスで設定されている場合は、カスタムメンテナンスプロファイルを使用します。

（メンテナンスまたは通常モードで）カスタムプロファイルを作成すると、次のメッセージが表示されます。

```
Please use the command system mode maintenance always-use-custom-profile
if you want to always use the custom profile.
```

- **after_maintenance** スナップショットが取得される前に遅延が追加されました。**no system mode maintenance** コマンドは、通常モードのすべての設定が適用され、モードが通常モードに変更され、**after_maintenance** スナップショットを取得するためのタイマーが開始されると終了します。タイマーの期限が切れると、**after_maintenance** スナップショットがバックグラウンドで取得され、スナップショットが完了すると新しい警告 Syslog、**MODE_SNAPSHOT_DONE** が送信されます。

CLI コマンド **no system mode maintenance** の最終出力は、**after_maintenance** スナップショットが生成されるタイミングを示します。

```
The after_maintenance snapshot will be generated in <delay> seconds.
After that time, please use show snapshots compare before_maintenance
after_maintenance to check the health of the system. The timer delay
for the after_maintenance snapshot is defaulted to 120 seconds but
it can be changed by a new configuration command.
```

after_maintenance snapshot のタイマー遅延を変更する新しい設定コマンドは、**system mode maintenance snapshot-delay <seconds>** です。この設定は、デフォルト設定の 120 秒を 0 ~ 65535 の任意の値に上書きします。これは ASCII 設定で表示されます。

現在のスナップショット遅延の値を表示する新しい **show** コマンド、**show maintenance snapshot-delay** も追加されています。この新しい **show** コマンドでは、XML 出力がサポートされています。

- システムがメンテナンス モードであるときに表示される CLI インジケータが追加されました（例：switch(m-mode)#）。
- CLI リロードまたはシステム リセットによってデバイスがメンテナンス モードから通常モードおよびその逆に移行するときの SNMP トラップのサポートが追加されました。**snmp-server enable traps mmode cseMaintModeChangeNotify** トラップは、メンテナンスモードのトラップ通知の変更を有効にするために追加されました。**snmp-server enable traps mmode cseNormalModeChangeNotify** は、通常モードへのトラップ通知の変更を有効にするために追加されました。デフォルトでは両方のトラップが無効になっています。

GIR 設定の確認

GIR 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 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-reasons	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。メンテナンスモードのリセット理由の説明については、 グレースフル削除のトリガー (434 ページ) を参照してください。
show maintenance profile [maintenance-mode normal-mode]	メンテナンスモードまたは通常モードの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 {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	スナップショットの取得時に生成された各ファイル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。

GIR の設定例

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が収集されます。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。

ポリシー設定

メンテナンス モードで `route-map my-rmap-deny` コマンドを使用して、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
```

メンテナンス モードで `route-map my-rmap-permit` コマンドを使用して、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
```



第 25 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 (SMU) を実行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。

- [SMU について \(443 ページ\)](#)
- [SMU の前提条件 \(446 ページ\)](#)
- [SMU の注意事項と制約事項 \(446 ページ\)](#)
- [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 \(447 ページ\)](#)
- [Guest Shell Bash のソフトウェア メンテナンス アップグレードの実行 \(464 ページ\)](#)
- [その他の参考資料 \(466 ページ\)](#)
- [SMU の履歴 \(466 ページ\)](#)

SMU について

ソフトウェア メンテナンス アップグレード (SMU) は、特定の障害の修正を含むパッケージ ファイルです。SMU は、直近の問題に対処するために作成され、新しい機能は含まれていません。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 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** : スーパーバイザおよびラインカードの平行リロードを引き起こします。

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。重要な問題に対する迅速な解決策を提供します。SMU で修正されたすべての不具合は、今後のソフトウェア トレーンの次のメンテナンス リリースに統合されます。SMU には、次の考慮事項もあります。

- SMU は次の目的で作成されます。
 - 回避策または修正のない重大な SIR PSIRT
 - 回避策または修正なしの重大度 1 および重大度 2 の問題
- 同じソフトウェア トレインのメンテナンス リリースで修正プログラムがすでに使用可能な場合、またはそれ以降の長期リリースですでにリリースされている場合、SMU は提供されません。メンテナンス リリースから修正を取得することをお勧めします。



(注) 修正によっては、SMU を提供できない場合があります。このような場合、唯一の選択肢は、次のメンテナンス リリースにアップグレードすることです。

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 9000 シリーズ NX-OS ソフトウェア アップグレードおよびダウングレードガイド](#)』を参照してください。

詳細については、『[Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide](#)』を参照してください。



(注) SMU をアクティブにすると、以前の SMU、または SMU が適用されるパッケージが自動的に非アクティブ化されることはありません。



(注) Cisco NX-OS リリース 7.0(3)I2(1) 以降、SMU パッケージ ファイルの拡張子は .rpm です。以前のファイルの拡張子は .bin です。

RPM パッチ

RPM パッチは、ISSU を実行する際の追加リロードを回避するのに役立ちます。ISSU コマンドを使用すれば、必要なパッチを指定できます。これらのパッチは、インストールのアップグレード前の段階で検証され、パッチ適用リポジトリに保存されます。これらは、新しいバージョンでの ISSU 中にシステムが起動したときに適用されます。

パッチはターゲット イメージと互換性がある必要があります。パッチがターゲット イメージと互換性がない場合には、警告メッセージが表示された場合、ISSU は停止します。パッチはバージョン固有であり、ターゲット イメージと互換性がない場合は適用されません。この互換性チェックは、アップグレードの前に実行されます。

パッチ適用に使用されるバンドルされた tar イメージには、NX-OS イメージとそのイメージにインストールされる RPM が含まれています。

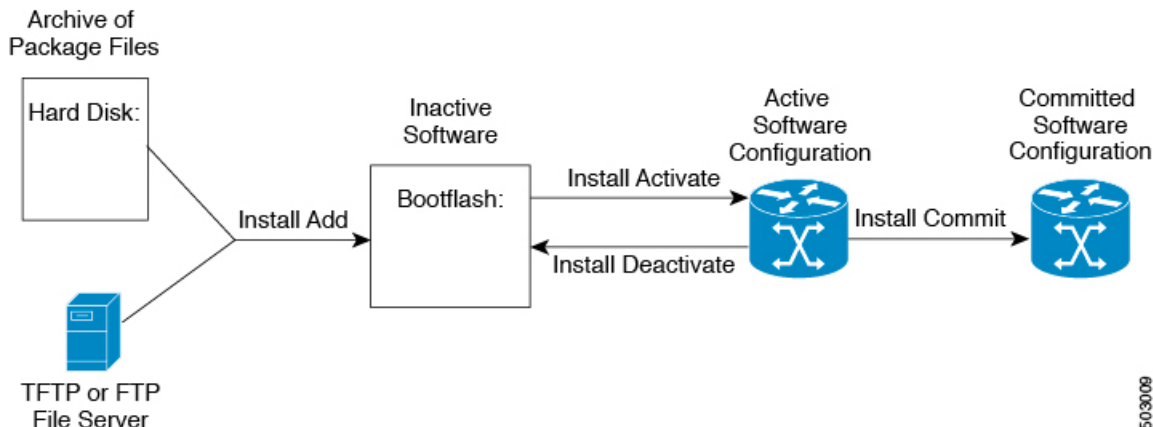
パッケージ管理

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。
5. (オプション) パッケージをアクティブでなくし、除去します。

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 6: 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



503009

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 カードのすべてのプロセスが再起動する場合があります。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 アクティブ化または非アクティブ化のプロセスが完了した後で、**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。

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。

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。
- 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。
- tarball SMU を使用して、複数の SMU をアクティブまたは非アクティブにできます。
- 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。
- 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 パッケージファイルの名前は
nxos.CSCab00001-n9k_ALL-1.0.0-7.0.3.I5.1.lib32_n9000.rpm で、n9k_EOR と n9k_TOR の両方のプラットフォームをサポートしています。
- 「7.0(3)I7(2)のシーケンス番号を使用して MAC ACE を削除できません」の問題を解決するパッチを適用する場合は、パッチを適用する前に ACL を削除する必要があります。そうしないと、問題が再度発生します。この問題は、redirect キーワードが含まれている ACL にのみ適用されます。

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。

始める前に

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ます。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 logging logfile grep -i "System ready" 例 : <pre>switch# show logging logfile grep -i "System ready"</pre>	システムが稼働しているかどうかを表示します。このコマンドを使用して、システムで SMU パッケージをインストールする準備ができていないことを確認します。システムの準備が整う前にインス

	コマンドまたはアクション	目的
		ツールコマンドを設定すると、「Install operation 11 failed because cannot lock config」エラーメッセージが表示されることがあります。
ステップ 2	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決定するため、またインストール操作完了後にアクティブなソフトウェアのレポートと比較するために、このコマンドを使用します。
ステップ 3	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。
ステップ 4	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。

例

次に、システムが稼働していることを確認する例を示します。「System ready」応答は、システムがSMUパッケージのインストールの準備ができていることを示します。

```
switch# show logging logfile | grep -i "System ready"
2018 Feb 19 11:13:04 switch %ASCII-CFG-2-CONF_CONTROL: System ready
```

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。

```
switch# show install active
Boot Image:
  NXOS Image: bootflash:///nxos.7.0.3.I7.3.1.bin

Active Packages:

switch#
```

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
```

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 [製品の選択 (Select a Product)] リストから、[スイッチ (Switches)] > [データセンタースイッチ (Data Center Switches)] > [Cisco Nexus 9000 シリーズ スイッチ (Cisco Nexus 9000 Series Switches)] > [モデル (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、[ダウンロード (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。

SMU パッケージ ファイルがリモート TFTP、FTP、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。
- 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 9000 シリーズ NX-OS セキュリティ設定ガイド』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 26: 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
<pre>copy tftp://hostname-or-ipaddress/directory-path/filename bootflash: switch# copy tftp://10.1.1.1/images/ nxos.CSCab00001-n9k_ALL-1.0.0-7.0.3.I5.1.lib32_n9000.rpm bootflash:</pre>	<p>TFTP サーバから bootflash: にパッケージ ファイルをコピーします。</p> <ul style="list-style-type: none"> • <i>hostname-or-ipaddress</i> : 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。 • <i>directory-path</i> : 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。 • <i>filename</i> : 追加するパッケージ ファイルの名前。

コマンド	目的
<pre>copy ftp://username:password@hostname-or-ipaddress/directory-path/filename bootflash: switch# copy ftp://john:secret@10.1.1.1/images/ nxos.CSCab00001-n9k_ALL-1.0.0-7.0.3.I5.1.lib32_n9000.rpm bootflash:</pre>	

コマンド	目的
	<p>FTP サーバから <code>bootflash:</code> にパッケージファイルをコピーします。</p> <ul style="list-style-type: none"> • <i>username</i> : 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。 • <i>password</i> : 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、ネットワークング デバイスは、anonymous FTP を受け入れます。 • <i>hostname-or-ipaddress</i> : 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。 • <i>directory-path</i> : 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。 <p>(注) FTP および rcp サービスの場合、<i>directory-path</i> は <i>username</i> 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。</p>

コマンド	目的
	<ul style="list-style-type: none"> • <i>filename</i> : 追加するパッケージファイルの名前。
<pre>copy sftp://hostname-or-ipaddress/directory-path/filename bootflash: switch# copy sftp://10.1.1.1/images/nxos.CSCab00001-n9k_ALL- 1.0.0-7.0.3.I5.1.lib32_n9000.rpm bootflash:</pre>	<p>SFTP サーバから bootflash: にパッケージファイルをコピーします。</p> <ul style="list-style-type: none"> • <i>hostname-or-ipaddress</i> : 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。 • <i>directory-path</i> : 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。 • <i>filename</i> : 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) この手順では、Cisco NX-OS CLI コマンドを使用して、RPM パッケージファイルを追加して有効化します。YUM コマンドを使用する場合は、『[Cisco Nexus 9000 Series NX-OS Programmability Guide](#)』の「Installing RPMs from Bash」の手順に従ってください。



- (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アクティブなその他の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) SMU をアクティブにすると、以前の SMU、または SMU が適用されるパッケージが自動的に非アクティブ化されることはありません。

始める前に

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 (449 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	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	(任意) dir bootflash:	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ブ化できるのは SMU パッケージ ファイルだけです。
ステップ 3	install add filename [activate] 例 : <pre>switch# install add bootflash: nxos.CSCab00001-n9k_ALL-1.0.0-7.0.3.I5.1. lib32_n9000.rpm</pre>	ローカル ストレージ デバイスまたはネットワーク サーバからパッケージ ソフトウェア ファイルを解凍してブート フラッシュおよびデバイスにインストールされているすべてのアクティブ スーパーバイザおよびスタンバイ スーパーバイザに追加します。 <i>filename</i> 引数は、次の形式をとることができます。 <ul style="list-style-type: none">• bootflash:filename• ftp://hostname-or-ipaddress/directory-path/filename• ftp://username:password@hostname-or-ipaddress/directory-path/filename• usb1:filename• usb2:filename CSCur02700 SMU パッケージを除くすべての SMU パッケージで、正常に追加された後に自動的にパッケージをアクティブにするには、オプションの activate 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
		<p>(注) CSCur02700 SMU パッケージの場合は、ステップ5の install activate コマンドを使用してパッケージをアクティブ化します。パッケージが失敗し、リポートが必要になる可能性があるため、install add コマンドでオプションの activate キーワードを使用しないでください。</p> <p>SMU パッケージの複数バージョンが、実行コンフィギュレーションに影響を与えずにストレージデバイスに追加できます。しかし、ラインカードに対して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です。</p> <p>(注) パッケージ名を部分的に入力してから ? を押すと、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。</p> <p>tarball SMU で install add コマンドを使用すると、複数の SMU を同時にインストールできます。</p>
ステップ4	<p>(任意) show install inactive</p> <p>例 :</p> <pre>switch# show install inactive</pre>	<p>デバイス上の非アクティブなパッケージを表示します。前述の手順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。</p>
ステップ5	<p>必須: install activate filename</p> <p>例 :</p> <pre>switch# install activate nxos.CSCab00001-n9k_ALL-1.0.0-7.0.3.I5.1. lib32_n9000.rpm</pre> <p>例 :</p> <pre>switch# install activate nxos.CSCab00001-n9k_ALL-1.0.0-7.0.3.I5.1.</pre>	<p>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。SMU パッケージは、アクティブにされるまで無効のままです。(install add activate コマンドを使用して、パッケージが前にアクティブにされた場合は、この手順を省略します。)</p>

	コマンドまたはアクション	目的
	<pre>lib32_n9000.rpm Install operation 18 !!WARNING!! This patch will get activated only after a reload of the switch. at Wed Jun 22 00:42:12 2016</pre>	ヒント アクティブ化プロセスが終了したら、 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。
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	(任意) show install active 例 : <pre>switch# show install active</pre>	すべてのアクティブなパッケージを表示します。このコマンドを使用して、正しいパッケージがアクティブであるかどうかを判断します。

例

次に、tarball を使用して複数の SMU パッケージ ファイルを追加し、追加されたパッケージ ファイルを確認する例を示します。

```
switch# install add bootflash:nxos.CSC123456-n9k_ALL-1.0.0-7.0.3.I7.3.
lib32_n9000.tar
[#####] 100%
Install operation 882 completed successfully at Tue Mar 6 17:30:31 2018

switch#
switch# show install inactive
Boot Image:
  NXOS Image: bootflash:///nxos.7.0.3.I7.3.bin-219-CCO

Inactive Packages:
  nxos.CSC123456_core-n9k_ALL-1.0.0-7.0.3.I7.3.lib32_n9000
  nxos.CSC123456_eth-n9k_ALL-1.0.0-7.0.3.I7.3.lib32_n9000

Inactive Base Packages:

switch#
```

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。



- (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。

始める前に

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 \(453 ページ\)](#) 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 : <pre>switch# install commit nxos.CSCab00001-n9k_ALL-1.0.0-7.0.3.I5.1.lib32_n9000.rpm</pre>	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	(任意) show install committed 例 : <pre>switch# show install committed</pre>	コミットされたパッケージを表示します。

例

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 nxos.CSCab00001-n9k_ALL-1.0.0-7.0.3.I5.1.lib32_n9000.rpm
Install operation 2 completed successfully at Wed Jun 22 01:20:46 2016
```

```
switch# show install committed
Committed Packages:
nxos.CSCab00001-n9k_ALL-1.0.0-7.0.3.I5.1.lib32_n9000.rpm
```

RPM パッケージのインストール

install all コマンドは、構成の互換性チェックと BIOS のアップグレードを自動的に実行するため、ソフトウェアアップグレードとダウングレードに推奨される方法です。ファイル名を指定しないで **install all** コマンドを入力した場合は、コマンドにより互換性チェックが実行され、アップグレードされるモジュールが通知されます。さらに、インストールを続行するかどうかの確認が求められます。続行を選択すると、スイッチで現在実行されている NXOS ソフトウェアイメージがインストールされ、必要に応じて、実行中のイメージのさまざまなモジュールの BIOS がアップグレードされます。

手順

	コマンドまたはアクション	目的
ステップ 1	install all nxos scheme package scheme 例 : <pre>switch# install all nxos bootflash:/nxos.9.2.1.bin package bootflash:/nxos.CSCkxstart-r9k-ALL-1.0.0-9.2.2.lib32_r9000.rpm2</pre>	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、RPM パッチようにパッケージの対象セットをインストールします。
ステップ 2	(任意) show install all status 例 : <pre>switch# show install all status</pre>	全体のインストール プロセスのステータスを表示します。

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。以前のパッケージセットの方が現在アクティブなパッケージセットよりも適切であることがわかった場合は、**install deactivate** および **install commit** コマンドを使用して、以前アクティブだったパッケージセットを再びアクティブにできます。



- (注) この手順では、Cisco NX-OS CLI コマンドを使用して、RPM パッケージファイルを非アクティブ化して削除します。YUM コマンドを使用する場合は、『[Cisco Nexus 9000 Series NX-OS Programmability Guide](#)』の「Erasing an RPM」の手順に従ってください。

始める前に

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時、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。

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 nxos.CSCab00001-r9k_ALL-1.0.0-7.0.3.I5.1.lib32_n9000.rpm	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。
ステップ 3	(任意) show install inactive 例： switch# show install inactive	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	(任意) install commit 例： switch# install commit	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	(任意) install remove {filename inactive} 例： switch# install remove nxos.CSCab00001-r9k_ALL-1.0.0-7.0.3.I5.1.lib32_n9000.rpm Proceed with removing nxos.CSCab00001-r9k_ALL-1.0.0-7.0.3.I5.1.lib32_n9000.rpm? (y/n)? [n] y 例： switch# install remove inactive Proceed with removing? (y/n)? [n] y	非アクティブなパッケージを削除します。 <ul style="list-style-type: none"> 削除できるのは非アクティブなパッケージだけです。 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 <i>filename</i> 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。

例

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 nxos.CSCab00001-n9k_ALL-1.0.0-7.0.3.I5.1.lib32_n9000.rpm
Install operation 3 completed successfully at Wed Jun 22 01:20:36 2016

switch# show install inactive
Inactive Packages:
nxos.CSCab00001-n9k_ALL-1.0.0-7.0.3.I5.1.lib32_n9000.rpm

switch# install commit
Install operation 4 completed successfully at Wed Jun 22 01:20:46 2016

switch# install remove nxos.CSCab00001-n9k_ALL-1.0.0-7.0.3.I5.1.lib32_n9000.rpm
Proceed with removing nxos.CSCab00001-n9k_ALL-1.0.0-7.0.3.I5.1.lib32_n9000.rpm? (y/n)?
[n] y
Install operation 5 completed successfully at Wed Jun 22 01:20:57 2016
```

次に、1つのコマンドで複数のパッケージを非アクティブにし、デバイスから非アクティブパッケージを削除し、パッケージ削除を確認する例を示します。

```
switch# install deactivate nxos.CSC123456_core-n9k_ALL-1.0.0-7.0.3.I7.3.lib32_n9000
nxos.CSC123456_eth-n9k_ALL-1.0.0-7.0.3.I7.3.lib32_n9000
[#####] 100%
Install operation 884 completed successfully at Tue Mar 6 17:34:02 2018

switch#
switch# show install inactive
Boot Image:
  NXOS Image: bootflash:///nxos.7.0.3.I7.3.bin-219-CCO

Inactive Packages:
  nxos.CSC123456_core-n9k_ALL-1.0.0-7.0.3.I7.3.lib32_n9000
  nxos.CSC123456_eth-n9k_ALL-1.0.0-7.0.3.I7.3.lib32_n9000

Inactive Base Packages:

switch#
switch# install remove nxos.CSC123456_core-n9k_ALL-1.0.0-7.0.3.I7.3.lib32_n9000
Proceed with removing nxos.CSC123456_core-n9k_ALL-1.0.0-7.0.3.I7.3.lib32_n9000? (y/n)?
[n] y
[#####] 100%
Install operation 885 completed successfully at Tue Mar 6 17:34:56 2018

switch# install remove nxos.CSC123456_eth-n9k_ALL-1.0.0-7.0.3.I7.3.lib32_n9000
Proceed with removing nxos.CSC123456_eth-n9k_ALL-1.0.0-7.0.3.I7.3.lib32_n9000? (y/n)?
[n] y
[#####] 100%
Install operation 886 completed successfully at Tue Mar 6 17:35:14 2018

switch#
switch# show install inactive
Boot Image:
  NXOS Image: bootflash:///nxos.7.0.3.I7.3.bin-219-CCO

Inactive Packages:
```



```
Inactive Base Packages:
switch#
```

機能 RPM のダウングレード

インストールされている機能 RPM を基本機能 RPM にダウングレードするには、この手順を実行します。



- (注) この手順では、Cisco NX-OS CLI コマンドを使用して、機能 RPM をダウングレードします。YUM コマンドを使用する場合は、『[Cisco Nexus 9000 Series NX-OS Programmability Guide](#)』の「Downgrading an RPM」の手順に従ってください。

手順

	コマンドまたはアクション	目的
ステップ 1	(任意) show install packages 例： switch# show install packages ntp.lib32_n9000 1.0.1-7.0.3.I2.2e installed	デバイス上の機能 RPM パッケージを表示します。
ステップ 2	必須: run bash 例： switch# run bash bash-4.2\$	Bash をロードします。
ステップ 3	必須: cd /rpms 例： bash-4.2\$ cd /rpms	Bash の RPM フォルダへの変更。
ステップ 4	必須: ls *feature* 例： bash-4.2\$ ls *ntp* ntp-1.0.0-7.0.3.I2.2e.lib32_n9000.rpm	指定された機能の RPM を一覧表示します。
ステップ 5	必須: cp filename /bootflash 例： bash-4.2\$ cp ntp-1.0.0-7.0.3.I2.2e.lib32_n9000.rpm /bootflash	基本機能 RPM をブートフラッシュにコピーします。
ステップ 6	必須: exit 例：	Bash を終了します。

	コマンドまたはアクション	目的
	bash-4.2\$ exit	
ステップ 7	<p>必須: install add bootflash:filename activate downgrade</p> <p>例 :</p> <pre>switch# install add bootflash:ntp-1.0.0-7.0.3.I2.2e.lib32_n9000.rpm activate downgrade Adding the patch (/ntp-1.0.0-7.0.3.I2.2e.lib32_n9000.rpm) [#####] 60% Adding the patch (/ntp-1.0.0-7.0.3.I2.2e.lib32_n9000.rpm) [#####] 100% Install operation 11 completed successfully at Thu Sep 8 15:35:35 2015 Activating the patch (/ntp-1.0.0-7.0.3.I2.2e.lib32_n9000.rpm) This install operation requires system reload. Do you wish to continue (y/n)? : [n] y [217.975959] [1473348971] writing reset reason 132, System reset due to reload patch(es) activation [217.991166] [1473348971]\ufffd\ufffd CISCO SWITCH Ver7.51 Device detected on 0:6:0 after 0 msecs Device detected on 0:1:1 after 0 msecs Device detected on 0:1:0 after 0 msecs MCFrequency 1333Mhz Relocated to memory</pre>	<p>機能 RPM をダウングレードします。</p> <p>(注) デバイスのリロードを要求されたら、Yを入力します。リロードは、NTP および SNMP 機能RPMをダウングレードする場合にのみ必要です。</p>
ステップ 8	<p>(任意) show install packages i feature</p> <p>例 :</p> <pre>switch# show install packages i ntp ntp.lib32_n9000 1.0.0-7.0.3.I2.2e installed</pre>	<p>デバイス上の基本機能 RPM を表示します。</p>

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
Wed Jun 22 01:26:09 2016
Install operation 1 by user 'admin' at Wed Jun 22 01:19:19 2016
Install add bootflash:nxos.CSCab00001-n9k_ALL-1.0.0-7.0.3.I5.1.lib32_n9000.rpm
Install operation 1 completed successfully at Wed Jun 22 01:19:24 2016
-----
Install operation 2 by user 'admin' at Wed Jun 22 01:19:29 2016
Install activate nxos.CSCab00001-n9k_ALL-1.0.0-7.0.3.I5.1.lib32_n9000.rpm
Install operation 2 completed successfully at Wed Jun 22 01:19:45 2016
-----
Install operation 3 by user 'admin' at Wed Jun 22 01:20:05 2016
Install commit nxos.CSCab00001-n9k_ALL-1.0.0-7.0.3.I5.1.lib32_n9000.rpm
Install operation 3 completed successfully at Wed Jun 22 01:20:08 2016
-----
Install operation 4 by user 'admin' at Wed Jun 22 01:20:21 2016
Install deactivate nxos.CSCab00001-n9k_ALL-1.0.0-7.0.3.I5.1.lib32_n9000.rpm
Install operation 4 completed successfully at Wed Jun 22 01:20:36 2016
-----
Install operation 5 by user 'admin' at Wed Jun 22 01:20:43 2016
Install commit nxos.CSCab00001-n9k_ALL-1.0.0-7.0.3.I5.1.lib32_n9000.rpm
Install operation 5 completed successfully at Wed Jun 22 01:20:46 2016
-----
Install operation 6 by user 'admin' at Wed Jun 22 01:20:55 2016
Install remove nxos.CSCab00001-n9k_ALL-1.0.0-7.0.3.I5.1.lib32_n9000.rpm
Install operation 6 completed successfully at Wed Jun 22 01:20:57 2016
-----
Install operation 7 by user 'admin' at Wed Jun 22 01:21:07 2016
Install remove
Install operation 7 completed successfully at Wed Jun 22 01:21:10 2016
```

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
Wed Jun 22 01:24:03 2016
Install operation 1 by user 'admin' at Wed Jun 22 01:19:19 2016
Installer started downloading the package:
/nxos.CSCab00001-n9k_ALL-1.0.0-7.0.3.I5.1.lib32_n9000.rpm
via bootflash
Install add bootflash:nxos.CSCab00001-n9k_ALL-1.0.0-7.0.3.I5.1.lib32_n9000.rpm
Copying file at Wed Jun 22 01:19:20 2016
Download success, 238545 bytes received
Verifying package
Checking MD5 at Wed Jun 22 01:19:21 2016
MD5 checksum OK
Checking HW platform at Wed Jun 22 01:19:22 2016
Checking SW platform at Wed Jun 22 01:19:23 2016
Package verified successfully
Sending patch file to plugin manager at Wed Jun 22 01:19:23 2016
The following package is now available to be activated: nxos.CSCab00001-n9k_ALL-1.0.0-7.0.3.I5.1.lib32_n9000.rpm
Install operation 1 completed successfully at Wed Jun 22 01:19:24 2016
-----
Install operation 2 by user 'admin' at Wed Jun 22 01:19:29 2016
Install activate nxos.CSCab00001-n9k_ALL-1.0.0-7.0.3.I5.1.lib32_n9000.rpm
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 Wed Jun 22 01:19:45 2016
-----
Install operation 3 by user 'admin' at Wed Jun 22 01:20:05 2016
Install commit nxos.CSCab00001-n9k_ALL-1.0.0-7.0.3.I5.1.lib32_n9000.rpm
MD5 checksum OK for patch: nxos.CSCab00001-n9k_ALL-1.0.0-7.0.3.I5.1.lib32_n9000.rpm
Install operation 3 completed successfully at Wed Jun 22 01:20:08 2016
-----
Install operation 4 by user 'admin' at Wed Jun 22 01:20:21 2016
Install deactivate nxos.CSCab00001-n9k_ALL-1.0.0-7.0.3.I5.1.lib32_n9000.rpm
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 Wed Jun 22 01:20:36 2016
-----
Install operation 5 by user 'admin' at Wed Jun 22 01:20:43 2016
Install commit nxos.CSCab00001-n9k_ALL-1.0.0-7.0.3.I5.1.lib32_n9000.rpm
MD5 checksum OK for patch: nxos.CSCab00001-n9k_ALL-1.0.0-7.0.3.I5.1.lib32_n9000.rpm
Install operation 5 completed successfully at Wed Jun 22 01:20:46 2016
-----
Install operation 6 by user 'admin' at Wed Jun 22 01:20:55 2016
Install remove nxos.CSCab00001-n9k_ALL-1.0.0-7.0.3.I5.1.lib32_n9000.rpm
Install operation 6 completed successfully at Wed Jun 22 01:20:57 2016
-----
Install operation 7 by user 'admin' at Wed Jun 22 01:21:07 2016
Install remove
Install operation 7 completed successfully at Wed Jun 22 01:21:10 2016

```

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 Wed Jun 22 00:42:10 2016
Install activate nxos.CSCab00001-n9k_ALL-1.0.0-7.0.3.I5.1.lib32_n9000.rpm
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 Wed Jun 22 00:42:12 2016

```

Guest Shell Bash のソフトウェアメンテナンス アップグレードの実行

Guest Shell の Bash のソフトウェアメンテナンス アップグレードを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	Cisco.com から Guest Shell Bash の SMU パッケージ ファイルをダウンロードします。	Cisco.com からパッケージファイルを取得します。この説明については、 Cisco.com からの SMU パッケージファ

	コマンドまたはアクション	目的
		イルのダウンロード (449 ページ) を参照してください。
ステップ 2	SMU パッケージファイルをスイッチの bootflash: にコピーします。	パッケージファイルをデバイスにコピーします。この説明については、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 (449 ページ) を参照してください。
ステップ 3	guestshell 例 : switch# guestshell guestshell:~\$	Guest Shell にアクセスします。
ステップ 4	sudo rpm -Uvh /bootflash/filename 例 : guestshell:~\$ sudo rpm -Uvh /bootflash/bash-4.2-r8.x86_64.rpm Preparing... ##### [100%] 1: bash ##### [100%] update-alternatives: Linking //bin/sh to /bin/bash	Guest Shell の既存の Bash ファイルをアップグレードします。
ステップ 5	rpm -qa grep bash 例 : guestshell:~\$ rpm -qa grep bash bash-4.2-r8.x86_64	Bash ファイルの新しいバージョンが正常にインストールされたことを確認します。
ステップ 6	guestshell sync 例 : switch# guestshell sync Access to the guest shell will be temporarily disabled while it synchronizes contents to standby. Are you sure you want to continue? (y/n) [n] y dt-n9k3-1# 2014 Oct 7 05:00:01	デュアルスーパーバイザシステムでは、スイッチオーバーを実行する前に、スタンバイスーパーバイザに対して rootfs を Bash SMU バージョンと同期します。このコマンドを実行しない場合は、スーパーバイザのスイッチオーバー後にこの手順を繰り返す必要があります。

	コマンドまたはアクション	目的
	<pre>dt-n9k3-1 %\$ VDC-1 %\$ %VMAN-2-INSTALL_STATE: Deactivating virtual service 'guestshell+' dt-n9k3-1# 2014 Oct 7 05:00:06 dt-n9k3-1 %\$ VDC-1 %\$ %VMAN-2-ACTIVATION_STATE: Successfully deactivated virtual service 'guestshell+' 2014 Oct 7 05:00:12 dt-n9k3-1 %\$ VDC-1 %\$ %VMAN-2-ACTIVATION_STATE: Successfully deactivated virtual service 'guestshell+' ; Starting sync to standby sup 2014 Oct 7 05:00:32 dt-n9k3-1 %\$ VDC-1 %\$ %VMAN-2-MOVE_STATE: Successfully synced virtual service 'guestshell+' ; Activating 2014 Oct 7 05:00:32 dt-n9k3-1 %\$ VDC-1 %\$ %VMAN-2-ACTIVATION_STATE: Activating virtual service 'guestshell+' 2014 Oct 7 05:00:56 dt-n9k3-1 %\$ VDC-1 %\$ %VMAN-2-ACTIVATION_STATE: Successfully activated virtual service 'guestshell+'</pre>	<p>(注) 新しいBash ファイルは、Guest Shell のリポート後または Guest Shell の無効化+有効化後に保持されます。ただし、Guest Shell の破棄と有効化の後に、Guest Shell Bash SMU パッケージファイルを再インストールする必要があります。</p>

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 9000 Series NX-OS Software Upgrade and Downgrade Guide』

SMU の履歴

次の表に、SMU パッケージファイルのリリースの履歴を示します。

SMU パッケージファイル	リリース	説明
bash-4.2-r8.x86_64.rpm	6.1(2)I3(1)	ゲストシェル Bash SMU for Bash の脆弱性 (CVE-2014-6277、CVE-2014-6278、CVE-2014-7186、および CVE-2014-7187)

SMU パッケージ ファイル	リリース	説明
n9000-dk9.6.1.2.I3.1.CSCur02700.bin	6.1(2)I3(1) およびすべての 6.1(2)I2(x) リリース	CSCur02700 向け Cisco NX-OS SMU (Bash の脆弱性 CVE-2014-6277、CVE-2014-6278、CVE-2014-7186、および CVE-2014-7187)
n9000-dk9.6.1.2.I2.1.CSCup81353.bin	6.1(2)I2(1)、6.1(2)I2(2)、6.1(2)I2(2a)、および 6.1(2)I2(3)	CSCup81353 用 Cisco NX-OS SMU



第 26 章

コンフィギュレーションの置換の実行

この章は、次の項で構成されています。

- [コンフィギュレーションの置換とコミットタイムアウトについて \(469 ページ\)](#)
- [概要 \(470 ページ\)](#)
- [コンフィギュレーションの置換に関する注意事項と制限事項 \(472 ページ\)](#)
- [コンフィギュレーションの置換の推奨ワークフロー \(474 ページ\)](#)
- [コンフィギュレーションの置換の実行 \(475 ページ\)](#)
- [コンフィギュレーションの置換の確認 \(477 ページ\)](#)
- [コンフィギュレーションの置換の例 \(478 ページ\)](#)

コンフィギュレーションの置換とコミットタイムアウトについて

コンフィギュレーションの置換機能を使用すると、デバイスをリロードすることなく Cisco Nexus スイッチの実行コンフィギュレーションをユーザ指定のコンフィギュレーションに置換できます。コンフィギュレーション自体でリロードが必要な場合にのみ、デバイスのリロードが必要になることがあります。ユーザが提供する実行コンフィギュレーションファイルは、実行ファイルのコピーを使用して取得する必要があります。**copy file: to running** と異なり、コンフィギュレーションの置換機能はマージ操作ではありません。この機能では、実行コンフィギュレーション全体が、ユーザによって提供される新しいコンフィギュレーションに置換されます。コンフィギュレーションの置換に障害がある場合は、元のコンフィギュレーションがスイッチで復元されます。Cisco NX-OS リリース 9.3(1) から、**best-effort** オプションが導入されました。このオプションを使用すると、コマンドでエラーが発生した場合でも、設定の置換によって完全なパッチが実行され、元の設定はスイッチに復元されません。

コミットタイムアウト機能を使用すると、コンフィギュレーションの置換操作の実行に成功した後以前にコンフィギュレーションにロールバックすることができます。コミットタイマーの期限が切れると、ロールバック操作は自動的に開始されます。



- (注)
- Cisco NX-OS デバイスで受信済みの有効な実行コンフィギュレーションを提供する必要があります。部分コンフィギュレーションにすることはできません。

概要

設定置換機能には、次の操作手順があります。

- コンフィギュレーションの置換では、Cisco Nexus スイッチの現在の実行コンフィギュレーションとユーザ指定のコンフィギュレーションとの間の違いをインテリジェントに計算し、2ファイルの差異のパッチファイルを生成します。コンフィギュレーションコマンドのセットが含まれているこのパッチファイルは表示できます。
- コンフィギュレーションの置換では、実行中のコマンドと同様にパッチファイルのコンフィギュレーションコマンドが適用されます。
- コンフィギュレーションは、次の状況下で以前の実行コンフィギュレーションにロールバックまたは復元されます。
 - パッチファイルが適用された後、コンフィギュレーションに不一致がある場合。
 - コミットタイムアウトを使用してコンフィギュレーション操作を実行し、コミットタイマーが期限切れになった場合。
- ベストエフォートオプションが使用されている場合、設定は以前の実行コンフィギュレーションにロールバックされず、復元もされません。このオプションを使用すると、コマンドでエラーが発生した場合でも、設定の置換によって完全なパッチが実行され、以前の設定にロールバックされません。
- **show config-replace log exec** コマンドを使用すると、エラーが発生したコンフィギュレーションそのものを表示できます。
- スイッチを元のコンフィギュレーションに復元するときエラーが発生しても復元操作は中断されません。復元操作は、残りのコンフィギュレーションを続行します。復元操作中にエラーが発生したコマンドを一覧表示するには、**show config-replace log exec** コマンドを使用します。
- タイマーの期限が切れる前に **configure replace commit** コマンドを入力した場合、コミットタイマーは停止し、コンフィギュレーションの置換機能によって適用されているユーザ指定のコンフィギュレーションでスイッチが稼働します。
- コミットタイマーの期限が切れると、以前のコンフィギュレーションへのロールバックは自動的に開始されます。
- Cisco NX-OS リリース 9.3(1) では、セマンティック検証のサポートが設定の置換に追加されました。このセマンティック検証は、設定置換の事前チェックの一部として実行されます。パッチは、セマンティック検証が成功した場合にのみ適用されます。パッチファイル

を適用すると、コンフィギュレーションの置換によって検証プロセスがトリガーされます。コンフィギュレーションの置換は、検証プロセスで、実行コンフィギュレーションとユーザー構成ファイルを比較します。不一致がある場合、デバイスは元のコンフィギュレーションに復元されます。

コンフィギュレーションの置換と実行コンフィギュレーションへのファイルのコピーとの違いは、次のとおりです。

コンフィギュレーションの置換	ファイルのコピー
configure replace <target-url> コマンドでは、現在の実行コンフィギュレーションにのみ含まれ、置換ファイルには存在しないコマンドは削除されます。また、現在の実行コンフィギュレーションに追加する必要があるコマンドも追加されます。	copy <source-url> running-config コマンドはマージ動作であり、ソースファイルと現在の実行コンフィギュレーションの両方のコマンドがすべて保持されます。このコマンドでは、現在の実行コンフィギュレーションにのみ含まれ、ソースファイルには存在しないコマンドが削除されることはありません。
configure replace <target-url> コマンドの交換ファイルには、完全な Cisco NX-OS コンフィギュレーションファイルを使用する必要があります。	copy <source-url> running-config コマンドのコピー元ファイルとして、部分コンフィギュレーションファイルを使用できます。

コンフィギュレーションの置換の利点

コンフィギュレーションの置換の利点は次のとおりです。

- スイッチをリロードしたり、CLIで実行コンフィギュレーションファイルに加えた変更を手動で元に戻したりすることなく、現在の実行コンフィギュレーションファイルをユーザ指定のコンフィギュレーションファイルと置換できます。その結果、システムのダウンタイムが減少します。
- 保存済みの Cisco NX-OS コンフィギュレーションの状態に戻すことができます。
- 追加や削除が必要なコマンドだけが影響を受ける場合、デバイスに完全なコンフィギュレーションファイルを適用することができるため、コンフィギュレーションの変更が簡素化されます。その他のサービスおよび変更されていないコンフィギュレーションには影響しません。
- コミットタイムアウト機能を設定すると、コンフィギュレーションの置換操作が成功したときでも以前のコンフィギュレーションにロールバックすることができます。

コンフィギュレーションの置換に関する注意事項と制限事項

コンフィギュレーションの置換機能には、コンフィギュレーションに関する次のガイドラインと制限事項があります。

- 設定置換機能は、Cisco Nexus 3000 シリーズおよび Cisco Nexus 9000 シリーズ スイッチでサポートされています。
- コンフィギュレーションの置換、チェックポイント、ロールバック操作、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。複数の Telnet、SSH または NX-API セッション経由の操作などのパラレル操作はサポートされていません。複数のコンフィギュレーションの置換またはロールバック要求はシリアル化され、たとえば、最初の要求の完了後にのみ、2 番目の要求の処理が開始されます。
- コミットタイマーの実行中に別のコンフィギュレーションの置換操作を開始することはできません。 **configure replace commit** コマンドを使用してタイマーを停止するか、またはコミットタイマーの期限が切れるまで待機してから別のコンフィギュレーションの置換操作を開始する必要があります。
- コミットタイムアウト機能は、コミットタイムアウトを使用してコンフィギュレーションの置換操作を実行する場合にのみ開始されます。タイマーの値の範囲は 30 ~ 3600 秒です。
- ユーザ指定のコンフィギュレーションファイルは、Cisco NX-OS デバイスから取得 (copy run file) された有効な show running-configuration の出力である必要があります。このコンフィギュレーションは部分コンフィギュレーションにすることはできず、user admin などの必須コマンドが含まれている必要があります。
- ソフトウェア バージョン違いで生成されたコンフィギュレーション ファイルでコンフィギュレーションの置換操作を実行することは、操作が失敗する可能性があるため推奨されません。ソフトウェアバージョンの変更があるたびに新しいコンフィギュレーション ファイルを再生成する必要があります。
- Multichassis EtherChannel トランク (MCT) 設定を仮想ピアリンク設定と置き換えようとした場合、コンフィギュレーションの置換操作はサポートされません。物理 MCT はイーサネットを介した CFS 配信モードを使用し、仮想ピアリンクは IP を介した CFS 配信モードを使用するため、この操作は許可されません。
- コンフィギュレーションの置換操作が進行中の場合、他のセッションからはコンフィギュレーションを変更しないことを推奨します。操作が失敗する可能性があります。
- コンフィギュレーションの置換機能については、次の点に注意してください。
 - -R ライン カード搭載の Cisco Nexus 9500 プラットフォーム スイッチでは、コンフィギュレーションの置換機能はサポートされません。

- Cisco Nexus C92160YC-X および Cisco Nexus -C93180LC-EX スイッチのハードウェア プロファイルポートモード機能では、コンフィギュレーションの置換機能はサポートされません。
 - コンフィギュレーションの置換機能は、`configure terminal` モード コマンドで**のみ**サポートされます。 `configure profile`、`configure jobs`、およびその他のモードはサポートされていません。
 - Cisco NX-OS リリース 9.3(4) 以降では、ブレイクアウト インターフェイス コンフィギュレーションの設定置換機能がサポートされています。
 - 実行コンフィギュレーションに **feature-set mpls** または **mpls static range** コマンドが含まれていて、MPLS なしでコンフィギュレーションに移動しようとしたり、ラベルの範囲を変更する場合、コンフィギュレーションの置換機能が失敗することがあります。
 - コンフィギュレーションの置換機能は、自動設定をサポートしていません。
- コンフィギュレーションの置換機能が適用されるラインカードがオフラインである場合、コンフィギュレーションの置換操作は失敗します。
 - 設定置換機能を使用してITDを変更する前に、ITD サービスをシャットダウンする必要があります (**shutdown**) 。
 - ユーザ コンフィギュレーションからのメンテナンス モードへの移行はサポートされていません。
 - メンテナンス モードから **configure replace** コマンドを使用すると、次の警告でユーザの確認が求められます。

```
Warning: System is in maintenance mode. Please ensure user config won't inadvertently
revert back config in maintenance mode profile.
Do you wish to proceed anyway? (y/n) [n]
```
 - `<non-interactive>` オプションを使用してメンテナンス モードから **configure replace** コマンドを使用することはサポートされています。デフォルトでは、`yes` のユーザ確認を受けてから進行します。
 - コンフィギュレーションを適用するためにCisco NX-OS デバイスをリロードする必要がある場合、これらのコンフィギュレーションをリロードしてからコンフィギュレーションの置換操作を行う必要があります。
 - ユーザ指定のコンフィギュレーションファイルでのコマンドの順序は、Cisco Nexus スイッチの実行コンフィギュレーションでのこれらのコマンドと同じにする必要があります。
 - **CR** を使用してスイッチの実行コンフィギュレーションを置き換える必要があるユーザ コンフィギュレーションファイルは、新しいコマンドを設定した後、スイッチの実行コンフィギュレーションから生成する必要があります。ユーザ コンフィギュレーション ファイルは、CLI コマンドを使用して手動で編集しないでください。また、コンフィギュレーション コマンドのシーケンスを変更しないでください。

- セマンティック検証は、4ギガビットメモリプラットフォームではサポートされていません。
- 異なるバージョンの機能が実行コンフィギュレーションとユーザコンフィギュレーションに存在する場合（VRRPv2とVRRPv3など）、セマンティック検証オプションが期待どおりに機能しません。この問題は既知の制限です。

コンフィギュレーションの置換の推奨ワークフロー

コンフィギュレーションの置換の推奨されるワークフローを次に示します。

1. Cisco Nexus シリーズ デバイスで最初にコンフィギュレーションを適用してコンフィギュレーション ファイルを生成してから、コンフィギュレーション ファイルとして **show running-configuration** 出力を使用します。このファイルを使用して、必要に応じてコンフィギュレーションを変更します。次に、この生成または更新されたコンフィギュレーション ファイルを使用して、コンフィギュレーションの置換を実行します。



(注) ソフトウェア バージョンの変更があるたびにコンフィギュレーション ファイルを再生成する必要があります。異なるソフトウェア バージョンで生成されたコンフィギュレーション ファイルを使用してコンフィギュレーションの置換操作を実行することは推奨されません。

2. **configure replace <file> show-patch** コマンドを実行してパッチ ファイルを表示し、確認します。この手順は任意です。
3. コミットタイムアウト機能を使用するか、またはスキップしてコンフィギュレーションの置換ファイルを実行します。要件に基づいて、次の手順のいずれかを実行できます。
 - コンフィギュレーションの置換で実行されるコマンドをコンソールに表示するには、**configure replace <file> verbose** を実行します。
 - コミット時間を設定するには、**configure replace [bootflash/scp/sftp] <user-configuration-file> verbose commit-timeouttime** コマンドを実行します。
4. **configure replace commit** コマンドを実行し、コミット タイマーを停止します。この手順は、コミットタイムアウト機能でコンフィギュレーションの置換操作を実行している場合に必要です。
5. コンフィギュレーションのセマンティック検証を含むプレチェックをコンフィギュレーションの置換で実行します。エラーがある場合、コンフィギュレーションの置換操作は失敗します。失敗したコンフィギュレーションの詳細を表示するには、**show config-replace log verify** コマンドを使用します。パッチファイルを適用すると、コンフィギュレーションの置換によって検証プロセスがトリガーされます。コンフィギュレーションの置換は、検証プロセスで、実行コンフィギュレーションとユーザー構成ファイルを比較します。不一致がある場合、デバイスは元のコンフィギュレーションに復元されます。不一致のコン

フィギュレーションを表示するには、**show config-replace log verify** コマンドを使用します。

6. Cisco NX-OS リリース9.3(1) では、次のコンフィギュレーションの置換操作を実行できます。
 - セマンティック検証およびベストエフォートモードなしのコンフィギュレーションの置換。
 - セマンティック検証なし、ベストエフォートモードありのコンフィギュレーションの置換。
 - セマンティック検証あり、ベストエフォートモードなしのコンフィギュレーションの置換。
 - セマンティック検証およびベストエフォートモードありのコンフィギュレーションの置換。

コンフィギュレーションの置換の実行

コンフィギュレーションの置換を実行するには、次の操作を行います。

手順

	コマンドまたはアクション	目的
ステップ 1	configure replace {<uri_local> <uri_remote>} [verbose show-patch]	コンフィギュレーションの置換を実行します。コンフィギュレーションの置換の進行中にセッションを通じてコンフィギュレーションを変更すると、コンフィギュレーションの置換操作は失敗します。1つのコンフィギュレーション要求がすでに進行中であるときにコンフィギュレーションの置換要求を送信すると、要求はシリアル化されます。
ステップ 2	configure replace [bootflash / scp / sftp] <user-configuration-file> show-patch	実行コンフィギュレーションとユーザ指定のコンフィギュレーションの違いを表示します。
ステップ 3	configure replace [bootflash / scp / sftp] <user-configuration-file> verbose	スイッチのコンフィギュレーションを、ユーザが提供する新しいユーザコンフィギュレーションに置換します。コンフィギュレーションの置換は常にアトミックです。

	コマンドまたはアクション	目的
ステップ 4	configure replace <user-configuration-file> [best-effort]	<p>スイッチの設定を新しいユーザ設定に置き換え、セマンティック検証による設定の置き換えを有効にします。</p> <p>best-effort オプションを使用すると、コマンドでエラーが発生した場合でも設定の置換によって完全なパッチが実行され、以前の設定がロールバックされないようになります。</p>
ステップ 5	configure replace <user-configuration-file> [verify-and-commit]	<p>スイッチの設定を新しいユーザ設定に置き換え、セマンティック検証による設定の置き換えを有効にします。</p> <p>verify-and-commit オプションは、セマンティック検証を有効にするために使用されます。パッチは、完全なパッチのセマンティック検証に合格した場合にのみ実行されます。</p> <p>ベストエフォート オプション、verify-and-commit オプション、または両方のオプションを同時に使用できます。</p>
ステップ 6	configure replace <user-configuration-file> [verify-only]	<p>パッチのみを表示し、パッチでセマンティック検証を実行し、結果を表示します。パッチはシステムに適用されません。</p>
ステップ 7	(任意) configure replace [bootflash / scp / sftp] <user-configuration-file> verbose <i>commit-timeout time</i>	<p>コミット時間を秒単位で設定します。タイマーは、コンフィギュレーションの置換操作が正常に完了した後に開始されます。</p>
ステップ 8	(任意) configure replace [commit]	<p>コミット タイマーを停止し、コンフィギュレーションの置換設定を続行します。</p> <p>(注) この手順は、コミットタイムアウト機能を設定している場合にのみ適用されます。</p>

	コマンドまたはアクション	目的
		(注) 以前のコンフィギュレーションにロールバックするには、コミット タイマーの期限が切れるまで待機する必要があります。タイマーの期限が切れると、スイッチは自動的に以前のコンフィギュレーションにロールバックされます。
ステップ 9	(任意) configure replace [bootflash/scp/sftp] <user-configuration-file> <i>non-interactive</i>	メンテナンス モードでは、ユーザ プロンプトはありません。デフォルトでは、 yes のユーザ確認を受けてからロールバックが進行します。非インタラクティブ オプションは、メンテナンス モードでのみ使用できます。

コンフィギュレーションの置換の確認

コンフィギュレーションの置換とそのステータスをチェックして確認するには、表に記載されているコマンドを使用します。

表 27: コンフィギュレーションの置換の確認

コマンド	目的
configure replace [bootflash/scp/sftp] <user-configuration-file> show-patch	実行コンフィギュレーションとユーザ指定のコンフィギュレーションの違いを表示します。
show config-replace log exec	実行したすべてのコンフィギュレーションと失敗したコンフィギュレーションのログを表示します。エラーの場合、そのコンフィギュレーションに対してエラーメッセージが表示されます。
show config-replace log verify	失敗したコンフィギュレーションをエラーメッセージとともに表示します。成功したコンフィギュレーションは表示されません。

コマンド	目的
show config-replace status	コンフィギュレーションの置換操作のステータス（進行中、成功、失敗など）を表示します。コミットタイムアウト機能を設定している場合、コミットとタイマーのステータスに加え、コミットタイムアウトの残り時間も表示されます。

コンフィギュレーションの置換の例

以下のコンフィギュレーションの置換の設定例を参照してください。

- **configure replace bootflash:** <file> **show-patch** CLI コマンドを使用して、実行コンフィギュレーションとユーザ指定のコンフィギュレーションの違いを表示します。

```
switch(config)# configure replace bootflash:<file> show-patch
Collecting Running-Config
Converting to checkpoint file
#Generating Rollback Patch
!!
no role name abc
```

- **configure replace bootflash:** <file> **verbose** CLI コマンドを使用して、スイッチの実行コンフィギュレーション全体をユーザコンフィギュレーションに置換します。

```
switch(config)# configure replace bootflash:<file> verbose
Collecting Running-Config
Generating Rollback patch for switch profile
Rollback Patch is Empty
Note: Applying config parallely may fail Rollback verification
Collecting Running-Config
#Generating Rollback Patch
Executing Rollback Patch
=====
config t
no role name abc
=====
Generating Running-config for verification
Generating Patch for verification

Rollback completed successfully.

Sample Example with adding of BGP configurations.
switch(config)# sh run | section bgp
switch(config)# sh file bootflash:file | section bgp
feature bgp
router bgp 1
  address-family ipv4 unicast
  neighbor 1.1.1.1
switch(config)#
switch(config)# configure replace bootflash:file verbose
Collecting Running-Config
Generating Rollback patch for switch profile
Rollback Patch is Empty
Note: Applying config parallely may fail Rollback verification
Collecting Running-Config
```

```
#Generating Rollback Patch
Executing Rollback Patch
=====
config t
feature bgp
router bgp 1
address-family ipv4 unicast
neighbor 1.1.1.1
=====
Generating Running-config for verification
Generating Patch for verification

Rollback completed successfully.

switch(config)# sh run | section bgp
feature bgp
router bgp 1
  address-family ipv4 unicast
  neighbor 1.1.1.1

Sample Example with ACL
switch(config)# configure replace bootflash:run_1.txt
Collecting Running-Config
Generating Rollback patch for switch profile
Rollback Patch is Empty
Note: Applying config parallely may fail Rollback verification
Collecting Running-Config
#Generating Rollback Patch
Executing Rollback Patch
=====
config t
no ip access-list nexus-50-new-xyz
ip access-list nexus-50-new-xyz-jkl-abc
10 remark Newark
20 permit ip 17.31.5.0/28 any
30 permit ip 17.34.146.193/32 any
40 permit ip 17.128.199.0/27 any
50 permit ip 17.150.128.0/22 any
=====
Generating Running-config for verification
Generating Patch for verification

Rollback completed successfully.

switch(config)#

switch(config)# show run aclmgr | sec nexus-50-new-xyz-jkl-abc
ip access-list nexus-50-new-xyz-jkl-abc
 10 remark Newark
 20 permit ip 17.31.5.0/28 any
 30 permit ip 17.34.146.193/32 any
 40 permit ip 17.128.199.0/27 any
 50 permit ip 17.150.128.0/22 any
```

- **configure replace bootflash:user-config.cfg verify-only** CLI コマンドを使用して、パッチを意味的に生成および確認します。

```
switch(config)# configure replace bootflash:user-config.cfg verify-only

Version match between user file and running configuration.
Pre-check for User config PASSED
Collecting Running-Config
Converting to checkpoint file
```

```

Generating Rollback Patch
Validating Patch
=====
`config t `
`interface Ethernet1/1`
`shutdown`
`no switchport trunk allowed vlan`
`no switchport mode`
`no switchport`
`exit`
Skip non dme command for CR validation
`interface Vlan1`
`shutdown`
`interface Ethernet1/1`
`shutdown`
`no switchport`
`ip address 1.1.1.1/24`
`exit`
Skip non dme command for CR validation
=====
Patch validation completed successful
switch(config)#

```

- パッチでセマティック検証を実行した後、**configure replace bootflash:user-config.cfg best-effort verify-and-commit** CLI コマンドを使用して、スイッチの実行コンフィギュレーションを特定のユーザ コンフィギュレーションに置き換えます。

```

switch(config)# configure replace bootflash:user-config.cfg best-effort
verify-and-commit

Version match between user file and running configuration.
Pre-check for User config PASSED
ADVISORY: Config Replace operation started...
Modifying running configuration from another VSH terminal in parallel
is not recommended, as this may lead to Config Replace failure.

Collecting Running-Config
Generating Rollback patch for switch profile
Rollback Patch is Empty
Collecting Running-Config
Generating Rollback Patch

Validating Patch
Patch validation completed successful
Executing Rollback Patch
During CR operation,will retain L3 configuration
when vrf member change on interface
Generating Running-config for verification
Generating Rollback Patch

Configure replace completed successfully. Please run 'show config-replace log exec'
to see if there is any configuration that requires reload to take effect.

switch(config)#

```

- show config-replace log exec** CLI コマンドを使用して、実行したコンフィギュレーションと、存在する場合はエラーをすべて確認します。

```

switch(config)# show config-replace log exec
Operation          : Rollback to Checkpoint File
Checkpoint file name : .replace_tmp_28081
Scheme             : tmp
Rollback done By    : admin

```

```
Rollback mode      : atomic
Verbose           : enabled
Start Time        : Wed, 06:39:34 25 Jan 2017
-----
```

```
time: Wed, 06:39:47 25 Jan 2017
Status: SUCCESS
End Time          : Wed, 06:39:47 25 Jan 2017
Rollback Status   : Success
```

Executing Patch:

```
-----
switch#config t
switch#no role name abc
```

- **show config-replace log verify** CLI コマンドを使用して、存在する場合は失敗したコンフィギュレーションを確認します。

```
switch(config)# show config-replace log verify
Operation          : Rollback to Checkpoint File
Checkpoint file name : .replace_tmp_28081
Scheme             : tmp
Rollback done By    : admin
Rollback mode       : atomic
Verbose             : enabled
Start Time          : Wed, 06:39:34 25 Jan 2017
End Time            : Wed, 06:39:47 25 Jan 2017
Status              : Success
```

Verification patch contains the following commands:

```
-----
!!
! No changes
-----
```

```
time: Wed, 06:39:47 25 Jan 2017
Status: SUCCESS
```

- **show config-replace status** CLI コマンドを使用して、コンフィギュレーションの置換のステータスを確認します。

```
switch(config)# show config-replace status
Last operation : Rollback to file
Details:
  Rollback type: atomic replace_tmp_28081
  Start Time: Wed Jan 25 06:39:28 2017
  End Time: Wed Jan 25 06:39:47 2017
  Operation Status: Success
switch(config)#
```

スイッチから生成された設定の代わりに手動で作成された設定を使用すると、[置換の設定 (Configure Replace)] が失敗することがあります。失敗の原因として考えられるのは、**show running configuration** に示されていないデフォルト設定の潜在的な違いです。次の例を参照してください。

power redundancy コマンドがデフォルトのコマンドである場合、デフォルトの設定では表示されません。ただし、**show run all** コマンドを使用すると表示されます。次の例を参照してください。

```
switch# show run all
```

```
!Command: show running-config all
!Running configuration last done at: Tue Nov 12 11:07:44 2019
!Time: Tue Nov 12 11:16:09 2019

version 9.3(1) Bios:version 05.39
power redundancy-mode ps-redundant
no hardware module boot-order reverse
no license grace-period
<snip>
hostname n9k13
```

電源冗長コマンドは、**show running configuration** コマンド出力には表示されません。次の例を参照してください。

```
!Command: show running-config
!Running configuration last done at: Tue Nov 12 11:07:44 2019
!Time: Tue Nov 12 11:17:24 2019

version 9.3(1) Bios:version 05.39
hostname n9k13
```

設定置換のユーザ コンフィギュレーションに **power redundancy-mode ps-redundant** コマンドが追加された場合。検証/コミットが失敗する可能性があります。次の例を参照してください。

```
switch# show file bootflash:test

!Command: show running-config
!Running configuration last done at: Tue Nov 12 10:56:49 2019
!Time: Tue Nov 12 11:04:57 2019

version 9.3(1) Bios:version 05.39
power redundancy-mode ps-redundant
hostname n9k13
```

power redundancy-mode ps-redundant コマンドは、設定置換の後の **show running** には表示されません。したがって、「欠落」と見なされ、CR は失敗します。次に例を示します。

```
switch# config replace bootflash:test verify-and-commit

Version match between user file and running configuration.
Pre-check for User config PASSED
ADVISORY: Config Replace operation started...
Modifying running configuration from another VSH terminal in parallel
is not recommended, as this may lead to Config Replace failure.

Collecting Running-Config
Generating Rollback patch for switch profile
Rollback Patch is Empty
Collecting Running-Config
.Generating Rollback Patch

Validating Patch
Patch validation completed successful
Executing Rollback Patch
During CR operation,will retain L3 configuration
when vrf member change on interface
Generating Running-config for verification
Generating Rollback Patch
Executing Rollback Patch
During CR operation,will retain L3 configuration
when vrf member change on interface
Generating Running-config for verification
Generating Patch for verification
Verification failed, Rolling back to previous configuration
```

```

Collecting Running-Config
Cleaning up switch-profile buffer
Generating Rollback patch for switch profile
Executing Rollback patch for switch profiles. WARNING - This will change the
configuration of switch profiles and will also affect any peers if configured
Collecting Running-Config
Generating Rollback Patch
Rollback Patch is Empty
Rolling back to previous configuration is successful

Configure replace failed. Use 'show config-replace log verify' or 'show config-replace
log exec' to see reasons for failure

n9k13# show config-replace log verify
Operation : Config-replace to user config
Checkpoint file name : .replace_tmp_31849
Scheme : tmp
Cfg-replace done By : agargula
Cfg-replace mode : atomic
Verbose : disabled
Start Time : Tue, 11:20:59 12 Nov 2019
Start Time UTC : Tue, 10:20:59 12 Nov 2019
-----
End Time : Tue, 11:21:28 12 Nov 2019
End Time UTC : Tue, 10:21:28 12 Nov 2019
Status : Failed

Verification patch contains the following commands:
-----
!!
Configuration To Be Added Missing in Running-config
=====
!
power redundancy-mode ps-redundant

Undo Log
-----
End Time : Tue, 11:21:32 12 Nov 2019
End Time UTC : Tue, 10:21:32 12 Nov 2019
Status : Success
n9k13#

```

上記の例では、CR は欠落しているデフォルトのコマンドを考慮します。



第 27 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。

この章は、次の内容で構成されています。

- [ロールバックについて \(485 ページ\)](#)
- [ロールバックの前提条件 \(487 ページ\)](#)
- [ロールバックの注意事項と制約事項 \(487 ページ\)](#)
- [ロールバックのデフォルト設定 \(488 ページ\)](#)
- [ロールバックの設定 \(488 ページ\)](#)
- [ロールバック コンフィギュレーションの確認 \(490 ページ\)](#)
- [ロールバックの設定例 \(491 ページ\)](#)
- [その他の参考資料 \(491 ページ\)](#)

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までに、すで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。

システム チェックポイントの自動生成

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、有効になっている機能を無効にする
- **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。

高可用性

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。異なるチェックポイント コピーを作成できます。

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。

ロールバックの注意事項と制約事項

ロールバック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。

- 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。
- チェックポイントのファイル名の先頭を `system` にすることはできません。
- チェックポイントのファイル名の先頭を `auto` にすることができます。
- チェックポイントのファイル名を、`summary` または `summary` の略語にすることができます。
- 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。
- 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。
- `checkpoint` および `checkpointcheckpoint_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。
- 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、リロードの直後に出現します。

- ブートフラッシュ時のファイルへのロールバックは、**checkpoint checkpoint_name** コマンドを使用して作成されたファイルでのみサポートされます。他の ASCII タイプのファイルではサポートされません。
- 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の上書きすることはできません。
- 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。
- ロールバック操作中にインターフェイスに複数のポート VLAN マッピングを設定すると、ロールバック機能が失敗します。

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ります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	<p>[no] checkpoint {[cp-name] [description descr] file file-name }</p> <p>例 :</p> <pre>switch# checkpoint stable</pre>	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

	コマンドまたはアクション	目的
		<p>イント名を <code>user-checkpoint-number</code> に設定します。ここで <code>number</code> は 1 ~ 10 の値です。</p> <p><code>description</code> 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。</p> <p>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。</p>
ステップ 2	<p>(任意) show checkpoint <i>cp-name</i> [all]</p> <p>例 :</p> <pre>switch# show checkpoint stable</pre>	<p>チェックポイント名の内容を表示します。</p>

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	<p>show diff rollback-patch { checkpoint <i>src-cp-name</i> running-config startup-config file <i>source-file</i> } { checkpoint <i>dest-cp-name</i> running-config startup-config file <i>dest-file</i> }</p> <p>例 :</p> <pre>switch# show diff rollback-patch checkpoint stable running-config</pre>	<p>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。</p>
ステップ 2	<p>rollback running-config { checkpoint <i>cp-name</i> file <i>cp-file</i> } [atomic best-effort stop-at-first-failure]</p> <p>例 :</p> <pre>switch# rollback running-config checkpoint stable</pre>	<p>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。</p>

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • 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。 <p>デフォルトは atomic です。</p> <p>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。</p>

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 checkpoint <i>name</i> [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 <i>src-cp-name</i> running-config startup-config file <i>source-file</i> } { checkpoint <i>dest-cp-name</i> running-config startup-config file <i>dest-file</i> }	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。

ロールバックの設定例

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
コンフィギュレーションファイル	『Cisco Nexus 9000 Series NX-OS Fundamentals Configuration Guide』



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 \(493 ページ\)](#)

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 2579	『 <i>Textual Conventions for SMIV2</i> 』
RFC 2819	『 <i>Remote Network Monitoring Management Information Base</i> 』
RFC 2863	『 <i>The Interfaces Group MIB</i> 』
RFC 3176	<i>InMon Corporation</i> の <i>sFlow</i> : スイッチドおよびルーテッドネットワークのトラフィックをモニタする方法
RFC 3411 および RFC 3418	『 <i>An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks</i> 』
RFC 3413	『 <i>Simple Network Management Protocol (SNMP) Applications</i> 』
RFC 3417	『 <i>Transport Mappings for the Simple Network Management Protocol (SNMP)</i> 』



付録 **B**

Embedded Event Manager システム イベント および設定例

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 \(495 ページ\)](#)
- [EEM イベント \(499 ページ\)](#)
- [EEM ポリシーの設定例 \(500 ページ\)](#)

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
__BootupPortLoopback	CallHome を実行し、影響があるポートのエラーを無効にして、GOLD "BootupPortLoopback" テストに1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エラーテストを記録します。
__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
__asicmem	GOLD "AsicMemory" テストに失敗した場合には、CallHome を実行し、エラーを記録します。テストの失敗の原因となる問題は一時的なものである可能性があるため、カーネルパニックによるリカバリリロードを試行します。 (注) テストが失敗したときにカーネルパニックを回避するには、EEM システム ポリシーを上書します。
__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。

イベント	説明
__fpgareg	<p>GOLD "FpgaRegTest" テストに 20 回連続で失敗した場合は、CallHome を実行し、エラーを記録し、その後 HM テストをディセーブルにします。テストの失敗の原因となる問題は一時的なものである可能性があるため、カーネルパニックによるリカバリ リロードを試行します。</p> <p>(注) テストが失敗したときにカーネルパニックを回避するには、EEM システム ポリシーを上書します。</p>
__L2ACLRedirect	<p>L2ACLRedirect テストを 10 回連続で失敗した場合は、CallHome を実行し、エラーを記録し、その後 HM テストをディセーブルにします。テストの失敗の原因となる問題は一時的なものである可能性があるため、カーネルパニックによるリカバリ リロードを試行します。</p> <p>(注) テストが失敗したときにカーネルパニックを回避するには、EEM システム ポリシーを上書します。</p>
__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。
__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

イベント	説明
__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ラインカードの 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ラインカー ドの HM テストをディセーブルにします。
__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	Call Home 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 トを無効にします。

イベント	説明
_usb	Call Home 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
application	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。
インターフェイス	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。
両側面)	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。
なし	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。

EEM イベント	説明
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。
温度	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。
トラック	トラッキング対象オブジェクトの状態が変化します。

EEM ポリシーの設定例

CLI イベントの設定例

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（無効化）する設定例

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
```

One Bad センサーの無効化

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無効にする方法

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（無効化）

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（無効）

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つのセンサーを有効にして、すべてのモジュールの残りのセンサーをすべて無効にする方法

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
```

複数のセンサーを有効にして、すべてのモジュールの残りのセンサーをすべて無効にする方法

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有効にして、残りのモジュールのすべてのセンサーを無効にする方法

1つのモジュールのすべてのセンサーを有効にして、残りのモジュールのすべてのセンサーを無効にする方法

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有効にして、残りのモジュールのすべてのセンサーを無効にする方法

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（無効化）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取り外しのためのシャットダウンの上書き（無効）

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、シャットダウンを無効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（無効）

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、シャットダウンを無効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（無効化）

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、シャットダウンを無効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を取り外すためのシャットダウンの上書き（無効）

1つ（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、シャットダウンを無効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
```

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（無効）

```
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（無効）

指定したファントレイのセット（ファントレイ 2、3、4）を除くファンを取り外せるように、シャットダウンを無効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（無効）

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、シャットダウンを無効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設定例

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設定例

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-type event-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 plb-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 通知の設定例

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 )
```

イベントポリシーのイベントへの応答で SNMP 通知を送信

```
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 ODI 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 トラッキングの設定例

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 キーペア 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 1.0 syslog priority alerts msg 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
```



(注) severity キーワードは廃止され、次のパターンのみが許可されます。

```
[0-9 a-zA-Z][0-9 a-zA-Z]*[-_ ,:/0-9a-zA-Z]*
```




付録 **C**

Cisco NX-OS システム管理の設定制限

設定制限は『Cisco Nexus 9000 シリーズ NX-OS 検証済みスケーラビリティ ガイド』にまとめられています。

- [Cisco NX-OS システム管理の設定制限 \(515 ページ\)](#)

Cisco NX-OS システム管理の設定制限

Cisco NX-OS がサポートする機能には、設定の最大制限があります。一部の機能には、最大値以下の制限をサポートする設定があります。

設定制限は『Cisco Nexus 9000 シリーズ NX-OS 検証済みスケーラビリティ ガイド』にまとめられています。



索引

A

abort [25, 161](#)
action [251, 258–259, 261](#)
alert-group {Configuration | Diagnostic | EEM | Environmental |
Inventory | License | Supervisor-Hardware | Syslog-group-port
| System | Test} user-def-cmd [133](#)

C

callhome [126, 128, 130–131, 133–136, 138–140](#)
callhome send [140](#)
callhome send configuration [140](#)
callhome send diagnostic [140](#)
callhome test [140](#)
cdp advertise {v1 | v2} [93](#)
cdp enable [92–93](#)
cdp format device-id {mac-address | serial-number | system-name} [94](#)
cdp holdtime [94](#)
cdp timer [94](#)
cfs ipv4 distribute [20](#)
checkpoint [488](#)
clear cdp table [95](#)
clear checkpoint database [490](#)
clear counters interface all [398](#)
clear counters mpls strip [417](#)
clear hardware rate-limiter sflow [398](#)
clear cdp counters [95](#)
clear lldp counters [364](#)
clear logging logfile [114](#)
clear logging onboard [290](#)
clear mpls strip label dynamic [417](#)
clear ntp session [85](#)
clear ntp statistics [85](#)
clear ptp corrections [67](#)
clear scheduler logfile [172](#)
clear sflow statistics [398](#)
collect counter [378](#)
collect ip version [378](#)
collect timestamp sys-uptime [378](#)
collect transport tcp flags [378](#)
collect [376](#)
commit [21, 23, 25, 128–129, 131–133, 135, 137–140, 160](#)
設定の同期 [20, 22, 24, 27](#)
configure session [159](#)

configure maintenance profile maintenance-mode [427](#)
configure maintenance profile normal-mode [429](#)
contract-id [127](#)
copy ftp [451](#)
copy sftp: [453](#)
copy tftp [450](#)
customer-id [127](#)

D

destination-profile [128, 130, 132](#)
destination-profile {CiscoTAC-1 | full-txt-destination |
short-txt-destination} alert-group [132](#)
destination-profile {CiscoTAC-1 | full-txt-destination |
short-txt-destination} email-addr [130](#)
destination-profile {CiscoTAC-1 | full-txt-destination |
short-txt-destination} http [130](#)
destination-profile {CiscoTAC-1 | full-txt-destination |
short-txt-destination} message-level [130](#)
destination-profile {CiscoTAC-1 | full-txt-destination |
short-txt-destination} message-size [131](#)
destination-profile {CiscoTAC-1 | full-txt-destination |
short-txt-destination} transport-method {email | http} [130](#)
diagnostic bootup level {complete | minimal | bypass} [236](#)
diagnostic clear result module [239](#)
diagnostic monitor interval module [237](#)
diagnostic monitor module [237](#)
diagnostic ondemand action-on-failure {continue failure-count |
stop} [238](#)
diagnostic ondemand iteration [238](#)
diagnostic test simulation [239–240](#)
dir [449](#)
dir bootflash: [454](#)
dscp [379](#)

E

email-contact [126](#)
ERSPAN [342, 349](#)
宛先 [349](#)
設定例 [349](#)
宛先セッション [342](#)
ERSPAN の設定 [342](#)
宛先セッションの設定 [342](#)

erspan ソースのモニタセッション 341
 erspan-id 332
 event cli 252
 event counter 253
 event fanabsent 253
 event fanbad 253
 event fib adjacency extra 253
 event fib resource team usage 253
 event fib route {extra | inconsistent | missing} 253
 event manager applet 251, 261, 264
 event manager environment 250
 event manager policy 260
 event memory {critical | minor | severe} 254
 event module-failure 254
 event none 254
 event oir 255
 event policy-default count 255
 event poweroverbudget 255
 event snmp 256
 event storm-control 256
 event syslog 256
 event syslog {occurs | period | pattern | priority} 264
 event syslog tag {occurs | period | pattern | priority} 264
 event sysmgr memory 256
 event sysmgr switchover count 256
 event temperature 257
 event timer 257
 event track 257
 exporter 381

F

feature lldp 355
 feature netflow 375
 feature ntp 75
 feature ptp 52
 feature scheduler 166
 feature sflow 390
 filter access-group 310

G

Guest Shell 同期 465
 guestshell 465

H

hardware acl tap-agg 407
 hardware multicast global-tx-span 316
 hw-module logging onboard 287
 hw-module logging onboard counter-stats 287
 hw-module logging onboard cpuhog 287
 hw-module logging onboard environmental-history 287
 hw-module logging onboard error-stats 288
 hw-module logging onboard interrupt-stats 288

hw-module logging onboard module 288
 hw-module logging onboard obfl-logs 288

I

インポート 24
 import running-config 24
 install activate 455
 install add bootflash 454
 install add ftp 454
 install add tftp 454
 install add usb1 454
 install add usb2 454
 install commit 457, 459
 install deactivate 459
 install remove 459
 ip access-list 159, 313, 340, 408
 ip dscp 332
 ip flow monitor 382
 IP TTL 332
 ip access-group 160
 ip port access-group 410, 413
 ipv6 flow monitor 382
 isolate 425

L

lldp dcba version 357
 lldp holdtime 363
 lldp receive 356, 362
 lldp reinit 363
 lldp timer 363
 lldp tlv-select 363
 lldp transmit 356, 362
 logging console 100
 logging event {link-status | trunk-status} {enable | default} 104
 logging logfile 103
 logging message interface type ethernet description 102
 logging monitor 101
 logging origin-id 102
 logging source-interface Loopback 108
 logging timestamp {microseconds | milliseconds | seconds} 107
 logging server 108–109

M

mac access-list 408
 mac port access-group 410, 413
 mac packet-classify 384
 marker-packet 333
 match datalink 377, 383
 match ip 377
 match ipv4 377
 match ipv6 377
 match transport 378

monitor erspan origin ip-address [330](#)
 monitor session all shut [317, 334](#)
 monitor session all type erspan-source [330](#)
 monitor session [308, 317, 330, 334](#)
 mpls strip [412](#)
 mpls strip dest-mac [415](#)
 mpls strip label [414](#)
 mpls strip label-age [416](#)
 mtu [314](#)

N

NetFlow [382, 384](#)
 timeouts [384](#)
 VLAN でのブリッジ [382](#)
 no duplicate-message throttle [139](#)
 no monitor session all shut [334](#)
 no monitor session [308, 330, 334](#)
 no scheduler job name [169](#)
 no shut [311, 333, 335](#)
 no snmp trap link-status [203](#)
 no snmp-server protocol enable [207](#)
 no switch-profile [27](#)
 no system mode maintenance [437](#)
 no system mode maintenance dont-generate-profile [437](#)
 no system mode maintenance on-reload reset-reason [435](#)
 no isolate [425](#)
 no shutdown [425](#)
 no system interface shutdown [425](#)
 ntp access-group {peer | serve | serve-only | query-only} [81](#)
 ntp logging [84](#)
 ntp master [76](#)
 ntp source [83](#)
 ntp source-interface [84](#)
 ntp authenticate [80](#)
 ntp authentication-key [79](#)
 ntp server [77](#)
 ntp trusted-key [79](#)
 ntp peer [77](#)

O

option exporter-stats [380](#)
 option interface-table [380](#)

P

permit [159, 408](#)
 permit ip [314, 340](#)
 permit udf [314, 340](#)
 phone-contact [127](#)
 ptp [55](#)
 ptp announce {interval | timeout} [56](#)
 ptp clock-mode [54](#)
 ptp delay-request minimum interval [57](#)

ptp device-type generalized-ptp [53](#)
 ptp domain [53](#)
 ptp priority1 [54](#)
 ptp priority2 [54](#)
 ptp source [53](#)
 ptp vlan [58](#)
 ptp device-type boundary-clock [53](#)
 PTP アナウンス間隔 [57](#)
 PTP 同期間隔 [58](#)
 python instance [425, 429](#)

R

record [381](#)
 reload [313, 316, 340](#)
 rmon alarm [218](#)
 rmon event [220](#)
 rmon hcalarm [219](#)
 rollback running-config {checkpoint | file} [490](#)
 run bash [461](#)

S

scheduler aaa-authentication password [167](#)
 scheduler aaa-authentication username [167](#)
 show scheduler job name [168–169](#)
 scheduler schedule name [170](#)
 sflow agent-ip [396](#)
 sflow collector-ip [394](#)
 sFlow collector-port [395](#)
 sFlow counter-poll-interval [392](#)
 sflow data-source interface ethernet [397](#)
 sflow data-source interface port-channel [397](#)
 sflow max-datagram-size [393](#)
 sflow max-sampled-size [392](#)
 sflow sampling-rate [391](#)
 show callhome destination-profile [129, 131–132, 141](#)
 show callhome destination-profile profile [129, 131–132](#)
 show callhome transport [135, 137, 141](#)
 show call-home user-def-cmds [133, 141](#)
 show cdp all [94](#)
 show cdp entry {all | name} [94](#)
 show cdp global [94](#)
 show cdp interface [93–94](#)
 show cdp neighbors {device-id | interface} [94](#)
 show cdp neighbors detail [90](#)
 show checkpoint [489–490](#)
 show checkpoint all [490](#)
 show checkpoint all system [490](#)
 show checkpoint all user [490](#)
 show checkpoint summary [490](#)
 show checkpoint summary system [490](#)
 show checkpoint summary user [490](#)
 show configuration session [159–161](#)
 show configuration session status [161](#)

- show configuration session summary 161
- show diagnostic bootup level 236, 240
- show diagnostic content module 238, 240
- show diagnostic description module 240
- show diagnostic events 240
- show diagnostic ondemand setting 240
- show diagnostic result module 240
- show diagnostic simulation module 240
- show diagnostic status module 239–240
- show diff rollback-patch {checkpoint | running-config | startup-config | file} 489–490
- show event manager environment 250, 265
- show event manager environment all 250, 265
- show event manager event-types 265
- show event manager event-types all 265
- show event manager event-types module 265
- show event manager history events 265
- show event manager policy-state 251, 261, 265
- show event manager script system 265
- show event manager script system all 265
- show event manager system-policy 244, 250, 265
- show event manager system-policy all 265
- show feature 390
- show flow cache 385
- show flow exporter 385
- show flow interface 385
- show flow record netflow layer2-switched input 384–385
- show flow record 376, 385
- show hardware capacity 240
- show install active 448, 456
- show install committed 457
- show install inactive 455, 459
- show install log 456, 462
- show install packages 461
- show interface brief 440
- show interface snmp-ifindex 204, 210
- show lldp all 364
- show lldp dcBX interface 364
- show lldp interface 356, 362, 364
- show lldp neighbors detail 364
- show lldp neighbors interface 364
- show lldp timers 363–364
- show lldp tlv-select 363–364
- show lldp traffic 364
- show lldp traffic interface 364
- show logging nvram 114–115
- show logging console 101, 114
- show logging info 104, 114
- show logging logfile 114–115
- show logging level 106, 114
- show logging logfile end-time 114–115
- show logging logfile start-time 114–115
- show logging module 105, 115
- show logging monitor 102, 115
- clear logging nvram 114
- show logging nvram last 114–115
- show logging onboard 289
- show logging onboard boot-uptime 289
- show logging onboard counter-stats 289
- show logging onboard credit-loss 289
- show logging onboard device-version 289
- show logging onboard endtime 289
- show logging onboard environmental-history 289
- show logging onboard error-stats 289
- show logging onboard exception-log 289
- show logging onboard interrupt-stats 289
- show logging onboard module 289
- show logging onboard obfl-history 289
- show logging onboard obfl-logs 289
- show logging onboard stack-trace 290
- show logging onboard starttime 290
- show logging onboard status 290
- show logging origin-id 103, 115
- show logging timestamp 107, 115
- show maintenance on-reload reset-reasons 440
- show maintenance profile 440
- show maintenance profile maintenance-mode 428, 440
- show maintenance profile normal-mode 430, 440
- show maintenance timeout 440
- show monitor 317
- show monitor session all 311, 318, 335, 337, 345
- show monitor session range 311, 318, 337, 345
- show monitor session 311, 315, 318, 333, 337, 341, 345
- show mpls strip Labels 416
- show mpls strip labels all 416
- show mpls strip labels dynamic 416
- show mpls strip labels static 416
- show ntp access-groups 82, 85
- show ntp logging-status 84–85
- show ntp peer-status 85
- show ntp peers 78, 85
- show ntp rts-update 85
- show ntp source 85
- show ntp source-interface 85
- show ntp statistics {io | local | memory | peer {ipaddr | name}} 85
- show ptp brief 58, 66
- show ptp clock 66
- show ptp clock foreign-masters-record 66
- show ptp corrections 66
- show ptp counters 66
- show ptp parent 66
- show ptp port interface 58
- show ptp port interface ethernet 67
- show ptp time-property 67
- show qos dcBxp interface 364
- show rmon {alarms | hcalarms} 219
- show rmon alarms 220
- show rmon events 220
- show rmon hcalarms 220
- show rmon logs 220
- show rollback log 490
- show rollback log exec 490

- show rollback log verify [490](#)
- show running-config | include "scheduler aaa-authentication" [168](#)
- show running-config | include "system memory" [263](#)
- show running-config callhome [141](#)
- show running-config eem [244, 265](#)
- show running-config lldp [355, 364](#)
- show running-config mmode [440](#)
- show running-config monitor [333, 335, 345](#)
- show running-config netflow [385](#)
- show running-config ntp [76, 85](#)
- show running-config ptp [67](#)
- show running-config sflow [398](#)
- show running-config sflow all [398](#)
- show running-config snmp [210](#)
- show running-config switch-profile [28](#)
- show scheduler config [166, 171–172](#)
- show scheduler job [169, 172](#)
- show scheduler logfile [172](#)
- show scheduler schedule [172](#)
- show sflow [391–393, 395–398](#)
- show snapshots [431, 440](#)
- show snapshots compare [431, 433, 440](#)
- show snapshots dump [440](#)
- show snapshots sections [433, 440](#)
- show snmp [205, 210](#)
- show snmp community [210](#)
- show snmp context [206, 210](#)
- show snmp engineID [210](#)
- show snmp group [210](#)
- show snmp host [193, 210](#)
- show snmp source-interface [190, 193, 211](#)
- show snmp trap [211](#)
- show snmp user [184, 211](#)
- show startup-config callhome [141](#)
- show startup-config eem [265](#)
- show startup-config mmode [440](#)
- show startup-config monitor [333, 335, 345](#)
- show startup-config switch-profile [28](#)
- show switch-profile [21–23, 25, 28](#)
- show system mode [436, 438, 440](#)
- show tech-support callhome [141](#)
- show ttag brief [67](#)
- show callhome [128, 136, 138, 141](#)
- show clock [448](#)
- show install log detail [463](#)
- show ip access-lists [345, 409–410](#)
- show logging last [113–114](#)
- show logging server [109, 115](#)
- show mac access-lists [409–410](#)
- show module [240, 448](#)
- show ntp authentication-keys [79, 85](#)
- show ntp authentication-status [80, 85](#)
- show ntp trusted-keys [80, 85](#)
- show process [398](#)
- show snmp session [210](#)
- shut [317, 334](#)
- shutdown [425](#)
- site-id [127](#)
- sleep instance [425](#)
- snapshot create [430](#)
- snapshot delete [431](#)
- snapshot section add [432](#)
- snapshot section delete [433](#)
- snmp-server aaa-user cache-timeout [208](#)
- snmp-server context [206](#)
- snmp-server counter cache timeout [208](#)
- snmp-server enable traps [197](#)
- snmp-server enable traps aaa [197](#)
- snmp-server enable traps bgp [197](#)
- snmp-server enable traps bridge [198](#)
- snmp-server enable traps callhome [198](#)
- snmp-server enable traps config [198](#)
- snmp-server enable traps eigrp [198](#)
- snmp-server enable traps entity [199](#)
- snmp-server enable traps feature-control [199](#)
- snmp-server enable traps hsrp [199](#)
- snmp-server enable traps license [200](#)
- snmp-server enable traps link [200](#)
- snmp-server enable traps ospf [201](#)
- snmp-server enable traps rf [201](#)
- snmp-server enable traps rmon [201](#)
- snmp-server enable traps snmp [201](#)
- snmp-server enable traps stpx [202](#)
- snmp-server enable traps syslog [202](#)
- snmp-server enable traps sysmgr [202](#)
- snmp-server enable traps upgrade [202](#)
- snmp-server enable traps vtp [203](#)
- snmp-server globalEnforcePriv [184](#)
- snmp-server mib community-map [206](#)
- snmp-server source-interface {traps | informs} [190](#)
- snmp-server source-interface traps [193](#)
- snmp-server tcp-session [204](#)
- snmp-server community [185, 187](#)
- snmp-server contact [126, 205](#)
- snmp-server host [188–189, 191, 193](#)
- snmp-server location [205](#)
- snmp-server user [184–185, 190](#)
- SPAN セッション [370](#)
- 設定 [370](#)
- statistics per-entry [408](#)
- storm-control action trap [203](#)
- streetaddress [127](#)
- switch-priority [127](#)
- switch-profile [20, 22, 24](#)
- switchport [21, 308, 384, 410, 413](#)
- switchport monitor [308](#)
- sync-peer destination [26](#)
- sync-peers destination [20, 26](#)
- system memory-thresholds minor [262](#)
- system memory-thresholds threshold critical no-process-kill [263](#)
- system mode maintenance dont-generate-profile [435](#)

system mode maintenance on-reload reset-reason [435](#)
 system interface shutdown [425](#)

T

tag [251](#)
 template data timeout [380](#)
 terminal event-manager bypass [259](#)
 terminal monitor [100](#)
 time daily [171](#)
 time monthly [171](#)
 time start [171](#)
 time start now [171](#)
 time start repeat [171](#)
 time weekly [171](#)
 transport email from [134](#)
 transport email mail-server [134](#)
 transport http proxy enable [136](#)
 transport http proxy server [136](#)
 transport http use-vrf [135](#)
 transport udp [379](#)

U

udf [312, 338](#)

V

verify [23, 160](#)
 version 9 [380](#)
 vlan configuration [382](#)
 vrf [332](#)

あ

宛先 [379](#)
 宛先 IP [332](#)
 宛先インターフェイス [310, 315](#)

い

一致 [376](#)
 イネーブル化 [139](#)
 イベント [251, 261](#)
 イベントアプリケーション [252](#)
 イベントインターフェイス [254](#)
 イベントゴールドモジュール [253](#)
 イベントモジュール [254](#)
 インターフェイスのインポート [24](#)

し

システムモードメンテナンスシャットダウン [435](#)

システムモードメンテナンスタイムアウト [435](#)
 ジョブ名 [170](#)
 診断開始モジュール [239](#)
 診断停止モジュール [239](#)

す

スケジューラ ログファイル サイズ [166](#)

せ

設定例 [349](#)
 ERSPAN [349](#)
 宛先 [349](#)
 説明 [251, 261, 308, 330, 376, 379, 381](#)

そ

送信元 [379](#)

て

定期的なインベントリ通知 [138](#)
 定期的なインベントリ通知 timeofday [138](#)
 定期的なインベントリ通知の間隔 [138](#)
 転送電子メール返送先 [134](#)

は

送信元インターフェイス [314, 341](#)

ふ

フローエクスポート [379](#)
 flow monitor [380](#)
 フローレコード [376, 383](#)

ほ

保存 [159, 161](#)

れ

レイヤ2スイッチドフローモニタ [384](#)

ろ

logging module [105](#)
 logging level [105, 107](#)