Cisco Nexus 5600 シリーズ NX-OS システム管理設定ガイド リリース 7.x

初版：2014 年 03 月 15 日

最終更新：2014 年 12 月 22 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/

Text Part Number: OL-31641-01-J

【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。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

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

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

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: 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.(1110R)

© 2014 Cisco Systems, Inc. All rights reserved.

目 次

はじめに xix

対象読者 xix

表記法 xix

Cisco Nexus 5600 シリーズ NX-OS ソフトウェアの関連資料 xxi

Cisco Nexus 6000 シリーズ NX-OS ソフトウェアの関連資料 xxiii

マニュアルに関するフィードバック xxv

マニュアルの入手方法およびテクニカル サポート xxv

新機能および変更された機能に関する情報 1

新機能および変更された機能に関する情報 1

概要 3

システム管理機能 3

スイッチ プロファイルの設定 9

スイッチ プロファイルに関する情報 10

スイッチ プロファイル:コンフィギュレーション モード 10

コンフィギュレーションの検証 11

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 12

スイッチ プロファイルの前提条件 13

スイッチ プロファイルの注意事項および制約事項 13

スイッチ プロファイルの設定 15

スイッチ プロファイルへのスイッチの追加 16

スイッチ プロファイルのコマンドの追加または変更 18

スイッチ プロファイルのインポート 20

vPC トポロジでの設定のインポート 23

スイッチ プロファイルのコマンドの確認 23

ピア スイッチの分離 24

スイッチ プロファイルの削除 24

スイッチ プロファイルからのスイッチの削除 25
スイッチ プロファイル バッファの表示 27
スイッチのリブート後のコンフィギュレーションの同期化 28
スイッチ プロファイル設定の show コマンド 28
スイッチ プロファイルの設定例 29
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例 29
同期ステータスの確認例 31
実行コンフィギュレーションの表示 31
ローカル スイッチとピア 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 スイッチとピア スイッチでの確認とコミットの表示 33
同期の成功と失敗の例 34
スイッチ プロファイル バッファの設定、バッファ移動、およびバッファの削除 34
Cisco Nexus 5000 シリーズ スイッチの交換 35
モジュール事前プロビジョニングの設定 37
モジュールの事前プロビジョニングに関する情報 37
注意事項と制約事項 38
モジュールの事前プロビジョニングのイネーブル化 38
モジュールの事前プロビジョニングの削除 39
事前プロビジョニングした設定の確認 40
事前プロビジョニングの設定例 40
CFS の使用 43
CFS について 43
Cisco Fabric Services over Ethernet 44
CFS の注意事項および制約事項 44
CFS 配信 45
CFS の配信モード 45
非協調型配信 46
協調型配信 46
無制限の非協調型配信 46
CFS 配信ステータスの確認 46
アプリケーションの CFS サポート 47

CFS のアプリケーション要件 47
アプリケーションの CFS のイネーブル化 47
アプリケーション登録スターテスの確認 47
ネットワークのロック 48
CFS ロック ステータスの確認 48
変更のコミット 49
変更の廃棄 50
設定の保存 50
ロック済みセッションのクリア 50
CFS リージョン 51
CFS リージョンの概要 51
シナリオ例 51
CFS リージョンの管理 52
CFS リージョンの作成 52
CFS リージョンへのアプリケーションの割り当て 52
別の CFS リージョンへのアプリケーションの移動 53
リージョンからのアプリケーションの削除 53
CFS リージョンの削除 54
IP を介した CFS の設定 54
IPv4 を介した CFS のイネーブル化 54
IPv6 を介した CFS のイネーブル化 55
IP を介した CFS 設定の確認 55
IP を介した CFS の IP マルチキャスト アドレスの設定 55
CFS の IPv4 マルチキャスト アドレスの設定 56
CFS の IPv6 マルチキャスト アドレスの設定 56
IP を介した CFS の IP マルチキャスト アドレス設定の確認 57
CFS のデフォルト設定 57
CFS をイネーブルにして Smart Call Home コンフィギュレーションを配信する 58
CFS をイネーブルにしてデバイス エイリアス設定を配信する 58
CFS をイネーブルにして DPVM コンフィギュレーションを配信する 59
CFS をイネーブルにして FC ドメイン コンフィギュレーションを配信する 60

CFS をイネーブルにして FC ポート セキュリティ コンフィギュレーションを配信する 61
CFS をイネーブルにして FC タイマー設定を配信する 62
CFS をイネーブルにして IVR コンフィギュレーションを配信する 63
CFS をイネーブルにして NTP コンフィギュレーションを配信する 64
CFS をイネーブルにして RADIUS コンフィギュレーションを配信する 65
CFS をイネーブルにして RSCN コンフィギュレーションを配信する 66
CFS をイネーブルにして TACACS+ コンフィギュレーションを配信する 67
CFS をイネーブルにしてユーザ ロール コンフィギュレーションを配信する 67
PTP の設定 69
PTP に関する情報 69
PTP デバイス タイプ 70
PTP プロセス 71
クロック管理 71
PTP のハイ アベイラビリティ 72
PTP のライセンス要件 72
PTP の注意事項および制約事項 72
PTP のデフォルト設定 73
PTP の設定 73
PTP のグローバルな設定 73
インターフェイスでの PTP の設定 75
PTP 設定の確認 77
ユーザ アカウントおよび RBAC の設定 79
ユーザ アカウントおよび RBAC の概要 79
ユーザ ロール 79
事前定義された SAN 管理者ユーザ ロール 80
ルール 81
SAN 管理者ロール機能のルール マッピング 82
ユーザ ロール ポリシー 84
ユーザ アカウントの設定の制限事項 84
ユーザ パスワードの要件 85
ユーザ アカウントの注意事項および制約事項 86

ユーザ アカウントの設定 86
SAN 管理者ユーザの設定 87
RBAC の設定 88
ユーザ ロールおよびルールの作成 88
機能グループの作成 90
ユーザ ロール インターフェイス ポリシーの変更 91
ユーザ ロール VLAN ポリシーの変更 92
ユーザ ロール VSAN ポリシーの変更 92
ユーザ アカウントと RBAC の設定の確認 93
ユーザ アカウントおよび RBAC のユーザ アカウント デフォルト設定 94
Session Manager の設定 95
Session Manager の概要 95
Session Manager の注意事項および制約事項 96
Session Manager の設定 96
セッションの作成 96
セッションでの ACL の設定 96
セッションの確認 97
セッションのコミット 97
セッションの保存 98
セッションの廃棄 98
Session Manager のコンフィギュレーション例 98
Session Manager 設定の確認 98
オンライン診断の設定 101
オンライン診断について 101
ブートアップ診断 101
ヘルスモニタリング診断 102
拡張モジュール診断 103
オンライン診断の設定 104
オンライン診断設定の確認 105
オンライン診断のデフォルト設定 105
システム メッセージ ロギングの設定 107
システム メッセージ ロギングの概要 107

Syslog サーバ 108
システム メッセージ ロギングのライセンス要件 109
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 109
システム メッセージ ロギングのデフォルト設定 109
システム メッセージ ロギングの設定 110
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 110
ファイルへのシステム メッセージ ロギングの設定 112
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 113
ロギング タイムスタンプの設定 115
syslog サーバの設定 116
UNIX または Linux システムでの syslog の設定 118
syslog サーバ設定の配布の設定 119
ログ ファイルの表示およびクリア 121
システム メッセージ ロギングの設定確認 121
ACL ロギングの設定 123
ACL ロギングに関する情報 123
ACL ロギング キャッシュの設定 124
インターフェイスへの ACL ロギングの適用 125
ロギング使用 VLAN アクセス マップの設定 126
ACL ログの一致レベルの設定 126
ACL ロギングのレート リミッタの設定 127
ACL ログのクリア 128
ACL ロギングの確認 128
Smart Call Home の設定 129
Smart Call Home に関する情報 129
Smart Call Home の概要 130
Smart Call Home 宛先プロファイル 130
Smart Call Home アラート グループ 131
Smart Call Home のメッセージ レベル 133
Call Home のメッセージ形式 134
Smart Call Home の注意事項および制約事項 139
Smart Call Home の前提条件 140

Call Home のデフォルト設定 140
Smart Call Home の設定 141
Smart Call Home の登録 141
連絡先情報の設定 141
宛先プロファイルの作成 143
宛先プロファイルの変更 144
アラート グループと宛先プロファイルの関連付け 146
アラート グループへの show コマンドの追加 147
電子メール サーバの詳細の設定 148
定期的なインベントリ通知の設定 149
重複メッセージ抑制のディセーブル化 150
Smart Call Home のイネーブル化またはディセーブル化 151
Smart Call Home 設定のテスト 151
Smart Call Home 設定の確認 152
フル テキスト形式での syslog アラート通知の例 153
XML 形式での syslog アラート通知の例 153
ロールバックの設定 157
ロールバックについて 157
ロールバックの注意事項および制約事項 157
チェックポイントの作成 158
ロールバックの実装 159
ロールバック コンフィギュレーションの確認 160
DNS の設定 163
DNS クライアントに関する情報 163
ネーム サーバ 163
DNS の動作 164
ハイ アベイラビリティ 164
DNS クライアントの前提条件 164
DNS クライアントのライセンス要件 164
DNS クライアントのデフォルト設定 165
DNS クライアントの設定 165
SNMP の設定 169

SNMP について 169
SNMP 機能の概要 169
SNMP 通知 170
SNMPv3 170
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 171
ユーザベースのセキュリティ モデル 172
CLI および SNMP ユーザの同期 173
グループベースの SNMP アクセス 174
SNMP のライセンス要件 174
SNMP の注意事項および制約事項 174
SNMP のデフォルト設定 174
SNMP の設定 175
SNMP ユーザの設定 175
SNMP メッセージ暗号化の適用 176
SNMPv3 ユーザに対する複数のロールの割り当て 176
SNMP コミュニティの作成 176
SNMP 要求のフィルタリング 177
SNMP 通知レシーバの設定 177
VRF を使用する SNMP 通知レシーバの設定 179
VRF に基づく SNMP 通知のフィルタリング 179
すべての SNMP 通知を送信するための送信元インターフェイスの設定 180
SNMP 通知のホスト レシーバの設定 181
インバンド アクセスのための SNMP の設定 182
SNMP 通知のイネーブル化 183
リンクの通知の設定 186
インターフェイスでのリンク通知のディセーブル化 186
TCP での SNMP に対するワンタイム認証のイネーブル化 187
SNMP スイッチの連絡先および場所の情報の割り当て 187
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 188
SNMP のディセーブル化 189
SNMP 設定の確認 189

RMON の設定 191

RMON について 191

RMON アラーム 191

RMON イベント 192

RMON の設定時の注意事項および制約事項 193

RMON の設定 193

RMON アラームの設定 193

RMON イベントの設定 194

RMON 設定の確認 195

デフォルトの RMON 設定 195

SPAN の設定 197

SPAN に関する情報 198

SPAN ソース 198

送信元ポートの特性 198

SPAN 宛先 199

宛先ポートの特性 199

複数の SPAN 宛先 200

ACL を使用した SPAN 200

SPAN on Drop 200

SPAN-on-Latency セッション 200

SPAN の注意事項および制約事項 201

SPAN セッションの作成または削除 204

イーサネット宛先ポートの設定 205

SPAN セッションごとの MTU の切り捨ての設定 206

送信元ポートの設定 207

SPAN セッションの説明の設定 208

SPAN セッションに対する ACL フィルタの設定 209

SPAN-on-Drop セッションの設定 210

SPAN-on-Latency セッションの設定 211

SPAN セッションのアクティブ化 213

SPAN セッションの問題のトラブルシューティング 213

多数の送信元ポートを使用する SPAN セッションの問題のトラブルシューティング 214
SPAN 情報の表示 215
SPAN ACL の設定例 216
SPAN-on-Latency セッションの設定例 216
ローカル SPAN および ERSPAN の設定 217
ERSPAN に関する情報 217
ERSPAN 送信元セッション 218
モニタ対象トラフィック 218
ERSPAN タイプ 219
ERSPAN 送信元 219
ERSPAN 宛先 220
切り捨てを適用する ERSPAN 220
ACL を使用した ERSPAN 221
ERSPAN SPAN on Drop 221
ERSPAN SPAN-on-Latency 221
ハイ アベイラビリティ 221
ERSPAN のライセンス要件 221
ERSPAN の前提条件 222
ERSPAN の注意事項および制約事項 222
ERSPAN タイプ III の注意事項および制約事項 226
ERSPAN のデフォルト設定 226
ERSPAN の設定 226
ERSPAN 送信元セッションの設定 226
ERSPAN タイプ III 送信元セッションの設定 229
切り捨てを適用する ERSPAN の設定 232
ERSPAN 宛先セッションの設定 233
ERSPAN SPAN-on-Drop セッションの設定 236
ERSPAN SPAN-on-Latency セッションの設定 237
ERSPAN セッションのシャットダウンまたはアクティブ化 239
ERSPAN 設定の確認 241
ERSPAN の設定例 242
ERSPAN 送信元セッションの設定例 242

ERSPAN タイプ III 送信元セッションの設定例 242
ERSPAN セッションの送信元としての IP アドレスの設定例 242
切り捨てを適用する ERSPAN の設定例 243
ERSPAN 宛先セッションの設定例 243
ERSPAN ACL の設定例 243
ERSPAN SPAN-on-Drop セッションの設定例 244
ERSPAN SPAN-on-Latency セッションの設定例 244
その他の参考資料 244
関連資料 244
NTP の設定 245
NTP の概要 245
NTP サーバに関する情報 245
タイム サーバとしての NTP 246
CFS を使用した NTP の配信 246
クロック マネージャ 246
ハイ アベイラビリティ 247
ライセンス要件 247
NTP の前提条件 247
NTP の注意事項と制約事項 247
NTP のデフォルト設定 248
NTP の設定 249
NTP のイネーブル化/ディセーブル化 249
正規の NTP サーバとしてのデバイスの設定 249
NTP サーバおよびピアの設定 250
NTP 認証の設定 252
NTP アクセス制限の設定 253
NTP ソース IP アドレスの設定 255
NTP ソース インターフェイスの設定 255
NTP ロギングの設定 256
NTP 用の CFS 配信のイネーブル化 257
NTP 設定変更のコミット 257
NTP 設定変更の廃棄 258

CFS セッション ロックの解放 258
NTP の設定確認 259
NTP の設定例 260
EEM の設定 263
Embedded Event Manager について 263
EEM ポリシー 264
EEM イベント文 265
EEM アクション文 266
VSH スクリプト ポリシー 267
EEM イベント相関 267
EEM 仮想化サポート 268
EEM のライセンス要件 268
EEM の前提条件 268
EEM の注意事項と制約事項 268
EEM のデフォルト設定 269
EEM の設定 269
環境変数の定義 269
CLI によるユーザ ポリシーの定義 270
イベント文の設定 272
アクション文の設定 274
VSH スクリプトによるポリシーの定義 276
VSH スクリプト ポリシーの登録およびアクティブ化 276
ポリシーの上書き 277
EEM パブリッシャとしての syslog の設定 279
Tcl スクリプト トリガーのための CLI を使用したユーザ ポリシーの定義 280
Python スクリプト トリガーのための CLI を使用したユーザ ポリシーの定義 282
EEM 設定の確認 283
EEM のコンフィギュレーション例 284
OpenFlow の設定 285
OpenFlow について 285
OpenFlow の制約事項 286
サポートされるインターフェイス タイプ 286

サポートされないインターフェイス タイプ 286
サポートされるインターフェイス モード 286
サポートされる match フィールド 287
サポートされるアクション 287
フロー数の拡張 288
パイプラインのサポート 288
OpenFlow の前提条件 288
OpenFlow 仮想サービスのセットアップ 290
OpenFlow のイネーブル化 290
OpenFlow スイッチの設定 291
OpenFlow の確認 293
NetFlow の設定 295
NetFlow の概要 295
フロー レコード 296
Flow Exporter 296
NetFlow の照合キー 297
match パラメータの指定 297
NetFlow の collect パラメータ 299
collect パラメータの指定 299
サンプリングされた NetFlow 300
NetFlow の注意事項と制約事項 300
NetFlow の設定方法 301
NetFlow 機能のイネーブル化 302
フロー レコードの作成 302
フロー エクスポータの作成 303
フロー モニタの作成 305
サンプラーの作成 306
インターフェイスへのフロー モニタの適用 307
VLAN 上でのブリッジ型 NetFlow の設定 308
NetFlow タイムアウトの設定 309
NetFlow 設定の確認 310
NetFlow のモニタリング 311

NetFlow の設定例 311
例：フローの作成と適用 311
例：NetFlow エクスポータの設定 311
GIR の設定（Cisco NX-OS Release 7.3(0)N1(1)） 313
GIR について 313
メンテナンス プロファイル 315
計画外のメンテナンス 316
メンテナンス モードのタイマー 317
Snapshot 317
FIB 保留の抑制 319
FEX グループの GIR 機能 319
GIR の注意事項および制約事項 320
カスタムのメンテナンス モードおよびカスタムの通常モードのプロファイルの設定 321
スナップショットの作成 322
スナップショットへの show コマンドの追加 324
スナップショット セクションのダンプ 325
メンテナンス モードの開始 326
通常モードへの復帰 330
メンテナンス プロファイルの削除 331
GIR の設定例 331
GIR の確認 339
プロトコル レベルでの GIR の確認 340
GIR の機能の履歴 342
GIR の設定（Cisco NX-OS Release 7.1(0)N1(1)） 343
GIR について 343
GIR の注意事項および制約事項 344
GIR サイクルの実行 344
通常モード プロファイル ファイルの設定 345
スナップショットの作成 346
メンテナンス モードの開始 347
通常モードへの復帰 348

メンテナンス モード プロファイル ファイルの設定 348
GIR の確認 350
クラスベース QoS MIB 353
クラスベース QoS MIB 353
クラスベース QoS MIB について 353
クラスベース QoS MIB のライセンス要件 354
QoS ポリシーの設定 354
クラスベース QoS MIB の設定と統計情報の表示 356
クラスベース QoS MIB のその他の参考資料 357
クラスベース QoS MIB の機能の履歴 358

はじめに

ここでは、次の項について説明します。

- 対象読者，xix ページ
- 表記法，xix ページ
- Cisco Nexus 5600 シリーズ NX-OS ソフトウェアの関連資料，xxi ページ
- Cisco Nexus 6000 シリーズ NX-OS ソフトウェアの関連資料，xxiii ページ
- マニュアルに関するフィードバック，xxv ページ
- マニュアルの入手方法およびテクニカル サポート，xxv ページ

対象読者

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

表記法

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

コマンドの説明には、次のような表記法が使用されます。

表記法	説明
bold	太字の文字は、表示どおりにユーザが入力するコマンドおよびキーワードです。

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

例では、次の表記法を使用しています。

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

このマニュアルでは、次の表記法を使用しています。

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

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

Cisco Nexus 5600 シリーズ NX-OS ソフトウェアの関連資料

Cisco NX-OS 5600 シリーズ全体のマニュアル セットは、次の URL から入手できます。

http://www.cisco.com/c/en/us/support/switches/nexus-5000-series-switches/tsd-products-support-series-home.html

リリース ノート

リリース ノートは、次の URL から入手できます。

http://www.cisco.com/c/en/us/support/switches/nexus-5000-series-switches/products-release-notes-list.html

コンフィギュレーション ガイド

これらのマニュアルは、次の URL から入手できます。

http://www.cisco.com/c/en/us/support/switches/nexus-5000-series-switches/products-installation-and-configuration-guides-list.html

このカテゴリのマニュアルには、次が含まれます。

- 『*Cisco Nexus 5600 Series NX-OS Adapter-FEX Configuration Guide*』
- 『*Cisco Nexus 5600 Series NX-OS FabricPath Configuration Guide*』
- 『*Cisco Nexus 5600 Series NX-OS Fibre Channel over Ethernet Configuration Guide*』
- 『*Cisco Nexus 5600 Series NX-OS Fundamentals Configuration Guide*』
- 『*Cisco Nexus 5600 Series NX-OS Interfaces Configuration Guide*』
- 『*Cisco Nexus 5600 Series NX-OS Layer 2 Switching Configuration Guide*』
- 『*Cisco Nexus 5600 Series NX-OS Multicast Routing Configuration Guide*』
- 『*Cisco Nexus 5600 Series NX-OS Quality of Service Configuration Guide*』
- 『*Cisco Nexus 5600 Series NX-OS SAN Switching Configuration Guide*』
- 『*Cisco Nexus 5600 Series NX-OS Security Configuration Guide*』

- 『*Cisco Nexus 5600 Series NX-OS System Management Configuration Guide*』
- 『*Cisco Nexus 5600 Series NX-OS Unicast Routing Configuration Guide*』

ライセンス ガイド

『*License and Copyright Information for Cisco NX-OS Software*』は、http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_0/nx-os/license_agreement/nx-ossw_lisns.html から入手できます。

コマンド リファレンス

これらのマニュアルは、次の URL から入手できます。

http://www.cisco.com/c/en/us/support/switches/nexus-5000-series-switches/products-command-reference-list.html

このカテゴリのマニュアルには、次が含まれます。

- 『*Cisco Nexus 5600 Series NX-OS Fabric Extender Command Reference*』
- 『*Cisco Nexus 5600 Series NX-OS FabricPath Command Reference*』
- 『*Cisco Nexus 5600 Series NX-OS Command Reference*』
- 『*Cisco Nexus 5600 Series NX-OS Fundamentals Command Reference*』
- 『*Cisco Nexus 5600 Series NX-OS Interfaces Command Reference*』
- 『*Cisco Nexus 5600 Series NX-OS Layer 2 Interfaces Command Reference*』
- 『*Cisco Nexus 5600 Series NX-OS Multicast Routing Command Reference*』
- 『*Cisco Nexus 5600 Series NX-OS QoS Command Reference*』
- 『*Cisco Nexus 5600 Series NX-OS Security Command Reference*』
- 『*Cisco Nexus 5600 Series NX-OS System Management Command Reference*』
- 『*Cisco Nexus 5600 Series NX-OS TrustSec Command Reference*』
- 『*Cisco Nexus 5600 Series NX-OS Unicast Routing Command Reference*』
- 『*Cisco Nexus 5600 Series NX-OS Virtual Port Channel Command Reference*』

エラー メッセージおよびシステム メッセージ

『*Cisco Nexus 5600 Series NX-OS System Message Guide*』は、http://www.cisco.com/en/US/docs/switches/datacenter/nexus5500/sw/system_messages/reference/sl_nxos_book.html から入手できます。

トラブルシューティング ガイド

『*Cisco Nexus 5600 Series NX-OS Troubleshooting Guide*』は、http://www.cisco.com/c/en/us/support/switches/nexus-5000-series-switches/products-troubleshooting-guides-list.html から入手できます。

Cisco Nexus 6000 シリーズ NX-OS ソフトウェアの関連資料

Cisco NX-OS 6000 シリーズ全体のマニュアル セットは、次の URL から入手できます。

http://www.cisco.com/en/US/products/ps12806/tsd_products_support_series_home.html

リリース ノート

リリース ノートは、次の URL から入手できます。

http://www.cisco.com/c/en/us/support/switches/nexus-6000-series-switches/products-release-notes-list.html

コンフィギュレーション ガイド

これらのマニュアルは、次の URL から入手できます。

http://www.cisco.com/c/en/us/support/switches/nexus-6000-series-switches/products-installation-and-configuration-guides-list.html

このカテゴリのマニュアルには、次が含まれます。

- 『*Cisco Nexus 6000 Series NX-OS Adapter-FEX Configuration Guide*』
- 『*Cisco Nexus 6000 Series NX-OS FabricPath Configuration Guide*』
- 『*Cisco Nexus 6000 Series NX-OS FCoE Configuration Guide*』
- 『*Cisco Nexus 6000 Series NX-OS Fundamentals Configuration Guide*』
- 『*Cisco Nexus 6000 Series NX-OS Interfaces Configuration Guide*』
- 『*Cisco Nexus 6000 Series NX-OS Layer 2 Switching Configuration Guide*』
- 『*Cisco Nexus 6000 Series NX-OS Multicast Routing Configuration Guide*』
- 『*Cisco Nexus 6000 Series NX-OS Quality of Service Configuration Guide*』
- 『*Cisco Nexus 6000 Series NX-OS SAN Switching Configuration Guide*』
- 『*Cisco Nexus 6000 Series NX-OS Security Configuration Guide*』
- 『*Cisco Nexus 6000 Series NX-OS System Management Configuration Guide*』
- 『*Cisco Nexus 6000 Series NX-OS Unicast Routing Configuration Guide*』

インストレーション ガイドおよびアップグレード ガイド

これらのマニュアルは、次の URL から入手できます。

http://www.cisco.com/c/en/us/support/switches/nexus-6000-series-switches/products-installation-guides-list.html

このカテゴリのマニュアルには、次が含まれます。

- 『*Cisco Nexus 6000 Series NX-OS Software Upgrade and Downgrade Guides*』

ライセンス ガイド

『*License and Copyright Information for Cisco NX-OS Software*』は、http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_0/nx-os/license_agreement/nx-ossw_lisns.html から入手できます。

コマンド リファレンス

これらのマニュアルは、次の URL から入手できます。

http://www.cisco.com/c/en/us/support/switches/nexus-6000-series-switches/products-command-reference-list.html

このカテゴリのマニュアルには、次が含まれます。

- 『*Cisco Nexus 6000 Series NX-OS Fabric Extender Command Reference*』
- 『*Cisco Nexus 6000 Series NX-OS FabricPath Command Reference*』
- 『*Cisco Nexus 6000 Series NX-OS Fundamentals Command Reference*』
- 『*Cisco Nexus 6000 Series NX-OS Interfaces Command Reference*』
- 『*Cisco Nexus 6000 Series NX-OS Layer 2 Interfaces Command Reference*』
- 『*Cisco Nexus 6000 Series NX-OS Multicast Routing Command Reference*』
- 『*Cisco Nexus 6000 Series NX-OS Quality of Service Command Reference*』
- 『*Cisco Nexus 6000 Series NX-OS Security Command Reference*』
- 『*Cisco Nexus 6000 Series NX-OS System Management Command Reference*』
- 『*Cisco Nexus 6000 Series NX-OS TrustSec Command Reference*』
- 『*Cisco Nexus 6000 Series NX-OS Unicast Routing Command Reference*』
- 『*Cisco Nexus 6000 Series NX-OS Virtual Port Channel Command Reference*』

テクニカル リファレンス

『*Cisco Nexus 6000 Series NX-OS MIB Reference*』は http://www.cisco.com/en/US/docs/switches/datacenter/nexus6000/sw/mib/reference/NX6000_MIBRef.html から入手できます。

エラー メッセージおよびシステム メッセージ

『*Cisco Nexus 6000 Series NX-OS System Message Guide*』は、http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus6000/sw/system_messages/reference/sl_nxos_book.html から入手できます。

トラブルシューティング ガイド

『*Cisco Nexus 6000 Series NX-OS Troubleshooting Guide*』は、http://www.cisco.com/c/en/us/support/switches/nexus-6000-series-switches/tsd-products-support-troubleshoot-and-alerts.html から入手できます。

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 ciscodfa-docfeedback@cisco.com までご連絡ください。

ご協力をよろしくお願いいたします。

マニュアルの入手方法およびテクニカル サポート

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

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

第 1 章

新機能および変更された機能に関する情報

- 新機能および変更された機能に関する情報，1 ページ

新機能および変更された機能に関する情報

次の表では、このコンフィギュレーション ガイドでの重要な変更点の概要を示します。この表は、このマニュアルのすべての変更点、または特定のリリースのすべての新機能をまとめたリストではありません。

機能	説明	リリース	参照先
GIR の強化	Cisco NX-OS Release 7.3(0)N1(1) 以降の GIR のデフォルト モードは isolate です。計画外のメンテナンス、メンテナンス モードのタイマー、FIB 保留の抑制、スナップショットへの show コマンドの追加、スナップショット セクションのダンプなどのサポートを提供します。GIR を使用して、スイッチおよび接続された FEX のメンテナンスとソフトウェア アップグレードを実行できます。FEX グループは、FEX の起動または停止の手順を最適化するために追加されました。	7.3(0)N1(1)	（Cisco NX-OS Release 7.3(0)N1(1)）
クラスベース QoS MIB	クラスマップとポリシーマップの設定と統計情報の取得を可能にする Simple Network Management Protocol（SNMP）MIB を提供します。	7.1(1)N1(1)	クラスベース QoS MIB

機能	説明	リリース	参照先
分離とメンテナンスモードの強化	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、デバッグやアップグレードを実行できます。スイッチは、通常のスイッチング パスから削除され、メンテナンスモードになります。スイッチのメンテナンスが完了すると、スイッチをフル動作モードにすることができます。	7.1(0)N1(1)	GIR の設定（Cisco NX-OS Release 7.1(0)N1(1)）

第 2 章

概要

この章の内容は、次のとおりです。

- システム管理機能，3 ページ

システム管理機能

このマニュアルに記載されているシステム管理機能について説明します。

機能	説明
スイッチ プロファイル	設定の同期を使用すると、管理者は、設定変更を1台のスイッチで行い、ピア スイッチに自動的に設定を同期させることができます。この機能により、設定ミスがなくなり、管理上のオーバーヘッドが軽減されます。 設定同期モード（config-sync）を使用すると、ローカルおよびピア スイッチを同期するためにスイッチ プロファイルを作成できます。

機能	説明
モジュールの事前プロビジョニング	モジュールの事前プロビジョニング機能を使用すると、Cisco Nexus シリーズ スイッチにモジュールを挿入または取り付ける前に、インターフェイスの事前設定を行うことができます。また、モジュールがオフラインになった場合に、オフラインモジュールのインターフェイス設定に変更を加えるため、事前プロビジョニングを使用できます。一部の vPC トポロジでは、設定の同期機能に事前プロビジョニングが必要です。事前プロビジョニングでは、あるピアでオンラインでも別のピアでオフラインであるインターフェイスの設定を同期させることができます。
シスコ ファブリック サービス	Cisco MDS NX-OS ソフトウェアは、データベースを効率的に分散し、デバイスの柔軟性を高めるため、Cisco Fabric Services（CFS）インフラストラクチャを使用します。CFS により、ファブリック内のすべてのスイッチに設定情報を自動的に配信できるため、SAN のプロビジョニングが簡単になります。
高精度時間プロトコル	高精度時間プロトコル（PTP）はネットワークに分散したノードの時刻同期プロトコルです。そのハードウェアのタイムスタンプ機能は、ネットワーク タイム プロトコル（NTP）などの他の時刻同期プロトコルより高い精度を実現します。
ユーザ アカウントおよび RBAC	ユーザ アカウントおよびロールベース アクセス コントロール（RBAC）では、割り当てられたロールのルールを定義できます。ロールは、ユーザが管理操作にアクセスするための許可を制限します。各ユーザ ロールに複数のルールを含めることができ、各ユーザが複数のロールを持つことができます。
Session Manager	Session Manager を使用すると、コンフィギュレーションを作成し、すべて正しく設定されていることを確認および検証したあとでバッチモードで適用できます。

機能	説明
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。
『System Message Logging』	システム メッセージ ロギングを使用して宛先を制御し、システム プロセスが生成するメッセージの重大度をフィルタリングできます。端末セッション、ログ ファイル、およびリモート システム上の syslog サーバへのロギングを設定できます。 システム メッセージ ロギングは RFC 3164 に準拠しています。システム メッセージのフォーマットおよびデバイスが生成するメッセージの詳細については、『*Cisco NX-OS System Messages Reference*』を参照してください。
Smart Call Home	Call Home は重要なシステム ポリシーを電子メールで通知します。Cisco NX-OS では、ポケット ベル サービス、標準的な電子メール、または XML ベースの自動化された解析アプリケーションとの最適な互換性のために、広範なメッセージ形式が提供されています。この機能を使用して、ネットワーク サポート エンジニアや Network Operations Center を呼び出せます。また、Cisco Smart Call Home サービスを使用して、TAC でケースを自動的に生成することもできます。

機能	説明
設定のロール バック	設定のロールバック機能を使用すると、Cisco NX-OS の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、スイッチ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スイッチに再適用できます。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。
SNMP	簡易ネットワーク管理プロトコル（SNMP）は、SNMP マネージャとエージェント間の通信用メッセージ フォーマットを提供する、アプリケーションレイヤ プロトコルです。SNMP では、ネットワーク内のデバイスのモニタリングと管理に使用する標準フレームワークと共通言語が提供されます。
RMON	RMON は、各種のネットワーク エージェントおよびコンソール システムがネットワーク モニタリングデータを交換できるようにするための、Internet Engineering Task Force（IETF）標準モニタリング仕様です。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。
SPAN	スイッチド ポート アナライザ（SPAN）機能（ポート ミラーリングまたはポート モニタリングとも呼ばれる）は、ネットワーク アナライザによる分析のためにネットワーク トラフィックを選択します。ネットワーク アナライザは、Cisco SwitchProbeまたはその他のリモート モニタリング（RMON）プローブです。

機能	説明
ERSPAN	Encapsulated Remote Switched Port Analyzer（ERSPAN）は、IP ネットワークでミラーリングされたトラフィックを転送するために使用します。ERSPAN は異なるスイッチ上の送信元ポート、送信元 VLAN、および宛先をサポートし、ネットワーク上にある複数のスイッチのリモートモニタリングを可能にします。ERSPAN は、スイッチ間でトラフィックを伝送するために、総称ルーティング カプセル化（GRE）を使用します。 ERSPAN は、ERSPAN 送信元セッション、ルーティング可能な ERSPAN GRE カプセル化トラフィック、および ERSPAN 宛先セッションで構成されています。異なるスイッチで ERSPAN 送信元セッションおよび宛先セッションを個別に設定します。 ERSPAN 送信元セッションを 1 台のスイッチ上で設定するには、送信元ポートまたは VLAN のセットを、宛先 IP アドレス、ERSPAN ID 番号、および仮想ルーティングおよび転送（VRF）名に対応付けます。ERSPAN 宛先セッションを別のスイッチ上で設定するには、宛先を送信元 IP アドレス、ERSPAN ID 番号、および VRF 名に対応付けます。 ERSPAN 送信元セッションは、送信元ポートまたは送信元 VLAN からのトラフィックをコピーし、このトラフィックを、ルーティング可能な GRE カプセル化パケットを使用して ERSPAN 宛先セッションに転送します。ERSPAN 宛先セッションはトラフィックを宛先へスイッチングします。

第 3 章

スイッチ プロファイルの設定

この章の内容は、次のとおりです。

- スイッチ プロファイルに関する情報，10 ページ
- スイッチ プロファイル:コンフィギュレーション モード，10 ページ
- コンフィギュレーションの検証，11 ページ
- 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，12 ページ
- スイッチ プロファイルの前提条件，13 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，13 ページ
- スイッチ プロファイルの設定，15 ページ
- スイッチ プロファイルへのスイッチの追加，16 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，18 ページ
- スイッチ プロファイルのインポート，20 ページ
- vPC トポロジでの設定のインポート，23 ページ
- スイッチ プロファイルのコマンドの確認，23 ページ
- ピア スイッチの分離，24 ページ
- スイッチ プロファイルの削除，24 ページ
- スイッチ プロファイルからのスイッチの削除，25 ページ
- スイッチ プロファイル バッファの表示，27 ページ
- スイッチのリブート後のコンフィギュレーションの同期化，28 ページ
- スイッチ プロファイル設定の show コマンド，28 ページ
- スイッチ プロファイルの設定例，29 ページ

スイッチ プロファイルに関する情報

一部のアプリケーションには、ネットワーク内の Cisco Nexus シリーズ スイッチ間で整合性のある設定が必要です。たとえば、バーチャル ポート チャネル（vPC）を使用する場合は、同じ設定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。
- ポート プロファイル コンフィギュレーションの設定および同期化をサポートします。
- 既存の vPC コンフィギュレーションをスイッチ プロファイルに移行するためのインポートコマンドを提供します。

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化モード
- スイッチ プロファイル モード
- スイッチ プロファイル インポート モード

コンフィギュレーション同期化モード

コンフィギュレーション同期化モード（config-sync）では、マスターとして使用するローカル スイッチ上で **config sync** コマンドを使用して、スイッチ プロファイルを作成できます。プロファイルを作成後、同期するピア スイッチで **config sync** コマンドを入力できます。

スイッチ プロファイル モード

スイッチ プロファイル モードを使用すると、後でピア スイッチと同期化するスイッチ プロファイル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 モードで入力したコマンドは、**commit** コマンドを入力するまでバッファに格納されます。

スイッチ プロファイル インポート モード

以前のリリースからアップグレードする場合、**import** コマンドを入力して、サポートされている実行コンフィギュレーション コマンドをスイッチ プロファイルにコピーすることができます。**import** コマンドを入力すると、スイッチ プロファイル モード（config-sync-sp）は、スイッチ プロファイル インポート モード（config-sync-sp-import）に変わります。スイッチ プロファイル インポートモードでは、実行コンフィギュレーションから既存のスイッチコンフィギュレーションをインポートし、スイッチ プロファイルに含めるコマンドを指定できます。

異なるトポロジで、スイッチ プロファイルに含まれる異なるコマンドが必要になるため、**import** コマンド モードでは、特定のトポロジに合うようにインポートされた一連のコマンドを変更できます。たとえば、デュアルホーム接続ファブリック エクステンダ（FEX）トポロジでは、大部分のコンフィギュレーションを同期化させる必要があります。他の vPC トポロジでは、同期化を必要とするコンフィギュレーションは、かなり小さいコマンド セットです。

インポート プロセスを完了し、スイッチ プロファイルにコンフィギュレーションを移動するには、**commit** コマンドを入力する必要があります。インポートプロセス中のコンフィギュレーション変更はサポートされていません。そのため、**commit** コマンドを入力する前に新しいコマンドを追加した場合、スイッチプロファイルは保存されていない状態であり、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。追加したコマンドを削除するか、インポートを中断することができます。プロセスを中断すると、保存されていないコンフィギュレーションは失われます。インポートを完了したら、新しいコマンドをスイッチ プロファイルに追加できます。

コンフィギュレーションの検証

次の 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、2 種類のスイッチ 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

スイッチ プロファイルに含まれるコンフィギュレーションが上書きされる可能性を減らすためには、相互排除（mutex）でスイッチ プロファイル コマンドをローカル スイッチに存在するコマンドとピア スイッチのコマンドに照合してチェックします。スイッチプロファイルに含まれるコマンドは、そのスイッチプロファイルの外部またはピア スイッチでは設定できません。この要件により、既存のコマンドが意図せずに上書きされる可能性が減少します。

ピア スイッチに到達可能である場合、mutex チェックは、共通プロセスの一環として両方のスイッチで行われます。それ以外の場合は、mutex チェックはローカルで実行されます。設定端末から行われるコンフィギュレーション変更は、ローカル スイッチのみに反映されます。

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。

相互排除ポリシーには、次の例外が適用されます。

- インターフェイス設定：ポート チャネル インターフェイスは、スイッチ プロファイル モードまたはグローバル コンフィギュレーション モードで設定が済んでいる必要があります。

（注） 一部のポート チャネル サブコマンドは、スイッチ プロファイル モードで設定できません。ただしこれらのコマンドは、ポート チャネルがスイッチ プロファイル モードで作成、設定されている場合でも、グローバル コンフィギュレーション モードからであれば設定することができます。

たとえば、次のコマンドはグローバル コンフィギュレーション モードでのみ設定可能です。

switchport private-vlan association trunk *primary-vlan secondary-vlan*

- 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、マージ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。

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

以前のリリースにダウングレードすると、以前のリリースではサポートされていない既存のスイッチ プロファイルを削除するように要求されます。

以前のリリースからアップグレードする場合、スイッチ プロファイルに一部の実行コンフィギュレーション コマンドを移動することを選択できます。**import** コマンドを使用すると、関連するスイッチプロファイルコマンドをインポートできます。バッファされた（コミットされていない）コンフィギュレーション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 プロファイルに含まれるスイッチの 1 つで In Service Software Upgrade（ISSU）を実行しても、コンフィギュレーションを同期化することはできません。これは、ピアに到達できないためです。

スイッチ プロファイルの前提条件

スイッチ プロファイルには次の前提条件があります。

- **cfs ipv4 distribute** コマンドを入力して、両方のスイッチで mgmt0 上の Cisco Fabric Series over IP（CFSoIP）配信を有効にする必要があります。
- **config sync** および **switch-profile** コマンドを入力して、両方のピア スイッチで同じ名前のスイッチ プロファイルを設定する必要があります。
- **sync-peers destination** コマンドを入力して、各スイッチをピア スイッチとして設定します。

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 プロファイルには次の注意事項と制約事項があります。

- mgmt0 インターフェイスを使用してのみ設定同期化をイネーブルにできます。
- 設定の同期は、mgmt 0 インターフェイスを使用して実行され、管理 SVI を使用して実行できません。
- 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（config-sync-sp）モードで設定できます。
- サポートされているスイッチプロファイル コマンドは、仮想ポート チャネル（vPC）コマンドに関連します。Fiber Channel over Ethernet（FCoE）のコマンドはサポートされません。
- 1 つのスイッチ プロファイル セッション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、コンフィギュレーション端末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。スイッチ プロファイル セッションが進行しているときは、コンフィギュレーション端末モードからサポートされていないコマンドの変更を行わないでください。
- **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。
- シスコでは、インターフェイス コンフィギュレーションが設定同期機能を使用して同期される、すべての Generic Expansion Module（GEM）モジュールおよび Cisco Nexus ファブリック エクステンダ モジュールで事前プロビジョニングをイネーブルにすることを推奨します。ファブリック エクステンダが 1 台のスイッチでオンラインでない可能性があり、その設定が変更され、他のスイッチで同期される、Cisco Nexus ファブリック エクステンダ アクティブ/アクティブ トポロジでは、次の注意事項に従ってください。このシナリオでは、事前プロビ

ジョニングをイネーブルにしない場合、コミットに失敗し、設定が両方のスイッチでロールバックされます。

- いったんスイッチ プロファイル モードで設定したポート チャネルを、グローバル コンフィギュレーション（config terminal）モードで設定することはできません。

（注） 一部のポート チャネル サブコマンドは、スイッチ プロファイル モードで設定できません。ただしこれらのコマンドは、ポート チャネルがスイッチ プロファイル モードで作成、設定されている場合でも、グローバル コンフィギュレーション モードからであれば設定することができます。

たとえば、次のコマンドはグローバル コンフィギュレーション モードでのみ設定可能です。

switchport private-vlan association trunk *primary-vlan secondary-vlan*

- shutdown および no shutdown は、グローバル コンフィギュレーション モードとスイッチ プロファイル モードのどちらでも設定できます。
- ポート チャネルをグローバル コンフィギュレーション モードで作成した場合は、メンバ インターフェイスを含むチャネル グループも、グローバル コンフィギュレーション モードを使用して作成する必要があります。
- スイッチ プロファイル モードで設定されたポート チャネルには、スイッチ プロファイルの内部と外部どちらからもメンバにすることができます。
- メンバー インターフェイスをスイッチ プロファイルにインポートする場合は、メンバー インターフェイスを含むポート チャネルがスイッチ プロファイル内にも存在する必要があります。

リブート、接続損失、または障害後の同期化に関する注意事項

- vPC ピア リンクの障害後の設定の同期化：ピア リンクに障害が発生したときに両方のスイッチが動作している場合、セカンダリ スイッチが vPC ポートをシャットダウンします。ファブリック エクステンダ A/A トポロジでは、A/A ファブリック エクステンダがセカンダリ スイッチから切断されます。プライマリ スイッチでスイッチ プロファイルを使用して設定が変更された場合、A/A ファブリック エクステンダが事前にプロビジョニングされていない限り、設定はセカンダリ スイッチで受け入れられません。設定の同期機能を使用する場合、すべての A/A ファブリック エクステンダを事前プロビジョニングすることを推奨します。
- mgmt0 インターフェイスの接続が失われた後の設定の同期化：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、両方のスイッチの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、両方のスイッチが自動的に同期されます。

  設定変更を 1 台のスイッチだけで実行する場合、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ると実行されます。

- ISSU が 1 台のスイッチで実行され、設定変更がピア スイッチで行われる場合の設定の同期化：vPC トポロジでは、ピア スイッチの設定変更は、ISSU が他のスイッチで実行される場合は許可されません。vPC のないトポロジでは、設定変更は許可され、アップグレードが完了すると、ISSU を実行しているスイッチは新しい設定を同期します。

スイッチ プロファイルの設定

スイッチ プロファイルは作成および設定できます。コンフィギュレーション同期モード（config-sync）で、**switch-profile** *name* コマンドを入力します。

はじめる前に

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

	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	**cfs ipv4 distribute**
	
	例：
	`switch(config)# cfs ipv4 distribute`
	`switch(config)#`
		ピア スイッチ間の CFS 配信をイネーブルにします。

ステップ 3	**config sync**
	
	例：
	`switch# 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	**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同期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	**sync-peers destination** *IP-address*
	
	例：
	`switch(config-sync-sp)# sync-peers destination 10.1.1.1`
	`switch(config-sync-sp)#`
		ピア スイッチを設定します。

	コマンドまたはアクション	目的

ステップ 6	**show switch-profile** *name* **status**
	
	例：
	`switch(config-sync-sp)# show switch-profile abc status`
	`switch(config-sync-sp)#`
		（任意）
		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 7	**exit**
	
	例：
	`switch(config-sync-sp)# exit`
	`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	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、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ステータスを表示する例を示します。

```
switch# configuration terminal
switch(config)# cfs ipv4 distribute
switch(config-sync)# switch-profile abc
switch(config-sync-sp)# sync-peers destination 10.1.1.1
switch(config-sync-sp)# show switch-profile abc status
Start-time:  15801 usecs after Mon Aug 23 06:21:08 2010
End-time:   6480 usecs after Mon Aug 23 06:21:13 2010

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: 10.1.1.1
Sync-status: In Sync.
Status: Commit Success
Error(s):
switch(config-sync-sp)# exit
switch#
```

スイッチ プロファイルへのスイッチの追加

スイッチ プロファイル コンフィギュレーション モードで **sync-peers destination** *destination IP* コマンドを入力し、スイッチ プロファイルにスイッチを追加します。

スイッチを追加する場合は、次の注意事項に従ってください。

- スイッチは IP アドレスで識別されます。
- 宛先 IP は同期するスイッチの IP アドレスです。
- コミットされたスイッチ プロファイルは、ピア スイッチでも設定の同期が設定されている場合に、新しく追加されたピアと（オンラインの場合）同期されます。

  メンバー インターフェイスをスイッチ プロファイルにインポートする場合は、メンバー インターフェイスを含むポート チャネルがスイッチ プロファイル内にも存在する必要があります。

はじめる前に

ローカル スイッチでスイッチ プロファイルを作成した後、同期に含まれる 2 番めのスイッチを追加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	**config sync**
	
	例：
	`switch# 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 2	**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同期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	**sync-peers destination** *destination IP*
	
	例：
	`switch(config-sync-sp)# sync-peers destination 10.1.1.1`
	`switch(config-sync-sp)#`
		スイッチプロファイルにスイッチを追加します。

ステップ 4	**exit**
	
	例：
	`switch(config-sync-sp)# exit`
	`switch#`
		スイッチ プロファイル コンフィギュレーション モードを終了します。

ステップ 5	**show switch-profile peer** 例： `switch# show switch-profile peer`	（任意） スイッチプロファイルのピアの設定を表示します。

	コマンドまたはアクション	目的
ステップ 6	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

スイッチ プロファイルのコマンドの追加または変更

スイッチプロファイルのコマンドを変更するには、変更されたコマンドをスイッチプロファイルに追加し、**commit** コマンドを入力してコマンドを適用し、ピア スイッチが到達可能な場合にスイッチ プロファイルを同期します。

スイッチプロファイルコマンドを追加または変更するときは、次の注意事項に従ってください。

- 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。

はじめる前に

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。コマンドは、**commit** コマンドを入力するまでスイッチ プロファイル バッファに追加されます。**commit** コマンドは次を行います。

- 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。
- ローカル スイッチおよびピア スイッチのコンフィギュレーションを適用します。
- 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。

手順

	コマンドまたはアクション	目的

ステップ 1	**config sync**
	
	例：
	`switch# 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 2	**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同期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	*Command argument*
	
	例：
	`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`
		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	**show switch-profile** *name* **buffer**
	
	例：
	`switch(config-sync-sp)# show switch-profile abc buffer`
	`switch(config-sync-sp)#`
		（任意）
		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	**verify** 例： `switch(config-sync-sp)# verify`	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。
ステップ 6	**commit** 例： `switch(config-sync-sp)# commit`	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。

ステップ 7	**show switch-profile** *name* **status**
	
	例：
	`switch(config-sync-sp)# show switch-profile abc status`
	`switch(config-sync-sp)#`
		（任意）
		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。

	コマンドまたはアクション	目的

ステップ 8	**exit**
	
	例：
	`switch(config-sync-sp)# exit`
	`switch#`
		スイッチ プロファイル コンフィギュレーション モードを終了します。

ステップ 9	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、スイッチ プロファイルを作成し、ピア スイッチを設定し、スイッチ プロファイルにコマンドを追加する例を示します。

```
switch# configuration terminal
switch(config)# cfs ipv4 distribute
switch(config-sync)# switch-profile abc
switch(config-sync-sp)# sync-peers destination 10.1.1.1
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)# verify
switch(config-sync-sp)# commit
switch(config-sync-sp)# exit
switch#
```

次に、定義されたスイッチ プロファイルがある既存のコンフィギュレーションの例を示します。2 番めの例は、スイッチ プロファイルに変更されたコマンドを追加することによって、スイッチ プロファイル コマンドを変更する方法を示します。

```
switch# show running-config
switch-profile abc
  interface Ethernet1/1
    switchport mode trunk
    switchport trunk allowed vlan 1-10

switch# config sync
switch(config-sync)# switch-profile abc
switch(config-sync-sp)# interface Ethernet1/1
switch(config-sync-sp-if)# switchport trunk allowed vlan 5-10
switch(config-sync-sp-if)# commit

switch# show running-config
switch-profile abc
  interface Ethernet1/1
    switchport mode trunk
    switchport trunk allowed vlan 5-10
```

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。コンフィギュレーション ターミナル モードを使用して、次のことを実行できます。

- 選択したコマンドをスイッチ プロファイルに追加する。
- インターフェイスに指定された、サポートされているコマンドを追加する。
- サポートされているシステムレベル コマンドを追加する。
- サポートされるシステムレベル コマンドを追加する（物理インターフェイス コマンドを除く）。

スイッチプロファイルにコマンドをインポートする場合、スイッチプロファイルバッファが空である必要があります。

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。**abort** コマンドを入力してインポートを停止します。スイッチ プロファイルのインポートの詳細については、「スイッチ プロファイル インポート モード」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	**config sync**
	
	例：
	`switch# 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 2	**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 プロファイル同期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	**import** {*interface port/slot* | *running-config* [**exclude interface ethernet**]}
	
	例：
	`switch(config-sync-sp)# import ethernet 1/2`
	`switch(config-sync-sp-import)#`
		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。
		• <CR>：選択したコマンドを追加します。
		• **interface**：指定したインターフェイスのサポートされるコマンドを追加します。
		• **running-config**：サポートされるシステムレベル コマンドを追加します。
		• **running-config exclude interface ethernet**：物理インターフェイス コマンドを除く、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
ステップ 4	**commit** 例： `switch(config-sync-sp-import)# commit`	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 5	**abort** 例： `switch(config-sync-sp-import)# abort`	（任意） インポート プロセスを中止します。

ステップ 6	**exit**
	
	例：
	`switch(config-sync-sp)# exit`
	`switch#`
		スイッチプロファイルインポートモードを終了します。

ステップ 7	**show switch-profile** 例： `switch# show switch-profile`	（任意） 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 8	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、sp というスイッチ プロファイルに、イーサネット インターフェイス コマンドを除く、サポートされるシステムレベル コマンドをインポートする例を示します。

```
switch(config-vlan)# conf sync
switch(config-sync)# switch-profile sp
Switch-Profile started, Profile ID is 1
switch(config-sync-sp)# show switch-profile buffer

switch-profile  : sp
----------------------------------------------------------
Seq-no  Command
----------------------------------------------------------

switch(config-sync-sp)# import running-config exclude interface ethernet
switch(config-sync-sp-import)#
switch(config-sync-sp-import)# show switch-profile buffer

switch-profile  : sp
----------------------------------------------------------
Seq-no  Command
----------------------------------------------------------
3       vlan 100-299
4       vlan 300
4.1       state suspend
5       vlan 301-345
6       interface port-channel100
6.1       spanning-tree port type network
7       interface port-channel105
```

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

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。

スイッチ プロファイルのコマンドの確認

スイッチ プロファイル モードで **verify** コマンドを入力し、スイッチ プロファイルに含まれるコマンドを確認できます。

手順

	コマンドまたはアクション	目的

ステップ 1	**config sync**
	
	例：
	`switch# 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 2	**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同期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	**verify** 例： `switch(config-sync-sp)# verify`	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 4	**exit**
	
	例：
	`switch(config-sync-sp)# exit`
	`switch#`
		スイッチプロファイルコンフィギュレーション モードを終了します。

ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

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する場合、または設定をデバッグするときに使用できます。

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スイッチを削除し、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。

一時的にピア スイッチを分離するには、次の手順を実行します。

1. スイッチ プロファイルからピア スイッチを削除します。
2. スイッチ プロファイルを変更して、変更をコミットします。
3. debug コマンドを入力します。
4. 手順 2 でスイッチ プロファイルに対して行った変更を元に戻し、コミットします。
5. スイッチ プロファイルにピア スイッチを追加します。

スイッチ プロファイルの削除

all-config または **local-config** オプションを選択してスイッチ プロファイルを削除できます。

- **all-config**：両方のピア スイッチでスイッチ プロファイルを削除します（両方が到達可能な場合）。このオプションを選択し、ピアの 1 つが到達不能である場合、ローカル スイッチ プロファイルだけが削除されます。**all-config** オプションは両方のピア スイッチでスイッチ プロファイルを完全に削除します。
- **local-config**：ローカル スイッチのみのスイッチ プロファイルを削除します。

手順

	コマンドまたはアクション	目的

ステップ 1	**config sync**
	
	例：
	`switch# 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 2	例：
	`switch(config-sync)# no switch-profile abc local-config`
	`switch(config-sync-sp)#`
		次の手順に従って、スイッチプロファイルを削除します。
		• **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。

ステップ 3	**exit**
	
	例：
	`switch(config-sync-sp)# exit`
	`switch#`
		コンフィギュレーション同期モードを終了します。

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

スイッチ プロファイルからのスイッチの削除

スイッチ プロファイルからスイッチを削除できます。

手順

	コマンドまたはアクション	目的

ステップ 1	**config sync**
	
	例：
	`switch# 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 2	**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同期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 sync-peers destination** *destination IP*
	
	例：
	`switch(config-sync-sp)# no sync-peers destination 10.1.1.1`
	`switch(config-sync-sp)#`
		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。

ステップ 4	**exit**
	
	例：
	`switch(config-sync-sp)# exit`
	`switch#`
		スイッチ プロファイル コンフィギュレーション モードを終了します。

ステップ 5	**show switch-profile** 例： `switch# show switch-profile`	（任意） 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 6	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

スイッチ プロファイル バッファの表示

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure 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 2	switch(config-sync) # **switch-profile** *profile-name*	指定されたスイッチ プロファイルに対するスイッチプロファイル同期コンフィギュレーション モードを開始します。
ステップ 3	switch(config-sync-sp) # **show switch-profile***profile-name* **buffer**	指定されたインターフェイスに対するインターフェイス スイッチ プロファイル同期コンフィギュレーション モードを開始します。

次に、sp という名前のサービス プロファイルのスイッチ プロファイル バッファの表示例を示します。

```
switch# configure sync
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config-sync)# switch-profile sp
Switch-Profile started, Profile ID is 1
switch(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

switch(config-sync-sp)# buffer-move 3 1
switch(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
switch(config-sync-sp)#
```

スイッチのリブート後のコンフィギュレーションの同期化

スイッチ プロファイルを使用してピア スイッチで新しい設定をコミット中に Cisco Nexus シリーズスイッチがリブートする場合、リロード後にピアスイッチを同期するには、次の手順を実行します。

手順

ステップ 1 リブート中にピア スイッチ上で変更された設定を再適用します。

ステップ 2 **commit** コマンドを入力します。

ステップ 3 設定が正しく適用されており、両方のピアが同期されていることを確認します。

スイッチ プロファイル設定の show コマンド

次の **show** コマンドは、スイッチ プロファイルに関する情報を表示します。

コマンド	目的
show switch-profile *name*	スイッチ プロファイル中のコマンドを表示します。
show switch-profile *name* **buffer**	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。
show switch-profile *name* **peer** *IP-address*	ピア スイッチの同期ステータスが表示されます。
show switch-profile *name* **session-history**	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。
show switch-profile *name* **status**	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。
show running-config expand-port-profile	ポート プロファイルについての詳細が表示されます。
show running-config exclude-provision	オフラインで事前プロビジョニングされた非表示のインターフェイスの設定を表示します。
show running-config switch-profile	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。

コマンド	目的
show startup-config switch-profile	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。

これらのコマンドの出力フィールドの詳細については、ご使用のプラットフォームの、システム管理コマンドのリファレンスを参照してください。

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例

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。

手順

	コマンドまたはアクション	目的

ステップ 1	ローカルおよびピア スイッチで CFSoIP 配信をイネーブルにします。
	
	例：
	`switch# configuration terminal`
	`switch(config)# cfs ipv4 distribute`	

ステップ 2	ローカルおよびピア スイッチでスイッチ プロファイルを作成します。
	
	例：
	`switch(config-sync)# switch-profile abc`
	`switch(config-sync-sp)# sync-peers destination 10.1.1.1`	

ステップ 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。
	
	例：
	`switch(config-sync-sp)# show switch-profile abc status`
	
	`Start-time:  15801 usecs after Mon Aug 23 06:21:08 2010`
	`End-time:  6480 usecs after Mon Aug 23 06:21:13 2010`
	
	`Profile-Revision: 1`
	`Session-type: Initial-Exchange`
	`Peer-triggered: Yes`
	`Profile-status: Sync Success`
	
	`Local information:`
	`----------`
	`Status: Commit Success`
	`Error(s):`	

	コマンドまたはアクション	目的

	`Peer information:`
	`----------`
	`IP-address: 10.1.1.1`
	`Sync-status: In Sync.`
	`Status: Commit Success`
	`Error(s):`	

ステップ 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。 例： `switch(config-sync-sp)#` **`class-map type qos c1`** `switch(config-sync-sp-cmap-qos)#` match cos 2 `switch(config-sync-sp-cmap-qos)#` class-map type qos c2 `switch(config-sync-sp-cmap-qos)#` match cos 5 `switch(config-sync-sp-cmap-qos)#` policy-map type qos p1 `switch(config-sync-sp-pmap-qos)#` class c1 `switch(config-sync-sp-pmap-c-qos)#` set qos-group 2 `switch(config-sync-sp-pmap-c-qos)#` class c2 `switch(config-sync-sp-pmap-c-qos)#` set qos-group 3 `switch(config-sync-sp-pmap-c-qos)#` system qos `switch(config-sync-sp-sys-qos)#` service-policy type qos input p1 `switch(config-sync-sp-sys-qos)#` vlan 1-50 `switch(config-sync-sp-vlan)#` interface port-channel 100 `switch(config-sync-sp-if)#` vpc peer-link `switch(config-sync-sp-if)#` switchport mode trunk `switch(config-sync-sp-if)#` interface port-channel 10 `switch(config-sync-sp-if)#` vpc 1 `switch(config-sync-sp-if)#` switchport mode trunk `switch(config-sync-sp-if)#` switchport trunk allowed vlan 1, 10-50	

ステップ 5	バッファリングされたコマンドを表示します。
	
	例：
	`switch(config-sync-sp-if)#` **`show switch-profile switch-profile buffer`**
	`----------`
	`Seq-no  Command`
	`----------`
	`1  class-map type qos match-all c1`
	`1.1  match cos 2`
	`2  class-map type qos match-all c2`
	`2.1  match cos 5`
	`3  policy-map type qos p1`
	`3.1  class c1`
	`3.1.1  set qos-group 2`
	`3.2  class c2`
	`3.2.1  set qos-group 3`
	`4  system qos`
	`4.1  service-policy type qos input p1`
	`5  vlan 2-50`
	`6  interface port-channel100`
	`6.1  vpc peer-link`
	`6.2  switchport mode trunk`
	`7  interface port-channel10`
	`7.1  vpc 1`	

	コマンドまたはアクション	目的
	7.2 switchport mode trunk 7.3 switchport trunk allowed vlan 1, 10-50	
ステップ 6	スイッチ プロファイルのコマンドを検証します。 例： switch(config-sync-sp-if)# **verify** Verification Successful	
ステップ 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。 例： switch(config-sync-sp)# **commit** Commit Successful switch(config-sync)#	

同期ステータスの確認例

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(config-sync)# show switch-profile switch-profile status
Start-time: 804935 usecs after Mon Aug 23 06:41:10 2010
End-time: 956631 usecs after Mon Aug 23 06:41:20 2010

Profile-Revision: 2
Session-type: Commit
Peer-triggered: No
Profile-status: Sync Success

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

Peer information:
----------------
IP-address: 10.1.1.1
Sync-status: In Sync.
Status: Commit Success
Error(s):

switch(config-sync)#
```

実行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例を示します。

```
switch# configure sync
switch(config-sync)# show running-config switch-profile
switch-profile sp
  sync-peers destination 10.1.1.1
```

```
  class-map type qos match-all c1
    match cos 2
  class-map type qos match-all c2
    match cos 5
  policy-map type qos p1
    class c1
      set qos-group 2
    class c2
      set qos-group 3
  system qos
    service-policy type qos input p1
  vlan 2-50

  interface port-channel10
    switchport mode trunk
    vpc 1
    switchport trunk allowed vlan 1,10-50

  interface port-channel100
    switchport mode trunk
    vpc peer-link
switch(config-sync)#
```

ローカル スイッチとピア 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 スイッチの同期ステータスを表示する例を示します。

```
switch1# show switch-profile sp status

Start-time: 491815 usecs after Thu Aug 12 11:54:51 2010
End-time: 449475 usecs after Thu Aug 12 11:54:58 2010

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):

switch1#


switch2# show switch-profile sp status

Start-time: 503194 usecs after Thu Aug 12 11:54:51 2010
End-time: 532989 usecs after Thu Aug 12 11:54:58 2010

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):

switch2#
```

ローカル スイッチとピア 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設定する例を示します。

```
switch1# configure sync
Enter configuration commands, one per line.  End with CNTL/Z.
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)# 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 Aug 11 17:51:28 2010
End-time: 676451 usecs after Wed Aug 11 17:51:43 2010

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 Wed Aug 11 16:51:28 2010
End-time: 734702 usecs after Wed Aug 11 16:51:43 2010

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):

switch2#
```

同期の成功と失敗の例

次に、ピア スイッチにおけるスイッチ プロファイルの同期の成功例を示します。

```
switch# show switch-profile abc peer

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

次に、到達不能ステータスのピアを使用した、ピアスイッチでのスイッチプロファイルの同期の失敗例を示します。

```
switch# 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)              :
switch#
```

スイッチ プロファイル バッファの設定、バッファ移動、およびバッファの削除

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。

```
switch# configure sync
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config-sync)# switch-profile sp
Switch-Profile started, Profile ID is 1
switch(config-sync-sp)# vlan 101
switch(config-sync-sp-vlan)# ip igmp snooping querier 10.101.1.1
switch(config-sync-sp-vlan)# exit
switch(config-sync-sp)# mac address-table static 0000.0000.0001 vlan 101 drop
switch(config-sync-sp)# interface ethernet1/2
switch(config-sync-sp-if)# switchport mode trunk
switch(config-sync-sp-if)# switchport trunk allowed vlan 101
switch(config-sync-sp-if)# exit
switch(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
```

```
switch(config-sync-sp)# buffer-move 3 1
switch(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

switch(config-sync-sp)# buffer-delete 1
switch(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

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

Cisco Nexus 5000 シリーズ スイッチの交換

Cisco Nexus 5000 シリーズ スイッチを交換した場合は、既存の Cisco Nexus 5000 シリーズ スイッチと同期をとるために、交換用スイッチで次の設定手順を実行します。この手順は、ハイブリッドなファブリック エクステンダ A/A トポロジおよびファブリック エクステンダのストレート型トポロジで実行できます。

1. ピア リンク、vPC、A/A、またはストレート型トポロジのファブリック 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。スイッチが設定なしで起動します。
3. すべてのファブリック エクステンダ A/A および ST モジュールで事前プロビジョニングを有効にします。
4. 交換用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 5 ～ 9 に従って設定を適用します。

   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例」の手順 1 および 2 を参照してから、以下の手順 10 を開始してください）。

   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10を開始します。
5. 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。
6. 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。
7. 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。

8. **show running-config** コマンドおよび **show provision failed-config** *slot* コマンドを入力し、設定が正しいことを確認します。
9. 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。
10. 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 ST トポロジ ポートをシャットダウンします。
11. ファブリック エクステンダ ST トポロジ ポートを接続します。
12. ファブリック エクステンダ ST トポロジ スイッチがオンラインになるまで待ちます。
13. 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。
14. ピア リンク ポートをピア スイッチに接続します。
15. ファブリック エクステンダ A/A トポロジ ポートを接続します。
16. スイッチ vPC ポートを接続します。
17. すべてのファブリック エクステンダ ST vPC ポートで **no shutdown** コマンドを入力します。
18. 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。
19. 設定同期機能を使用している場合、手順4でイネーブル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。
20. 設定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。

第 4 章

モジュール事前プロビジョニングの設定

この章の内容は、次のとおりです。

- モジュールの事前プロビジョニングに関する情報，37 ページ
- 注意事項と制約事項，38 ページ
- モジュールの事前プロビジョニングのイネーブル化，38 ページ
- モジュールの事前プロビジョニングの削除，39 ページ
- 事前プロビジョニングした設定の確認，40 ページ
- 事前プロビジョニングの設定例，40 ページ

モジュールの事前プロビジョニングに関する情報

事前プロビジョニング機能では、モジュールを挿入または取り付ける前にインターフェイスを事前に設定できます。また、モジュールがオフラインになった場合に、事前プロビジョニングを使用して、オフライン モジュールのインターフェイス設定を変更できます。事前プロビジョニングされたモジュールがオンラインになると、事前プロビジョニング設定が適用されます。いずれの設定も適用されない場合は、syslog が生成されます。syslog には、拒否された設定が示されます。

一部の仮想ポート チャネル（vPC）トポロジでは、同期機能の設定に事前プロビジョニングが必要です。事前プロビジョニングによって、1 つのピアでオンラインになっているが、他のピアでオフラインになっているインターフェイスの設定を同期させることができます。

（注） サポートされるハードウェアのリストについては、『Cisco Nexus 5600 Series Release Notes』の表 2「Hardware Supported by Cisco NX-OS Release 7.x Software」を参照してください。

注意事項と制約事項

事前プロビジョニング設定時の注意事項と制限事項は次のとおりです。

- モジュールがオンラインになると、適用されないコマンドが syslog に表示されます。
- スロットがモジュール A 用に事前プロビジョニングされていて、スロットにモジュール B を挿入する場合は、モジュール B はオンラインになりません。
- 事前プロビジョニングされたインターフェイスに対する MIB サポートはありません。
- Cisco DCNM はサポートされません。

モジュールの事前プロビジョニングのイネーブル化

オフラインのモジュールの事前プロビジョニングをイネーブルにできます。**provision model** *model* コマンドをモジュール事前プロビジョニング モードで入力します。

（注） 事前プロビジョニングをイネーブルにした後、オンラインであるかのようにインターフェイスを設定できます。

手順

	コマンドまたはアクション	目的

ステップ 1	**configuration terminal**
	
	例：
	`switch# config t`
	`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	**slot** *slot*
	
	例：
	`switch(config)# slot 101`
	`switch(config-slot)#`
		事前プロビジョニングするスロットを選択し、スロ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	**provision model** *model*
	
	例：
	`switch(config-slot)# provision model N2K-C2248T`
	`switch(config-slot)#`
		事前プロビジョニングするモジュールを選択します。

ステップ 4	**exit**
	
	例：
	`switch(config-slot)# exit`
	`switch#`
		スロット コンフィギュレーション モードを終了します。

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

次に、スロット 101 および N2K-C2232P モジュールを選択して事前プロビジョニングする例を示します。

```
switch# configure terminal
switch(config)# slot 101
switch(config-slot)# provision model N2K-C2232P
switch(config-slot)# exit
```

モジュールの事前プロビジョニングの削除

事前プロビジョニングされたモジュールを削除できます。

手順

	コマンドまたはアクション	目的

ステップ 1	**configuration terminal**
	
	例：
	`switch# config t`
	`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	**slot** *slot*
	
	例：
	`switch(config)# slot 101`
	`switch(config-slot)#`
		事前プロビジョニングするスロットを選択し、スロ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	**no provision model** *model*
	
	例：
	`switch(config-slot)# no provision model N2K-C2248T`
	`switch(config-slot)#`
		モジュールから事前プロビジョニングを削除します。

ステップ 4	**exit**
	
	例：
	`switch(config-slot)# exit`
	`switch#`
		スロット コンフィギュレーション モードを終了します。

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

次に、シャーシ スロットから事前プロビジョニングしたモジュールを削除する例を示します。

```
switch(config)# slot 2
switch(config-slot)# no provision model N5K-M1404
switch(config-slot)#
```

事前プロビジョニングした設定の確認

事前プロビジョニングした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 module	モジュール情報を表示します。
show switch-profile	スイッチ プロファイル情報を表示します。
show running-config exclude-provision	オフラインである事前プロビジョニングされたインターフェイスまたはモジュールがない実行コンフィギュレーションを表示します。
show provision failed-config	インターフェイスまたはモジュールがオンラインになったときに設定に適用されなかった、事前プロビジョニングされたコマンドを表示します。 このコマンドは、失敗したコマンドの履歴も表示します。
show running-config	事前プロビジョニングされた設定を含む、実行コンフィギュレーションを表示します。
show startup-config	事前プロビジョニングされた設定を含む、スタートアップ コンフィギュレーションを表示します。

事前プロビジョニングの設定例

次に、Cisco Nexus 2232P ファブリック エクステンダのスロット 110 で事前プロビジョニングをイネーブルにし、イーサネット 110/1/1 インターフェイスでインターフェイス コンフィギュレーション コマンドを事前プロビジョニングする例を示します。

```
switch# configure terminal
switch(config)# slot 110
```

```
switch(config-slot)# provision model N2K-C2232P
switch(config-slot)# exit

switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# interface Ethernet110/1/1
switch(config-if)# description module is preprovisioned
switch(config-if)# show running-config interface Ethernet110/1/1
Time: Wed Aug 25 21:29:44 2010

version 5.0(2)N1(1)

interface Ethernet110/1/1
  description module is preprovisioned
```

次に、モジュールがオンラインになったときに適用されなかった事前プロビジョニングされたコマンドのリストを表示する例を示します。

```
switch(config-if-range)# show provision failed-config 101
The following config was not applied for slot 33
================================================

interface Ethernet101/1/1
  service-policy input test


interface Ethernet101/1/2
  service-policy input test


interface Ethernet101/1/3
  service-policy input test
```

次に、スロットから事前プロビジョニングされたすべてのモジュールを削除する例を示します。

```
switch(config)# slot 2
switch(config-slot)# no provision model
switch(config-slot)#
```

第 5 章

CFS の使用

この章の内容は、次のとおりです。

- CFS について，43 ページ
- CFS の注意事項および制約事項，44 ページ
- CFS 配信，45 ページ
- アプリケーションの CFS サポート，47 ページ
- CFS リージョン，51 ページ
- IP を介した CFS の設定，54 ページ
- CFS のデフォルト設定，57 ページ

CFS について

Cisco Nexus シリーズ スイッチの一部の機能は、正常に動作するため、ネットワーク内の他のスイッチとの設定の同期化を必要とします。ネットワーク内のスイッチごとに手動設定によって同期化を行うことは、面倒で、エラーが発生しやすくなります。

CFS はネットワーク内の自動設定同期化に対して共通のインフラストラクチャを提供します。また、トランスポート機能、および機能に対する共通サービスのセットを提供します。CFS にはネットワーク内の CFS 対応スイッチを検出し、すべての CFS 対応スイッチの機能能力を検出する機能が備わっています。

Cisco Nexus シリーズ スイッチは、IPv4 ネットワークを介した CFS メッセージ配信をサポートします。

CFS には次の機能があります。

- CFS レイヤでクライアント/サーバ関係を持たないピアツーピア プロトコル
- IPv4 および IPv6 ネットワークを介した CFS メッセージ配信。
- 3 つの配信モード

- 協調型配信：ネットワーク内でいつでも使用できる配信は 1 つだけです。
- 非協調型配信：協調型配信が実行中の場合を除き、ネットワーク内で複数の同時配信を使用できます。
- 無制限の非協調型配信：既存の協調型配信がある場合にネットワーク内で複数の同時配信が許可されます。無制限の非協調型配信は、他のすべての配信タイプの配信と同時に実行できます。

IP を介した CFS 配信では、次の機能がサポートされます。

- IP ネットワークを介した配信の 1 つの範囲：
  - 物理範囲：IP ネットワーク全体に配信されます。

Cisco Fabric Services over Ethernet

Cisco Fabric Services over Ethernet（CFSoE）は、vPC ピア デバイスの動作を同期化するために使用される信頼性の高い状態転送メカニズムです。CFSoE は、vPC にリンクされている、STP、IGMP などの多くの機能のメッセージとパケットを伝送します。情報は、CFS/CFSoE プロトコルデータユニット（PDU）に入れて伝送されます。

CFSoE は、vPC 機能をイネーブルにすると、デバイスによって自動的にイネーブルになります。何も設定する必要はありません。vPC の CFSoE 分散には、IP を介してまたは CFS リージョンに分散する機能は必要ありません。CFSoE 機能が vPC 上で正常に機能するために必要な設定は一切ありません。

show mac address-table コマンドを使用すれば、CFSoE が vPC ピア リンクのために同期する MAC アドレスを表示できます。

（注） **no cfs eth distribute** コマンドと **no cfs distribute** コマンドは入力しないでください。vPC 機能に対しては CFSoE をイネーブルにする必要があります。vPC がイネーブルの場合にこれらのコマンドのいずれかを入力すると、エラー メッセージが表示されます。

show cfs application コマンドを入力すると、出力に「Physical-eth」と表示されます。これは、CFSoE を使用しているアプリケーションを表します。

CFS の注意事項および制約事項

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

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

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

- 同様のマルチキャスト アドレスを持つ CFSoIP がイネーブルになっているすべてのデバイスは 1 つの CFSoIP ファブリックを形成します。
- 設定するアプリケーションについて CFS がイネーブルになっていることを確認してください。
- ファブリックをロックすると、リスタートとスイッチオーバーにわたってユーザ名が記憶されます。
- ファブリックをロックすると、他のユーザによるコンフィギュレーションの変更の試みは拒否されます。
- ファブリックのロック中、アプリケーションでは実行コンフィギュレーションではなく保留データベースまたは一時ストレージにコンフィギュレーションの変更の作業コピーが保持されます。
- まだコミットされていない設定の変更内容（まだ作業中のコピーとして保存されている）、実行コンフィギュレーションには存在せず、**show** コマンドの出力には表示されません。
- ファブリックのロックが必要な CFS セッションを開始した後に、セッションが終了されなかった場合、管理者はセッションをクリアできます。
- 以前コンフィギュレーションの変更が行われていない場合は、空のコミットを行えます。この場合、**commit** コマンドにより、ロックを取得し、現在のデータベースを配信するセッションが作成されます。
- **commit** コマンドは、ファブリック ロックが取得されたデバイスで使用できます。
- CFSoIP と CFSoE の同時使用はサポートされません。
- CFS リージョンは、CFSoIP アプリケーションにのみ適用できます。

CFS 配信

CFS 配信機能は、下位層の転送とは無関係です。Cisco Nexus シリーズ スイッチは IP を介した CFS 配信をサポートします。CFS を使用する機能は、下位層の転送を認識しません。

CFS の配信モード

CFS では異なる機能要件をサポートするために、3 つの配信モードをサポートします。

- 非協調型配信
- 協調型配信
- 無制限の非協調型配信

常に 1 つのモードだけを適用できます。

非協調型配信

非協調型配信は、ピアからの情報と競合させたくない情報を配信する場合に使用されます。1 つの機能に対して非協調的な並列配信を適用できます。

協調型配信

協調型配信は、いかなる時も 1 つの機能配信だけ適用できます。CFS は、ロックを使用してこの機能を強制します。ネットワーク内のいずれかの機能でロックが取得されていれば、協調型配信は開始できません。協調型配信は、次の 3 段階で構成されています。

- ネットワーク ロックが取得されます。
- 設定が配信され、コミットされます。
- ネットワーク ロックが解除されます。

協調型配信には、次の 2 種類があります。

- CFS によるもの：機能が介在することなく、機能要求に応じて CFS が各段階を実行します。
- 機能によるもの：各段階は機能によって完全に管理されます。

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

無制限の非協調型配信

無制限の非協調型配信では、既存の協調型配信がある場合にネットワーク内で複数の同時配信が許可されます。無制限の非協調型配信は、他のすべての配信タイプの配信と同時に実行できます。

CFS 配信ステータスの確認

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

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

アプリケーションの CFS サポート

CFS のアプリケーション要件

ネットワーク内のすべてのスイッチが CFS に対応している必要があります。CFS に対応していないスイッチは配信を受信できないため、ネットワークの一部が意図された配信を受信できなくなります。CFS には、次の要件があります。

- CFS の暗黙的な使用：CFS 対応アプリケーションの CFS 作業を初めて行う場合、設定変更プロセスが開始され、アプリケーションがネットワークをロックします。
- 保留データベース：保留データベースはコミットされていない情報を保持する一時的なバッファです。データベースが、ネットワーク内の他のスイッチのデータベースと確実に同期するために、コミットされていない変更はすぐには適用されません。変更をコミットすると、保留データベースはコンフィギュレーション データベース（別名、アクティブ データベースまたは有効データベース）を上書きします。
- アプリケーション単位でイネーブル化またはディセーブル化される CFS 配信：CFS 配信ステートのデフォルト（イネーブルまたはディセーブル）は、アプリケーション間で異なります。アプリケーションでCFSの配信がディセーブルにされている場合、そのアプリケーションは設定を配信せず、またネットワーク内のその他のスイッチからの配信も受け入れません。
- 明示的な CFS コミット - 大半のアプリケーションでは、新しいデータベースをネットワークに配信したりネットワーク ロックを解除したりするために、一時的なバッファ内の変更をアプリケーションデータベースにコピーする明示的なコミット操作が必要です。コミット操作を実行しないと、一時的バッファ内の変更は適用されません。

アプリケーションの CFS のイネーブル化

すべての CFS ベースのアプリケーションでは、配信機能をイネーブルまたはディセーブルにできます。

アプリケーションでは、配信はデフォルトでイネーブルにされています。

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

アプリケーション登録スターテスの確認

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

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

```
switch# show cfs application

----------------------------------------------
 Application    Enabled   Scope
----------------------------------------------
 ntp            No        Physical-all
 fscm           Yes       Physical-fc
 rscn           No        Logical
 fctimer        No        Physical-fc
 syslogd        No        Physical-all
 callhome       No        Physical-all
 fcdomain       Yes       Logical
 device-alias   Yes       Physical-fc
Total number of entries = 8
```

show cfs application name コマンドは、特定のアプリケーションの詳細を表示します。表示されるのは、有効/無効の状態、CFS に登録されているタイムアウト、マージ機能（マージがサポートされるよう CFS に登録されている場合）、および配信範囲です。

```
switch# show cfs application name fscm

Enabled         : Yes
 Timeout        : 100s
 Merge Capable  : No
 Scope          : Physical-fc
```

ネットワークのロック

CFS インフラストラクチャを使用する機能（アプリケーション）を初めて設定する場合、この機能は CFS セッションを開始して、ネットワークをロックします。ネットワークがロックされた場合、スイッチ ソフトウェアでは、ロックを保持しているスイッチからのみこの機能への設定変更を行うことができます。別のスイッチから機能への設定変更を行う場合、ロックされているステータスを知らせるメッセージが、スイッチから発行されます。設定変更は、該当アプリケーションによって保留データベースに保持されます。

ネットワーク ロックを要求する CFS セッションを開始し、セッションを終了するのを忘れた場合は、管理者がそのセッションをクリアできます。いつでもネットワークをロックした場合、ユーザ名は再起動およびスイッチオーバーを行っても保持されます。（同じマシン上で）別のユーザが設定タスクを実行しようとしても、拒否されます。

CFS ロック ステータスの確認

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

ます。アプリケーションが論理範囲で取得されている場合、このコマンドはロックが取得された VSAN、ドメイン、IP アドレス、ユーザ名、およびロック所持者のユーザ タイプを表示します。

```
switch# show cfs lock

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

Application: port-security
Scope      : Logical
-------------------------------------------------------------
VSAN   Domain   IP Address       User Name    User Type
-------------------------------------------------------------
 1      238      10.76.100.167    admin        CLI/SNMP v3
 2      211      10.76.100.167    admin        CLI/SNMP v3
 Total number of entries = 2
```

show cfs lock name コマンドは、指定したアプリケーションで使用されているロックの詳細情報を表示します。

```
switch# show cfs lock name ntp

Scope      : Physical
----------------------------------------------------------------------
 Switch WWN               IP Address       User Name    User Type
----------------------------------------------------------------------
 20:00:00:05:30:00:6b:9e  10.76.100.167    admin        CLI/SNMP v3

 Total number of entries = 1
```

変更のコミット

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

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

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

- 1 つまたは複数の外部スイッチが正常なステータスを報告する場合 - アプリケーションは変更をローカルに適用し、ネットワーク ロックを解除します。
- どの外部スイッチも成功ステートを報告しない - アプリケーションはこのステートを失敗として認識し、ネットワーク内のどのスイッチにも変更を適用しません。ネットワーク ロックは解除されません。

commit コマンドを入力すると、指定した機能の変更をコミットできます。

変更の廃棄

設定変更を廃棄すると、アプリケーションは保留中のデータベースを一気に消去し、ネットワーク内のロックを解除します。中断およびコミット機能の両方を使用できるのは、ネットワークロックが取得されたスイッチだけです。

abort コマンドを使用すると、指定した機能の変更を廃棄できます。

設定の保存

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

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

ロック済みセッションのクリア

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

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

はじめる前に

ロックを解放するには、管理者権限が必要です。

手順

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

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

CFS リージョン

CFS リージョンの概要

CFS リージョンは、物理配信範囲の所定の機能またはアプリケーションに対するスイッチのユーザ定義のサブセットです。ネットワークが広い範囲に及ぶ場合、場合によっては、物理的な隣接性に基づき、スイッチ セット間での特定のプロファイルの配信を局所化または制限する必要があります。CFS リージョンを使用すると、ネットワーク内で特定の CFS 機能またはアプリケーションに、配信の複数アイランドができます。CFS リージョンは、機能設定の配信をネットワーク内のスイッチの特定のセットまたはグループに制限するよう設計されています。

（注） CFS リージョンの設定は、物理スイッチだけで行えます。CFS リージョンの設定は、VSAN では行えません。

シナリオ例

Smart Call Home アプリケーションは、困難な状況、あるいは異常が発生した時にネットワーク管理者にアラートを送信します。ネットワークが広い地域に及び、複数のネットワーク管理者がネットワーク内のスイッチの各サブセットを担当している場合は、Smart Call Home アプリケーションは、場所に関係なく、すべてのネットワーク管理者にアラートを送信します。Smart Call Home アプリケーションで、選択したネットワーク管理者にメッセージ アラートを送信するには、アプリケーションの物理範囲を微調整するか、絞り込む必要があります。CFS リージョンの実装によって、このシナリオを実現できます。

CFS リージョンは、0 ～ 200 の数字で識別されます。リージョン 0 はデフォルト リージョンとして予約されており、ネットワーク内のすべてのスイッチを含みます。1 ～ 200 のリージョンを設定できます。デフォルト リージョンでは下位互換性を維持しています。

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

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

CFS リージョンの管理

CFS リージョンの作成

CFS リージョンを作成できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **cfs region***region-id*	リージョンを作成します。

CFS リージョンへのアプリケーションの割り当て

スイッチでリージョンにアプリケーションを割り当てることができます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure** terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **cfs region***region-id*	リージョンを作成します。
ステップ 3	switch(config-cfs-region)# *application*	リージョンにアプリケーションを追加します。 （注） リージョンにスイッチ上の任意の数のアプリケーションを追加できます。同じリージョンにアプリケーションを複数回追加しようとすると、「Application already present in the same region」というエラーメッセージが表示されます。

次に、リージョンにアプリケーションを割り当てる例を示します。

```
switch# configure terminal
switch(config)# cfs region 1
switch(config-cfs-region)# ntp
switch(config-cfs-region)# callhome
```

別の CFS リージョンへのアプリケーションの移動

あるリージョンから別のリージョンにアプリケーションを移動できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **cfs region***region-id*	CFS リージョン サブモードを開始します。
ステップ 3	switch(config-cfs-region)# *application*	あるリージョンから別のリージョンに移動するアプリケーションを示します。 （注） 同じリージョンにアプリケーションを複数回移動しようとすると、「Application already present in the same region」というエラー メッセージが表示されます。

次に、リージョン 1 に割り当てられていたアプリケーションをリージョン 2 に移動する例を示します。

```
switch# configure terminal
switch(config)# cfs region 2
switch(config-cfs-region)# ntp
```

リージョンからのアプリケーションの削除

リージョンからのアプリケーションの削除は、アプリケーションをデフォルト リージョン（リージョン 0）に戻す場合と同じです。これによって、ネットワーク全体がアプリケーションの配信の範囲になります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **cfs region***region-id*	CFS リージョン サブモードを開始します。
ステップ 3	switch(config-cfs-region)# **no***application*	リージョンに属しているアプリケーションを削除します。

CFS リージョンの削除

リージョンの削除とは、リージョン定義を無効にすることです。リージョンを削除すると、リージョンによってバインドされているすべてのアプリケーションがデフォルト リージョンに戻ります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **no cfs region***region-id*	リージョンを削除します。 （注） 「All the applications in the region will be moved to the default region」という警告が表示されます。

IP を介した CFS の設定

IPv4 を介した CFS のイネーブル化

IPv4 を介した CFS をイネーブルまたはディセーブルにできます。

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **cfs ipv4 distribute**	スイッチのすべてのアプリケーションに対して IPv4 を介した CFS をグローバルでイネーブルにします。

	コマンドまたはアクション	目的
ステップ 3	switch(config)# **no cfs ipv4 distribute**	（任意） スイッチの IPv4 を介した CFS をディセーブルにします（デフォルト）。

IPv6 を介した CFS のイネーブル化

IPv6 を介した CFS をイネーブルまたはディセーブルにできます。

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **cfs ipv6 distribute**	スイッチのすべてのアプリケーションに対して IPv6 を介した CFS をグローバルでイネーブルにします。
ステップ 3	switch(config)# **no cfs ipv6 distribute**	（任意） スイッチの IPv6 を介した CFS をディセーブルにします（デフォルト）。

IP を介した CFS 設定の確認

次に、IP を介した CFS 設定を確認する例を示します。

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

IP を介した CFS の IP マルチキャスト アドレスの設定

類似のマルチキャスト アドレスを持つ IP を介した CFS 対応スイッチのすべては、IP ネットワークを介した 1 つの CFS を形成します。ネットワーク トポロジ変更を検出するためのキープアライ

ブ メカニズムのような CFS プロトコル特有の配信は、IP マルチキャスト アドレスを使用して情報を送受信します。

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

CFS の IPv4 マルチキャスト アドレスの設定

IP を介した CFS の IPv4 のマルチキャスト アドレス値を設定できます。デフォルトの IPv4 マルチキャスト アドレスは 239.255.70.83 です。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **cfs ipv4 mcast-address***ipv4-address*	IPv4 を介した CFS 配信の IPv4 マルチキャスト アドレスを設定します。有効な IPv4 アドレスの範囲は 239.255.0.0 ～ 239.255.255.255 および 239.192/16 ～ 239.251/16 です。
ステップ 3	switch(config)# **no cfs ipv4 mcast-address***ipv4-address*	（任意） IPv4 を介した CFS 配信の デフォルトの IPv4 マルチキャスト アドレスに戻します。CFS のデフォルトの IPv4 マルチキャスト アドレスは 239.255.70.83 です。

CFS の IPv6 マルチキャスト アドレスの設定

IPv6 の CFS over IP マルチキャスト アドレスの値を設定できます。デフォルトの IPv6 マルチキャスト アドレスは ff13:7743:4653 です。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **cfs ipv6 mcast-address***ipv4-address*	IPv6 を介した CFS 配信の IPv6 マルチキャスト アドレスを設定します。有効な IPv6 アドレスの範囲は

	コマンドまたはアクション	目的
		ff15::/16（ff15::0000:0000 ～ ff15::ffff:ffff）および ff18::/16（ff18::0000:0000 ～ ff18::ffff:ffff）です。
ステップ 3	switch(config)# **no cfs ipv6 mcast-address***ipv4-address*	（任意） IPv6 を介した CFS 配信のデフォルトの IPv6 マルチキャスト アドレスに戻します。IP を介した CFS のデフォルトの IPv6 マルチキャスト アドレスは ff15::efff:4653 です。

IP を介した CFS の IP マルチキャスト アドレス設定の確認

次に、CFS over IP の IP マルチキャスト アドレス設定を確認する例を示します。

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

CFS のデフォルト設定

次の表に、CFS のデフォルト設定を示します。

表 *1*：デフォルトの *CFS* パラメータ

パラメータ（Parameters）	デフォルト
スイッチでの CFS 配信	イネーブル
データベース変更	最初の設定変更によって暗黙的にイネーブル化
アプリケーションの配信	アプリケーションごとに異なる
コミット	明示的な設定が必要
IP を介した CFS	ディセーブル
IPv4 マルチキャスト アドレス	239.255.70.83
IPv6 マルチキャスト アドレス	ff15::efff:4653

CISCO-CFS-MIB には CFS 関連機能の SNMP 設定情報が含まれます。ご使用のプラットフォームの MIB リファレンスを参照してください。

CFS をイネーブルにして Smart Call Home コンフィギュレーションを配信する

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **callhome**	Call Home コンフィギュレーション モードを開始します。
ステップ 3	switch(config-callhome)# **distribute**	CFS をイネーブルにして、Smart Call Home コンフィギュレーションのアップデートを配信します。
ステップ 4	switch(config-callhome)# **show***application-name***status**	（任意） 指定されたアプリケーションについて、CFS 配信ステータスを表示します。
ステップ 5	switch(config-callhome)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

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

CFS をイネーブルにしてデバイス エイリアス設定を配信する

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

はじめる前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **device-alias distribute**	デバイスエイリアス設定アップデートを配信するように CFS をイネーブルにします。
ステップ 3	switch(config)# **show cfs application**	（任意） CFS 配信ステータスを表示します。
ステップ 4	switch(config)# **copy running-config startup config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

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

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

CFS をイネーブルにして DPVM コンフィギュレーションを配信する

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

はじめる前に

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

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **dpvm distribute**	CFS をイネーブルにして、DPVM コンフィギュレーションのアップデートを配信します。
ステップ 3	switch(config)# **show***application-name***status**	（任意） 指定されたアプリケーションについて、CFS配信ステータスを表示します。
ステップ 4	switch(config)# **copy running-config startup config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

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

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

CFS をイネーブルにして FC ドメイン コンフィギュレーションを配信する

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

はじめる前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **fcdomain distribute**	CFS をイネーブルにして、FC ドメイン コンフィギュレーションのアップデートを配信します。
ステップ 3	switch(config)# **show***application-name***status**	（任意） 指定されたアプリケーションについて、CFS配信ステータスを表示します。
ステップ 4	switch(config)# **copy running-config startup config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

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

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

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

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

はじめる前に

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

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **fc-port-security distribute**	CFS をイネーブルにして、FC ポート セキュリティ コンフィギュレーションのアップデートを配信します。
ステップ 3	switch(config)# **show cfs application**	（任意） CFS 配信ステータスを表示します。
ステップ 4	switch(config)# **copy running-config startup config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

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

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

CFS をイネーブルにして FC タイマー設定を配信する

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

はじめる前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **fctimer distribute**	CFS をイネーブルにして、FC タイマー コンフィギュレーションのアップデートを配信します。
ステップ 3	switch(config)# **show***application-name***status**	（任意） 指定されたアプリケーションについて、CFS配信ステータスを表示します。
ステップ 4	switch(config)# **copy running-config startup config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

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

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

CFS をイネーブルにして IVR コンフィギュレーションを配信する

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

はじめる前に

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

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

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **ivr distribute**	CFS をイネーブルにして、IVR コンフィギュレーションのアップデートを配信します。 （注） ファブリック内のすべての IVR 対応スイッチ上で IVR 配信をイネーブルにする必要があります。
ステップ 3	switch(config)# **show cfs application**	（任意） CFS 配信ステータスを表示します。
ステップ 4	switch(config)# **copy running-config startup config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

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

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

CFS をイネーブルにして NTP コンフィギュレーションを配信する

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

はじめる前に

NTP 機能がイネーブルであることを確認します（**feature ntp** コマンドを使用）。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。

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

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

CFS をイネーブルにして RADIUS コンフィギュレーションを配信する

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **radius distribute**	CFS をイネーブルにして、RADIUS コンフィギュレーションのアップデートを配信します。
ステップ 3	switch(config)# **show***application-name***status**	（任意） 指定されたアプリケーションについて、CFS 配信ステータスを表示します。
ステップ 4	switch(config)# **copy running-config startup config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

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

CFS をイネーブルにして RSCN コンフィギュレーションを配信する

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

はじめる前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **rscn distribute**	CFS をイネーブルにして、RSCN コンフィギュレーションのアップデートを配信します。
ステップ 3	switch(config)# **show cfs application**	（任意） CFS 配信ステータスを表示します。
ステップ 4	switch(config)# **copy running-config startup config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

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

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

CFS をイネーブルにして TACACS+ コンフィギュレーションを配信する

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

はじめる前に

TACACS+ 機能がイネーブルであることを確認します（**feature tacacs+** コマンドを使用）。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **tacacs+ distribute**	CFS をイネーブルにして、TACACS+ コンフィギュレーションのアップデートを配信します。
ステップ 3	switch(config)# **show***application-name***status**	（任意） 指定されたアプリケーションについて、CFS配信ステータスを表示します。
ステップ 4	switch(config)# **copy running-config startup config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

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

CFS をイネーブルにしてユーザ ロール コンフィギュレーションを配信する

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **role distribute**	CFS をイネーブルにしてユーザ ロール コンフィギュレーションを配信します。
ステップ 3	switch(config)# **show***application-name***status**	（任意） 指定されたアプリケーションについて、CFS 配信ステータスを表示します。
ステップ 4	switch(config)# **copy running-config startup config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

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

第 6 章

PTP の設定

この章の内容は、次のとおりです。

- PTP に関する情報，69 ページ
- PTP デバイス タイプ，70 ページ
- PTP プロセス，71 ページ
- クロック管理，71 ページ
- PTP のハイ アベイラビリティ，72 ページ
- PTP のライセンス要件，72 ページ
- PTP の注意事項および制約事項，72 ページ
- PTP のデフォルト設定，73 ページ
- PTP の設定，73 ページ

PTP に関する情報

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

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

PTP は、システムのリアルタイム PTP クロックが相互に同期する方法を指定する分散プロトコルです。これらのクロックは、グランドマスター クロック（階層の最上部にあるクロック）を持つマスター/スレーブ同期階層に編成され、システム全体の時間基準を決定します。同期は、タイミング情報を使用して階層のマスターの時刻にクロックを調整するメンバーと、PTP タイミング

メッセージを交換することによって実現されます。PTP は、PTP ドメインと呼ばれる論理範囲内で動作します。

PTP デバイス タイプ

次のクロックは、一般的な PTP デバイスです。

オーディナリ クロック

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

境界クロック

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

トランスペアレント クロック

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

次の 2 種類のトランスペアレント クロックがあります。

エンドツーエンド トランスペアレント クロック

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

ピアツーピア トランスペアレント クロック

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

（注） PTP は境界クロック モードのみで動作します。Grand Master Clock（10 MHz）アップストリームを導入することを推奨します。サーバには、同期する必要があり、スイッチに接続されたクロックが含まれます。

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

PTP プロセス

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

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

- 受信したすべての（マスター ステートのポートによって発行された）アナウンス メッセージの内容を検査します
- 外部マスターのデータ セット（アナウンス メッセージ内）とローカル クロックで、優先順位、クロック クラス、精度などを比較します
- 自身のステートがマスターまたはスレーブのいずれであるかを決定します

マスター/スレーブ階層が確立されると、クロックは次のように同期されます。

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

クロック管理

デフォルトでは、Cisco NX-OS のシステム クロックを更新するために NTP を使用します。ただし、**クロックのプロトコル**の特性が **PTP** に設定されている場合、PTP のシステム クロックを更新できます。

PTP がイネーブルの場合、NTP はシステム時刻を更新しません。

PTP のハイ アベイラビリティ

PTP のステートフル リスタートがサポートされています。リブート後またはスーパーバイザ スイッチオーバー後に、実行コンフィギュレーションが適用されます。

PTP のライセンス要件

PTP にはライセンスは不要です。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

PTP の注意事項および制約事項

- PTP は境界クロック モードのみで動作します。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 はユーザデータグラム プロトコル（UDP）上の転送をサポートします。イーサネット上の転送はサポートされません。
- PTP はマルチキャスト通信だけをサポートします。ネゴシエートされたユニキャスト通信はサポートされません。
- PTP はネットワークごとに 1 つのドメインに制限されます。
- すべての管理メッセージはPTPがイネーブルのポートに転送されます。管理メッセージの処理はサポートされていません。
- PTP はスイッチ ポートでのみ設定できます。FEX ポートの PTP の設定はサポートされていません。
- PTP 対応ポートは、ポート上で PTP をイネーブルにしない場合、PTP パケットを識別せず、これらのパケットにタイムスタンプを適用したり、パケットをリダイレクトしたりしません。
- PTP は、物理イーサネット ベースのポートだけでサポートされます。
- VPC 環境では、PTP を各メンバ ポートで個別に設定する必要があります。
- FabricPath を介した PTP はサポートされていません。
- Cisco NX-OS リリース 7.1(1)N1(1) よりも前のリリースから最新リリースへの非中断 ISSU の場合は、PTP 機能を有効にする前にリロードを行います。

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 *2*：デフォルトの *PTP* パラメータ

パラメータ（Parameters）	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 最小遅延要求間隔	0 ログ秒
PTP VLAN	1

PTP の設定

PTP のグローバルな設定

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config) # [**no**] **feature ptp**	デバイス上で PTP をイネーブルまたはディセーブルにします。 （注） スイッチのPTPをイネーブルにしても、各インターフェイスのPTPはイネーブルになりません。
ステップ 3	switch(config) # [**no**] **ptp source** *ip-address* [**vrf** *vrf*]	すべての PTP パケットのソース IP アドレスを設定します。 *ip-address* には IPv4 または IPv6 形式を使用できます。
ステップ 4	switch(config) # [**no**] **ptp domain** *number*	（任意） このクロックで使用するドメイン番号を設定します。PTP ドメインを使用すると、1 つのネットワーク上で、複数の独立した PTP クロッキング サブドメインを使用できます。 *number* の範囲は 0 ～ 128 です。
ステップ 5	switch(config) # [**no**] **ptp priority1** *value*	（任意） このクロックをアドバタイズするときに使用する priority1 の値を設定します。この値はベスト マスター クロック選択のデフォルトの基準（クロック品質、クロック クラスなど）を上書きします。低い値が優先されます。 *value* の範囲は 0 ～ 255 です。
ステップ 6	switch(config) # [**no**] **ptp priority2** *value*	（任意） このクロックをアドバタイズするときに使用する priority2 の値を設定します。この値は、デフォルトの基準では同等に一致する 2 台のデバイスのうち、どちらを優先するかを決めるために使用されます。たとえば、priority2 値を使用して、特定のスイッチが他の同等のスイッチよりも優先されるようにすることができます。 *value* の範囲は 0 ～ 255 です。
ステップ 7	switch(config) # **show ptp brief**	（任意） PTP のステータスを表示します。

	コマンドまたはアクション	目的
ステップ 8	switch(config) # **show ptp clock**	（任意） ローカル クロックのプロパティを表示します。
ステップ 9	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

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

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

インターフェイスでの PTP の設定

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

はじめる前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config) # **interface ethernet** *slot/port*	PTP をイネーブルにするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if) # [**no**] **feature ptp**	インターフェイスで PTP をイネーブルまたはディセーブルにします。
ステップ 4	switch(config-if) # [**no**] **ptp announce** {**interval** *log seconds* | **timeout** *count*}	（任意） インターフェイス上の PTP アナウンス メッセージ間の間隔またはタイムアウトがインターフェイスで発生する前の PTP 間隔の数を設定します。 PTP アナウンス間隔の範囲は 0 ～ 4 秒で、間隔のタイムアウトの範囲は 2 ～ 10 です。
ステップ 5	switch(config-if) # [**no**] **ptp delay request minimum interval** *log seconds*	（任意） ポートがマスター ステートの場合に PTP 遅延要求メッセージ間で許可される最小間隔を設定します。 範囲はログ（-6）～ログ（1）秒です。ログ（-2）は、1 秒あたり 2 フレームです。
ステップ 6	switch(config-if) # [**no**] **ptp sync interval** *log seconds*	（任意） インターフェイス上の PTP 同期メッセージの送信間隔を設定します。
ステップ 7	switch(config-if) # [**no**] **ptp vlan** *vlan-id*	（任意） PTP をイネーブルにするインターフェイスの VLAN を指定します。インターフェイスの 1 つの VLAN でイネーブルにできるのは、1 つの PTP のみです。 指定できる範囲は 1 ～ 4094 です。
ステップ 8	switch(config-if) # **show ptp brief**	（任意） PTP のステータスを表示します。
ステップ 9	switch(config-if) # **show ptp port interface** *interface slot/port*	（任意） PTP ポートのステータスを表示します。

	コマンドまたはアクション	目的
ステップ 10	switch(config-if)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

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

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

PTP 設定の確認

次のいずれかのコマンドを使用して、設定を確認します。

表 *3* : ***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。

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

第 7 章

ユーザ アカウントおよび RBAC の設定

この章の内容は、次のとおりです。

- ユーザ アカウントおよび RBAC の概要，79 ページ
- ユーザ アカウントの注意事項および制約事項，86 ページ
- ユーザ アカウントの設定，86 ページ
- RBAC の設定，88 ページ
- ユーザ アカウントと RBAC の設定の確認，93 ページ
- ユーザ アカウントおよび RBAC のユーザ アカウント デフォルト設定，94 ページ

ユーザ アカウントおよび RBAC の概要

Cisco Nexus シリーズ スイッチは、ロールベース アクセス コントロール（RBAC）を使用して、ユーザがスイッチにログインするときに各ユーザが持つアクセス権の量を定義します。

RBAC では、1 つまたは複数のユーザ ロールを定義し、各ユーザ ロールがどの管理操作を実行できるかを指定します。スイッチのユーザ アカウントを作成するとき、そのアカウントにユーザ ロールを関連付けます。これにより個々のユーザがスイッチで行うことができる操作が決まります。

ユーザ ロール

ユーザ ロールには、そのロールを割り当てられたユーザが実行できる操作を定義するルールが含まれています。各ユーザ ロールに複数のルールを含めることができ、各ユーザが複数のロールを持つことができます。たとえば、role1 では設定操作へのアクセスだけが許可されており、role2 ではデバッグ操作へのアクセスだけが許可されている場合、role1 と role2 の両方に属するユーザは、設定操作とデバッグ操作にアクセスできます。特定の VSAN、VLAN、およびインターフェイスへのアクセスを制限することもできます。

スイッチには、次のデフォルト ユーザ ロールが用意されています。

network-admin（スーパーユーザ）

スイッチ全体に対する完全な読み取りと書き込みのアクセス権。

ネットワーク オペレータ

スイッチに対する完全な読み取りアクセス権。

san-admin

SNMP または CLI を使用した FCoE 管理タスクへの完全な読み取りと書き込みのアクセス権。

（注） 複数のロールに属するユーザは、そのロールで許可されるすべてのコマンドの組み合わせを実行できます。コマンドへのアクセス権は、コマンドへのアクセス拒否よりも優先されます。たとえば、ユーザが、コンフィギュレーション コマンドへのアクセスが拒否されたロール A を持っていたとします。しかし、同じユーザが RoleB も持ち、このロールではコンフィギュレーション コマンドにアクセスできるとします。この場合、このユーザはコンフィギュレーション コマンドにアクセスできます。

（注） ネットワーク管理者ユーザのみが RBAC ロールでチェックポイントまたはロールバックを実行できます。他のユーザが自分のロールの許可ルールとしてこれらのコマンドを持つ場合でも、コマンドを実行しようとするとユーザ アクセスが拒否されます。

事前定義された SAN 管理者ユーザ ロール

SAN 管理者ユーザ ロールは、LAN および SAN の管理タスクを分離するように設計された、編集不可能な事前定義されたユーザ ロールです。SAN 管理者ユーザ ロールを割り当てられたユーザは、すべてのイーサネット コンフィギュレーション タスクへの読み取り専用アクセスがあります。別のユーザ ロールによって割り当てられていない場合、SAN の管理者ユーザには、イーサネット機能に対する書き込みアクセスが許可されません。

SAN 管理者ユーザには、次の機能が許可されます。

- インターフェイス コンフィギュレーション
- VSAN の設定（データベースやメンバーシップなど）
- FCoE 用に事前設定された VLAN の VSAN へのマッピング
- ゾーン分割設定
- SNMP コミュニティと SNMP ユーザを除く SNMP 関連パラメータの設定
- 他のすべての設定に対する読み取り専用アクセス
- 次のような SAN 機能の設定および管理：

- FC-SP
- FC-PORT-SECURITY
- FCoE
- FCoE-NPV
- FPORT-CHANNEL-TRUNK
- PORT-TRACK
- FABRIC-BINDING

- 次の EXEC モード コマンドの設定および管理：
  - DEBUG
  - FCDOMAIN
  - FCPING
  - SAN-PORT-CHANNEL
  - SHOW
  - ZONE
  - ZONESET

（注） SAN 管理者ロールは、、すべてのインターフェイス タイプでの設定を許可します。事前定義された SAN 管理者ユーザ ロールは、イーサネット インターフェイスを含むすべてのインターフェイスへのアクセスを許可するように設計されています。そのため、SNMP の動作は妨げられません。

ルール

ルールは、ロールの基本要素です。ルールは、そのロールがユーザにどの操作の実行を許可するかを定義します。ルールは次のパラメータで適用できます。

コマンド

正規表現で定義されたコマンドまたはコマンド グループ

機能

Cisco Nexus デバイスにより提供される機能に適用されるコマンド。**show role feature** コマンドを入力すると、このパラメータに指定できる機能名が表示されます。

機能グループ

機能のデフォルト グループまたはユーザ定義グループ**show role feature-group** コマンドを入力すると、このパラメータに指定できるデフォルトの機能グループが表示されます。

これらのパラメータは、階層状の関係を作成します。最も基本的な制御パラメータはcommandです。次の制御パラメータはfeatureです。これは、その機能にアソシエートされているすべてのコマンドを表します。最後の制御パラメータが、feature groupです。機能グループは、関連する機能を組み合わせたものです。機能グループによりルールを簡単に管理できます。

ロールごとに最大256のルールを設定できます。ルールが適用される順序は、ユーザ指定のルール番号で決まります。ルールは降順で適用されます。たとえば、1つのロールが3つのルールを持っている場合、ルール3がルール2よりも前に適用され、ルール2はルール1よりも前に適用されます。

SAN 管理者ロール機能のルール マッピング

SAN管理者ロールは編集不可です。次のロール機能は、設定済みのロールの一部です。事前設定されたロールには、完全な読み取りアクセス権があり、次のルールが適用されます。

表 *4*：*SAN* 管理者ユーザロールのロール機能のルール

機能	権限
copy	コピー関連コマンドに対する読み取りおよび書き込み権限
fabric-binding	ファブリック バインディング関連コマンドに対する読み取りおよび書き込み権限
fcoe	Fibre Channel over Ethernet 関連コマンドに対する読み取りおよび書き込み権限
fdmi	Fabric Device Management Interface（FDMI）関連コマンドに対する読み取りおよび書き込み権限
fspf	Fabric Shortest Path First（FSPF）関連コマンドに対する読み取りおよび書き込み権限
interface	インターフェイス関連コマンドに対する読み取りおよび書き込み権限です。
port-track	ポート トラック関連コマンドに対する読み取りおよび書き込み権限

機能	権限
port-security	ポートセキュリティ関連コマンドに対する読み取りおよび書き込み権限
rdl	Remote Domain Loopback（RDL）関連コマンドに対する読み取りおよび書き込み権限
rmon	RMON 関連コマンドに対する読み取りおよび書き込み権限
rscn	Registered State Change Notification（RSCN）関連コマンドに対する読み取りおよび書き込み権限
snmp	SNMP 関連コマンドに対する読み取りおよび書き込み権限
snmpTargetAddrEntry	SNMP トラップ ターゲット関連コマンドに対する読み取りおよび書き込み権限
snmpTargetParamsEntry	SNMP トラップ ターゲット パラメータ関連コマンドに対する読み取りおよび書き込み権限
span	SPAN 関連コマンドに対する読み取りおよび書き込み権限
trapRegEntry	SNMP トラップ レジストリ関連コマンドに対する読み取りおよび書き込み権限
vsan	VSAN 関連コマンドに対する読み取りおよび書き込み権限
vsanIfvsan	FCoE VLAN と VSAN 間マッピング コマンド関連コマンドに対する読み取りおよび書き込み権限
wwnm	World Wide Name（WWN）関連コマンドに対する読み取りおよび書き込み権限
zone	ゾーン分割コマンドに対する読み取りおよび書き込み権限

ユーザ ロール ポリシー

ユーザがアクセスできるスイッチリソースを制限するために、またはインターフェイス、VLAN、VSAN へのアクセスを制限するために、ユーザ ロール ポリシーを定義できます。

ユーザロールポリシーは、ロールに定義されている規則で制約されます。たとえば、特定のインターフェイスへのアクセスを許可するインターフェイス ポリシーを定義した場合、**interface** コマンドを許可するコマンド ルールをロールに設定しないと、ユーザはインターフェイスにアクセスできません。

コマンド ルールが特定のリソース（インターフェイス、VLAN、または VSAN）へのアクセスを許可した場合、ユーザがそのユーザに関連付けられたユーザ ロール ポリシーに表示されていなくても、ユーザはこれらのリソースへのアクセスを許可されます。

ユーザ アカウントの設定の制限事項

次の語は予約済みであり、ユーザ設定に使用できません。

- adm
- bin
- daemon
- ftp
- ftpuser
- games
- gdm
- gopher
- halt
- lp
- mail
- mailnull
- man
- mtsuser
- news
- nobody
- san-admin
- シャットダウン
- sync
- sys

- uucp
- xfs

注意 Cisco Nexus 5000 および 6000 シリーズ スイッチでは、すべて数字のユーザ名が TACACS+ または RADIUS で作成されている場合でも、すべて数字のユーザ名はサポートされません。AAA サーバに数字だけのユーザ名が登録されていて、ログイン時に入力しても、スイッチはログイン要求を拒否します。

ユーザ名の先頭は英数字とする必要があります。ユーザ名には特殊文字 (+ = . _ \ -) のみを含めることができます。# 記号と ! 記号はサポートされていません。ユーザ名に許可されていない文字が含まれている場合、指定したユーザはログインできません。Cisco NX-OS release 7.3(0)N1(1) 以降、アンダースコア（_）から始まるユーザ名がサポートされます。

ユーザ パスワードの要件

Cisco Nexus デバイス パスワードには大文字小文字の区別があり、英数字だけを含むことができます。ドル記号（$）やパーセント記号（%）などの特殊文字は使用できません。

パスワードが脆弱な場合（短い、解読されやすいなど）、Cisco Nexus デバイスはパスワードを拒否します。各ユーザ アカウントには強力なパスワードを設定するようにしてください。強力なパスワードは、次の特性を持ちます。

- 長さが 8 文字以上である
- 複数の連続する文字（「abcd」など）を含んでいない
- 複数の同じ文字の繰り返し（「aaabbb」など）を含んでいない
- 辞書に載っている単語を含んでいない
- 正しい名前を含んでいない
- 大文字および小文字の両方が含まれている
- 数字が含まれている

強力なパスワードの例を次に示します。

- If2CoM18
- 2009AsdfLkj30
- Cb1955S21

（注） セキュリティ上の理由から、ユーザ パスワードはコンフィギュレーション ファイルに表示されません。

ユーザ アカウントの注意事項および制約事項

ユーザ アカウントおよび RBAC を設定する場合、ユーザ アカウントには次の注意事項および制約事項があります。

- 最大 256 個のルールをユーザ ロールに追加できます。
- 最大 64 個のユーザ ロールをユーザ アカウントに割り当てることができます。
- 1 つのユーザ ロールを複数のユーザ アカウントに割り当てることができます。
- network-admin、network-operator、san-admin などの事前定義されたロールは編集不可です。
- ルールの追加、削除、編集は、SAN 管理者ユーザ ロールではサポートされません。
- インターフェイス、VLAN、または VSAN 範囲は SAN 管理者ユーザ ロールでは変更できません。

（注） ユーザ アカウントは、少なくとも 1 つのユーザ ロールを持たなければなりません。

ユーザ アカウントの設定

（注） ユーザ アカウントの属性に加えられた変更は、そのユーザがログインして新しいセッションを作成するまで有効になりません。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **show role**	（任意） 使用可能なユーザ ロールを表示します。必要に応じて、他のユーザ ロールを設定できます。
ステップ 3	switch(config) # **username***user-id* [**password***password*] [**expire***date*] [**role***role-name*]	ユーザ アカウントを設定します。 *user-id* は、最大 28 文字の英数字の文字列で、大文字と小文字が区別されます。 デフォルトの *password* は定義されていません。

	コマンドまたはアクション	目的
		（注） パスワードを指定しなかった場合、ユーザはスイッチにログインできない場合があります。 **expire***date* オプションの形式は、YYYY-MM-DD です。デフォルトでは、失効日はありません。
ステップ 4	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 5	switch# **show user-account**	（任意） ロール設定を表示します。
ステップ 6	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、ユーザ アカウントを設定する例を示します。

```
switch# configure terminal
switch(config)# username NewUser password 4Ty18Rnt
switch(config)# exit
switch# show user-account
```

SAN 管理者ユーザの設定

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config) # **username** *user-id* **role san-admin password** *password*	指定したユーザに対する SAN 管理者ユーザ ロールのアクセス権を設定します。
ステップ 3	switch(config) # **show user-account**	（任意） ロール設定を表示します。
ステップ 4	switch(config) # **show snmp-user**	（任意） SNMP ユーザの設定を表示します。
ステップ 5	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィ

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

次に、SAN 管理者ユーザを設定し、ユーザ アカウントおよび SNMP ユーザ設定を表示する例を示します。

```
switch# configure terminal
switch(config)# username user1 role san-admin password xyz123
switch(config)# show user-account
user:admin
     this user account has no expiry date
     roles:network-admin
user:user1
     this user account has no expiry date
     roles:san-admin
switch(config) # show snmp user
_____________________________________________________________________
     SNMP USERS
_____________________________________________________________________

User     Auth  Priv(enforce)  Groups
____     ____  _____________  ______
admin    md5   des(no)        network-admin
user1    md5   des(no)        san-admin

_____________________________________________________________________
NOTIFICATION TARGET USES (configured for sending V3 Inform)
_____________________________________________________________________

User     Auth   Priv
____     ____   ____

switch(config) #
```

RBAC の設定

ユーザ ロールおよびルールの作成

指定するルール番号により、ルールが適用される順番が決まります。ルールは降順で適用されます。たとえば、1 つのロールが 3 つのルールを持っている場合、ルール 3 がルール 2 よりも前に適用され、ルール 2 はルール 1 よりも前に適用されます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config) # **role name***role-name*	ユーザ ロールを指定し、ロール 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
		role-name 引数は、最大 16 文字の英数字の文字列で、大文字と小文字が区別されます。
ステップ 3	switch(config-role) #**rule***number* {**deny** | **permit**} **command***command-string*	コマンド規則を設定します。 *command-string* には、スペースおよび正規表現を含めることができます。たとえば、「interface ethernet *」は、すべてのイーサネットインターフェイスが含まれます。 必要な規則の数だけこのコマンドを繰り返します。
ステップ 4	switch(config-role)# **rule***number* {**deny** | **permit**} {**read**| **read-write**}	すべての操作の読み取り専用ルールまたは読み取り/書き込みルールを設定します。
ステップ 5	switch(config-role)# **rule***number* {**deny** | **permit**} {**read**| **read-write**} **feature***feature-name*	機能に対して、読み取り専用規則か読み取りと書き込みの規則かを設定します。 機能の一覧を表示するには、**show role feature** コマンドを使用します。 必要な規則の数だけこのコマンドを繰り返します。
ステップ 6	switch(config-role)# **rule***number* {**deny** | **permit**} {**read**| **read-write**} **feature-group***group-name*	機能グループに対して、読み取り専用規則か読み取りと書き込みの規則かを設定します。 機能グループの一覧を表示するには、**show role feature-group** コマンドを使用します。 必要な規則の数だけこのコマンドを繰り返します。
ステップ 7	switch(config-role)# **description***text*	（任意） ロールの説明を設定します。説明にはスペースも含めることができます。
ステップ 8	switch(config-role)# **end**	ロール コンフィギュレーション モードを終了します。
ステップ 9	switch# **show role**	（任意） ユーザ ロールの設定を表示します。
ステップ 10	switch# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。

次に、ユーザ ロールを作成してルールを指定する例を示します。

```
switch# configure terminal
switch(config)# role name UserA
switch(config-role)# rule deny command clear users
switch(config-role)# rule deny read-write
switch(config-role)# description This role does not allow users to use clear commands
switch(config-role)# end
switch(config)# show role
```

機能グループの作成

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config) # **role feature-group***group-name*	ユーザ ロール機能グループを指定して、ロール機能グループ コンフィギュレーション モードを開始します。 *group-name* は、最大 32 文字の英数字の文字列で、大文字と小文字が区別されます。
ステップ 3	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 4	switch# **show role feature-group**	（任意） ロール機能グループ設定を表示します。
ステップ 5	switch# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、機能グループを作成する例を示します。

```
switch# configure terminal
switch(config) # role feature-group group1
switch(config) # exit
switch# show role feature-group
switch# copy running-config startup-config
switch#
```

ユーザ ロール インターフェイス ポリシーの変更

ユーザ ロール インターフェイス ポリシーを変更することで、ユーザがアクセスできるインターフェイスを制限できます。ロールがアクセスできるインターフェイスのリストを指定します。これを必要なインターフェイスの数だけ指定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config) # **role name***role-name*	ユーザロールを指定し、ロールコンフィギュレーション モードを開始します。
ステップ 3	switch(config-role) # **interface policy deny**	ロール インターフェイス ポリシー コンフィギュレーション モードを開始します。
ステップ 4	switch(config-role-interface) # **permit interface***interface-list*	ロールがアクセスできるインターフェイスのリストを指定します。 必要なインターフェイスの数だけこのコマンドを繰り返します。 このコマンドには、イーサネットまたは仮想ファイバチャネルインターフェイスを指定できます。
ステップ 5	switch(config-role-interface) # **exit**	ロール インターフェイス ポリシー コンフィギュレーション モードを終了します。
ステップ 6	switch(config-role) # **show role**	（任意） ロール設定を表示します。
ステップ 7	switch(config-role) # **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

次に、ユーザがアクセスできるインターフェイスを制限するために、ユーザ ロールインターフェイス ポリシーを変更する例を示します。

```
switch# configure terminal
switch(config)# role name UserB
switch(config-role)# interface policy deny
switch(config-role-interface)# permit interface ethernet 2/1
switch(config-role-interface)# permit interface vfc 30/1
```

ユーザ ロール VLAN ポリシーの変更

ユーザ ロール VLAN ポリシーを変更することで、ユーザがアクセスできる VLAN を制限できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config) # **role name***role-name*	ユーザ ロールを指定し、ロール コンフィギュレーション モードを開始します。
ステップ 3	switch(config-role)# **vlan policy deny**	ロール VLAN ポリシー コンフィギュレーション モードを開始します。
ステップ 4	switch(config-role-vlan # **permit vlan***vlan-list*	ロールがアクセスできる VLAN の範囲を指定します。 必要な VLAN の数だけこのコマンドを繰り返します。
ステップ 5	switch(config-role-vlan) # **exit**	ロール VLAN ポリシー コンフィギュレーション モードを終了します。
ステップ 6	switch# **show role**	（任意） ロール設定を表示します。
ステップ 7	switch# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

ユーザ ロール VSAN ポリシーの変更

ユーザ ロール VSAN ポリシーを変更して、ユーザがアクセスできる VSAN を制限できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config-role) # **role name***role-name*	ユーザ ロールを指定し、ロール コンフィギュレーション モードを開始します。
ステップ 3	switch(config-role) # **vsan policy deny**	ロール VSAN ポリシー コンフィギュレーション モードを開始します。
ステップ 4	switch(config-role-vsan) # **permit vsan***vsan-list*	ロールがアクセスできる VSAN 範囲を指定します。 必要な VSAN の数だけ、このコマンドを繰り返します。
ステップ 5	switch(config-role-vsan) # **exit**	ロール VSAN ポリシー コンフィギュレーション モードを終了します。
ステップ 6	switch# **show role**	（任意） ロール設定を表示します。
ステップ 7	switch# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

ユーザ アカウントと RBAC の設定の確認

次のいずれかのコマンドを使用して、設定を確認します。

コマンド	目的
show role [*role-name*]	ユーザ ロールの設定を表示します。
show role feature	機能リストを表示します。
show role feature-group	機能グループの設定を表示します。
show startup-config security	スタートアップ コンフィギュレーションのユーザ アカウント設定を表示します。

コマンド	目的
show running-config security [**all**]	実行コンフィギュレーションのユーザアカウント設定を表示します。**all** キーワードを指定すると、ユーザアカウントのデフォルト値が表示されます。
show user-account	ユーザ アカウント情報を表示します。

ユーザ アカウントおよび RBAC のユーザ アカウント デフォルト設定

次の表に、ユーザ アカウントおよび RBAC パラメータのデフォルト設定を示します。

表 *5*：デフォルトのユーザ アカウントおよび *RBAC* パラメータ

パラメータ（Parameters）	デフォルト
ユーザ アカウント パスワード	未定義
ユーザ アカウントの有効期限	なし。
インターフェイス ポリシー	すべてのインターフェイスがアクセス可能
VLAN ポリシー	すべての VLAN がアクセス可能
VFC ポリシー	すべての VFC にアクセス可能。
VETH ポリシー	すべての VETH にアクセス可能。

第 8 章

Session Manager の設定

この章の内容は、次のとおりです。

- Session Manager の概要，95 ページ
- Session Manager の注意事項および制約事項，96 ページ
- Session Manager の設定，96 ページ
- Session Manager 設定の確認，98 ページ

Session Manager の概要

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：セッション マネージャ モードで実行するコマンドのリストを作成します。
- 検証：設定の基本的なセマンティック チェックを行います。Cisco NX-OS は、設定の一部でセマンティクス検査が失敗した場合にエラーを返します。
- 検証：既存のハードウェア設定、ソフトウェア設定、およびリソースに基づいて、設定全体を確認します。Cisco NX-OS は、設定がこの確認フェーズで合格しなかった場合にエラーを返します。
- コミット：Cisco NX-OS は設定全体を確認して、デバイスに対する変更をアトミックに実行します。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。

Session Manager の注意事項および制約事項

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

- Session Manager は、アクセス コントロール リスト（ACL）機能のみサポートします。
- 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。

Session Manager の設定

セッションの作成

作成できるコンフィギュレーション セッションの最大数は 32 です。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure session***name*	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	switch(config-s)# **show configuration session** [*name*]	（任意） セッションの内容を表示します。
ステップ 3	switch(config-s)# **save***location*	（任意） セッションをファイルに保存します。保存場所には、bootflash または volatile を指定できます。

セッションでの ACL の設定

コンフィギュレーション セッションで ACL を設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure session***name*	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	switch(config-s)# **ip access-list***name*	ACL を作成します。
ステップ 3	switch(config-s-acl)# **permit***protocol source destination*	（任意） ACL に許可文を追加します。
ステップ 4	switch(config-s-acl)# **interface***interface-type number*	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	switch(config-s-if)# **ip port access-group***name***in**	インターフェイスにポートアクセスグループを追加します。
ステップ 6	switch# **show configuration session** [*name*]	（任意） セッションの内容を表示します。

セッションの確認

セッションを確認するには、セッション モードで次のコマンドを使用します。

コマンド	目的
switch(config-s)# **verify** [**verbose**]	コンフィギュレーションセッションのコマンドを確認します。

セッションのコミット

セッションをコミットするには、セッション モードで次のコマンドを使用します。

コマンド	目的
switch(config-s)# **commit** [**verbose**]	コンフィギュレーションセッションのコマンドをコミットします。

セッションの保存

セッションを保存するには、セッション モードで次のコマンドを使用します。

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

セッションの廃棄

セッションを廃棄するには、セッション モードで次のコマンドを使用します。

コマンド	目的
switch(config-s)# **abort**	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 のコンフィギュレーション例

次に、ACL 用のコンフィギュレーション セッションを作成する例を示します。

```
switch# configure session name test2
switch(config-s)# ip access-list acl2
switch(config-s-acl)# permit tcp any any
switch(config-s-acl)# exit
switch(config-s)# interface Ethernet 1/4
switch(config-s-ip)# ip port access-group acl2 in
switch(config-s-ip)# exit
switch(config-s)# verify
switch(config-s)# exit
switch# show configuration session test2
```

Session Manager 設定の確認

セッション マネージャの設定情報を確認するには、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。

コマンド	目的
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。

第 9 章

オンライン診断の設定

この章の内容は、次のとおりです。

- オンライン診断について，101 ページ
- オンライン診断の設定，104 ページ
- オンライン診断設定の確認，105 ページ
- オンライン診断のデフォルト設定，105 ページ

オンライン診断について

オンライン診断では、スイッチの起動時またはリセット時にハードウェア コンポーネントを確認し、通常の動作時にはハードウェアの状態を監視します。

Cisco Nexus シリーズ スイッチは、起動時診断および実行時診断をサポートします。起動時診断には、システム起動時とリセット時に実行する、中断を伴うテストおよび非中断テストが含まれます。

実行時診断（ヘルス モニタリング診断）には、スイッチの通常の動作時にバックグラウンドで実行する非中断テストが含まれます。

ブートアップ診断

起動時診断は、スイッチをオンラインにする前にハードウェアの障害を検出します。起動診断では、スーパーバイザと ASIC の間のデータ パスと制御パスの接続も確認します。次の表に、スイッチの起動時またはリセット時にだけ実行される診断を示します。

表 *6*：ブートアップ診断

診断	説明
PCIe	PCI express（PCIe）アクセスをテストします。

診断	説明
NVRAM	NVRAM（不揮発性RAM）の整合性を確認します。
インバンド ポート	インバンドポートとスーパーバイザの接続をテストします。
管理ポート	管理ポートをテストします。
メモリ	DRAM の整合性を確認します。

起動時診断には、ヘルス モニタリング診断と共通するテスト セットも含まれます。

起動時診断では、オンボード障害ロギング（OBFL）システムに障害を記録します。また、障害により LED が表示され、診断テストのステート（on、off、pass、または fail）を示します。

起動診断テストをバイパスするように Cisco Nexus 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。

ヘルスモニタリング診断

ヘルス モニタリング診断では、スイッチの状態に関する情報を提供します。実行時のハードウェア エラー、メモリ エラー、ソフトウェア障害、およびリソースの不足を検出します。

ヘルス モニタリング診断は中断されずにバックグラウンドで実行され、ライブ ネットワーク トラフィックを処理するスイッチの状態を確認します。

次の表に、スイッチのヘルス モニタリング診断を示します。

表 7: ヘルス モニタリング診断テスト

診断	説明
LED	ポートおよびシステムのステータス LED を監視します。
電源モジュール	電源装置のヘルス ステータスを監視します。
温度センサー	温度センサーの読み取り値を監視します。
テスト ファン	ファンの速度およびファンの制御をモニタします。

（注） スイッチが吸気温度のしきい値に達し、120 秒の制限内には温度が低下しない場合、スイッチを復旧するには、スイッチの電源をオフにして、電源装置を再装着する必要があります。

次の表に、システム起動時とリセット時にも実行されるヘルス モニタリング診断を示します。

表 *8*：ヘルス モニタリングおよび起動時診断テスト

診断	説明
SPROM	バックプレーンとスーパーバイザ SPROM の整合性を確認します。
ファブリック エンジン	スイッチ ファブリック ASIC をテストします。
ファブリック ポート	スイッチ ファブリック ASIC 上のポートをテストします。
転送エンジン	転送エンジン ASIC をテストします。
転送エンジン ポート	転送エンジン ASIC 上のポートをテストします。
前面ポート	前面ポート上のコンポーネント（PHY および MAC など）をテストします。

（注） スイッチが 40 度（摂氏）の吸気温度しきい値を超え、120 秒のしきい値の範囲内では温度が低下しない場合、スイッチを復旧するには、スイッチの電源をオフにして、電源装置を再装着する必要があります。

拡張モジュール診断

スイッチの起動時またはリセット時の起動時診断には、スイッチのインサービス拡張モジュールのテストが含まれます。

稼働中のスイッチに拡張モジュールを挿入すると、診断テスト セットが実行されます。次の表に、拡張モジュールの起動時診断を示します。これらのテストは、起動時診断と共通です。起動時診断が失敗した場合、拡張モジュールはサービス状態になりません。

表 *9*：拡張モジュールの起動時診断およびヘルス モニタリング診断

診断	説明
SPROM	バックプレーンとスーパーバイザ SPROM の整合性を確認します。
ファブリック エンジン	スイッチ ファブリック ASIC をテストします。
ファブリック ポート	スイッチ ファブリック ASIC 上のポートをテストします。
転送エンジン	転送エンジン ASIC をテストします。
転送エンジン ポート	転送エンジン ASIC 上のポートをテストします。
前面ポート	前面ポート上のコンポーネント（PHY および MAC など）をテストします。

ヘルス モニタリング診断は、IS 拡張モジュールで実行されます。次の表で、拡張モジュールのヘルス モニタリング診断に固有の追加のテストについて説明します。

表 *10*：拡張モジュールのヘルス モニタリング診断

診断	説明
LED	ポートおよびシステムのステータス LED を監視します。
温度センサー	温度センサーの読み取り値を監視します。

オンライン診断の設定

完全なテスト セットを実行するよう起動時診断を設定できます。もしくは、高速モジュール起動時のすべての起動時診断テストをバイパスできます。

（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	switch# **configure terminal**	グローバルコンフィギュレーションモードを開始します。
ステップ 2	switch(config)# **diagnostic bootup level** [**complete** | **bypass**]	デバイスの起動時に診断を実行するよう起動時診断レベルを次のように設定します。 • **complete**：すべての起動時診断を実行します。これはデフォルト値です。 • **bypass**：起動時診断を実行しません。
ステップ 3	switch# **show diagnostic bootup level**	（任意） 現在、スイッチで実行されている起動時診断レベル（bypass または complete）を表示します。

次に、完全な診断を実行するよう起動時診断レベルを設定する例を示します。

```
switch# configure terminal
switch(config)# diagnostic bootup level complete
```

オンライン診断設定の確認

オンライン診断の設定情報を確認するには、次のコマンドを使用します。

コマンド	目的
show diagnostic bootup level	起動時診断レベルを表示します。
show diagnostic result module*slot*	診断テストの結果を表示します。

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。

表 *11*： デフォルトのオンライン診断パラメータ

パラメータ（**Parameters**）	デフォルト
起動時診断レベル	complete

第 10 章

システム メッセージ ロギングの設定

この章の内容は、次のとおりです。

- システム メッセージ ロギングの概要，107 ページ
- システム メッセージ ロギングのライセンス要件，109 ページ
- システム メッセージ ロギングの注意事項および制約事項，109 ページ
- システム メッセージ ロギングのデフォルト設定，109 ページ
- システム メッセージ ロギングの設定，110 ページ
- システム メッセージ ロギングの設定確認，121 ページ
- ACL ロギングの設定，123 ページ

システム メッセージ ロギングの概要

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

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

デフォルトでは、Cisco Nexus デバイスはメッセージをターミナル セッションへ出力します。

デフォルトでは、スイッチはシステム メッセージをログ ファイルに記録します。

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。

表 *12*： システム メッセージの重大度

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

重大度 0、1、または 2 の最新のメッセージを 100 個まで不揮発性 RAM（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よう設定されたリモート システムで稼働します。最大 8 台の syslog サーバにログを送信するように Cisco Nexus シリーズ スイッチを設定できます。

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

（注） スイッチを最初に初期化する場合、ネットワークが初期化されてからメッセージが Syslog サーバに送信されます。

システム メッセージ ロギングのライセンス要件

製品	ライセンス要件
Cisco NX-OS	システム メッセージ ロギングにライセンスは不要です。ライセンスパッケージに含まれていない機能はすべてCisco NX-OS システムイメージにバンドルされており、追加費用は一切発生しません。NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

システムメッセージロギングの注意事項および制約事項

システム メッセージは、デフォルトでコンソールおよびログ ファイルに記録されます。

システム メッセージ ロギングのデフォルト設定

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

表 *13*： 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（Parameters）	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 2 でイネーブル
ログ ファイル ロギング	重大度 5 のメッセージ ロギングがイネーブル
モジュール ロギング	重大度 5 でイネーブル
ファシリティ ロギング	イネーブル
タイムスタンプ単位	Seconds
Syslog サーバ ロギング	ディセーブル
Syslog サーバ設定の配布	ディセーブル

システム メッセージ ロギングの設定

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

コンソール、Telnet、およびセキュア シェル セッションに対する重大度によって、メッセージを記録するようスイッチを設定できます。

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。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **terminal monitor**	コンソールから現在の端末セッションに syslog メッセージをコピーします。
ステップ 2	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	switch(config)# **logging console** [*severity-level*]	指定された重大度（またはそれ以上）に基づくコンソール セッションへのメッセージの記録をイネーブルにします（数字が小さいほうが大きい重大度を示します）。重大度は 0 ～ 7 の範囲です。 • 0：緊急 • 1：アラート • 2：クリティカル • 3：エラー • 4：警告 • 5：通知 • 6：情報 • 7：デバッグ 重大度が指定されていない場合、デフォルトの2が使用されます。
ステップ 4	switch(config)# **no logging console** [*severity-level*]	（任意） コンソールへのロギング メッセージをディセーブルにします。
ステップ 5	switch(config)# **logging monitor** [*severity-level*]	指定された重大度（またはそれ以上）に基づくモニタへのメッセージの記録をイネーブルにします（数字が

	コマンドまたはアクション	目的
		小さいほうが大きい重大度を示します）。重大度は0～7の範囲です。 • 0：緊急 • 1：アラート • 2：クリティカル • 3：エラー • 4：警告 • 5：通知 • 6：情報 • 7：デバッグ 重大度が指定されていない場合、デフォルトの2が使用されます。 設定はTelnetおよびSSHセッションに適用されます。
ステップ 6	switch(config)# **no logging monitor** [*severity-level*]	（任意） Telnet および SSH セッションへのメッセージ ロギングをディセーブルにします。
ステップ 7	switch# **show logging console**	（任意） コンソール ロギング設定を表示します。
ステップ 8	switch# **show logging monitor**	（任意） モニタ ロギング設定を表示します。
ステップ 9	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、コンソールのロギング レベルを 3 に設定する例を示します。

```
switch# configure terminal
switch(config)# logging console 3
```

次に、コンソールのロギングの設定を表示する例を示します。

```
switch# show logging console
Logging console:                enabled (Severity: error)
```

次に、コンソールのロギングをディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# no logging console
```

次に、ターミナル セッションのログ レベルを 4 に設定する例を示します。

```
switch# terminal monitor
switch# configure terminal
switch(config)# logging monitor 4
```

次に、ターミナル セッションのロギングの設定を表示する例を示します。

```
switch# show logging monitor
Logging monitor:                enabled (Severity: warning)
```

次に、ターミナル セッションのロギングをディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# no logging monitor
```

ファイルへのシステム メッセージ ロギングの設定

システム メッセージをファイルに記録するようスイッチを設定できます。デフォルトでは、システム メッセージはファイル log:messages に記録されます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **logging logfile***logfile-name***severity-level** [**size***bytes*]	システム メッセージを保存するのに使用するログ ファイルの名前と、記録する最小重大度を設定します。任意で最大ファイル サイズを指定できます。デフォルトの重大度は 5 です。ファイル サイズは 4194304 です。 重大度は 0 ～ 7 の範囲です。 • 0：緊急 • 1：アラート • 2：クリティカル • 3：エラー • 4：警告 • 5：通知 • 6：情報 • 7：デバッグ

	コマンドまたはアクション	目的
		ファイル サイズは 4096 ～ 10485760 バイトです。
ステップ 3	switch(config)# **no logging logfile** [*logfile-nameseverity-level* [**size***bytes*]]	（任意） ログファイルへのロギングをディセーブルにします。任意で最大ファイル サイズを指定できます。デフォルトの重大度は 5 です。ファイル サイズは 4194304 です。
ステップ 4	switch# **show logging info**	（任意） ロギング設定を表示します。任意で最大ファイル サイズを指定できます。デフォルトの重大度は5です。ファイル サイズは 4194304 です。
ステップ 5	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、システム メッセージをファイルに記録するようスイッチを設定する例を示します。

```
switch# configure terminal
switch(config)# logging logfile my_log 6 size 4194304
```

次の例は、ロギング設定の表示方法を示しています（簡潔にするため、一部の出力が削除されています）。

```
switch# show logging info
Logging console:                enabled (Severity: debugging)
Logging monitor:                enabled (Severity: debugging)
Logging linecard:               enabled (Severity: notifications)
Logging fex:                    enabled (Severity: notifications)
Logging timestamp:              Seconds
Logging server:                 disabled
Logging logfile:                enabled
        Name - my_log: Severity - informational Size - 4194304
Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
aaa                     3                       3
aclmgr                  3                       3
afm                     3                       3
altos                   3                       3
auth                    0                       0
authpriv                3                       3
bootvar                 5                       5
callhome                2                       2
capability              2                       2
cdp                     2                       2
cert_enroll             2                       2
...
```

モジュールおよびファシリティ メッセージのロギングの設定

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **logging module** [*severity-level*]	指定された重大度またはそれ以上の重大度であるモジュール ログ メッセージをイネーブルにします。重大度は 0 ～ 7 の範囲です。 • 0：緊急 • 1：アラート • 2：クリティカル • 3：エラー • 4：警告 • 5：通知 • 6：情報 • 7：デバッグ 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。
ステップ 3	switch(config)# **logging level***facility severity-level*	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 です。 • 0：緊急 • 1：アラート • 2：クリティカル • 3：エラー • 4：警告 • 5：通知 • 6：情報 • 7：デバッグ 同じ重大度をすべてのファシリティに適用するには、all ファシリティを使用します。デフォルト値については、**show logging level** コマンドを参照してください。

	コマンドまたはアクション	目的
		（注） コンポーネントのデフォルトの重大度と現在のセッションにおける重大度が同じ場合、コンポーネントのログ レベルは実行コンフィギュレーションに表示されません。
ステップ 4	switch(config)# **no logging module**[*severity-level*]	（任意） モジュール ログ メッセージをディセーブルにします。
ステップ 5	switch(config)# **no logging level** [*facility severity-level*]	（任意） 指定されたファシリティのロギング重大度をデフォルトレベルにリセットします。ファシリティおよび重大度を指定しないと、スイッチはすべてのファシリティをデフォルト レベルにリセットします。
ステップ 6	switch# **show logging module**	（任意） モジュール ロギング設定を表示します。
ステップ 7	switch# **show logging level** [*facility*]	（任意） ファシリティごとに、ロギング レベル設定およびシステムのデフォルト レベルを表示します。ファシリティを指定しないと、スイッチはすべてのファシリティのレベルを表示します。
ステップ 8	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、モジュールおよび特定のファシリティ メッセージの重大度を設定する例を示します。

```
switch# configure terminal
switch(config)# logging module 3
switch(config)# logging level aaa 2
```

ロギング タイムスタンプの設定

Cisco Nexus シリーズ スイッチによって記録されるメッセージのタイムスタンプの単位を設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **logging timestamp** {**microseconds** | **milliseconds** | **seconds**}	ロギング タイムスタンプ単位を設定します。デフォルトでは、単位は秒です。
ステップ 3	switch(config)# **no logging timestamp** {**microseconds** | **milliseconds** | **seconds**}	（任意） ロギング タイムスタンプ単位をデフォルトの秒にリセットします。
ステップ 4	switch# **show logging timestamp**	（任意） 設定されたロギング タイムスタンプ単位を表示します。
ステップ 5	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、メッセージのタイムスタンプ単位を設定する例を示します。

```
switch# configure terminal
switch(config)# logging timestamp milliseconds
switch(config)# exit
switch# show logging timestamp
Logging timestamp:              Milliseconds
```

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。

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	**logging server***host* [*severity-level* [**use-vrf***vrf-name* [**facility***facility*]]] 例： `switch(config)# logging server 172.28.254.254 5 use-vrf default facility local3`	ホストが syslog メッセージを受信するように設定します。 • *host* 引数は、syslog サーバ ホストのホスト名または IPv4 または IPv6 アドレスを示します。 • *severity-level* 引数は、指定したレベルに syslog サーバへのメッセージのロギングを制限します。重大度は 0 ～ 7 の範囲です。表 12： システム メッセージの重大度，（108 ページ）を参照してください。 • **use vrf** *vrf-name* キーワードと引数は、仮想ルーティングおよび転送（VRF）名の *default* または *management* 値を示します。特定の VRF が指定されない場合は、management がデフォルトです。ただし、management が設定されているときは、それがデフォルトであるため、**show running** コマンドの出力には表示されません。特定の VRF が設定されている場合、**show-running** コマンドの出力には、各サーバの VRF が表示されます。 （注） 現在の Cisco Fabric Services（CFS）配信では VRF をサポートしていません。CFS 配信がイネーブルの場合、デフォルト VRF で設定されているロギング サーバは管理 VRF として配布されます。 • facility 引数は syslog ファシリティ タイプを指定します。デフォルトの発信ファシリティは local7 です。 ファシリティは、使用している Cisco Nexus シリーズ ソフトウェアのコマンド リファレンスに記載されています。 （注） デバッグは CLI ファシリティですが、デバッグの syslog はサーバに送信されません。
ステップ 3	**no logging server***host* 例： `switch(config)# no logging server 172.28.254.254 5`	（任意） 指定されたホストのロギング サーバを削除します。
ステップ 4	**show logging server** 例： `switch# show logging server`	（任意） Syslog サーバ設定を表示します。

	コマンドまたはアクション	目的
ステップ 5	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、syslog サーバを設定する例を示します。

```
switch# configure terminal
switch(config)# logging server 172.28.254.254 5
use-vrf default facility local3

switch# configure terminal
switch(config)# logging server 172.28.254.254 5 use-vrf management facility local3
```

UNIX または Linux システムでの syslog 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 *14*： *syslog.conf* の *syslog* フィールド

フィールド	説明
ファシリティ	メッセージの作成者。auth、authpriv、cron、daemon、kern、lpr、mail、mark、news、syslog、user、local0 ～ local7 です。アスタリスク（*）を使用するとすべてを指定します。これらのファシリティ指定により、発信元に基づいてメッセージの宛先を制御できます。 （注） ローカル ファシリティを使用する前に設定をチェックします。
レベル	メッセージを記録する最小重大度。debug、info、notice、warning、err、crit、alert、emerg です。アスタリスク（*）を使用するとすべてを指定します。none を使用するとファシリティをディセーブルにできます。

フィールド	説明
アクション	メッセージの宛先。ファイル名、前にアットマーク（@）が付いたホスト名、カンマで区切られたユーザ リストです。アスタリスク（*）を使用するとすべてのログインユーザを指定します。

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。

```
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。

```
$ 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。

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

syslog サーバ設定の配布の設定

Cisco Fabric Services（CFS）インフラストラクチャを使用して、ネットワーク内の他のスイッチへ Syslog サーバ設定を配布できます。

Syslog サーバ設定の配布をイネーブルにすると、配布設定をコミットする前に Syslog サーバ設定を変更し、保留中の変更を表示できます。配布がイネーブルである限り、スイッチは Syslog サーバ設定に対する保留中の変更を維持します。

（注） スイッチを再起動すると、揮発性メモリに保存されている syslog サーバ設定の変更は失われることがあります。

はじめる前に

1 つまたは複数の syslog サーバを設定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	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **logging distribute**	CFS インフラストラクチャを使用して、ネットワーク スイッチへの syslog サーバ設定の配布をイネーブルにします。デフォルトでは、配布はディセーブルです。
ステップ 3	switch(config)# **logging commit**	ファブリック内のスイッチへ配布するための Syslog サーバ設定に対する保留中の変更をコミットします。
ステップ 4	switch(config)# **logging abort**	Syslog サーバ設定に対する保留中の変更をキャンセルします。
ステップ 5	switch(config)# **no logging distribute**	（任意） CFS インフラストラクチャを使用して、ネットワーク スイッチへの syslog サーバ設定の配布をディセーブルにします。設定変更が保留中の場合は、配布をディセーブルにできません。**logging commit** および **logging abort** コマンドを参照してください。デフォルトでは、配布はディセーブルです。
ステップ 6	switch# **show logging pending**	（任意） Syslog サーバ設定に対する保留中の変更を表示します。
ステップ 7	switch# **show logging pending-diff**	（任意） syslog サーバ設定の保留中の変更に対して、現在の syslog サーバ設定との違いを表示します。
ステップ 8	switch# **show logging internal info**	（任意） syslog サーバ配布の現在の状態と最後に実行したアクションに関する情報を表示します。
ステップ 9	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ログ ファイルの表示およびクリア

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

手順

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

次に、ログ ファイルのメッセージを表示する例を示します。

```
switch# show logging last 40
switch# show logging logfile start-time 2007 nov 1 15:10:0
switch# show logging nvram last 10
```

次に、ログ ファイルのメッセージをクリアする例を示します。

```
switch# clear logging logfile
switch# clear logging nvram
```

システム メッセージ ロギングの設定確認

システム メッセージのロギング設定情報を確認するには、次のコマンドを使用します。

コマンド	目的
show 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。

コマンド	目的
show logging internal info	Syslog 配布情報を表示します。
show logging ip access-list cache	IP アクセス リスト キャッシュを表示します。
show logging ip access-list cache detail	IP アクセス リスト キャッシュに関する詳細情報を表示します。
show logging ip access-list status	IP アクセス リスト キャッシュのステータスを表示します。
show logging last*number-lines*	ログ ファイルの末尾から指定行数を表示します。
show logging level [*facility*]	ファシリティ ロギング重大度設定を表示します。
show logging logfile [**start-time***yyyymmmddhh:mm:ss*] [**end-time***yyyymmmddhh:mm:ss*]	ログ ファイルのメッセージを表示します。
show logging module	モジュール ロギング設定を表示します。
show logging monitor	モニタ ロギング設定を表示します。
show logging nvram [**last***number-lines*]	NVRAM ログのメッセージを表示します。
show logging pending	Syslog サーバの保留中の配布設定を表示します。
show logging pending-diff	Syslog サーバの保留中の配布設定の違いを表示します。
show logging server	Syslog サーバ設定を表示します。
show logging session	ロギング セッションのステータスを表示します。
show logging status	ロギング ステータスを表示します。
show logging timestamp	ロギング タイムスタンプ単位設定を表示します。
show running-config acllog	ACL ログファイルの実行コンフィギュレーションを表示します。

ACL ロギングの設定

ACL ロギングに関する情報

アクセス コントロール リスト（ACL）のロギング機能により、IPv4 ACL にヒットするパケットのロギングが可能になります。ログメッセージはフローベースで表示されます。フローは、送信元 IP アドレス、宛先 IP アドレス、レイヤ 4 プロトコル、およびインターフェイスのレイヤ 4 送信元/宛先ポートの組み合わせを使用して識別されます。ログメッセージは、次の基準に基づいて生成されます。

- 新しいフローが作成される場合（INFO メッセージ）
- フローのパケットしきい値に到達したとき（WARNING メッセージ）
- 一定の間隔の終わりに（デフォルトは5分）、フローにヒットしたパケット数とともに（INFO メッセージ：設定可能）

上記に加え、フロー数が指定された間隔内にしきい値を超えると、警告メッセージが記録され、フローはロギング キャッシュに追加されません。

次の表に、Cisco Nexus デバイスの制限について説明します。

表 *15*：*ACL* ロギング サポート表

機能	Cisco Nexus デバイス	
	ロギング サポート	
PACL	Yes	ドロップのみ
入力 RACL	Yes	ドロップのみ
出力 RACL	Yes	ドロップのみ
入力 VACL	Yes	ドロップのみ
出力 VACL	Yes	ドロップのみ
RBACL	該当なし	
VTY ACL In/Out	Yes	許可/ドロップ
mgmt0 の入力 RACL	Yes	許可/ドロップ
SNMP ACL		
NTP ACL		

VTY ACL を除く他のすべての ACL は「拒否」ACE エントリの ACL ロギングのみサポートします。しかし、同一の ACL は vty ACL と他の機能の両方に適用される場合があるため、「permit <> log」CLI はブロックできません。ただし、ある ACL をそのようにインターフェイスや VLAN に適用することは回避可能です。Mgmt0 は、許可のロギングをサポートしています。

Cisco Nexus デバイスでは、CTS はサポートされていないので、RBACL はサポートされません。

IPv6 および MAC ACL の ACL ロギングはサポートされません。FEX HIF インターフェイスを含め、PACL、RACL、VACL および VTY を適用可能なすべてのインターフェイスでサポートされます。

ACL ロギングはレート制限されます。ACL にヒットするパケットはすべて、sup に送信されません。レート リミッタ機能は、スイッチごとに、すべての ASIC と TCAM リージョンに適用されます。レートを設定するため、次の CLI が提供されます。

ACL ロギング キャッシュの設定

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **logging ip access-list cache entries** *num_entries*	ソフトウェア内にキャッシュする最大ログエントリ数を設定します。範囲は 0 ～ 1000000 エントリです。デフォルト値は 8000 エントリです。
ステップ 3	switch(config)# **logging ip access-list cache interval** *seconds*	ログの更新の間隔を秒数で設定します。この時間中エントリが非アクティブの場合、キャッシュから削除されます。指定できる範囲は 5 ～ 86400 秒です。デフォルト値は 300 秒です。
ステップ 4	switch(config)# **logging ip access-list cache threshold** *num_packets*	エントリがログに記録されるまでに一致するパケット数を設定します。範囲は 0 ～ 1000000 パケットです。デフォルト値は 0 パケットです。つまり、パケットの一致数によってロギングがトリガーされることはありません。
ステップ 5	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、ログ エントリの最大数を 5000、間隔を 120 秒、およびしきい値を 500000 に設定する例を示します。

```
switch# configure terminal
switch(config)# logging ip access-list cache entries 5000
switch(config)# logging ip access-list cache interval 120
switch(config)# logging ip access-list cache threshold 500000
switch(config)# copy running-config startup-config
```

インターフェイスへの ACL ロギングの適用

はじめる前に

- ロギング用に設定された少なくとも 1 つのアクセス コントロール エントリ（ACE）で IP アクセス リストを作成します。
- ACL ロギング キャッシュを設定します。
- ACL ログの一致レベルを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface mgmt0**	mgmt0 インターフェイスを指定します。
ステップ 3	switch(config-if)# **ip access-group** *name* **in**	指定したインターフェイスの入力トラフィックで ACL ロギングをイネーブルにします。
ステップ 4	switch(config-if)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、すべての入力トラフィックに対して acl1 で指定されたロギングに mgmt0 インターフェイスを適用する例を示します。

```
switch# configure terminal
switch(config)# interface mgmt0
switch(config-if)# ip access-group acl1 in
switch(config-if)# copy running-config startup-config
```

ロギング使用 VLAN アクセス マップの設定

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **vlan access-map** *map-name*	指定したアクセス マップのアクセス マップ コンフィギュレーション モードを開始します。
ステップ 3	switch(config-access-map)# **match ip address** *ip-access-list*	マップの IPv4 および IPV6 ACL を指定します。
ステップ 4	switch(config-access-map)# **action drop log**	スイッチが、ACL に一致したトラフィックに適用するアクションを指定します。
ステップ 5	switch(config-access-map)# **exit**	アクセス マップ コンフィギュレーション モードを終了します。

次に、ロギング用に VLAN アクセス マップを作成する例を示します。

```
switch# configure terminal
switch(config)# vlan access-map vacl1
switch(config-access-map)# match ip address pacl1
switch(config-access-map)# action drop log
switch(config-access-map)# exit
switch(config)#
```

ACL ログの一致レベルの設定

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	switch(config)# **acllog match-log-level** *number*	ACL ログ（acllog）で記録するエントリと一致するようにログ レベルを指定します。*number* は 0 ～ 7 までの値です。デフォルト値は 6 です。 （注） ログに入力するログ メッセージでは、ACL ログ ファシリティ（acllog）のログ レベルとログ ファイルのロギング重大度は、ACL ログの一致ログ レベル設定よりも大きいか、同じです。詳細については、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，（113 ページ）およびファイルへのシステム メッセージ ロギングの設定，（112 ページ）を参照してください。
ステップ 3	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

ACL ロギングのレート リミッタの設定

キャッシュに記録される、スーパーバイザ（CPU）に送信されるログに記録されるパケット数を制限できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**hardware rate-limiter access-list-log packets** *num-packets*	*num-packets*：パケット/秒の値。有効な範囲は 50 ～ 600000 です。デフォルトは 100 パケット/秒です。

次に、1000 パケット/秒にレート リミッタを設定する例を示します。

```
switch# configure terminal
switch(config)# hardware rate-limiter access-list-log packets 1000
```

ACL ログのクリア

ACL ログをクリアできます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **clear logging ip access-list cache**	IP コンフィギュレーションのアクセス リスト キャッシュをクリアします。

ACL ロギングの確認

次のいずれかのコマンドを使用して、設定を確認します。

コマンド	目的
show logging ip access-list status	ACLLOG のステータスを表示します。
show logging ip access-list cache [**detail**]	キャッシュ内のエントリと任意選択の詳細を表示します。

第 11 章

Smart Call Home の設定

この章の内容は、次のとおりです。

- Smart Call Home に関する情報，129 ページ
- Smart Call Home の注意事項および制約事項，139 ページ
- Smart Call Home の前提条件，140 ページ
- Call Home のデフォルト設定，140 ページ
- Smart Call Home の設定，141 ページ
- Smart Call Home 設定の確認，152 ページ
- フル テキスト形式での syslog アラート通知の例，153 ページ
- XML 形式での syslog アラート通知の例，153 ページ

Smart Call Home に関する情報

Smart Call Home は電子メールを使用して、重要なシステム イベントを通知します。Cisco Nexus シリーズ スイッチは、幅広いメッセージ フォーマットを提供し、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最適な互換性を保てます。この機能を使用して、ネットワーク サポート エンジニアや Network Operations Center を呼び出せます。また、Cisco Smart Call Home サービスを使用して、TAC でケースを自動的に生成することもできます。

シスコと直接サービス契約を結んでいる場合は、Smart Call Home サービス用のデバイスを登録できます。Smart Call Home は、ご使用のデバイスから送信された Smart Call Home メッセージを分析し、背景情報および推奨事項を提供して、システムの問題を迅速に解決します。既知と特定できる問題、特に GOLD 診断エラーについては、シスコ TAC によって自動サービス リクエストが生成されます。

Smart Call Home には、次の機能があります。

- 継続的なデバイス ヘルス モニタリングとリアルタイムの診断アラート。

- ご使用のデバイスからの Smart Call Home メッセージの分析と、必要に応じた自動サービスリクエストの生成は、問題を迅速に解決するための詳細な診断情報とともに、適切な TAC チームにルーティングされます。
- 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、またはダウンロード可能な Transport Gateway（TG）集約ポイントを経由して行われます。複数のデバイスでサポートを必要としている場合、またはセキュリティ要件の関係でご使用のデバイスをインターネットに直接接続できない場合は、TG 集約ポイントを使用できます。
- Smart Call Home メッセージと推奨事項、すべての Smart Call Home デバイスのインベントリおよび設定情報、および Field Notice、セキュリティ勧告、およびサポート終了日情報への Web ベースのアクセス。

Smart Call Home の概要

Smart Call Home を使用すると、重要なイベントがデバイスで発生した場合に外部エンティティに通知できます。Smart Call Home では、ユーザが宛先プロファイルに設定する複数の受信者にアラートが配信されます。

Smart Call Home には、スイッチで事前に定義された一連のアラートが含まれます。これらのアラートはアラート グループにグループ化され、アラート グループのアラートが発生したときに実行する CLI コマンドが割り当てられています。スイッチには、転送された Smart Call Home メッセージのコマンド出力が含まれます。

Smart Call Home 機能には、次のものがあります。

- 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されたレポートに適している文字。
  - 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 スキーマ定義（XSD）を使用した、判読可能なフォーマットです。XML 形式では、シスコ TAC と通信できます。
- 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。

Smart Call Home 宛先プロファイル

Smart Call Home 宛先プロファイルには、次の情報が含まれています。

- 1 つ以上のアラート グループ：アラートの発生時に、特定の Smart Call Home メッセージを送信するアラートのグループ。

- 1 つ以上の電子メール宛先：この宛先プロファイルに割り当てられたアラート グループによって生成された Smart Call Home メッセージの受信者リスト。
- メッセージ フォーマット：Smart Call Home メッセージのフォーマット（ショート テキスト、フル テキスト、または XML）。
- メッセージ重大度：スイッチ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、スイッチ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 Nexus スイッチは、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。
- 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、スイッチは 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。

表 *16*：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。

アラート グループ	説明	実行されるコマンド
診断	診断によって生成されたイベント。	**show diagnostic result module all detail** **show moduleshow version** **show tech-support platform callhome**
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 moduleshow version** **show tech-support platform callhome**
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 moduleshow version** **show tech-support platform callhome**
設定（Configuration）	設定に関連した定期的なイベント。	**show version** **show module** **show running-config all** **show startup-config**
システム	装置の動作に重要なソフトウェア システムの障害によって生成されるイベント	**show system redundancy status** **show tech-support**
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 1000** **show module show version** **show tech-support platform callhome**
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 module** **show version** **show license usage** **show inventory** **show sprom all** **show system uptime**

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。各宛先プロファイル（定義済みおよびユーザ定義）を、Smart Call Home メッセージ レベルしきい値にアソシエートすることができます。宛先プロファイルのこのしきい値よりも小さい値を持つ Smart Call Home メッセージは、スイッチによって生成されません。Smart Call Home メッセージ レベルの範囲は 0（緊急度が最小）～9（緊急度が最大）です。デフォルトは 0 です（スイッチはすべてのメッセージを送信します）。

syslog アラート グループに送信される Smart Call Home メッセージでは、syslog の重大度が Smart Call Home のメッセージ レベルにマッピングされます。

（注） Smart Call Home は、メッセージ テキストで syslog メッセージ レベルを変更しません。

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

表 *17*： 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。

Smart Call Home レベル	キーワード	Syslog レベル	説明
4	Minor	エラー（3）	軽微な状態。
3	Warning	警告（4）	警告状態。
2	Notification	通知（5）	基本的な通知および情報メッセージです。
1	Normal	情報（6）	標準状態に戻ることを示す標準イベントです。
0	Debugging	デバッグ（7）	デバッグ メッセージ。

Call Home のメッセージ形式

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
- すべてのフル テキストと XML メッセージに共通のフィールド
- 対処的または予防的イベント メッセージに挿入されるフィールド
- コンポーネント イベント メッセージの挿入フィールド
- ユーザが作成したテスト メッセージの挿入フィールド

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。

表 *18*：ショート テキスト メッセージ フォーマット

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

次の表に、フル テキストまたは XML の共通するイベント メッセージ形式について説明します。

表 *19*：すべてのフル テキストと *XML* メッセージに共通のフィールド

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）
タイム スタンプ	ISO 時刻通知でのイベントの日付/タイム スタンプ *YYYY-MM-DDHH:MM:SS GMT+HH:MM*	/aml/header/time
メッセージ名	メッセージの名前。特定のイベント名は上記の表に記載。	/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	ルーティングのための製品タイプ。	/aml/header/source
デバイス ID	メッセージを生成したエンドデバイスの固有デバイス識別情報（UDI）。メッセージがデバイスに対して固有でない場合は、このフィールドを空にする必要があります。形式は、*type@Sid@serial*。 • *type* は、バックプレーン IDPROM からの製品の型番。 • @ は区切り文字です。 • *Sid* は C で、シリアル ID をシャーシ シリアル番号として特定します。 • *serial* は、Sid フィールドによって識別される番号です。 例：WS-C6509@C@12345678	/aml/ header/deviceID

データ項目（プレーン テキストおよび XML）	説明（プレーン テキストおよび XML）	XML タグ（XML のみ）
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
契約 ID	サポート サービスによって契約情報やその他の ID に使用されるオプションのユーザ設定可能なフィールド。	/aml/ header /contractID
サイト ID	シスコが提供したサイト ID または別のサポート サービスにとって意味のあるその他のデータに使用されるオプションのユーザ設定可能なフィールド。	/aml/ header/siteID
サーバ ID	デバイスからメッセージが生成された場合、これはデバイスの Unique Device Identifier（UDI）フォーマットです。 形式は、*type@Sid@serial*。 • *type* は、バックプレーン IDPROM からの製品の型番。 • @ は区切り文字です。 • *Sid* は C で、シリアル ID をシャーシ シリアル番号として特定します。 • *serial* は、Sid フィールドによって識別される番号です。 例：WS-C6509@C@12345678	/aml/header/serverID
メッセージの説明	エラーを説明するショート テキスト	/aml/body/msgDesc
デバイス名	イベントが発生したノード（デバイスのホスト名）	/aml/body/sysName

データ項目（プレーン テキストおよび XML）	説明（プレーン テキストおよび XML）	XML タグ（XML のみ）
担当者名	イベントが発生したノード関連の問題について問い合わせる担当者名	/aml/body/sysContact
連絡先 E メール	この装置の担当者の E 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
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
特定のアラート グループ メッセージの固有のフィールドは、ここに挿入されます。		
このアラート グループに対して複数の CLI コマンドが実行されると、次のフィールドが繰り返される場合があります。		
コマンド出力名	実行された CLI コマンドの正確な名前	/aml/attachments/attachment/name
添付タイプ	特定のコマンド出力	/aml/attachments/attachment/type
MIME タイプ	プレーン テキストまたは符号化タイプ	/aml/attachments/attachment/mime
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

次の表に、フルテキストまたはXMLのリ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。

表 *20*：対処的または予防的イベントメッセージに挿入されるフィールド

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

次の表に、フルテキストまたはXML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。

表 *21*：コンポーネントイベントメッセージの挿入フィールド

データ項目（プレーンテキストおよび XML）	説明（プレーンテキストおよび XML）	XML タグ（XML のみ）
シャーシのハードウェアバージョン	シャーシのハードウェアバージョン	/aml/body/chassis/hwVersion
スーパーバイザモジュールソフトウェアバージョン	最上レベルのソフトウェアバージョン。	/aml/body/chassis/swVersion

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 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

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。

表 *22*：ユーザが作成したテスト メッセージの挿入フィールド

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
プロセス例外	原因コードの例外。	/aml/body/process/exception

Smart Call Home の注意事項および制約事項

- 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、スイッチは Smart Call Home メッセージを送信できません。
- 任意の SMTP 電子メール サーバで動作します。

Smart Call Home の前提条件

- 電子メール サーバに接続できる必要があります。
- コンタクト名（SNMP サーバのコンタクト）、電話番号、および住所情報へアクセスできる必要があります。
- スイッチと電子メール サーバ間に IP 接続が必要です。
- 設定するデバイスに対して有効なサービス契約が必要です。

Call Home のデフォルト設定

表 *23*： デフォルトの *Call Home* パラメータ

パラメータ（Parameters）	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	4000000
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	4000000
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
プロファイルとアラート グループの関連付け	フルテキスト宛先プロファイルおよびショートテキスト宛先プロファイルの場合はすべて。CiscoTAC-1 宛先プロファイルの場合は cisco-tac アラート グループ
フォーマット タイプ	XML
Call Home のメッセージ レベル	0（ゼロ）

Smart Call Home の設定

Smart Call Home の登録

はじめる前に

- ご使用のスイッチの sMARTnet 契約番号を確認してください
- 電子メール アドレスを確認してください
- Cisco.com ID を確認してください

手順

ステップ 1 ブラウザで、Smart Call Home Web ページに移動します。
http://www.cisco.com/go/smartcall/

ステップ 2 [Getting Started] で、Smart Call Home の登録指示に従ってください。

次の作業

連絡先情報を設定します。

連絡先情報の設定

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **snmp-server contact***sys-contact*	SNMP sysContact を設定します。
ステップ 3	switch(config)# **callhome**	Smart Call Home コンフィギュレーション モードを開始します。
ステップ 4	switch(config-callhome)# **email-contact***email-address*	スイッチの担当者の電子メール アドレスを設定します。

	コマンドまたはアクション	目的
		email-address には、電子メール アドレスの形式で、最大255の英数字を使用できます。 （注） 任意の有効なEメール アドレスを使用できます。アドレスには、空白を含めることはできません。
ステップ 5	switch(config-callhome)# **phone-contact***international-phone-number*	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。 *international-phone-number* は、最大17文字の英数字で、国際電話フォーマットにする必要があります。 （注） 電話番号には、空白を含めることはできません。番号の前にプラス（+）プレフィックスを使用します。
ステップ 6	switch(config-callhome)# **streetaddress***address*	スイッチの主担当者の住所を設定します。 *address* には、最大 255 の英数字を使用できます。スペースを使用できます。
ステップ 7	switch(config-callhome)# **contract-id***contract-number*	（任意） サービス契約からこのスイッチの契約番号を設定します。 *contract-number* には最大255の英数字を使用できます。
ステップ 8	switch(config-callhome)# **customer-id***customer-number*	（任意） サービス契約からこのスイッチのカスタマー番号を設定します。 *customer-number* には最大 255 の英数字を使用できます。
ステップ 9	switch(config-callhome)# **site-id***site-number*	（任意） このスイッチのサイト番号を設定します。 *site-number* は、最大255文字の英数字を自由なフォーマットで指定できます。
ステップ 10	switch(config-callhome)# **switch-priority***number*	（任意） このスイッチのスイッチ プライオリティを設定します。 指定できる範囲は 0 ～ 7 です。0 は最高のプライオリティを、7は最低のプライオリティを示します。デフォルト値は 7 です。

	コマンドまたはアクション	目的
		（注） スイッチのプライオリティは、運用要員または TAC サポート要員によって、最初に対処すべき Call Home メッセージを決定するために使用されます。各スイッチから送信される重大度が同じ Call Home アラートに優先順位を設定できます。
ステップ 11	switch# **show callhome**	（任意） Smart Call Home コンフィギュレーションの概要を表示します。
ステップ 12	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、Call Home に関する担当者情報を設定する例を示します。

```
switch# configuration terminal
switch(config)# snmp-server contact personname@companyname.com
switch(config)# callhome
switch(config-callhome)# email-contact personname@companyname.com
switch(config-callhome)# phone-contact +1-800-123-4567
switch(config-callhome)# street-address 123 Anystreet St., Anycity, Anywhere
```

次の作業

宛先プロファイルを作成します。

宛先プロファイルの作成

ユーザ定義の宛先プロファイルを作成し、新しい宛先プロファイルにメッセージ フォーマット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	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **callhome**	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
ステップ 3	switch(config-callhome)# **destination-profile** {**ciscoTAC-1** {**alert-group***group* | **email-addr***address* | **http***URL* | **transport-method** {**email** | **http**}} | *profilename* {**alert-group***group* | **email-addr***address* | **format** {**XML** | **full-txt** | **short-txt**} | **http***URL* | **message-level***level* | **message-size***size* | **transport-method** {**email** | **http**}} | **full-txt-destination** {**alert-group***group* | **email-addr***address* | **http***URL* | **message-level***level* | **message-size***size* | **transport-method** {**email** | **http**}} | **short-txt-destination** {**alert-group***group* | **email-addr***address* | **http***URL* | **message-level***level* | **message-size***size* | **transport-method** {**email** | **http**}}}	新しい宛先プロファイルを作成し、そのプロファイルのメッセージフォーマットを設定します。プロファイル名は、最大 31 文字の英数字で指定できます。 このコマンドについての詳細は、プラットフォームのコマンドリファレンスを参照してください。
ステップ 4	switch# **show callhome destination-profile** [**profile***name*]	（任意） 1 つまたは複数の宛先プロファイルに関する情報を表示します。
ステップ 5	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。

次に、Smart Call Home の宛先プロファイルを作成する例を示します。

```
switch# configuration terminal
switch(config)# callhome
switch(config-callhome)# destination-profile Noc101 format full-text
```

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。

- 宛先アドレス：アラートの送信先となる実際のアドレス（トランスポートメカニズムに関係します）。
- メッセージ フォーマット：アラート送信に使用されるメッセージ フォーマット（フル テキスト、ショート テキスト、または XML）。
- メッセージ レベル：この宛先プロファイルの 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 Call Home メッセージの長さ

（注） CiscoTAC-1 宛先プロファイルは変更または削除できません。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **callhome**	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	switch(config-callhome)# **destination-profile** {*name* | **full-txt-destination** | **short-txt-destination**} **email-addr***address*	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 E メール アドレスを設定できます。
ステップ 4	**destination-profile** {*name* | **full-txt-destination** | **short-txt-destination**} **message-level***number*	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。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。*number* に指定できる範囲は 0 ～ 9 です。9 は最大の重大度を示します。
ステップ 5	switch(config-callhome)# **destination-profile** {*name* | **full-txt-destination** | **short-txt-destination**} **message-size***number*	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。full-txt-destination の値の範囲は 0 ～ 5000000 で、デフォルトは 2500000 です。short-txt-destination の値の範囲は 0 ～ 100000 で、デフォルトは 4000 です。CiscoTAC-1 では、値は 5000000 で、これは変更不可能です。
ステップ 6	switch# **show callhome destination-profile** [**profile***name*]	（任意） 1 つまたは複数の宛先プロファイルに関する情報を表示します。
ステップ 7	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、Smart Call Home の宛先プロファイルを変更する例を示します。

```
switch# configuration terminal
switch(config)# callhome
switch(config-callhome)# destination-profile full-text-destination email-addr
person@example.com
switch(config-callhome)# destination-profile full-text-destination message-level 5
switch(config-callhome)# destination-profile full-text-destination message-size 10000
switch(config-callhome)#
```

次の作業

アラート グループと宛先プロファイルをアソシエートします。

アラート グループと宛先プロファイルの関連付け

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **callhome**	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	switch(config-callhome)# **destination-profile***name***alert-group** {**All** | **Cisco-TAC** | **Configuration** | **Diagnostic** | **Environmental** | **Inventory** | **License** | **Linecard-Hardware** | **Supervisor-Hardware** | **Syslog-group-port** | **System** | **Test**}	アラート グループをこの宛先プロファイルにアソシエートします。キーワード **All** を使用して、すべてのアラート グループをこの宛先プロファイルにアソシエートします。
ステップ 4	switch# **show callhome destination-profile** [**profile***name*]	（任意） 1 つまたは複数の宛先プロファイルに関する情報を表示します。
ステップ 5	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、すべてのアラート グループを宛先プロファイル Noc101 にアソシエートする例を示します。

```
switch# configuration terminal
switch(config)# callhome
switch(config-callhome)# destination-profile Noc101 alert-group All
switch(config-callhome)#
```

次の作業

オプションで **show** コマンドをアラート グループに追加し、SMTP 電子メール サーバを設定することができます。

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 個のユーザ定義 **show** コマンドを割り当てることができます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **callhome**	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	switch(config-callhome)# **alert-group** {**Configuration** | **Diagnostic** | **Environmental** | **Inventory** | **License** | **Linecard-Hardware** | **Supervisor-Hardware** | **Syslog-group-port** | **System** | **Test**} **user-def-cmd***show-cmd*	**show** コマンド出力を、このアラート グループに送信された 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。 （注） CiscoTAC-1 宛先プロファイルには、ユーザ定義の **show** コマンドを追加できません。
ステップ 4	switch# **show callhome user-def-cmds**	（任意） アラート グループに追加されたすべてのユーザ定義 **show** コマンドに関する情報を表示します。
ステップ 5	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、**show ip routing** コマンドを Cisco-TAC アラート グループに追加する例を示します。

```
switch# configuration terminal
switch(config)# callhome
switch(config-callhome)# alert-group Configuration user-def-cmd show ip routing
switch(config-callhome)#
```

次の作業

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

電子メール サーバの詳細の設定

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。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **callhome**	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	switch(config-callhome)# **transport email smtp-server***ip-address* [**port***number*] [**use-vrf***vrf-name*]	SMTP サーバを、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設定します。 番号の範囲は 1 ～ 65535 です。デフォルトのポート番号は 25 です。 この SMTP サーバと通信する際に使用するよう任意で VRF インスタンスを設定できます。
ステップ 4	switch(config-callhome)# **transport email from***email-address*	（任意） Smart Call Home メッセージの送信元電子メール フィールドを設定します。
ステップ 5	switch(config-callhome)# **transport email reply-to***email-address*	（任意） Smart Call Home メッセージの返信先電子メール フィールドを設定します。
ステップ 6	switch# **show callhome transport-email**	（任意） Smart Call Home の電子メール設定に関する情報を表示します。
ステップ 7	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、Smart Call Home メッセージの電子メール オプションを設定する例を示します。

```
switch# configuration terminal
switch(config)# callhome
switch(config-callhome)# transport email smtp-server 192.0.2.10 use-vrf Red
switch(config-callhome)# transport email from person@example.com
```

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

次の作業

定期的なインベントリ通知を設定します。

定期的なインベントリ通知の設定

ハードウェアのインベントリ情報に加えて、デバイス上で現在イネーブルになっているすべてのソフトウェア サービスおよび実行中のすべてのソフトウェア サービスのインベントリに関するメッセージを定期的に送信するようにスイッチを設定できます。スイッチは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。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **callhome**	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	switch(config-callhome)# **periodic-inventory notification** [**interval***days*] [**timeofday***time*]	定期的なインベントリ メッセージを設定します。 **interval** *days* の範囲は 1 ～ 30 日です。 デフォルトは 7 日です。 **timeofday** *time* は HH:MM フォーマットです。
ステップ 4	switch# **show callhome**	（任意） Smart Call Home に関する情報を表示します。
ステップ 5	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、定期的なインベントリ メッセージを 20 日ごとに生成するよう設定する例を示します。

```
switch# configuration terminal
switch(config)# callhome
switch(config-callhome)# periodic-inventory notification interval 20
switch(config-callhome)#
```

次の作業

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、スイッチは同じイベントについて受信する重複メッセージの数を制限します。2 時間の時間枠内で送信された重複メッセージの数が 30 メッセージを超えると、スイッチは同じアラート 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	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **callhome**	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	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	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、重複メッセージ抑制をディセーブルにする例を示します。

```
switch# configuration terminal
switch(config)# callhome
switch(config-callhome)# no duplicate-message throttle
switch(config-callhome)#
```

次の作業

Smart Call Home をイネーブルにします。

Smart Call Home のイネーブル化またはディセーブル化

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **callhome**	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	switch(config-callhome) # [**no**] **enable**	Smart Call Home をイネーブルまたはディセーブルにします。 Smart Call Home は、デフォルトでディセーブルです。
ステップ 4	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次の例は、Smart Call Home をイネーブルにする方法を示します。

```
switch# configuration terminal
switch(config)# callhome
switch(config-callhome)# enable
switch(config-callhome)#
```

次の作業

任意でテスト メッセージを生成します。

Smart Call Home 設定のテスト

はじめる前に

宛先プロファイルのメッセージ レベルが 2 以下に設定されていることを確認します。

重要 Smart Call Home のテストは、宛先プロファイルのメッセージ レベルが 3 以上に設定されている場合は失敗します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **callhome**	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	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	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	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次の例は、Smart Call Home をイネーブルにする方法を示します。

```
switch# configuration terminal
switch(config)# callhome
switch(config-callhome)# callhome send diagnostic
switch(config-callhome)# callhome test
switch(config-callhome)#
```

Smart Call Home 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。

コマンド	目的
show callhome	Smart Call Home のステータスを表示します。
show callhome destination-profile*name*	1 つまたは複数の Smart Call Home 宛先プロファイルを表示します。
show callhome pending-diff	保留中の Smart Call Home 設定と実行中の Smart Call Home 設定の違いを表示します。
show callhome status	Smart Call Home ステータスを表示します。

コマンド	目的
show callhome transport-email	Smart Call Home の電子メール設定を表示します。
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** | **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。

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。

```
source:MDS9000
Switch Priority:7
Device Id:WS-C6509@C@FG@07120011
Customer Id:Example.com
Contract Id:123
Site Id:San Jose
Server Id:WS-C6509@C@FG@07120011
Time of Event:2004-10-08T11:10:44
Message Name:SYSLOG_ALERT
Message Type:Syslog
Severity Level:2
System Name:10.76.100.177
Contact Name:User Name
Contact Email:person@example.com
Contact Phone:+1-408-555-1212
Street Address:#1234 Any Street, Any City, Any State, 12345
Event Description:2006 Oct  8 11:10:44 10.76.100.177 %PORT-5-IF_TRUNK_UP:
%$VLAN 1%$ Interface e2/5, vlan 1 is up
syslog_facility:PORT
start chassis information:
Affected Chassis:WS-C6509
Affected Chassis Serial Number:FG@07120011
Affected Chassis Hardware Version:0.104
Affected Chassis Software Version:3.1(1)
Affected Chassis Part No:73-8607-01
end chassis information:
```

XML 形式での syslog アラート通知の例

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。

```
From: example
Sent: Wednesday, April 25, 2007 7:20 AM
```

```
To: User (user)
Subject: System Notification From Router - syslog - 2007-04-25 14:19:55
GMT+00:00
<?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.example.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.example.com/services/DDCEService</aml-session:To>
<aml-session:Path>
<aml-session:Via>http://www.example.com/appliance/uri</aml-session:Via>
</aml-session:Path>
<aml-session:From>http://www.example.com/appliance/uri</aml-session:From>
<aml-session:MessageId>M2:69000101:C9D9E20B</aml-session:MessageId>
</aml-session:Session>
</soap-env:Header>
<soap-env:Body>
<aml-block:Block xmlns:aml-block="http://www.example.com/2004/01/aml-block">
<aml-block:Header>
<aml-block:Type>http://www.example.com/2005/05/callhome/syslog</aml-block:Type>
<aml-block:CreationDate>2007-04-25 14:19:55 GMT+00:00</aml-block:CreationDate>
<aml-block:Builder>
<aml-block:Name>Cat6500</aml-block:Name>
<aml-block:Version>2.0</aml-block:Version>
</aml-block:Builder>
<aml-block:BlockGroup>
<aml-block:GroupId>G3:69000101:C9F9E20C</aml-block:GroupId>
<aml-block:Number>0</aml-block:Number>
<aml-block:IsLast>true</aml-block:IsLast>
<aml-block:IsPrimary>true</aml-block:IsPrimary>
<aml-block:WaitForPrimary>false</aml-block:WaitForPrimary>
</aml-block:BlockGroup>
<aml-block:Severity>2</aml-block:Severity>
</aml-block:Header>
<aml-block:Content>
<ch:Call Home xmlns:ch="http://www.example.com/2005/05/callhome" version="1.0">
<ch:EventTime>2007-04-25 14:19:55 GMT+00:00</ch:EventTime>
<ch:MessageDescription>03:29:29: %CLEAR-5-COUNTERS: Clear counter on all
interfaces by console</ch:MessageDescription>
<ch:Event>
<ch:Type>syslog</ch:Type>
<ch:SubType>
</ch:SubType>
<ch:Brand>Cisco Systems</ch:Brand>
<ch:Series>Catalyst 6500 Series Switches</ch:Series>
</ch:Event>
<ch:CustomerData>
<ch:UserData>
<ch:Email>person@example.com</ch:Email>
</ch:UserData>
<ch:ContractData>
<ch:CustomerId>12345</ch:CustomerId>
<ch:SiteId>building 1</ch:SiteId>
<ch:ContractId>abcdefg12345</ch:ContractId>
<ch:DeviceId>WS-C6509@C@69000101</ch:DeviceId>
</ch:ContractData>
<ch:SystemInfo>
<ch:Name>Router</ch:Name>
<ch:Contact>
</ch:Contact>
<ch:ContactEmail>user@example.com</ch:ContactEmail>
<ch:ContactPhoneNumber>+1-408-555-1212</ch:ContactPhoneNumber>
<ch:StreetAddress>#1234 Any Street, Any City, Any State, 12345
</ch:StreetAddress>
</ch:SystemInfo>
</ch:CustomerData>
<ch:Device>
<rme:Chassis xmlns:rme="http://www.example.com/rme/4.0">
<rme:Model>WS-C6509</rme:Model>
<rme:HardwareVersion>1.0</rme:HardwareVersion>
<rme:SerialNumber>69000101</rme:SerialNumber>
<rme:AdditionalInformation>
```

```
<rme:AD name="PartNumber" value="73-3438-03 01" />
<rme:AD name="SoftwareVersion" value="4.0(20080421:012711)" />
</rme:AdditionalInformation>
</rme:Chassis>
</ch:Device>
</ch:Call Home>
</aml-block:Content>
<aml-block:Attachments>
<aml-block:Attachment type="inline">
<aml-block:Name>show logging</aml-block:Name>
<aml-block:Data encoding="plain">
Syslog logging: enabled (0 messages dropped, 0 messages
rate-limited, 0 flushes, 0 overruns, xml disabled, filtering disabled)
    Console logging: level debugging, 53 messages logged, xml disabled,
filtering disabled    Monitor logging: level debugging, 0 messages logged,
xml disabled,filtering disabled    Buffer logging: level debugging,
53 messages logged, xml disabled,      filtering disabled    Exception
Logging: size (4096 bytes)    Count and timestamp logging messages: disabled
    Trap logging: level informational, 72 message lines logged
Log Buffer (8192 bytes):
00:00:54: curr is 0x20000
00:00:54: RP: Currently running ROMMON from F2 region
00:01:05: %SYS-5-CONFIG_I: Configured from memory by console
00:01:09: %SYS-5-RESTART: System restarted --Cisco IOS Software,
s72033_rp Software (s72033_rp-ADVENTERPRISEK9_DBG-VM), Experimental
Version 12.2(20070421:012711) Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Thu 26-Apr-07 15:54 by xxx
Firmware compiled 11-Apr-07 03:34 by integ Build [100]00:01:01: %PFREDUN-6-ACTIVE:
 Initializing as ACTIVE processor for this switch00:01:01: %SYS-3-LOGGER_FLUSHED:
System was paused for 00:00:00 to ensure console debugging output.00:03:00: SP: SP:
 Currently running ROMMON from F1 region00:03:07: %C6K_PLATFORM-SP-4-CONFREG_BREAK
_ENABLED: The default factory setting for config register is 0x2102.It is advisable
 to retain 1 in 0x2102 as it prevents returning to ROMMON when break is issued.00:03:18:
 %SYS-SP-5-RESTART: System restarted --Cisco IOS Software, s72033_sp Software
 (s72033_sp-ADVENTERPRISEK9_DBG-VM), Experimental Version 12.2(20070421:012711)Copyright
 (c) 1986-2007 by Cisco Systems, Inc.
Compiled Thu 26-Apr-07 18:00 by xxx
00:03:18: %SYS-SP-6-BOOTTIME: Time taken to reboot after reload =  339 seconds
00:03:18: %OIR-SP-6-INSPS: Power supply inserted in slot 1
00:03:18: %C6KPWR-SP-4-PSOK: power supply 1 turned on.
00:03:18: %OIR-SP-6-INSPS: Power supply inserted in slot00:01:09: %SSH-5-ENABLED:
 SSH 1.99 has been enabled
00:03:18: %C6KPWR-SP-4-PSOK: power supply 2 turned on.
00:03:18: %C6KPWR-SP-4-PSREDUNDANTMISMATCH: power supplies rated outputs do not match.
00:03:18: %C6KPWR-SP-4-PSREDUNDANTBOTHSUPPLY: in power-redundancy mode, system is
 operating on both power supplies.
00:01:10: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
00:01:10: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
00:03:20: %C6KENV-SP-4-FANHIOUTPUT: Version 2 high-output fan-tray is in effect
00:03:22: %C6KPWR-SP-4-PSNOREDUNDANCY: Power supplies are not in full redundancy,
 power usage exceeds lower capacity supply
00:03:26: %FABRIC-SP-5-FABRIC_MODULE_ACTIVE: The Switch Fabric Module in slot 6
 became active.
00:03:28: %DIAG-SP-6-RUN_MINIMUM: Module 6: Running Minimal Diagnostics...
00:03:50: %DIAG-SP-6-DIAG_OK: Module 6: Passed Online Diagnostics
00:03:50: %OIR-SP-6-INSCARD: Card inserted in slot 6, interfaces are now online
00:03:51: %DIAG-SP-6-RUN_MINIMUM: Module 3: Running Minimal Diagnostics...
00:03:51: %DIAG-SP-6-RUN_MINIMUM: Module 7: Running Minimal Diagnostics...
00:03:51: %DIAG-SP-6-RUN_MINIMUM: Module 9: Running Minimal Diagnostics...
00:01:51: %MFIB_CONST_RP-6-REPLICATION_MODE_CHANGE: Replication Mode Change Detected.
 Current system replication mode is Ingress
00:04:01: %DIAG-SP-6-DIAG_OK: Module 3: Passed Online Diagnostics
00:04:01: %OIR-SP-6-DOWNGRADE: Fabric capable module 3 not at an appropriate hardware
 revision level, and can only run in flowthrough mode
00:04:02: %OIR-SP-6-INSCARD: Card inserted in slot 3, interfaces are now online
00:04:11: %DIAG-SP-6-DIAG_OK: Module 7: Passed Online Diagnostics
00:04:14: %OIR-SP-6-INSCARD: Card inserted in slot 7, interfaces are now online
00:04:35: %DIAG-SP-6-DIAG_OK: Module 9: Passed Online Diagnostics
00:04:37: %OIR-SP-6-INSCARD: Card inserted in slot 9, interfaces are now online
00:00:09: DaughterBoard (Distributed Forwarding Card 3)
Firmware compiled 11-Apr-07 03:34 by integ Build [100]
00:00:22: %SYS-DFC4-5-RESTART: System restarted --
Cisco DCOS Software, c6lc2 Software (c6lc2-SPDBG-VM), Experimental Version 4.0
```

```
(20080421:012711)Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 26-Apr-08 17:20 by xxx
00:00:23: DFC4: Currently running ROMMON from F2 region
00:00:25: %SYS-DFC2-5-RESTART: System restarted --
Cisco IOS Software, c6slc Software (c6slc-SPDBG-VM), Experimental Version 12.2
(20070421:012711)Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Thu 26-Apr-08 16:40 by username1
00:00:26: DFC2: Currently running ROMMON from F2 region
00:04:56: %DIAG-SP-6-RUN_MINIMUM: Module 4: Running Minimal Diagnostics...
00:00:09: DaughterBoard (Distributed Forwarding Card 3)
Firmware compiled 11-Apr-08 03:34 by integ Build [100]
slot_id is 8
00:00:31: %FLASHFS_HES-DFC8-3-BADCARD: /bootflash:: The flash card seems to
 be corrupted
00:00:31: %SYS-DFC8-5-RESTART: System restarted --
Cisco DCOS Software, c6lc2 Software (c6lc2-SPDBG-VM), Experimental Version 4.0
(20080421:012711)Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 26-Apr-08 17:20 by username1
00:00:31: DFC8: Currently running ROMMON from S (Gold) region
00:04:59: %DIAG-SP-6-RUN_MINIMUM: Module 2: Running Minimal Diagnostics...
00:05:12: %DIAG-SP-6-RUN_MINIMUM: Module 8: Running Minimal Diagnostics...
00:05:13: %DIAG-SP-6-RUN_MINIMUM: Module 1: Running Minimal Diagnostics...
00:00:24: %SYS-DFC1-5-RESTART: System restarted --
Cisco DCOS Software, c6slc Software (c6slc-SPDBG-VM), Experimental Version 4.0
(20080421:012711)Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 26-Apr-08 16:40 by username1
00:00:25: DFC1: Currently running ROMMON from F2 region
00:05:30: %DIAG-SP-6-DIAG_OK: Module 4: Passed Online Diagnostics
00:05:31: %SPAN-SP-6-SPAN_EGRESS_REPLICATION_MODE_CHANGE: Span Egress HW
Replication Mode Change Detected. Current replication mode for unused asic
 session 0 is Centralized
00:05:31: %SPAN-SP-6-SPAN_EGRESS_REPLICATION_MODE_CHANGE: Span Egress HW
Replication Mode Change Detected. Current replication mode for unused asic
 session 1 is Centralized
00:05:31: %OIR-SP-6-INSCARD: Card inserted in slot 4, interfaces are now online
00:06:02: %DIAG-SP-6-DIAG_OK: Module 1: Passed Online Diagnostics
00:06:03: %OIR-SP-6-INSCARD: Card inserted in slot 1, interfaces are now online
00:06:31: %DIAG-SP-6-DIAG_OK: Module 2: Passed Online Diagnostics
00:06:33: %OIR-SP-6-INSCARD: Card inserted in slot 2, interfaces are now online
00:04:30: %XDR-6-XDRIPCNOTIFY: Message not sent to slot 4/0 (4) because of IPC
 error timeout. Disabling linecard. (Expected during linecard OIR)
00:06:59: %DIAG-SP-6-DIAG_OK: Module 8: Passed Online Diagnostics
00:06:59: %OIR-SP-6-DOWNGRADE_EARL: Module 8 DFC installed is not identical to
 system PFC and will perform at current system operating mode.
00:07:06: %OIR-SP-6-INSCARD: Card inserted in slot 8, interfaces are now online
Router#
</aml-block:Data>
</aml-block:Attachment>
</aml-block:Attachments>
</aml-block:Block>
</soap-env:Body>
</soap-env:Envelope>
```

第 12 章

ロールバックの設定

この章の内容は、次のとおりです。

- ロールバックについて，157 ページ
- ロールバックの注意事項および制約事項，157 ページ
- チェックポイントの作成，158 ページ
- ロールバックの実装，159 ページ
- ロールバック コンフィギュレーションの確認，160 ページ

ロールバックについて

ロールバック機能を使用すると、Cisco NX-OS の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、スイッチ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スイッチに再適用できます。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。

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、atomic ロールバックを発生させることができます。atomic ロールバックでは、エラーが発生しなかった場合に限り、ロールバックを実行します。

ロールバックの注意事項および制約事項

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。
- あるスイッチのチェックポイント ファイルを別のスイッチに適用することはできません。
- チェックポイント ファイル名の長さは、最大 75 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。
- FCoE をイネーブルにすると、チェック ポイントおよび設定のロール バックの機能はディセーブルになります。
- 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。
- **write erase** および **reload** コマンドを入力すると、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。
- ブートフラッシュでチェックポイントを作成した場合、ロールバックの実行前は実行システム コンフィギュレーションとの違いは実行できず、「変更なし」と報告されます。
- チェック ポイントはスイッチに対してローカルです。
- **checkpoint** および **checkpoint***checkpoint_name* コマンドを使用して作成されたチェックポイントは、すべてのスイッチの 1 つのスイッチオーバーに対して存在します。
- 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で上書きすることはできません。
- チェックポイントは、アップグレード後またはダウングレード後にサポートされません。
- 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。

チェックポイントの作成

1 台のスイッチで作成できるコンフィギュレーションの最大チェックポイント数は 10 です。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **checkpoint** { [*cp-name*] [**description** *descr*] |**file***file-name* 例： `switch# checkpoint stable`	ユーザチェックポイント名またはファイルのいずれかに対して、実行中のコンフィギュレーションのチェックポイントを作成します。チェックポイント名には最大 80 文字の任意の英数字を使用できますが、スペースを含めることはできません。チェックポイント名を指定しなかった場合、Cisco NX-OS はチェックポイント名を user-checkpoint-<number> に設定します。ここで number は 1 ～ 10 の値です。 description には、スペースも含めて最大 80 文字の英数字を指定できます。
ステップ 2	switch# **no checkpoint***cp-name* 例： `switch# no checkpoint stable`	（任意） **checkpoint** コマンドの **no** 形式を使用すると、チェックポイント名を削除できます。 **delete** コマンドを使用して、チェックポイント ファイルを削除できます。
ステップ 3	switch# **show checkpoint***cp-name* 例： [**all**] `switch# show checkpoint stable`	（任意） チェックポイント名の内容を表示します。

ロールバックの実装

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

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

手順

	コマンドまたはアクション	目的
ステップ 1	**show diff rollback-patch** {**checkpoint** *src-cp-name* | **running-config** | **startup-config** | **file** *source-file*} {**checkpoint** *dest-cp-name* | **running-config** | **startup-config** | **file** *dest-file*} 例： `switch# show diff rollback-patch checkpoint stable running-config`	ソースと宛先のチェックポイント間の差異を表示します。
ステップ 2	**rollback running-config** {**checkpoint** *cp-name* | **file** *cp-file*} **atomic** 例： `switch# rollback running-config checkpoint stable`	エラーが発生しなければ、指定されたチェックポイント名またはファイルへの atomic ロール バックを作成します。

チェックポイント ファイルを作成し、次に、ユーザ チェックポイント名への atomic ロール バックを実装する例を以下に示します。

```
switch# checkpoint stable
switch# rollback running-config checkpoint stable atomic
```

ロールバック コンフィギュレーションの確認

ロールバックの設定を確認するには、次のコマンドを使用します。

コマンド	目的
show checkpoint *name* [**all**]	チェックポイント名の内容を表示します。
show checkpoint all [**user** | **system**]	現行のスイッチ内の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**]	現在のスイッチ内のすべてのチェックポイントのリストを表示します。表示されるチェックポイントを、ユーザまたはシステムで生成されるチェックポイントに限定できます。
show diff rollback-patch {**checkpoint** *src-cp-name* | **running-config** | **startup-config** | **file** *source-file*} {**checkpoint** *dest-cp-name* | **running-config** | **startup-config** | **file** *dest-file*}	ソースと宛先のチェックポイント間の差異を表示します。

コマンド	目的
show rollback log [**exec** | **verify**]	ロールバック ログの内容を表示します。

（注） 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。

第 13 章

DNS の設定

この章の内容は、次のとおりです。

- DNS クライアントに関する情報，163 ページ
- DNS クライアントの前提条件，164 ページ
- DNS クライアントのライセンス要件，164 ページ
- DNS クライアントのデフォルト設定，165 ページ
- DNS クライアントの設定，165 ページ

DNS クライアントに関する情報

自分で名前の割り当てを管理していないネットワーク内のデバイスとの接続を、ネットワーク デバイスが必要とする場合は、DNS を使用して、ネットワーク間でデバイスを特定する一意のデバイス名を割り当てることができます。DNS は、階層方式を使用して、ネットワーク ノードのホスト名を確立します。これにより、クライアントサーバ方式によるネットワークのセグメントのローカル制御が可能となります。DNS システムは、デバイスのホスト名をその関連する IP アドレスに変換することで、ネットワーク デバイスを検出できます。

インターネット上のドメインは、組織のタイプや場所に基づく一般的なネットワークのグループを表す命名階層ツリーの一部です。ドメイン名は、ピリオド（.）を区切り文字として使用して構成されています。たとえば、シスコは、インターネットでは com ドメインで表される営利団体であるため、そのドメイン名は cisco.com です。このドメイン内の特定のホスト名、たとえばファイル転送プロトコル（FTP）システムは ftp.cisco.com で識別されます。

ネーム サーバ

ネームサーバはドメイン名の動向を把握し、自身が完全な情報を持っているドメインツリーの部分を認識しています。ネームサーバは、ドメインツリーの他の部分の情報を格納している場合も

あります。Cisco NX-OS 内の IP アドレスにドメイン名をマッピングするには、最初にホスト名を示し、その後にネーム サーバを指定して、DNS サービスをイネーブルにする必要があります。

Cisco NX-OS では、スタティックに IP アドレスをドメイン名にマッピングできます。また、1 つ以上のドメイン ネーム サーバを使用してホスト名の IP アドレスを見つけるよう、Cisco NX-OS を設定することもできます。

DNS の動作

ネーム サーバは、次に示すように、特定のゾーン内でローカルに定義されるホストの DNS サーバに対してクライアントが発行したクエリーを処理します。

- 権限ネーム サーバは、その権限ゾーン内のドメイン名を求める DNS ユーザ照会に、自身のホストテーブル内にキャッシュされた永久的なエントリを使用して応答します。照会で求められているのが、自身の権限ゾーン内であるが、設定情報が登録されていないドメイン名の場合、権限ネーム サーバはその情報が存在しないと応答します。
- 権限ネーム サーバとして設定されていないネーム サーバは、以前に受信した照会への返信からキャッシュした情報を使用して、DNS ユーザ照会に応答します。ゾーンの権限ネーム サーバとして設定されたルータがない場合は、ローカルに定義されたホストを求める DNS サーバへの照会には、正規の応答は送信されません。

ネームサーバは、特定のドメインに設定された転送パラメータおよびルックアップパラメータに従って、DNS 照会に応答します（着信 DNS 照会を転送するか、内部的に生成された DNS 照会を解決します）。

ハイ アベイラビリティ

Cisco NX-OS は、DNS クライアントのステートレス 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。

DNS クライアントの前提条件

DNS クライアントには次の前提条件があります。

- ネットワーク上に DNS ネーム サーバが必要です。

DNS クライアントのライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	DNS にはライセンスは不要です。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

DNS クライアントのデフォルト設定

次の表に、DNS クライアント 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
DNS クライアント	イネーブル

DNS クライアントの設定

ネットワーク上の DNS サーバを使用するよう、DNS クライアントを設定できます。

はじめる前に

- ネットワーク上にドメイン ネーム サーバが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	switch# **configuration terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# vrf context managment	設定可能な仮想およびルーティング（VRF）名を指定します。
ステップ 3	switch(config)# **ip host***name address1 [address2... address6]*	ホスト名キャッシュに、6 つまでのスタティック ホスト名/アドレス マッピングを定義します。
ステップ 4	switch(config)# **ip domain name***name* [**use-vrf***vrf-name*]	（任意） Cisco NX-OS が非完全修飾ホスト名に使用するデフォルトのドメイン ネーム サーバを定義します。このドメイン名を設定した VRF でこのドメイン ネーム サーバを解決できない場合は、任意で、Cisco NX-OS がこのドメイン ネーム サーバを解決するために使用する VRF を定義することもできます。

	コマンドまたはアクション	目的
		Cisco NX-OS は、ドメイン名ルックアップを開始する前に、完全なドメイン名を含まないあらゆるホスト名にデフォルト ドメイン名を追加します。
ステップ 5	switch(config)# **ip domain-list***name* [**use-vrf***vrf-name*]	（任意） Cisco NX-OS が非完全修飾ホスト名に使用できる追加のドメイン ネーム サーバを定義します。このドメイン名を設定した VRF でこのドメイン ネーム サーバを解決できない場合は、任意で、Cisco NX-OS がこのドメイン ネーム サーバを解決するために使用する VRF を定義することもできます。 Cisco NX-OS はドメイン リスト内の各エントリを使用して、ドメイン名ルックアップを開始する前に、完全なドメイン名を含まないあらゆるホスト名にこのドメイン名を追加します。Cisco NX-OS は、一致するものが見つかるまで、ドメイン リストの各エントリにこれを実行します。
ステップ 6	switch(config)# **ip name-server** *server-address1 [server-address2... server-address6]* [**use-vrf***vrf-name*]	（任意） 最大 6 台のネーム サーバを定義します。使用可能なアドレスは、IPv4 アドレスまたは IPv6 アドレスです。 このネーム サーバを設定した VRF でこのネーム サーバに到達できない場合は、任意で、Cisco NX-OS がこのネーム サーバに到達するために使用する VRF を定義することもできます。
ステップ 7	switch(config)# **ip domain-lookup**	（任意） DNS ベースのアドレス変換をイネーブルにします。この機能は、デフォルトでイネーブルにされています。
ステップ 8	switch(config)# **show hosts**	（任意） DNS に関する情報を表示します。
ステップ 9	switch(config)# **exit**	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 10	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、デフォルト ドメイン名を設定し、DNS ルックアップをイネーブルにする例を示します。

```
switch# config t
switch(config)# vrf context management
switch(config)# ip domain-name mycompany.com
switch(config)# ip name-server 172.68.0.10
switch(config)# ip domain-lookup
```

第 14 章

SNMP の設定

この章の内容は、次のとおりです。

- SNMP について，169 ページ
- SNMP のライセンス要件，174 ページ
- SNMP の注意事項および制約事項，174 ページ
- SNMP のデフォルト設定，174 ページ
- SNMP の設定，175 ページ
- SNMP のディセーブル化，189 ページ
- SNMP 設定の確認，189 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。

- 管理情報ベース（Management Information Base）：SNMP エージェントの管理対象オブジェクトのコレクション

（注） Cisco NX-OS は、イーサネット MIB の SNMP セットをサポートしません。

Cisco Nexus 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 は、RFC 3410（http://tools.ietf.org/html/rfc3410）、RFC 3411（http://tools.ietf.org/html/rfc3411）、RFC 3412（http://tools.ietf.org/html/rfc3412）、RFC 3413（http://tools.ietf.org/html/rfc3413）、RFC 3414（http://tools.ietf.org/html/rfc3414）、RFC 3415（http://tools.ietf.org/html/rfc3415）、RFC 3416（http://tools.ietf.org/html/rfc3416）、RFC 3417（http://tools.ietf.org/html/rfc3417）、RFC 3418（http://tools.ietf.org/html/rfc3418）、および RFC 3584（http://tools.ietf.org/html/rfc3584）で定義されています。

SNMP 通知

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

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

トラップの信頼性はインフォームより低くなります。SNMP マネージャはトラップを受信しても確認応答（ACK）を送信しないからです。このため、トラップが受信されたかどうかをスイッチが判断できません。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。Cisco Nexus 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。

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。

表 *24*：***SNMP*** セキュリティ モデルおよびセキュリティ レベル

モデル	レベル	認証	暗号化	結果
v1	noAuthNoPriv	コミュニティ ストリング	No	コミュニティ ストリングの照合を使用して認証します。
v2c	noAuthNoPriv	コミュニティ ストリング	No	コミュニティ ストリングの照合を使用して認証します。

モデル	レベル	認証	暗号化	結果
v3	authNoPriv	HMAC-MD5 または HMAC-SHA	No	Hash-Based Message Authentication Code（HMAC）メッセージダイジェスト 5（MD5）アルゴリズムまたは HMAC Secure Hash Algorithm（SHA）アルゴリズムに基づいて認証します。
v3	authPriv	HMAC-MD5 または HMAC-SHA	DES	HMAC-MD5 アルゴリズムまたは HMAC-SHA アルゴリズムに基づいて認証します。データ暗号規格（DES）の 56 ビット暗号化、および暗号ブロック連鎖（CBC）DES（DES-56）標準に基づいて認証します。

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。
- メッセージの発信元の認証：データを受信したユーザが提示した ID の発信元を確認します。
- メッセージの機密性：情報が使用不可であること、または不正なユーザ、エンティティ、またはプロセスに開示されないことを保証します。

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

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

- HMAC-MD5-96 認証プロトコル

- HMAC-SHA-96 認証プロトコル

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

priv オプションで、SNMP セキュリティ暗号化方式として、DES または 128 ビット AES 暗号化を選択できます。**priv** オプションと **aes-128** トークンを併用すると、このプライバシー パスワードは 128 ビットの AES キー番号を生成するためのパスワードになります。AES priv パスワードは、8 文字以上の長さにできます。パスフレーズをクリア テキストで指定する場合、最大 64 文字を指定できます。ローカライズド キーを使用する場合は、最大 130 文字を指定できます。

（注） 外部の AAA サーバを使用して SNMPv3 を使う場合、外部 AAA サーバのユーザ設定でプライバシー プロトコルに AES を指定する必要があります。

CLI および SNMP ユーザの同期

SNMPv3 ユーザ管理は、Access Authentication and Accounting（AAA）サーバ レベルで集中化できます。この中央集中型ユーザ管理により、Cisco NX-OSの SNMP エージェントは AAA サーバのユーザ認証サービスを利用できます。ユーザ認証が検証されると、SNMP PDU の処理が進行します。AAA サーバはユーザ グループ名の格納にも使用されます。SNMP はグループ名を使用して、スイッチでローカルに使用できるアクセス ポリシーまたはロール ポリシーを適用します。

ユーザ グループ、ロール、またはパスワードの設定が変更されると、SNMP と AAA の両方のデータベースが同期化されます。

Cisco NX-OSは、次のようにユーザ設定を同期化します。

- **snmp-server user** コマンドで指定された **auth** パスフレーズは、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は、SNMP ユーザの **auth** および **priv** パスフレーズになります。
- SNMP または CLI を使用してユーザを作成または削除すると、SNMP と CLI の両方でユーザが作成または削除されます。
- ユーザとロールの対応関係の変更は、SNMP と CLI で同期化されます。
- ロール変更（CLI からの削除または変更）は、SNMP と同期化されます。

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

グループベースの SNMP アクセス

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

SNMP アクセス権は、グループ別に編成されます。SNMP 内の各グループは、CLI を使用する場合のロールに似ています。各グループは 3 つのアクセス権により定義されます。つまり、読み取りアクセス、書き込みアクセス、および通知アクセスです。それぞれのアクセスを、各グループでイネーブルまたはディセーブルに設定できます。

ユーザ名が作成され、ユーザのロールが管理者によって設定され、ユーザがそのロールに追加されていれば、そのユーザはエージェントとの通信を開始できます。

SNMP のライセンス要件

この機能には、ライセンスは必要ありません。ライセンス パッケージに含まれていない機能はすべてCisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

SNMP の注意事項および制約事項

Cisco NX-OS は、イーサネット MIB への読み取り専用アクセスをサポートします。

サポートされる MIB の詳細については、次の URL を参照してください。

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Cisco NX-OS では、SNMPv3 noAuthNoPriv セキュリティ レベルはサポートされていません。

SNMP のデフォルト設定

表 *25*： デフォルトの *SNMP* パラメータ

パラメータ（Parameters）	デフォルト
ライセンス通知	イネーブル
linkUp/Down 通知タイプ	ietf-extended

SNMP の設定

SNMP ユーザの設定

（注） Cisco NX-OS で SNMP ユーザを設定するために使用するコマンドは、Cisco IOS でユーザを設定するために使用されるものとは異なります。

手順

	コマンドまたはアクション	目的

ステップ 1	**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	switch(config)# **snmp-server user***name* [**auth** {**md5** | **sha**} *passphrase* [**auto**] [**priv** [**aes-128**] *passphrase*] [**engineID***id*] [**localizedkey**]] 例： `switch(config)# snmp-server user Admin auth sha abcd1234 priv abcdefgh`	認証およびプライバシー パラメータのある SNMP ユーザを設定します。 パスフレーズには最大 64 文字の英数字を使用できます。大文字と小文字が区別されます。 **localizedkey** キーワードを使用する場合は、パスフレーズに大文字と小文字を区別した英数字を 130 文字まで使用できます。 engineID の形式は、12 桁のコロンで区切った 10 進数字です。
ステップ 3	switch# **show snmp user** 例： `switch(config) # show snmp user`	（任意） 1 人または複数の SNMP ユーザに関する情報を表示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、SNMP ユーザを設定する例を示します。

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# snmp-server user Admin auth sha abcd1234 priv abcdefgh
```

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、認証エラーで応答します。

SNMP メッセージの暗号化を特定のユーザに強制するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
switch(config)# **snmp-server user***name***enforcePriv**	このユーザに対して SNMP メッセージ暗号化を適用します。

SNMP メッセージの暗号化をすべてのユーザに強制するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
switch(config)# **snmp-server globalEnforcePriv**	すべてのユーザに対して SNMP メッセージ暗号化を適用します。

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。

コマンド	目的
switch(config)# **snmp-server user***namegroup*	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。

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。

コマンド	目的
switch(config)# **snmp-server community***namegroup* {**ro** | **rw**}	SNMP コミュニティ ストリングを作成します。

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）をコミュニティに割り当てて、着信 SNMP 要求にフィルタを適用できます。割り当てた ACL により着信要求パケットが許可される場合、SNMP はその要求を処理します。ACL により要求が拒否される場合、SNMP はその要求を廃棄して、システム メッセージを送信します。

ACL は次のパラメータで作成します。

- 送信元 IP アドレス
- 宛先 IP アドレス
- 送信元ポート
- 宛先ポート
- プロトコル（UDP または TCP）

ACL は、UDP および TCP を介する IPv4 および IPv6 の両方に適用されます。ACL を作成したら、ACL を SNMP コミュニティに割り当てます。

ヒント　ACL の作成の詳細については、使用している Cisco Nexus シリーズ ソフトウェアの NX-OS セキュリティ コンフィギュレーション ガイドを参照してください。

IPv4 または IPv6 ACL を SNMPv3 コミュニティに割り当てて SNMP 要求をフィルタするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
switch(config)# **snmp-server community***name* [**use-ipv4acl***ipv4acl-name*] [**use-ipv6acl***ipv6acl-name*] `switch(config)# snmp-server community public use-ipv4acl myacl`	SNMPv3 コミュニティに IPv4 ACL または IPv6 ACL を割り当てて SNMP 要求をフィルタします。

SNMP 通知レシーバの設定

複数のホスト レシーバーに対して SNMP 通知を生成するよう Cisco NX-OSを設定できます。

グローバル コンフィギュレーション モードで SNMPv1 トラップのホスト レシーバを設定できます。

コマンド	目的
switch(config)# **snmp-server host***ip-address***traps version 1***community* [**udp_port***number*]	SNMPv1 トラップのホスト レシーバを設定します。*ip-address* は IPv4 または IPv6 アドレスを使用できます。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。

グローバル コンフィギュレーション モードで SNMPv2c トラップまたはインフォームのホスト レシーバを設定できます。

コマンド	目的
switch(config)# **snmp-server host***ip-address* {**traps** | **informs**} **version 2c***community* [**udp_port***number*]	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。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。

グローバル コンフィギュレーション モードで SNMPv3 トラップまたはインフォームのホスト レシーバを設定できます。

コマンド	目的
switch(config)# **snmp-server host***ip-address* {**traps** | **informs**} **version 3** {**auth** | **noauth** | **priv**} *username* [**udp_port***number*]	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。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暗号解除するため、Cisco Nexus デバイスの SNMP engineID に基づくユーザ クレデンシャル（authKey/PrivKey）を認識していなければなりません。

次に、SNMPv1 トラップのホスト レシーバを設定する例を示します。

```
switch(config)# snmp-server host 192.0.2.1 traps version 1 public
```

次に、SNMPv2 インフォームのホスト レシーバを設定する例を示します。

```
switch(config)# snmp-server host 192.0.2.1 informs version 2c public
```

次に、SNMPv3 インフォームのホスト レシーバを設定する例を示します。

```
switch(config)# snmp-server host 192.0.2.1 informs version 3 auth NMS
```

VRF を使用する SNMP 通知レシーバの設定

設定された VRF をホスト レシーバに接続するように Cisco NX-OS を設定できます。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。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch#**snmp-server host***ip-address***use-vrf***vrf_name* [**udp_port***number*]	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 アドレスは、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。
ステップ 3	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、IP アドレス 192.0.2.1 の SNMP サーバ ホストを「Blue」という名前の VRF を使用するように設定する例を示します。

```
switch# configuration terminal
switch(config)# snmp-server host 192.0.2.1 use-vrf Blue
switch(config)# copy running-config startup-config
```

VRF に基づく SNMP 通知のフィルタリング

通知が発生した VRF に基づいて、Cisco NX-OS 通知をフィルタリングするように設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバルコンフィギュレーションモードを開始します。
ステップ 2	switch(config)# **snmp-server host***ip-address***filter-vrf***vrf_name* [**udp_port***number*]	設定された VRF に基づいて、通知ホストレシーバへの通知をフィルタリングします。IP アドレスは、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。
ステップ 3	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、VRF に基づいて SNMP 通知のフィルタリングを設定する例を示します。

```
switch# configuration terminal
switch(config)# snmp-server host 192.0.2.1 filter-vrf Red
switch(config)# copy running-config startup-config
```

すべての SNMP 通知を送信するための送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。

（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。

すべての SNMP 通知を送信するよう送信元インターフェイスを設定するには、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	**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	switch(config) # **snmp-server source-interface** {**traps** | **informs**} *if-type if-number* 例： `switch(config) # snmp-server source-interface traps ethernet 2/1`	SNMPv2c トラップまたは応答要求を送信するよう発信元インターフェイスを設定します。**?** を使用して、サポートされているインターフェイス タイプを特定します。

次に、SNMPv2c トラップを送信するよう送信元インターフェイスを設定する例を示します。

```
switch# configure terminal
switch(config) # snmp-server source-interface traps ethernet 2/1
```

次の作業

設定した送信元インターフェイスの情報を表示するには、**show snmp source-interface** コマンドを入力します。

SNMP 通知のホスト レシーバの設定

（注） 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。

すべての SNMP 通知を受信する、送信元インターフェイス上のホスト レシーバを設定するには、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	**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	switch(config) # **snmp-server host** *ip-address* **source-interface** *if-type if-number* [**udp_port** *number*] 例： `switch(config) # snmp-server host 192.0.2.1 source-interface traps ethernet 2/1`	SNMPv2c トラップまたはインフォームのホスト レシーバを設定します。*ip-address* は IPv4 または IPv6 アドレスを使用できます。**?** を使用して、サポートされているインターフェイス タイプを特定します。

次に、すべての SNMP 通知を受信する、送信元インターフェイスを設定する例を示します。

```
switch# config t
switch(config) # snmp-server host 192.0.2.1 source-interface ethernet 2/1
```

次の作業

設定した送信元インターフェイスの情報を表示するには、**show snmp source-interface** コマンドを入力します。

インバンド アクセスのための SNMP の設定

次のものを使用して、インバンド アクセス用に SNMP を設定できます。

- コンテキストのない SNMP v2 の使用：コンテキストにマッピングされたコミュニティを使用できます。この場合、SNMP クライアントはコンテキストについて認識する必要はありません。
- コンテキストのある SNMP v2 の使用：SNMP クライアントはコミュニティ、たとえば、<community>@<context> を指定して、コンテキストを指定する必要があります。
- SNMP v3 の使用：コンテキストを指定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)#**snmp-server context***context-name***vrf***vrf-name*	管理 VRF またはデフォルト VRF に SNMP コンテキストをマッピングします。カスタム VRF はサポートされません。名前には最大 32 の英数字を使用できます。

	コマンドまたはアクション	目的
ステップ 3	switch(config)# **snmp-server community***community-name***group***group-name*	SNMPv2c コミュニティと SNMP コンテキストにマッピングし、コミュニティが属するグループを識別します。名前には最大 32 の英数字を使用できます。
ステップ 4	switch(config)#**snmp-server mib community-map***community-name***context***context-name*	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。

次の SNMPv2 の例は、コンテキストに snmpdefault という名前のコミュニティをマッピングする方法を示しています。

```
switch# config t
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# snmp-server context def vrf default
switch(config)# snmp-server community snmpdefault group network-admin
switch(config)# snmp-server mib community-map snmpdefault context def
switch(config)#
```

次の SNMPv2 の例は、マッピングされていないコミュニティ comm を設定し、インバンドアクセスする方法を示しています。

```
switch# config t
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# snmp-server context def vrf default
switch(config)# snmp-server community comm group network-admin
switch(config)#
```

次の SNMPv3 の例は、v3 ユーザ名とパスワードを使用する方法を示しています。

```
switch# config t
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# snmp-server context def vrf default
switch(config)#
```

SNMP 通知のイネーブル化

通知をイネーブルまたはディセーブルにできます。通知名を指定しないと、Cisco NX-OSは通知をすべてイネーブルにします。

（注） **snmp-server enable traps** CLI コマンドを使用すると、設定通知ホスト レシーバーによっては、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 の通知をイネーブルにする CLI コマンドを示します。

表 *26*： ***SNMP*** 通知のイネーブル化

MIB	関連コマンド
すべての通知	**snmp-server enable traps**
BRIDGE-MIB	**snmp-server enable traps bridge newroot** **snmp-server enable traps bridge topologychange**
CISCO-AAA-SERVER-MIB	**snmp-server enable traps aaa**
ENITY-MIB、 CISCO-ENTITY-FRU-CONTROL-MIB、 CISCO-ENTITY-SENSOR-MIB	**snmp-server enable traps entity** **snmp-server enable traps entity fru**
CISCO-LICENSE-MGR-MIB	**snmp-server enable traps license**
IF-MIB	**snmp-server enable traps link**
CISCO-PSM-MIB	**snmp-server enable traps port-security**
SNMPv2-MIB	**snmp-server enable traps snmp** **snmp-server enable traps snmp authentication**
CISCO-FCC-MIB	**snmp-server enable traps fcc**
CISCO-DM-MIB	**snmp-server enable traps fcdomain**
CISCO-NS-MIB	**snmp-server enable traps fcns**
CISCO-FCS-MIB	**snmp-server enable traps fcs discovery-complete** **snmp-server enable traps fcs request-reject**
CISCO-FDMI-MIB	**snmp-server enable traps fdmi**
CISCO-FSPF-MIB	**snmp-server enable traps fspf**
CISCO-PSM-MIB	**snmp-server enable traps port-security**
CISCO-RSCN-MIB	**snmp-server enable traps rscn** **snmp-server enable traps rscn els** **snmp-server enable traps rscn ils**

MIB	関連コマンド
CISCO-ZS-MIB	**snmp-server enable traps zone** **snmp-server enable traps zone default-zone-behavior-change** **snmp-server enable traps zone enhanced-zone-db-change** **snmp-server enable traps zone merge-failure** **snmp-server enable traps zone merge-success** **snmp-server enable traps zone request-reject** **snmp-server enable traps zone unsupp-mem**
CISCO-CONFIG-MAN-MIB （注） ccmCLIRunningConfigChanged 通知を除き、MIB オブジェクトをサポートしていません。	**snmp-server enable traps config**

（注） ライセンス通知は、デフォルトではイネーブルです。

グローバルコンフィギュレーションモードで指定の通知をイネーブルにするには、次の作業を行います。

コマンド	目的
switch(config)# **snmp-server enable traps**	すべての SNMP 通知をイネーブルにします。
switch(config)# **snmp-server enable traps aaa** [**server-state-change**]	AAA SNMP 通知をイネーブルにします。
switch(config)# **snmp-server enable traps entity** [**fru**]	ENTITY-MIB SNMP 通知をイネーブルにします。
switch(config)# **snmp-server enable traps license**	ライセンス SNMP 通知をイネーブルにします。
switch(config)# **snmp-server enable traps port-security**	ポート セキュリティ SNMP 通知をイネーブルにします。
switch(config)# **snmp-server enable traps snmp** [**authentication**]	SNMP エージェント通知をイネーブルにします。

リンクの通知の設定

デバイスに対して、イネーブルにする linkUp/linkDown 通知を設定できます。次のタイプの linkUp/linkDown 通知をイネーブルにできます。

- cieLinkDown：シスコ拡張リンク ステート ダウン通知をイネーブルにします。
- cieLinkUp：シスコ拡張リンク ステート アップ通知をイネーブルにします。
- cisco-xcvr-mon-status-chg：シスコ インターフェイス トランシーバ モニタ ステータス変更通知をイネーブルにします。
- delayed-link-state-change：遅延リンク ステート変更をイネーブルにします。
- extended-linkUp：IETF 拡張リンク ステート アップ通知をイネーブルにします。
- extended-linkDown：IETF 拡張リンク ステート ダウン通知をイネーブルにします。
- linkDown：IETF リンク ステート ダウン通知をイネーブルにします。
- linkUp：IETF リンク ステート アップ通知をイネーブルにします。

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 enable traps link** [**cieLinkDown** | **cieLinkUp** | **cisco-xcvr-mon-status-chg** | **delayed-link-state-change**] | **extended-linkUp** | **extended-linkDown** | **linkDown** | **linkUp**] 例： `switch(config)# snmp-server enable traps link cieLinkDown`	リンク SNMP 通知をイネーブルにします。

インターフェイスでのリンク通知のディセーブル化

個別のインターフェイスで linkUp および linkDown 通知をディセーブルにできます。これにより、フラッピング インターフェイス（アップとダウン間の移行を繰り返しているインターフェイス）に関する通知を制限できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバルコンフィギュレーションモードを開始します。
ステップ 2	switch(config)# **interface***typeslot*/*port*	変更するインターフェイスを指定します。 （注） これが 10G ブレークアウト ポートの場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。
ステップ 3	switch(config -if)# **no snmp trap link-status**	インターフェイスの SNMP リンクステート トラップをディセーブルにします。この機能は、デフォルトでイネーブルにされています。

TCP での SNMP に対するワンタイム認証のイネーブル化

TCP セッション上で SNMP に対するワンタイム認証をイネーブルにできます。

コマンド	目的
switch(config)# **snmp-server tcp-session** [**auth**]	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。この機能はデフォルトで無効に設定されています。

SNMP スイッチの連絡先および場所の情報の割り当て

スイッチの連絡先情報（スペースを含めず、最大32文字まで）およびスイッチの場所を割り当てることができます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **snmp-server contact***name*	sysContact（SNMP 担当者名）を設定します。

	コマンドまたはアクション	目的
ステップ 3	switch(config)# **snmp-server location***name*	sysLocation（SNMP ロケーション）を設定します。
ステップ 4	switch# **show snmp**	（任意） 1 つまたは複数の宛先プロファイルに関する情報を表示します。
ステップ 5	switch# **copy running-config startup-config**	（任意） この設定変更を保存します。

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。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **snmp-server context** *context-name* [**instance** *instance-name*] [**vrf** *vrf-name*] [**topology** *topology-name*]	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。
ステップ 3	switch(config)# **snmp-server mib community-map** *community-name* **context** *context-name*	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	switch(config)# **no snmp-server context** *context-name* [**instance** *instance-name*] [**vrf** *vrf-name*] [**topology** *topology-name*]	（任意） 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。名前には最大 32 の英数字を使用できます。 （注） コンテキスト マッピングを削除する目的で、インスタンス、VRF、またはトポロジを入力しないでください。**instance**、**vrf**、または **topology** キーワードを使用すると、コンテキストとゼロ長ストリング間のマッピングが設定されます。

	コマンドまたはアクション	目的

SNMP のディセーブル化

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	switch(config) # **no snmp-server protocol enable** 例： `no snmp-server protocol enable`	SNMP をディセーブルにします。 SNMP は、デフォルトでディセーブルになっています。

SNMP 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 snmp	SNMP ステータスを表示します。
show snmp community	SNMP コミュニティストリングを表示します。
show snmp engineID	SNMP engineID を表示します。
show snmp group	SNMP ロールを表示します。
show snmp sessions	SNMP セッションを表示します。
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。

第 15 章

RMON の設定

この章の内容は、次のとおりです。

- RMON について，191 ページ
- RMON の設定時の注意事項および制約事項，193 ページ
- RMON の設定，193 ページ
- RMON 設定の確認，195 ページ
- デフォルトの RMON 設定，195 ページ

RMON について

RMON は、各種のネットワーク エージェントおよびコンソール システムがネットワーク モニタリング データを交換できるようにするための、Internet Engineering Task Force（IETF）標準モニタリング仕様です。Cisco NX-OS は、Cisco Nexus デバイスをモニタリングするための RMON アラーム、イベント、およびログをサポートします。

RMON アラームは、指定された期間、特定の管理情報ベース（MIB）オブジェクトをモニタリングし、指定されたしきい値でアラームを発生させ、別のしきい値でアラームをリセットします。アラームと RMON イベントを組み合わせて使用し、RMON アラームが発生したときにログ エントリまたは SNMP 通知を生成できます。

Cisco Nexus デバイスでは RMON はデフォルトでディセーブルに設定されており、イベントまたはアラームは設定されていません。RMON アラームおよびイベントを設定するには、CLI または SNMP 互換ネットワーク管理ステーションを使用します。

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、1.3.6.1.2.1.2.2.1.17 は ifOutOctets.17 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。

- モニタリングする MIB オブジェクト
- サンプリング間隔：MIB オブジェクトのサンプル値を収集するのに Cisco Nexus 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：Cisco Nexus 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：Cisco Nexus 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 Cisco Nexus デバイスが実行するアクション

（注） hcalarms オプションを使用して、アラームを 64 ビットの整数の MIB オブジェクトに設定します。

たとえば、エラー カウンタ MIB オブジェクトにデルタ タイプ上限アラームを設定できます。エラー カウンタ デルタがこの値を超えた場合、SNMP 通知を送信し、上限アラーム イベントを記録するイベントを発生させることができます。この上限アラームは、エラーカウンタのデルタ サンプルが下限しきい値を下回るまで再度発生しません。

（注） 下限しきい値には、上限しきい値よりも小さな値を指定してください。

RMON イベント

特定のイベントを各 RMON アラームにアソシエートさせることができます。RMON は次のイベント タイプをサポートします。

- SNMP 通知：関連したアラームが発生したときに、SNMP risingAlarm または fallingAlarm 通知を送信します。
- ログ：関連したアラームが発生した場合、RMON ログ テーブルにエントリを追加します。
- 両方：関連したアラームが発生した場合、SNMP 通知を送信し、RMON ログ テーブルにエントリを追加します。

下限アラームおよび上限アラームに異なるイベントを指定できます。

RMON の設定時の注意事項および制約事項

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 の設定

RMON アラームの設定

任意の整数の SNMP MIB オブジェクトに RMON アラームを設定できます。

次のパラメータを任意で指定することもできます。

- 上限および下限しきい値が指定値を超えた場合に発生させるイベント番号。
- アラームのオーナー

SNMP ユーザが設定され、SNMP 通知がイネーブルであることを確認します。

はじめる前に

SNMP ユーザが設定され、SNMP 通知がイネーブルであることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **rmon alarm***index mib-object sample-interval* {**absolute** | **delta**} **rising-threshold***value* [*event-index*] **falling-threshold***value* [*event-index*] [**owner***name*]	RMON アラームを作成します。値の範囲は -2147483647 ～ 2147483647 です。オーナー名は任意の英数字ストリングです。
ステップ 3	switch(config)# **rmon hcalarm***index mib-object sample-interval* {**absolute** | **delta**} **rising-threshold-high***value***rising-threshold-low***value* [*event-index*] **falling-threshold-high***value***falling-threshold-low***value* [*event-index*] [**owner***name*] [**storagetype***type*]	RMON 高容量アラームを作成します。値の範囲は -2147483647 ～ 2147483647 です。オーナー名は任意の英数字ストリングです。 ストレージ タイプの範囲は 1 ～ 5 です。

	コマンドまたはアクション	目的
ステップ 4	switch# **show rmon** {**alarms** | **hcalarms**}	（任意） RMON アラームまたは高容量アラームに関する情報を表示します。
ステップ 5	switch# **copy running-config startup-config**	（任意） この設定変更を保存します。

次に、RMON アラームを設定する例を示します。

```
switch# configure terminal
switch(config)# rmon alarm 1 1.3.6.1.2.1.2.2.1.17.83886080 5 delta rising-threshold 5 1
falling-threshold 0 owner test
switch(config)# exit
switch# show rmon alarms
Alarm 1 is active, owned by test
 Monitors 1.3.6.1.2.1.2.2.1.17.83886080 every 5 second(s)
 Taking delta samples, last value was 0
 Rising threshold is 5, assigned to event 1
 Falling threshold is 0, assigned to event 0
 On startup enable rising or falling alarm
```

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。

SNMP ユーザが設定され、SNMP 通知がイネーブルであることを確認します。

はじめる前に

SNMP ユーザが設定され、SNMP 通知がイネーブルであることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバルコンフィギュレーションモードを開始します。
ステップ 2	switch(config)# **rmon event***index* [**description***string*] [**log**] [**trap**] [**owner***name*]	RMON イベントを設定します。説明のストリングおよびオーナー名は、任意の英数字ストリングです。

	コマンドまたはアクション	目的
ステップ 3	switch(config)# **show rmon** {**alarms** | **hcalarms**}	（任意） RMONアラームまたは高容量アラームに関する情報を表示します。
ステップ 4	switch# **copy running-config startup-config**	（任意） この設定変更を保存します。

RMON 設定の確認

RMON の設定情報を確認するには、次のコマンドを使用します。

コマンド	目的
show 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。

デフォルトの RMON 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。

表 *27*： デフォルトの *RMON* パラメータ

パラメータ（Parameters）	デフォルト
アラーム	未設定
イベント	未設定

第 16 章

SPAN の設定

この章の内容は、次のとおりです。

- SPAN に関する情報，198 ページ
- SPAN ソース，198 ページ
- 送信元ポートの特性，198 ページ
- SPAN 宛先，199 ページ
- 宛先ポートの特性，199 ページ
- 複数の SPAN 宛先，200 ページ
- ACL を使用した SPAN，200 ページ
- SPAN on Drop，200 ページ
- SPAN-on-Latency セッション，200 ページ
- SPAN の注意事項および制約事項，201 ページ
- SPAN セッションの作成または削除，204 ページ
- イーサネット宛先ポートの設定，205 ページ
- SPAN セッションごとの MTU の切り捨ての設定，206 ページ
- 送信元ポートの設定，207 ページ
- SPAN セッションの説明の設定，208 ページ
- SPAN セッションに対する ACL フィルタの設定，209 ページ
- SPAN-on-Drop セッションの設定，210 ページ
- SPAN-on-Latency セッションの設定，211 ページ
- SPAN セッションのアクティブ化，213 ページ
- SPAN セッションの問題のトラブルシューティング，213 ページ

- SPAN 情報の表示，215 ページ
- SPAN ACL の設定例，216 ページ
- SPAN-on-Latency セッションの設定例，216 ページ

SPAN に関する情報

スイッチド ポート アナライザ（SPAN）機能（ポート ミラーリングまたはポート モニタリングとも呼ばれる）は、ネットワーク アナライザによる分析のためにネットワーク トラフィックを選択します。ネットワーク アナライザは、Cisco SwitchProbe またはその他のリモート モニタリング（RMON）プローブです。

SPAN ソース

SPAN 送信元とは、トラフィックをモニタリングできるインターフェイスを表します。Cisco Nexus デバイスは、SPAN 送信元として、イーサネット、ポート チャネル、SAN ポート チャネル、VSAN、および VLAN をサポートします。VLAN または VSAN では、指定された VLAN または VSAN でサポートされているすべてのインターフェイスが SPAN 送信元として含まれます。イーサネット、および仮想ファイバ チャネルの送信元インターフェイスで、入力方向、出力方向、または両方向の SPAN トラフィックを選択できます。

- 入力送信元（Rx）：この送信元ポートを介してデバイスに入るトラフィックは、SPAN 宛先ポートにコピーされます。
- 出力送信元（Tx）：この送信元ポートを介してデバイスから出るトラフィックは、SPAN 宛先ポートにコピーされます。

（注） VSAN ポートは、SPAN セッションの入力送信元ポートとして設定できません。

送信元ポートの特性

送信元ポート（モニタリング対象ポートとも呼ばれる）は、ネットワーク トラフィック分析のためにモニタリングするスイッチド インターフェイスです。スイッチは、任意の数の入力送信元ポート（スイッチで使用できる最大数のポート）と任意の数の送信元 VLAN または VSAN をサポートします。

送信元ポートの特性は、次のとおりです。

- イーサネット、ポート チャネル、仮想ファイバ チャネル、SAN ポート チャネル、VSAN または VLAN ポート タイプにできます。
- 複数の SPAN セッションではモニタリングできません。

- 宛先ポートには設定できません。
- モニタする方向（入力、出力、または両方）を設定できます。VLAN および VSAN 送信元の場合、モニタリング方向は入力のみであり、グループ内のすべての物理ポートに適用されます。RX と TX のオプションは、VLAN または VSAN の SPAN セッションでは使用できません。
- 同じまたは別の VLAN または VSAN に設定できます。
- VLAN または VSAN の SPAN 送信元では、ソース VLAN または VSAN のすべてのアクティブ ポートが送信元ポートとして含まれます。

（注）

- 一部の FEX ポートが送信元ポートとして SPAN セッションで使用されている場合、残りの FEX ポートを別の SPAN セッションに含めることはできません。
- SPAN セッションあたりの送信元ポートの最大数は 128 ポートです。
- Nexus 5000 シリーズおよび Nexus 5500 シリーズ スイッチでサポートされる SPAN セッションの最大数は 4 です。
- Nexus 5600 シリーズおよび Nexus 6000 シリーズ スイッチでサポートされる SPAN セッションの最大数は 16 です。

SPAN 宛先

SPAN 宛先とは、送信元ポートをモニタリングするインターフェイスを表します。Cisco Nexus シリーズ デバイスは、SPAN 宛先として、イーサネット インターフェイスをサポートします。

送信元 SPAN	宛先 SPAN
イーサネット	イーサネット
仮想ファイバ チャネル	イーサネット（FCoE）

宛先ポートの特性

各ローカル SPAN セッションには、送信元ポート、VSAN、または VLAN からトラフィックのコピーを受信する宛先ポート（モニタリング ポートとも呼ばれる）が必要です。宛先ポートの特性は、次のとおりです。

- すべての物理ポートが可能です。送信元イーサネットおよび FCoE ポートは、宛先ポートにできません。
- ソース ポートにはなれません。

- ポート チャネルまたは SAN ポート チャネル グループにはできません。
- SPAN セッションがアクティブなときは、スパニングツリーに参加しません。
- 任意の SPAN セッションのソース VLAN に属する場合、送信元リストから除外され、モニタリングされません。
- すべてのモニタリング対象送信元ポートの送受信トラフィックのコピーを受信します。
- FEX インターフェイスを SPAN 宛先にできません。

複数の SPAN 宛先

ローカル SPAN および SPAN-on-Drop セッションは複数の宛先ポートをサポートできます。これにより、単一のローカル SPAN セッションまたは SPAN-on-Drop セッションのトラフィックをモニタし、複数の宛先に送信することもできます。

（注） ERSPAN、または SPAN-on-Latency セッションでは複数の宛先はサポートされません。

ACL を使用した SPAN

ACL フィルタリング機能を使用した SPAN では、帯域幅の輻輳を緩和できるように SPAN トラフィックをフィルタすることができます。ACL フィルタリング機能を使用した SPAN を設定するには、セッションの ACL を使用して、スパンしないトラフィックをフィルタリングにより除外します。ACL は、システム内の任意のエンティティに関連付けられた権限のリストです。モニタリング セッションのコンテキストでは ACL はルールのリストであり、ACL の基準に一致するトラフィックのみをスパンすることで、より重要なデータに帯域幅を割り当てることができます。フィルタは、セッション内のすべての送信元に適用できます。

SPAN on Drop

SPAN-on-drop 機能を使用すると、入力でバッファまたはキュー空間が使用できない場合に通常はドロップされるパケットのスパニングが可能になります。システムは、輻輳が生じたときにパケットをドロップせずに別の SPAN-on-drop バッファに保存し、その後で、指定された SPAN-on-drop の宛先ポートへパケットを送信します。

SPAN-on-Latency セッション

SPAN-on-Latency 機能により、システムは、事前設定された遅延しきい値を超えるパケットを SPAN することができます。

待ち時間の長いフローでは、事前設定された SPAN の任意の宛先へコピーを送信するようにシステムを設定できます。これにより、ネットワークにおいてどのアプリケーションが遅延時間が長くなる影響を受けるかを確認するための分析用データ セットが作成されます。この機能を使用して、輻輳が発生するトラフィック フローを識別することもできます。

遅延の測定値を超える、送信元ポートから出力されるパケットのみが SPAN されます。

（注） SPAN コピーは、IPFIX/ERSPAN のカプセル化を使用して、ローカル アナライザ ポート、またはリモートアナライザに転送できます。SPAN コピーを切り捨てて、帯域幅を節約することができます。

SPAN の注意事項および制約事項

Cisco Nexus 6000 デバイスは、16 のアクティブなローカル SPAN セッションまたは ERSPAN 送信元セッション、16 のアクティブな ERSPAN 宛先セッション、および 1 つのアクティブな SPAN-on-Drop セッションまたは SPAN-on-Drop-ERSPAN セッションをサポートします。

複数の宛先が設定されている場合、SPAN セッションには次の注意事項と制約事項が適用されます。

- 複数の宛先は、ローカル SPAN または SPAN-on-Drop セッションでのみサポートされます。ERSPAN、または SPAN-on-Latency セッションでは複数の宛先はサポートされません。
- アクティブなすべてのセッションに設定される、一意の宛先の最大数は 16 です。1 つの SPAN セッションは最大で 16 の宛先を持つことが可能で、1 つの SPAN-on-Drop セッションは最大で 17 の宛先を持つことができます。この場合には、追加の SPAN セッションは設定できません。
- 単一の送信元 VLAN を複数の宛先ポートに SPAN することはできません。
- SPAN 宛先ポートをスイッチ デバイスに接続することはサポートされていません。

SPAN-on-Drop セッションには、次の注意事項と制約事項が適用されます。

- イーサネットの送信元インターフェイスのみがサポートされます（ポートチャネルはサポートされません）。送信元は、同時に SPAN-on-Drop セッション、およびローカル SPAN セッションの一部になることができます。
- 一度にアクティブにできるのは、1 つの SPAN-on-Drop セッションまたは SPAN-on-Drop ERSPAN セッションのみです。
- 送信元インターフェイスの方向はサポートされません。
- Fex インターフェイスは、送信元としてサポートされません。ただし、ファブリック インターフェイスはサポートされます。ファブリック インターフェイスを送信元として設定すると、ファブリック インターフェイスに関連付けられているすべての Fex ポート上で、SPAN-on-Drop セッションをイネーブルにすることができます。

- マルチキャスト出力ドロップはスパニングされません。SPAN-on-Drop は、バッファ リソース不足が原因で入力でドロップされたパケット、または Virtual Output Queueing（VOQ）のサイズが事前にプログラムで設定されたしきい値を超えた場合に入力でドロップされたパケットにのみ適用されます。
- ACL-based SPAN はサポートされていません。
- パケットに対する最大伝送単位（MTU）の切り捨てサイズの設定は、SPAN-on-Drop セッションではサポートされません。

SPAN-on-Latency セッションには、次の注意事項と制約事項が適用されます。

- SPAN-on-Latency の検出はポートごとに実行されますが、span ポインタの設定はグローバルな値です。
- 最大の遅延しきい値の設定は、40 ギガビット ポート単位です。したがってシステムが 10 ギガビットのポートを所有している場合、遅延しきい値は 4 個の 10 ギガビット ポートで共有されます。
- 一度にアクティブにできるのは、1 つの SPAN-on-Latency セッションまたは SPAN-on-Latency ERSPAN セッションのみです。
- スイッチをリロードする場合、またはモジュールの電源をオンにする場合は、**clear hardware profile latency monitor all** コマンドを発行する必要があります。このコマンドを発行するまで、パケットはスパニングされません。
- ファブリック インターフェイスが送信元としてサポートされていても、FEX インターフェイスおよびポート チャネルは、ソースとしてサポートされません。
- Span-on-Latency 送信元は、ローカル SPAN または Span-on-drop などのその他のスパンセッションに含めることはできません。
- ACL ベースの SOL はサポートされていません。

SPAN（ローカル SPAN）セッションのアクセス コントロール リスト（ACL）設定には、次の制約事項が適用されます。

- システムの制約により、SPAN セッションに関連付けられている ACL が拡張可能な範囲は、SPAN の送信元がどのように設定されたかによって決まります。次の表は、様々なシナリオと、それに対応するサポート対象の最大 ACL サイズを示しています。

（注） これらの計算では、ACL の各 ACE によって、1 つの最終的な TCAM エントリが生成されると仮定しています。

シナリオ	最大 ACL サイズ
SPAN には、Tx と Rx 両方の送信元として単一のスイッチ ポートがあります。	現在使用可能な TCAM エントリ/2

シナリオ	最大 ACL サイズ
SPAN には、Tx と Rx 両方の送信元として複数のスイッチ ポートがあります。	現在使用可能な TCAM エントリ/3
SPAN には、Tx および RX 両方の送信元として（1 つ以上のメンバ スイッチ ポートを持つ）ポート チャネルがあります。	現在使用可能な TCAM エントリ/3
SPAN には、Tx と Rx 両方の送信元として単一の HIF ポートがあります。	現在使用可能な TCAM エントリ/3
SPAN には、Tx と Rx 両方の送信元として複数の HIF ポートがあります。	現在使用可能な TCAM エントリ/4
SPAN には、Tx および RX 両方の送信元として（1 つ以上のメンバ HIF ポートを持つ）HIF ポート チャネルがあります。	現在使用可能な TCAM エントリ/4

- 次のシナリオは、ACL および SPAN セッションのスケーリングについては、システムの制約事項に影響されません。
  - SPAN には、Tx のみの送信元として単一のスイッチ ポートがあります。
  - SPAN には、Tx のみの送信元として複数のスイッチ ポートがあります。
  - SPAN には、Tx のみの送信元として（1 つ以上のメンバ スイッチ ポートを持つ）ポート チャネルがあります。
  - SPAN には、Tx のみの送信元として単一のホスト インターフェイス（HIF）ポートがあります。
  - SPAN には、Tx のみの送信元として複数の HIF ポートがあります。
  - SPAN には、Tx のみの送信元として（1 つ以上のメンバ HIF ポートを持つ）単一のポート HIF チャネルがあります。
  - SPAN には、Rx のみの送信元として単一のスイッチ ポートがあります。
  - SPAN には、Rx のみの送信元として複数のスイッチ ポートがあります。
  - SPAN には、Rx のみの送信元として（1 つ以上のメンバ スイッチ ポートを持つ）ポート チャネルがあります。
  - SPAN には、Rx のみの送信元として単一の HIF ポートがあります。
  - SPAN には、Rx のみの送信元として複数の HIF ポートがあります。
  - SPAN には、Rx のみの送信元として（1 つ以上のメンバ HIF ポートを持つ）HIF ポート チャネルがあります。

- ACL でローカル SPAN セッションを設定する場合には、次の注意事項が適用されます。
  - ACL を SPAN セッションに関連付ける場合は、サイズが、上記の表に記載されている計算を超えていないことを確認します。上記の計算を超えると、SPAN セッションが失敗し、「TCAM resource unavailable」エラーが生成されます。ACL にレイヤ 4 操作があり、TCAM リソース拡張が可能な場合、最大 ACL サイズを計算するには、予想される拡張サイズを確認し、その拡張サイズを使用する必要があります。
  - SPAN セッションに追加された ACL を変更すると、ACL のサイズが、許可されている最大 ACL のサイズを超える可能性があります。このシナリオでは、SPAN セッションは変更された ACL を引き続き使用します。ただし、サイズを許可された最大 ACL サイズに限定するには、ACL に追加された ACE を元に戻す必要があります。
  - SPAN セッションがすでに存在する場合にこのセッションを追加し、最初の SPAN セッションを変更するには、関連する ACL 内の ACE の数と同じサイズの空き TCAM エントリが必要です（各 ACE に 1 つの TCAM エントリが必要と仮定した場合。拡張されている場合は、拡張されたサイズを考慮する必要があります）。そのため、2 つめの SPAN セッションで使用される TCAM エントリを解放する必要があります。
  - 大きい ACL を別の大きい ACL で置き換える（SPAN セッションが一般的なエラー状態になる可能性がある）には、（**no filter access-group***current acl name* コマンドを使用して）最初に既存のフィルタ アクセス グループを削除し、次に（**filter access-group***new acl name* コマンドを使用して）新しいフィルタ アクセス グループを設定する必要があります。
- ローカル SPAN/ドロップ時 SPAN/遅延時 SPAN は VPC を認識しません。
- 次は、SPAN 宛先としての HIF と仮想イーサネット（Veth）の制約です。
  - 複数宛先の SPAN はサポートされません。HIF/VETH ポートが宛先である場合、モニタセッションには単一の宛先が必要です。

SPAN セッションの作成または削除

monitor session コマンドを使用してセッション番号を割り当てることによって、SPAN セッションを作成できます。セッションがすでに存在する場合、既存のセッションにさらに設定情報が追加されます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	switch(config)# **monitor session***session-number*	モニタ コンフィギュレーション モードを開始します。既存のセッション設定に新しいセッション設定が追加されます。

次に、SPAN モニタ セッションを設定する例を示します。

```
switch# configure terminal
switch(config) # monitor session 2
switch(config) #
```

イーサネット宛先ポートの設定

SPAN 宛先ポートとしてイーサネット インターフェイスを設定できます。

（注） SPAN 宛先ポートは、スイッチ上の物理ポートにのみ設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface ethernet***slot*/*port*	指定されたスロットとポートでイーサネット インターフェイスのインターフェイス コンフィギュレーション モードを開始します。 （注） これが 10G ブレークアウト ポートの場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。 （注） 仮想イーサネット ポートで **switchport monitor** コマンドを有効にするには、**interface vethernet***slot*/*port* コマンドを使用します。
ステップ 3	switch(config-if)# **switchport monitor**	指定されたイーサネットインターフェイスのモニタモードを開始します。ポートがSPAN宛先として設定されている場合、プライオリティ フロー制御はディセーブルです。
ステップ 4	switch(config-if)# **exit**	グローバルコンフィギュレーションモードに戻ります。

	コマンドまたはアクション	目的
ステップ 5	switch(config)# **monitor session***session-number*	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 6	switch(config-monitor)# **destination interface ethernet***slot*/*port*	イーサネット SPAN 宛先ポートを設定します。 （注） これが 10G ブレークアウト ポートの場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。 （注） モニタ コンフィギュレーションで宛先インターフェイスとして仮想イーサネット ポートを有効にするには、**destination interface vethernet***slot*/*port* コマンドを使用します。

次に、イーサネット SPAN 宛先ポート（HIF）を設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet100/1/24
switch(config-if)# switchport monitor
switch(config-if)# exit
switch(config)# monitor session 1
switch(config-monitor)# destination interface ethernet100/1/24
switch(config-monitor)#
```

次に、仮想イーサネット（VETH）SPAN 宛先ポートを設定する例を示します。

```
switch# configure terminal
switch(config)# interface vethernet10
switch(config-if)# switchport monitor
switch(config-if)# exit
switch(config)# monitor session 2
switch(config-monitor)# destination interface vethernet10
switch(config-monitor)#
```

SPAN セッションごとの MTU の切り捨ての設定

SPAN トラフィック帯域幅を減らすには、SPAN セッションの各複製パケットで許可される最大バイト数を設定できます。この値は、最大伝送単位（MTU）の切り捨てサイズと呼ばれます。設定されたサイズよりも大きい SPAN パケットはすべて、設定されたサイズに切り捨てられます。

（注） SPAN-on-Drop セッションに対して MTU の切り捨て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	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config) # **monitor session***session-number*	モニタ コンフィギュレーション モードを開始し、MTU 切り捨てサイズが設定された SPAN セッションを指定します。
ステップ 3	switch(config-monitor) # [**no**] **mtu**	指定した SPAN セッションのパケットの MTU 切り捨てサイズを設定します。指定できる範囲は 64 ～ 1518 バイトです。
ステップ 4	switch(config-monitor) # **show monitor session***session-number*	（任意） MTU 切り捨ての設定ステータス、セッションごとに各パケットで許可される最大バイト数、MTU 切り捨てがサポートされるモジュールとサポートされないモジュールを含む、SPAN セッションのステータスを表示します。
ステップ 5	switch(config-monitor) # **copy running-config** startup-config	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、SPAN セッションの MTU 切り捨てを設定する例を示します。

```
switch# configure terminal
switch(config) # monitor session 3
switch(config-monitor) # mtu
switch(config-monitor) # copy running-config startup-config
switch(config-monitor) #
```

送信元ポートの設定

送信元ポートには、イーサネット ポート、ポート チャネル、ファイバ チャネル ポート、SAN ポート チャネル、VLAN、または VSAN ポートを使用できます。宛先ポートにすることはできません。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config) # **monitor session***session-number*	指定したモニタリング 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	switch(config-monitor) # **source interface***typeslot*/*port* [**rx** | **tx** | **both**]	イーサネット SPAN の送信元ポートを追加し、パケットを複製するトラフィック方向を指定します。イーサネット、ファイバ チャネル、または仮想ファイバ チャネルのポート範囲を入力できます。複製するトラフィック方向を、入力（Rx）、出力（Tx）、または両方向（both）として指定できます。デフォルトはbothです。 （注） これが 10G ブレークアウト ポートの場合、*slot*/*port* 構文は *slot*/*QSFP-module*/*port* になります。

次に、イーサネット SPAN 送信元ポートを設定する例を示します。

```
switch# configure terminal
switch(config)# monitor session 2
switch(config-monitor)# source interface ethernet 1/16
switch(config-monitor)#
```

次に、仮想ファイバ チャネル SPAN 送信元ポートを設定する例を示します。

```
switch# configure terminal
switch(config)# monitor session 2
switch(config-monitor)# source interface vfc 129
switch(config-monitor)#
```

SPAN セッションの説明の設定

参照しやすいように、SPAN セッションにわかりやすい名前を付けることができます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config) # **monitor session** *session-number*	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。

	コマンドまたはアクション	目的
ステップ 3	switch(config-monitor) # **description***description*	SPAN セッションのわかりやすい名前を作成します。

次に、SPAN セッションの説明を設定する例を示します。

```
switch# configure terminal
switch(config) # monitor session 2
switch(config-monitor) # description monitoring ports eth2/2-eth2/4
switch(config-monitor) #
```

SPAN セッションに対する ACL フィルタの設定

SPAN セッションのトラフィックを選択的にモニタするために、パケットをフィルタするようアクセス コントロール リスト（ACL）を設定することができます。SPAN セッションは、アクセス リストで指定された許可または拒否のすべてのアクションを無視して、アクセス リストのフィルタ基準に一致するパケットのみをスパンします。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config) # **monitor session** *session-number*	モニタ コンフィギュレーション モードを開始し、ACL フィルタを設定する SPAN セッションを指定します。
ステップ 3	switch(config-monitor) # [**no**] **filter access-group** *acl_filter*	指定した SPAN セッションのパケットの ACL フィルタを設定します。ACL フィルタとして、MAC または IP アクセス リストを使用できます。
ステップ 4	switch(config-monitor) # **show monitor session***session-number*	（任意） ACL フィルタの設定ステータスなど、SPAN セッションのステータスを表示します。
ステップ 5	switch(config-monitor) # **copy running-config** startup-config	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、SPAN セッションの ACL フィルタを設定する例を示します。

```
switch# configure terminal
switch(config) # monitor session 3
switch(config-monitor) # filter access-group acl_span_ses_3
switch(config) # copy running-config startup-config
switch(config) #
```

SPAN-on-Drop セッションの設定

SPAN-on-Drop セッションを設定するには、monitor session コマンドを使用します。各セッションは、一意の SPAN-on-Drop セッション番号で識別されます。

（注） アクティブにできるのは、常に SPAN-on-Drop または SPAN-on-Drop ERSPAN セッション 1 つだけです。

（注） 1 つの SPAN-on-Drop セッションに対して複数の宛先を設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config) # **monitor session** *span-on-drop-session-number* **type span-on-drop**	指定した SPAN-on-drop セッションの SPAN-on-Drop 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	switch(config-span-on-drop) # **description***description*	SPAN-on-Drop セッションのわかりやすい名前を作成します。
ステップ 4	switch(config-span-on-drop) # **source interface ethernet***slot*/*port***rx**	セッションの送信元を設定します。イーサネット ポートの範囲を入力できます。SPAN-on-Drop セッションは入力トラフィックのみをサポートします。
ステップ 5	switch(config-span-on-drop) # **destination interface ethernet***slot*/*port*	イーサネット SPAN-on-Drop 宛先ポートを設定します。
ステップ 6	switch(config) # **show monitor session***session-number*	（任意） SPAN-on-Drop セッションのステータスを表示します。

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

次に、SPAN-on-Drop セッションを設定する例を示します。

```
switch# configure terminal
switch(config) # monitor session 3 type span-on-drop
switch(config-span-on-drop) # description span-on-drop-session_3
switch(config-span-on-drop) # source interface ethernet 1/3
switch(config-span-on-drop) # destination interface ethernet 1/2
switch(config) # copy running-config startup-config
switch(config) #
```

SPAN-on-Latency セッションの設定

SPAN パケットの送信で使用されるファブリックの量またはネットワーク帯域幅の量を減らすには、SPAN トラフィックの最大伝送単位（MTU）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	イネーブル化 例： `switch> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。

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	**interface ethernet***slot/port* 例： `switch(config)# interface ethernet 1/1`	インターフェイスコンフィギュレーションモードを開始します。
ステップ 4	**packet latency threshold***threshold* 例： `switch(config-if)# packet latency threshold 53000000`	インターフェイスの遅延しきい値を設定します。有効な値は 8 ～ 536870904 ナノ秒です。

	コマンドまたはアクション	目的

ステップ 5	**monitor session***session_number***typespan-on-latency**
	
	例：
	`switch(config)# monitor session 1 type span-on-latency`
	`switch(config-span-on-latency)#`
		セッション ID とセッション タイプを使用して SPAN 送信元セッションを定義し、SPAN のモニタ送信元セッション コンフィギュレーションモードでコマンドを開始します。
		
		session_number 引数の範囲は 1 ～ 1024 です。同じセッション番号は複数回使用できません。
		
		セッション ID（span_session number 引数によって設定）およびセッション タイプ（span-on-latency キーワードによって設定）は、入力後は変更できません。セッション ID またはセッション タイプを変更するには、コマンドの no バージョンを使用してセッションを削除してから、新しいセッション ID または新しいセッション タイプでコマンドを使用してセッションを再作成します。

ステップ 6	**description***description* 例： `switch(config-span-on-latency)# description SPAN-on-Latency-session`	セッション設定に説明を追加します。
ステップ 7	**source interface ethernet***slot/port* 例： `switch(config-span-on-latency)# source interface ethernet 1/3`	イーサネット インターフェイスを送信元 SPAN ポートとして使用するように指定します。
ステップ 8	**destination interface ethernet***slot/port* 例： `switch(config-span-on-latency)# destination interface ethernet 1/1`	イーサネットインターフェイスをセッションの宛先ポートとして使用するよう指定します。
ステップ 9	**mtu***mtu-value* 例： `switch(config-span-on-latency)# mtu 1500`	SPANパケットのMTU切り捨てサイズを定義します。有効値は 64 ～ 1518 です。 デフォルトでは、切り捨てはイネーブルではありません。
ステップ 10	**exit** 例： `switch(config-span-on-latency)# exit`	設定を更新し、SPAN-on-Latency セッションのコンフィギュレーションモードを終了します。

	コマンドまたはアクション	目的
ステップ 11	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

SPAN セッションのアクティブ化

デフォルトでは、セション ステートは shut のままになります。送信元から宛先へパケットをコピーするセッションを開くことができます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **no monitor session** {**all** | *session-number*} **shut**	指定された SPAN セッションまたはすべてのセッションを開始します。

次に、SPAN セッションをアクティブにする例を示します。

```
switch# configure terminal
switch(config) # no monitor session 3 shut
```

SPAN セッションの問題のトラブルシューティング

SPAN セッションがダウンしている場合は、次の手順を実行してください。

- 次のコマンドを実行して、宛先ポートの 1 つが動作していることを確認します。
  - **show running interface***interface* コマンドを使用して、スイッチポート モニタが設定されていることを確認します。
  - **show interface** *interface* コマンドを使用して、宛先インターフェイスのステータスが「admin up」と表示されることを確認します。
- **show interface** *interface* コマンドを使用して、送信元ポートが動作していること、および送信元インターフェイスのステータスが「admin up」と表示されることを確認します。

- ACL フィルタが適用されている場合は、フィルタ定義が存在することを確認します。**show access-lists** *listname* コマンドを使用して、設定されたアクセス リストとエントリを確認します。

多数の送信元ポートを使用する SPAN セッションの問題のトラブルシューティング

表 *28*：多数の送信元ポートを使用する *SPAN* セッションのトラブルシューティング

問題の説明	ソリューション	推奨事項
サポートされる最大範囲である 128 の送信元ポートを一度に使用して SPAN セッションが設定されると、コンフィギュレーションセッションで「Service not responding」メッセージが表示されることがあります。	ポートを削除してから狭い範囲（例：1 ～ 48）で設定し、セッションで **shutdown** および **no shutdown** コマンドを使用します。	個々のポートを狭い範囲（例：1 ～ 48）で設定します。
最大ポート数（例：128）を使用して設定された SPAN セッション範囲で **shutdown** および **no shutdown** を使用すると、一部のセッションが開始しません。	特定の SPAN セッションから一部のポートを削除します。削除したポートを同じ SPAN セッションに再度追加してから、**no shutdown** コマンドを使用します。	各ポートで **shutdown** コマンドを使用します。

128 の送信元ポートを使用して SPAN セッションを作成すると、**no shutdown** コマンドで「Service not responding」メッセージが表示されます。	**no shutdown** コマンドを繰り返し使用して、SPAN セッションを開始します。	

SPAN 情報の表示

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **show monitor** [**session** {**all** | *session-number* | **range***session-range*} [**brief**]]	SPAN 設定を表示します。

次に、SPAN セッションの情報を表示する例を示します。

```
switch# show monitor
SESSION  STATE        REASON                  DESCRIPTION
-------  -----------  ----------------------  ---------------------------------
2        up           The session is up
3        down         Session suspended
4        down         No hardware resource
```

次に、SPAN セッションの詳細を表示する例を示します。

```
switch# show monitor session 2
   session 2
---------------
type              : local
state             : up

source intf       :

source VLANs      :
    rx            :
source VSANs      :
    rx            : 1
destination ports : Eth3/1
```

次に、複数の宛先ポートを持つ SPAN セッションの詳細の例を示します。

```
switch(config-monitor)# show monitor session 5
   session 5
---------------
type              : local
state             : up
source intf       :
    rx            : Eth1/1
    tx            : Eth1/1
    both          : Eth1/1
```

```
source VLANs      :
    rx            :
source VSANs      :
    rx            :
destination ports : Eth1/8, Eth1/9
```

次に、SPAN-on-Drop セッションの詳細の例を示します。

```
switch(config-monitor)# show monitor session 48
  session 48
---------------
description       : span-on-drop-session
type              : span-on-drop
state             : up
mtu               : 0
source ports      : Eth1/2
destination ports : Eth1/3
```

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)# monitor session 1
switch(config-erspan-src)# filter access-group match_11_pkts
```

SPAN-on-Latency セッションの設定例

次に、SPAN-on-Latency セッションを設定する例を示します。

```
switch# configure terminal
switch(config) # interface ethernet 1/1
switch(config-if) # packet latency threshold 530000000
switch(config) # monitor session 11 type span-on-latency
switch(config-span-on-latency) # description span-on-latency-session_11
switch(config-span-on-latency) # source interface ethernet 1/3
switch(config-span-on-latency) # destination interface ethernet 1/1
switch(config-span-on-latency) # mtu 1500
switch(config) # copy running-config startup-config
switch(config) #
```

第 17 章

ローカル SPAN および ERSPAN の設定

この章の内容は、次のとおりです。

- ERSPAN に関する情報，217 ページ
- ERSPAN のライセンス要件，221 ページ
- ERSPAN の前提条件，222 ページ
- ERSPAN の注意事項および制約事項，222 ページ
- ERSPAN タイプ III の注意事項および制約事項，226 ページ
- ERSPAN のデフォルト設定，226 ページ
- ERSPAN の設定，226 ページ
- ERSPAN の設定例，242 ページ
- その他の参考資料，244 ページ

ERSPAN に関する情報

Cisco NX-OS システムは、発信元および宛先ポートの両方で Encapsulated Remote Switching Port Analyzer（ERSPAN）機能をサポートします。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ます。トラフィックは、送信元ルータでカプセル化され、ネットワーク間を転送されます。パケットは宛先ルータでカプセル化解除され、宛先インターフェイスに送信されます。

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

ERSPAN 送信元セッション

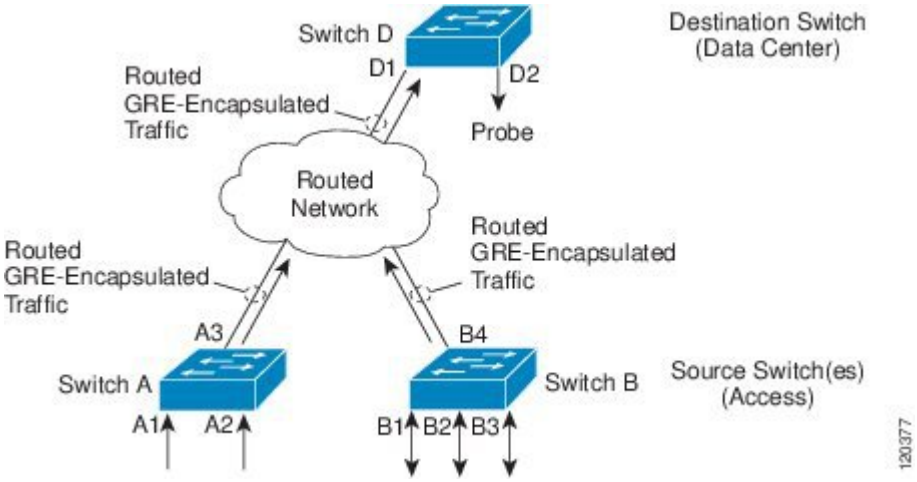
ERSPAN 送信元セッションは、次によって定義されます。

- セッション ID。
- セッションでモニタされる送信元ポート、送信元 VLAN、または送信元 VSAN のリスト。
- ERSPAN フロー ID。
- IP TOS や TTL など、GRE エンベロープに関連するオプション属性
- 宛先の IP アドレス。
- 仮想ルーティングおよび転送テーブル。

ERSPAN 送信元セッションは、ERSPAN GRE カプセル化されたトラフィックを送信元ポートからコピーしません。ERSPAN 送信元セッションごとに、送信元としてポート、VLAN、または VSAN を設定できます。ただし、次のようないくつかの制限があります。詳細については、ERSPAN の注意事項および制約事項, （222 ページ）を参照してください。

次の図は、ERSPAN 設定の例を示します。

図 *1*：*ERSPAN* の設定



モニタ対象トラフィック

デフォルトでは、ERSPAN は、マルチキャストおよびブリッジ プロトコル データ ユニット（BPDU）フレームを含む、すべてのトラフィックを監視します。

ERSPAN がモニタするトラフィックの方向は、次のように送信元によって決まります。

- 送信元ポートについては、ERSPAN は、入力トラフィック、出力トラフィック、または入出力トラフィックをモニタできます。

- 送信元 VLAN または送信元 VSAN については、ERSPAN は入力トラフィックのみをモニタできます。

ERSPAN タイプ

Cisco NX-OS Release 7.1(1)N1(1) は、ERSPAN の 2 つのタイプ（ERSPAN タイプ II（デフォルト）と ERSPAN タイプ III）をサポートします。以前のすべての Cisco NX-OS リリースでは ERSPAN タイプ II のみがサポートされました。

ERSPAN タイプ III は ERSPAN タイプ II のすべての特徴と機能をサポートし、以下の拡張機能が追加されています。

- ERSPAN タイプ III ヘッダーに、エッジ、集約、およびコア スイッチ間でパケット遅延を計算するために使用できるタイムスタンプ情報を表示。
- ERSPAN タイプ III ヘッダー フィールドを使用して潜在的なトラフィック ソースを識別。
- ERSPAN タイプ III は、複数のスイッチ間のトラフィック フローを識別するために使用できる設定可能なスイッチ ID を提供。

表 *29* : *ERSPAN* タイプ *II* と *ERSPAN* タイプ *III* の相違点

属性	タイプ II	タイプ III
Timestamp	該当なし	提供されるタイムスタンプ。
プラットフォーム固有の情報	該当なし	プラットフォーム固有の情報は、Nexus 5500、Nexus 5600、および Nexus 6000 プラットフォームに必要です。
終端スイッチの送信元ポート ID	限定的な ID。	詳細な ID。スイッチ ID のプロビジョニング。

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 ソースと呼びます。送信元では、監視するトラフィックを指定し、さらに入力、出力、または両方向のトラフィックをコピーするかどうかを指定します。ERSPAN 送信元には次のものが含まれます。

- イーサネット ポートおよびポート チャネル。
- VLAN：VLAN が ERSPAN 送信元として指定されている場合、VLAN でサポートされているすべてのインターフェイスが ERSPAN 送信元となります。

ERSPAN 送信元ポートには、次の特性があります。

- 送信元ポートとして設定されたポートを宛先ポートとしても設定することはできません。
- ERSPAN は送信元に関係なく、スーパーバイザによって生成されるパケットをモニタしません。
- ACL を使用して送信元ポートで入力トラフィックをフィルタし、ACL 基準に一致する情報のパケットのみがミラーリングされるようにすることができます。

ERSPAN 宛先

ERSPAN宛先セッションは、イーサネット ポートまたはポート チャネル上のERSPAN送信元セッションで送信されたパケットを取得し、宛先ポートに送信します。宛先ポートは ERSPAN 送信元からコピーされたトラフィックを受信します。

ERSPAN 宛先セッションは、設定された送信元 IP アドレスおよび ERSPAN ID によって識別されます。これにより、複数の送信元セッションがERSPANトラフィックを同じ宛先IPおよびERSPAN ID に送信できるようになり、1 つの宛先で同時に終端する複数の送信元を持つことができます。

ERSPAN 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を送信元ポートとしても設定することはできません。
- 宛先ポートはスパニングツリー インスタンスまたはレイヤ 3 プロトコルに参加しません。
- 入力および入力学習オプションは、モニタ宛先ポートではサポートされていません。
- ホスト インターフェイス（HIF）ポート チャネルおよびファブリック ポート チャネル ポートは、SPAN 宛先ポートとしてはサポートされていません。

切り捨てを適用する ERSPAN

切り捨てを適用する ERSPAN を使用して、ERSPAN パケットの送信で使用されるファブリックまたはネットワーク帯域幅の量を減らすことができます。

デフォルトでは切り捨ては行われないため、大規模な ERSPAN パケットを受信するスイッチまたはルータは、これらの大きすぎるパケットをドロップする可能性があります。

（注） Cisco Nexus 6000 シリーズ スイッチは、これらの切り捨てを適用するパケットをドロップするため、宛先 ERSPAN ルータが Cisco Nexus 6001 または Cisco Nexus 6004 スイッチの場合、切り捨てを適用する ERSPAN の機能を有効にしないでください。

ACL を使用した ERSPAN

ERSPAN トラフィックでは宛先がリモートになり、帯域幅の輻輳の全体的な影響が重大になることがあります。ACL フィルタリング機能を使用した ERSPAN では、帯域幅の輻輳を緩和するように ERSPAN トラフィックをフィルタすることができます。ACL フィルタリング機能を使用した ERSPAN を設定するには、セッションの ACL を使用して、スパンしないトラフィックを除去します。ACL は、システム内の任意のエンティティに関連付けられた権限のリストです。モニタリング セッションのコンテキストでは ACL はルールのリストであり、ACL の基準に一致するトラフィックのみにスパンすることで、より重要なデータに帯域幅を割り当てることができます。フィルタは、セッション内のすべての送信元（vlan またはインターフェイス）に適用されます。

ERSPAN SPAN on Drop

ERSPAN SPAN-on-drop 機能を使用すると、入力でバッファまたはキュー空間が使用できない場合に通常はドロップされるパケットのスパニングが可能になります。システムは、輻輳が生じたときにパケットをドロップせずに別の SPAN-on-drop バッファに保存し、その後で、指定された ERSPAN-on-drop の宛先 IP アドレスへパケットを送信します。

ERSPAN SPAN-on-Latency

ERSPAN-on-Latency 機能により、システムは、事前設定された遅延しきい値を超えるパケットを SPAN することができます。

待ち時間の長いフローでは、事前設定された SPAN の任意の宛先へコピーを送信するようにシステムを設定できます。これにより、ネットワークにおいてどのアプリケーションが遅延時間が長くなる影響を受けるかを確認するための分析用データ セットが作成されます。この機能を使用して、輻輳が発生するトラフィック フローを識別することもできます。

（注） SPAN コピーは、IPFIX/ERSPAN のカプセル化を使用して、ローカル アナライザ ポート、またはリモート アナライザに転送できます。SPAN コピーを切り捨てて、帯域幅を節約することができます。

ハイ アベイラビリティ

ERSPAN 機能はステートレスおよびステートフル リスタートをサポートします。リブートまたはスーパーバイザ スイッチオーバー後に、実行コンフィギュレーションが適用されます。

ERSPAN のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	ERSPAN にはライセンスは不要です。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。Cisco NX-OS のライセンス スキームの詳細は、*Cisco NX-OS* ソフトウェアのライセンスおよび版権情報は、次の URL から入手できます。http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_0/nx-os/license_agreement/nx-ossw_lisns.html

ERSPAN の前提条件

ERSPAN の前提条件は、次のとおりです。

•所定の ERSPAN 設定をサポートするには、まず各デバイス上でポートのイーサネット インターフェイスを設定する必要があります。詳細については、お使いのプラットフォームのインターフェイス コンフィギュレーション 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

ERSPAN には、次の注意事項および制約事項があります。

- 最大16のアクティブセッションがサポートされます。ERSPANセッションのみでも、ERSPAN と SPAN セッションの混合でも問題ありません。
- 各 ERSPAN セッションの最大ポート数は 128 です。
- 各セッションの VLAN の最大数は 32 です。
- 1 つの ERSPAN セッションに送信元ポート、送信元 VLAN、および送信元 VSAN を設定できます。
- VLAN が VSAN にマップされていない限り、ERSPAN は、送信元ポートでは入力、出力、または入出力トラフィックをモニタでき、送信元 VLAN または送信元 VSAN では入力トラフィックのみをモニタできます。ERSPAN では、送信元VLANとVSAN上の出力トラフィックをモニタできません。
- ERSPAN モニタ セッションを起動するには、**monitor erspan origin ip-address***ip-address***global** コマンドを使用して、最初にグローバルな元アドレスを設定する必要があります。
- 送信元ポートと送信元 VLAN は、同じ ERSPAN セッション内に存在できます。
- ERSPAN トラフィックは、レイヤ 2 インターフェイス、レイヤ 3 インターフェイス、ポートチャネル、または FabricPath コア ポートからスイッチを終了できます。

- リモート スイッチの宛先 IP アドレスは、仮想イーサネット ポートまたは FEX ポートを介して到達できません。この機能はサポートされません。
- ERSPAN トラフィックは、宛先 IP アドレスへの到達可能性がレイヤ 3 ECMP またはポート チャネルである場合、ロード バランシングされません。ECMP の場合、ERSPAN トラフィックは、ポート チャネルの 1 つのネクスト ホップ ルータまたは 1 つのメンバーのみに送信されます。
- ERSPAN は、送信元セッションの送信元ポートとしてファスト イーサネット、ギガビット イーサネット、TenGigabit イーサネット、およびポート チャネル インターフェイスをサポートします。
- ERSPAN コンフィギュレーション コマンドを使用してセッションを設定する場合、セッション ID とセッション タイプは変更できません。これらを変更するには、まずコンフィギュレーション コマンドの no バージョンを使用してセッションを削除してから、セッションを再設定する必要があります。
- ERSPAN トラフィックは通常のデータ トラフィックと競合する場合があります。
- ERSPAN トラフィックは QoS class-default システム クラス（qos-group 0）に割り当てられます。
- データ トラフィックを ERSPAN トラフィックに優先させるには、ERSPAN 宛先ポートの class-default システム クラスよりも大きいプライオリティを設定して QoS システム クラスを作成できます。

  レイヤ 3 ネットワークでは、ERSPAN トラフィックは、ip dscp コマンドを使用して目的の DiffServ コード ポイント（DSCP）値でマークできます。デフォルトでは、ERSPAN トラフィックは、DSCP 値 0 でマークされます。
- **rate limit** コマンドは使用できません。

ERSPAN 送信元セッションのアクセス コントロール リスト（ACL）の設定には、次の制約事項が適用されます。

- ACL は、ERSPAN 送信元セッションでのみサポートされます。ACL は、ERSPAN 宛先セッションではサポートされません。
- システムの制約により、ERSPAN セッションに関連付けられている ACL が拡張可能な範囲は、SPAN の送信元がどのように設定されたかによって決まります。次の表は、様々なシナリオと、それに対応するサポート対象の最大 ACL サイズを示しています。

（注） これらの計算では、ACL の各 ACE によって、1 つの最終的な TCAM エントリが生成されると仮定しています。

シナリオ	最大 ACL サイズ
ERSPAN には、Tx と Rx 両方の送信元として単一のスイッチ ポートがあります。	現在使用可能な TCAM エントリ/2

シナリオ	最大 ACL サイズ
ERSPAN には、Tx と Rx 両方の送信元として複数のスイッチ ポートがあります。	現在使用可能な TCAM エントリ/3
ERSPAN には、Tx および RX 両方の送信元として（1 つ以上のメンバ スイッチ ポートを持つ）ポート チャネルがあります。	現在使用可能な TCAM エントリ/3
ERSPAN には、Tx と Rx 両方の送信元として単一の HIF ポートがあります。	現在使用可能な TCAM エントリ/3
ERSPAN には、Tx と Rx 両方の送信元として複数の HIF ポートがあります。	現在使用可能な TCAM エントリ/4
ERSPAN には、Tx および RX 両方の送信元として（1 つ以上のメンバ HIF ポートを持つ）HIF ポート チャネルがあります。	現在使用可能な TCAM エントリ/4

- システムの制約により、ERSPAN セッションに関連付けられている ACL が拡張可能な範囲は、SPAN の送信元がどのように設定されたかによって決まります。次の表は、様々なシナリオと、それに対応するサポート対象の最大 ACL サイズを示しています。

（注） これらの計算では、ACL の各 ACE によって、1 つの最終的な TCAM エントリが生成されると仮定しています。

シナリオ	最大 ACL サイズ
ERSPAN には、Tx と Rx 両方の送信元として単一のスイッチ ポートがあります。	現在使用可能な TCAM エントリ/2
ERSPAN には、Tx と Rx 両方の送信元として複数のスイッチ ポートがあります。	現在使用可能な TCAM エントリ/3
ERSPAN には、Tx および RX 両方の送信元として（1 つ以上のメンバ スイッチ ポートを持つ）ポート チャネルがあります。	現在使用可能な TCAM エントリ/3
ERSPAN には、Tx と Rx 両方の送信元として単一の HIF ポートがあります。	現在使用可能な TCAM エントリ/3
ERSPAN には、Tx と Rx 両方の送信元として複数の HIF ポートがあります。	現在使用可能な TCAM エントリ/4

シナリオ	最大 ACL サイズ
ERSPAN には、Tx および RX 両方の送信元として（1 つ以上のメンバ HIF ポートを持つ）HIF ポート チャネルがあります。	現在使用可能な TCAM エントリ/4

- 次のシナリオは、ACL および SPAN セッションのスケーリングについては、システムの制約事項に影響されません。
  - ERSPAN には、Tx のみの送信元として単一のスイッチ ポートがあります。
  - ERSPAN には、Tx のみの送信元として複数のスイッチ ポートがあります。
  - ERSPAN には、Tx のみの送信元として（1 つ以上のメンバ スイッチ ポートを持つ）ポート チャネルがあります。
  - ERSPAN には、Tx のみの送信元として単一のホスト インターフェイス（HIF）ポートがあります。
  - ERSPAN には、Tx のみの送信元として複数の HIF ポートがあります。
  - ERSPAN には、Tx のみの送信元として（1 つ以上のメンバ HIF ポートを持つ）単一のポート HIF チャネルがあります。
  - ERSPAN には、Rx のみの送信元として単一のスイッチ ポートがあります。
  - ERSPAN には、Rx のみの送信元として複数のスイッチ ポートがあります。
  - ERSPAN には、Rx のみで送信元として（1 つ以上のメンバ スイッチ ポートを持つ）ポート チャネルがあります。
  - ERSPAN には、Rx のみの送信元として単一の HIF ポートがあります。
  - ERSPAN には、Rx のみの送信元として複数の HIF ポートがあります。
  - ERSPAN には、Rx のみの送信元として（1 つ以上のメンバ HIF ポートを持つ）HIF ポート チャネルがあります。
- ACL で ERSPAN 送信元セッションを設定する場合には、次の注意事項が適用されます。
  - ACL を ERSPAN セッションに関連付ける場合は、そのサイズが上記の表に記載されている計算を超えていないことを確認します。上記の計算を超えると、ERSPAN セッションが失敗し、「TCAM resource unavailable」エラーが生成されます。ACL にレイヤ 4 操作があり、TCAM リソース拡張が可能な場合、最大 ACL サイズを計算するには、予想される拡張サイズを確認し、その拡張サイズを使用する必要があります。
  - ERSPAN セッションに追加された ACL を変更すると、ACL のサイズが、許可されている最大 ACL のサイズを超える可能性があります。このシナリオでは、SPAN セッションは変更された ACL を引き続き使用します。ただし、サイズを許可された最大 ACL サイズに限定するには、ACL に追加された ACE を元に戻す必要があります。

- ERSPAN セッションがすでに存在する場合にこのセッションを追加し、最初の SPAN セッションを変更するには、関連する ACL 内の ACE の数と同じサイズの空き TCAM エントリが必要です（各 ACE に 1 つの TCAM エントリが必要と仮定した場合。拡張されている場合は、拡張されたサイズを考慮する必要があります）。そのため、2 つめの ERSPAN セッションで使用される TCAM エントリを解放する必要があります。
- 大きい ACL を別の大きい ACL で置き換える（ERSPAN セッションが一般的なエラー状態になる可能性がある）には、（**no filter access-group***current acl name* コマンドを使用して）最初に既存のフィルタ アクセス グループを削除し、次に（**filter access-group***new acl name* コマンドを使用して）新しいフィルタ アクセス グループを設定する必要があります。

ERSPAN タイプ III の注意事項および制約事項

ERSPAN タイプ III には、次の注意事項と制約事項があります。

- IPv4 ネットワークのみ ERSPAN タイプ III でサポートされています。IPv6 ネットワークは ERSPAN タイプ III ではサポートされていませんが、IPv6 パケットは ERSPAN でキャプチャできます。
- ポート間のパケット遅延を計算するには、Precision Time Protocol（PTP）クロックから ERSPAN のタイムスタンプを取得し、スイッチの PTP 機能を有効にする必要があります。

ERSPAN のデフォルト設定

次の表に、ERSPAN パラメータのデフォルト設定を示します。

表 *30*：デフォルトの *ERSPAN* パラメータ

パラメータ（Parameters）	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 の設定

ERSPAN 送信元セッションの設定

ERSPAN 送信元セッションは、モニタするセッション設定パラメータおよびポートまたは VLAN を定義します。ここでは、ERSPAN 送信元セッションを設定する方法について説明します。

手順

	コマンドまたはアクション	目的

ステップ 1	**configuration terminal**
	
	例：
	`switch# config t`
	`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***span-session-number***type** {**erspan-source** | **local**}
	
	例：
	`switch(config)# monitor session 1 type erspan-source`
	`switch(config-erspan-src)#`
		セッション ID とセッション タイプを使用して ERSPAN 送信元セッションを定義し、ERSPAN のモニタ送信元セッション コンフィギュレーション モードでコマンドを開始します。
		
		span-session-number 引数の範囲は 1 ～ 1024 です。同じセッション番号は複数回使用できません。
		
		送信元セッションのセッションIDは同じグローバルな ID スペース内にあるため、各セッション ID はグローバルに一意です。
		
		セッション ID（*span-session-number* 引数によって設定）およびセッション タイプ（**erspan-source** キーワードによって設定）は、入力後は変更できません。セッション ID またはセッションタイプを変更するには、コマンドの **no** バージョンを使用してセッションを削除してから、新しいセッション ID または新しいセッション タイプでコマンドを使用してセッションを再作成します。

ステップ 3	**description***erspan_session_description*
	
	例：
	`switch(config-erspan-src)#`
	`description source1`
		（任意）
		ERSPAN 送信元セッションの説明を入力します。
		
		erspan_session_description 引数には最大 32 文字を使用できます。ただし、特殊文字またはスペースは使用できません。

ステップ 4	**source interface** { **ethernet***slot/chassis number* | **portchannel***number* } 例： `switch(config-erspan-src)# source interface eth 1/1`	ERSPAN 送信元セッション番号を送信元ポート（1 ～ 255）にアソシエートします。

	コマンドまたはアクション	目的
ステップ 5	**source vlan***number* 例： `switch(config-erspan-src)# source vlan 1`	ERSPAN 送信元セッション番号を VLAN（1 ～ 4096）にアソシエートします。
ステップ 6	**source vsan***number* 例： `switch(config-erspan-src)# source vsan 1`	VSAN ID 番号を指定します。指定できる範囲は 1 ～ 4093 です。
ステップ 7	**destination ip***ip-address* 例： `switch(config-erspan-src)# destination ip 192.0.2.2`	ERSPAN セッションの宛先 IP アドレスを設定します。ERSPAN 送信元セッションごとに 1 つの宛先 IP アドレスのみがサポートされます。
ステップ 8	**erspan-id***flow-id* 例： `switch(config-erspan-src)# erspan-id 5`	ERSPAN フローを識別するフロー ID を設定します。指定できる範囲は 1 ～ 1023 です。
ステップ 9	**vrf** {*vrf-name* | **default** } 例： `switch(config-erspan-src)# vrf default`	グローバル ルーティング テーブルの代わりに使用する VRF を設定します。特に設定した VRF、またはデフォルト VRF を使用できます。
ステップ 10	[**no**] **filter access-group** *acl_filter* 例： `switch(config-erspan-src)# filter access-group erspan_acl_filter`	この ERSPAN セッションのパケットに対して ACL フィルタを設定します。ACL フィルタとして、MAC または IP アクセス リストを使用できます。
ステップ 11	**ip ttl***ttl-number* 例： `switch(config-erspan-src)# ip ttl 5`	（任意） ERSPAN トラフィック内のパケットの IP 存続可能時間（TTL）値を設定します。有効な値は、1 ～ 255 です。デフォルト値は 255 です。
ステップ 12	**ip dscp***dscp_value* 例： `switch(config-erspan-src)# ip dscp 42`	（任意） ERSPAN トラフィックのパケットの IP DiffServ コード ポイント（DSCP）値を設定します。有効値は 0 ～ 63 です。デフォルト値は 0 です
ステップ 13	**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 ステートで作成されます。

	コマンドまたはアクション	目的

ステップ 14	**exit**
	
	例：
	`switch(config-erspan-src)# exit`
	`switch(config)# exit`
		設定を更新し、ERSPAN送信元セッション コンフィギュレーション モードを終了します。

ステップ 15	**copy running-config startup-config** 例： `switch(config-erspan-src)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ERSPAN タイプ III 送信元セッションの設定

手順

	コマンドまたはアクション	目的

ステップ 1	**configuration terminal**
	
	例：
	`switch# config t`
	`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 switch-id***switch-id* 例： `switch(config)# monitor erspan switch-id 1009`	ERSPAN グローバル スイッチ ID を設定します。このスイッチ ID は、すべての ERSPAN タイプ III セッションに適用できます。デフォルト値は 0 です。
ステップ 3	**monitor erspan granularity 1588** 例： `switch(config)# monitor erspan granularity 1588`	すべての ERSPAN タイプ III セッションの粒度を指定します。1588（秒またはナノ秒単位）が、使用可能な唯一のオプションであり、デフォルト値です。

ステップ 4	**monitor session***span-session-number***type** {**erspan-source | local**}
	
	例：
	`switch(config)# monitor session 1 type erspan-source`
	`switch(config-erspan-src)#`
		セッション ID とセッション タイプを使用して ERSPAN 送信元セッションを定義し、ERSPAN のモニタ送信元セッション コンフィギュレーション モードでコマンドを開始します。
		
		span-session-number 引数の範囲は 1 ～ 1024 です。同じセッション番号は複数回使用できません。

	コマンドまたはアクション	目的
		送信元セッションのセッションIDは同じグローバルなIDスペース内にあるため、各セッションIDは両方のセッションタイプに対してグローバルに一意です。 セッション ID（*span-session-number* 引数によって設定）およびセッション タイプ（**erspan-source** キーワードによって設定）は、入力後は変更できません。セッションIDまたはセッションタイプを変更するには、コマンドの **no** バージョンを使用してセッションを削除してから、新しいセッション ID または新しいセッションタイプでコマンドを使用してセッションを再作成します。
ステップ 5	**header-type***version* 例： `switch(config-erspan-src)# header-type 3`	ERSPAN 送信元セッションをタイプ II からタイプ III に変更します。 （注） ERSPAN 送信元セッションをタイプ III からタイプ II に変更するには、このコマンドの **no** 形式を使用します。
ステップ 6	**description***erspan_session_description* 例： `switch(config-erspan-src)# description source1`	（任意） ERSPAN送信元セッションの説明を入力します。 *erspan_session_description* 引数には最大 240 文字を使用できます。ただし、特殊文字またはスペースは使用できません。
ステップ 7	**source interface** { **ethernet***slot/chassis number* | **portchannel***number* } 例： `switch(config-erspan-src)# source interface eth 1/1`	ERSPAN 送信元セッション番号を送信元ポート（1 ～ 255）にアソシエートします。
ステップ 8	**source vlan***number* 例： `switch(config-erspan-src)# source vlan 1`	ERSPAN 送信元セッション番号を VLAN（1 ～ 4096）にアソシエートします。
ステップ 9	**source vsan***number* 例： `switch(config-erspan-src)# source vsan 1`	Cisco Nexus 5000 シリーズ スイッチでは、VSAN ID 番号を指定します。指定できる範囲は 1 ～ 4093 です。Cisco Nexus 5500 シリーズ スイッチでは、送信元 VSAN を設定できません。

	コマンドまたはアクション	目的
ステップ 10	**destination ip***ip-address* 例： `switch(config-erspan-src)# destination ip 192.0.2.2`	ERSPAN セッションの宛先 IP アドレスを設定します。ERSPAN 送信元セッションごとに 1 つの宛先 IP アドレスのみがサポートされます。
ステップ 11	**erspan-id***flow-id* 例： `switch(config-erspan-src)# erspan-id 5`	ERSPAN フローを識別するフロー ID を設定します。指定できる範囲は 1 ～ 1023 です。
ステップ 12	**vrf** {*vrf-name* | **default** } 例： `switch(config-erspan-src)# vrf default`	グローバルルーティングテーブルの代わりに使用する VRF を設定します。特に設定した VRF、またはデフォルト VRF を使用できます。
ステップ 13	[**no**] **filter access-group** *acl_filter* 例： `switch(config-erspan-src)# filter access-group erspan_acl_filter`	この ERSPAN セッションのパケットに対して ACL フィルタを設定します。ACL フィルタとして、MAC または IP アクセス リストを使用できます。
ステップ 14	**ip ttl***ttl-number* 例： `switch(config-erspan-src)# ip ttl 5`	（任意） ERSPAN トラフィック内のパケットの IP 存続可能時間（TTL）値を設定します。有効な値は、1 ～ 255 です。デフォルト値は 255 です。
ステップ 15	**ip dscp***dscp_value* 例： `switch(config-erspan-src)# ip dscp 42`	（任意） ERSPAN トラフィックのパケットの IP DiffServ コード ポイント（DSCP）値を設定します。有効値は 0 ～ 63 です。デフォルト値は 0 です
ステップ 16	**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 ステートで作成されます。 （注） Cisco Nexus 5000 シリーズ スイッチでは、2 つの ERSPAN 送信元セッションのみを同時に実行できます。Cisco Nexus 5500 シリーズ スイッチでは、最大 4 つの送信元セッションを同時に実行できます。
ステップ 17	**exit** 例： `switch(config-erspan-src)# exit switch(config)# exit`	設定を更新し、ERSPAN 送信元セッション コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 18	**copy running-config startup-config** 例： `switch(config-erspan-src)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

切り捨てを適用する ERSPAN の設定

ERSPAN パケットの送信で使用されるファブリックの量またはネットワーク帯域幅の量を減らすには、ERSPAN トラフィックの MTU 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	イネーブル化 例： `switch> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。

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	**monitor session** *erspan_session_number* **type** {**erspan-source** | **local**}
	
	例：
	
	`switch(config)# monitor session 1 type erspan-source`
	`switch(config-erspan-src)#`
		セッション ID とセッション タイプを使用して ERSPAN 送信元セッションを定義し、ERSPAN のモニタ送信元セッション コンフィギュレーション モードでコマンドを開始します。
		
		span-session-number 引数の範囲は 1 ～ 1024 です。同じセッション番号は複数回使用できません。
		
		送信元セッションのセッション ID は同じグローバルな ID スペース内にあるため、各セッション ID は両方のセッション タイプに対してグローバルに一意です。
		
		セッション ID（span-session number 引数によって設定）およびセッション タイプ（erspan-source キーワードによって設定）は、入力後は変更できません。セッション ID またはセッション タイプを変更するには、コマンドの no バージョンを使用してセッションを削除してから、新しいセッション ID また

	コマンドまたはアクション	目的
		は新しいセッション タイプでコマンドを使用してセッションを再作成します。
ステップ 4	**mtu** *mtu-value* 例： `switch(config-erspan-src)# mtu 64`	ERSPAN パケットの最大伝送単位（MTU）の切り捨てサイズを定義します。有効値は 64 ～ 1518 です。 デフォルトでは、切り捨てはイネーブルではありません。
ステップ 5	**exit** 例： `switch(config-mon-erspan-src)# exit`	設定を更新し、ERSPAN 送信元セッション コンフィギュレーション モードを終了します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

ERSPAN 宛先セッションの設定

送信元 IP アドレスからローカル デバイス上の宛先ポートにパケットをコピーするように ERSPAN 宛先セッションを設定できます。デフォルトでは、ERSPAN 宛先セッションはシャット ステートで作成されます。

はじめる前に

すでにモニタ モードで宛先ポートが設定されていることを確認します。

手順

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`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*[-*port*]
	
	例：
	`switch(config)# interface ethernet 2/5`
	`switch(config-if)#`
		選択したスロットおよびポートまたはポート範囲で、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**switchport monitor** 例： `switch(config-if)# switchport monitor`	モニタ モードでスイッチ インターフェイスを設定します。 （**destination interface ethernet***interface* コマンドを使用して）インターフェイスを ERSPAN または SPAN 宛先に設定するには、最初にモニタ モードで設定する必要があります。
ステップ 4	**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 5	**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 6	**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 7	**source ip***ip-address* 例： `switch(config-erspan-dst)# source ip 10.1.1.1`	ERSPAN セッションの送信元 IP アドレスを設定します。ERSPAN 宛先セッションごとに 1 つの送信元 IP アドレスのみがサポートされます。 この IP アドレスは、対応する ERSPAN 送信元セッションに設定されている宛先 IP アドレスと一致する必要があります。
ステップ 8	**destination** {[**interface** [*type slot/port*[-*port*], [*type slot/port* [*port*]]] [**port-channel***channel-number*]]} 例： `switch(config-erspan-dst)# destination interface ethernet 2/5`	コピーされたソース パケットの宛先を設定します。宛先として、インターフェイスのみ設定できます。 （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 9	**erspan-id***erspan-id* 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。この ID は、送信元および宛先の ERSPAN セッションのペアを一意に識別します。対応する宛先の ERSPAN セッションに設定される ERSPAN ID は、送信元のセッションで設定されているものと同じにする必要があります。
ステップ 10	**vrf***default* 例： `switch(config-erspan-dst)# vrf default`	ERSPAN 宛先セッションがトラフィックの転送に使用する VRF インスタンスを設定します。 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。
ステップ 11	**no shut** 例： `switch(config)# no shut`	ERSPAN宛先セッションをイネーブルにします。デフォルトでは、セッションはシャット ステートで作成されます。 （注） 同時に実行できるアクティブな ERSPAN 宛先セッションは 16 個だけです。
ステップ 12	**show monitor session** {**all** | *session-number* | **range***session-range*} 例： `switch(config)# show monitor session 3`	（任意） ERSPAN セッション設定を表示します。
ステップ 13	**show running-config monitor** 例： `switch(config-erspan-src)# show running-config monitor`	（任意） ERSPAN の実行コンフィギュレーションを表示します。
ステップ 14	**show startup-config monitor** 例： `switch(config-erspan-src)# show startup-config monitor`	（任意） ERSPAN のスタートアップ コンフィギュレーションを表示します。
ステップ 15	**copy running-config startup-config** 例： `switch(config-erspan-src)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ERSPAN SPAN-on-Drop セッションの設定

ERSPAN SPAN-on-Drop セッションを設定するには、monitor session コマンドを使用します。各セッションは、一意のセッション番号で識別されます。

（注） アクティブにできるのは、常に SPAN-on-Drop または SPAN-on-Drop ERSPAN セッション 1 つだけです。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config) # **monitor session** *session-number* **type erspan-span-on-drop**	指定した SPAN-on-drop セッションの SPAN-on-Drop 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	switch(config-span-on-drop-erspan) # **description***description*	SPAN-on-Drop セッションのわかりやすい名前を作成します。
ステップ 4	switch(config-span-on-drop-erspan) # **source interface ethernet***slot*/*port***rx**	送信元およびパケットをコピーするトラフィック方向を設定します。イーサネット ポートの範囲を入力できます。トラフィックの方向を指定して、入力（rx）としてのみ複製することができます。
ステップ 5	switch(config-span-on-drop-erspan) # **destination ip***ip-address*	ERSPAN SPAN-on-Drop セッションに対して宛先 IP アドレスを設定します。
ステップ 6	switch(config-span-on-drop-erspan) # **erspan-id***erspan-id*	ERSPAN SPAN-on-Drop セッションに対して ERSPAN ID を設定します。指定できる範囲は 1 ～ 1023 です。この ID は、送信元および宛先の ERSPAN セッションのペアを一意に識別します。対応する宛先の ERSPAN セッションに設定される ERSPAN ID は、送信元のセッションで設定されているものと同じにする必要があります。
ステップ 7	switch(config-span-on-drop-erspan) # **ip ttl***ttl-value*	ERSPAN トラフィックの IP 存続可能時間（TTL）値を設定します。
ステップ 8	switch(config-span-on-drop-erspan) # **ip dscp***dscp-value*	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。

	コマンドまたはアクション	目的
ステップ 9	switch(config) # **show monitor session***session-number*	（任意） ERSPAN SPAN-on-Drop セッションのステータスを表示します。
ステップ 10	switch(config) # **copy running-config** startup-config	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ERSPAN SPAN-on-Latency セッションの設定

ERSPAN パケットの送信で使用されるファブリックの量またはネットワーク帯域幅の量を減らすには、ERSPAN トラフィックの MTU 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	イネーブル化 例： `switch> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。

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	**interface ethernet***slot/port* 例： `switch(config)# interface ethernet 1/1`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**packet latency threshold***threshold* 例： `switch(config-if)# packet latency threshold 53000000`	インターフェイスの遅延しきい値を設定します。有効な値は 8 ～ 536870904 ナノ秒です。

ステップ 5	**monitor session***session_number***typespan-on-latency-erspan**
	
	例：
	
	`switch(config)# monitor session 1 type span-on-latency-erspan`
	`switch(config-span-on-latency-erspan)#`
		セッション ID とセッション タイプを使用して ERSPAN 送信元セッションを定義し、ERSPAN のモニタ送信元セッション コンフィギュレーション モードでコマンドを開始します。

	コマンドまたはアクション	目的
		session_number 引数の範囲は 1 ～ 1024 です。同じセッション番号は複数回使用できません。 セッション ID（span_session number 引数によって設定）およびセッション タイプ（span-on-latency-erspan キーワードによって設定）は、入力後は変更できません。セッション ID またはセッションタイプを変更するには、コマンドの no バージョンを使用してセッションを削除してから、新しいセッション ID または新しいセッション タイプでコマンドを使用してセッションを再作成します。
ステップ 6	**description***description* 例： `switch(config-span-on-latency-erspan)# description SPAN-on-Latency-ERSPAN-session`	セッション設定に説明を追加します。
ステップ 7	**source interface ethernet***slot/port* 例： `switch(config-span-on-latency-erspan)# source interface ethernet 1/3`	イーサネット インターフェイスを送信元 SPAN ポートとして使用するように指定します。 （注） 複数の SPAN 送信元ポートを設定できます。
ステップ 8	**destination ip***ip-address* 例： `switch(config-span-on-latency-erspan)# destination ip 10.0.3.1`	セッションの宛先 IP アドレスを設定します。
ステップ 9	**erspan-id***flow-id* 例： `switch(config-span-on-latency-erspan)# erspan-id 30`	セッションのフロー ID を設定します。 指定できる範囲は 1 ～ 1023 です。
ステップ 10	**ip ttl***flow-id* 例： `switch(config-span-on-latency-erspan)# erspan-id 30`	（任意） （任意）ERSPAN トラフィックの IP 存続可能時間（TTL）値を設定します。 範囲は 1 ～ 255 です。

	コマンドまたはアクション	目的
ステップ 11	**ip dscp***flow-id* 例： `switch(config-span-on-latency-erspan)# ip dscp 63`	（任意） （任意）ERSPAN トラフィックのパケットの DiffServ コード ポイント（DSCP）値を設定します。 範囲は 0 ～ 63 です。
ステップ 12	**mtu***mtu-value* 例： `switch(config-span-on-latency-erspan)# mtu 1500`	（任意） （任意）ERSPAN パケットの最大伝送単位（MTU）の切り捨てサイズを定義します。有効値は 64 ～ 1518 です。 デフォルトでは、切り捨てはイネーブルではありません。
ステップ 13	**exit** 例： `switch(config-span-on-latency-erspan)# exit`	設定を更新し、ERSPAN SPAN-on-Latency セッションのコンフィギュレーション モードを終了します。
ステップ 14	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

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。同時に実行できる ERSPAN セッション数は限定されているため、あるセッションをシャットダウンしてハードウェア リソースを解放することによって、別のセッションが使用できるようになります。デフォルトでは、ERSPAN セッションはシャット ステートで作成されます。

ERSPAN セッションをイネーブルにすると、送信元から宛先へのパケットのコピーをアクティブ化できます。すでにイネーブルになっていて、動作状況がダウンの ERSPAN セッションをイネーブルにするには、そのセッションをいったんシャットダウンしてから、改めてイネーブルにする必要があります。ERSPAN セッション ステートをシャットダウンおよびイネーブルにするには、グローバルまたはモニタ コンフィギュレーション モードのいずれかのコマンドを使用できます。

手順

	コマンドまたはアクション	目的

ステップ 1	**configuration terminal**
	
	例：
	`switch# configuration 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。セッションの範囲は 1 ～ 48 です。デフォルトでは、セッションはシャット ステートで作成されます。 （注） • Cisco Nexus 5000 および 5500 プラットフォームでは、2 つのセッションを同時に実行できます。 • Cisco Nexus 5600 および 6000 プラットフォームでは、16 のセッションを同時に実行できます。
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。セッションの範囲は 1 ～ 48 です。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。同時に実行できるのは2つのセッションのみです. （注） モニタ セッションがイネーブルで動作状況がダウンの場合、セッションをイネーブルにするには、最初に **monitor session shut** コマンドを指定してから、**no monitor session shut** コマンドを続ける必要があります。

ステップ 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	**monitor session***session-number***type erspan-destination** 例： `switch(config-erspan-src)# monitor session 3 type erspan-destination`	ERSPAN 宛先タイプのモニタ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 6	**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 ステートで作成されます。
ステップ 7	**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 8	**show monitor session all** 例： `switch(config-erspan-src)# show monitor session all`	（任意） ERSPANセッションのステータスを表示します。
ステップ 9	**show running-config monitor** 例： `switch(config-erspan-src)# show running-config monitor`	（任意） ERSPANの実行コンフィギュレーションを表示します。
ステップ 10	**show startup-config monitor** 例： `switch(config-erspan-src)# show startup-config monitor`	（任意） ERSPANのスタートアップ コンフィギュレーションを表示します。
ステップ 11	**copy running-config startup-config** 例： `switch(config-erspan-src)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ERSPAN 設定の確認

ERSPAN の設定情報を確認するには、次のコマンドを使用します。

コマンド	目的
show monitor session {**all** | *session-number* | **range***session-range*}	ERSPAN セッション設定を表示します。
show running-config monitor	ERSPANの実行コンフィギュレーションを表示します。
show startup-config monitor	ERSPAN のスタートアップ コンフィギュレーションを表示します。

ERSPAN の設定例

ERSPAN 送信元セッションの設定例

次に、ERSPAN 送信元セッション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)# monitor session 1 type erspan-source
switch(config-erspan-src)# description source1
switch(config-erspan-src)# source interface ethernet 1/1
switch(config-erspan-src)# source vlan 1
switch(config-erspan-src)# source vsan 1
switch(config-erspan-src)# destination ip 192.0.2.2
switch(config-erspan-src)# erspan-id 1
switch(config-erspan-src)# vrf default
switch(config-erspan-src)# ip ttl 5
switch(config-erspan-src)# ip dscp 5
switch(config-erspan-src)# no shut
switch(config-erspan-src)# exit
switch(config)# copy running-config startup config
```

ERSPAN タイプ III 送信元セッションの設定例

次に、ERSPAN タイプ III 送信元セッションを設定する例を示します。

```
switch# configuration terminal
switch(config)# monitor erspan switch-id 1009
switch(config)# monitor erspan granularity 1588
switch(config)# monitor session 1 type erspan-source
switch(config-erspan-src)# header-type 3
switch(config-erspan-src)# description source1
switch(config-erspan-src)# source interface ethernet 1/1
switch(config-erspan-src)# source vlan 1
switch(config-erspan-src)# source vsan 1
switch(config-erspan-src)# destination ip 192.0.2.2
switch(config-erspan-src)# erspan-id 5
switch(config-erspan-src)# vrf default
switch(config-erspan-src)# filter access-group erspan_acl_filter
switch(config-erspan-src)# ip ttl 5
switch(config-erspan-src)# ip dscp 42
switch(config-erspan-src)# no shut
switch(config-erspan-src)# exit
switch(config)# exit
```

ERSPAN セッションの送信元としての IP アドレスの設定例

次に、ERSPAN セッションの送信元として IP アドレスを設定する例を示します。

```
switch# configure terminal
switch(config)# monitor erspan origin ip-address 192.0.2.1
switch(config)#  exit
switch(config)# copy running-config startup config
```

切り捨てを適用する ERSPAN の設定例

次に、切り捨てを適用する ERSPAN を設定する例を示します。

```
switch# configure terminal
switch(config)# monitor session 1 type erspan-source
switch(config-erspan-src)# mtu 64
switch(config-mon-erspan-src)# exit
switch(config)# copy running-config startup config
```

ERSPAN 宛先セッションの設定例

次に、ERSPAN 宛先セッションを設定する例を示します。

```
switch# config t
switch(config)# interface e14/29
switch(config-if)# no shut
switch(config-if)# switchport
switch(config-if)# switchport monitor
switch(config-if)# exit
switch(config)# monitor session 2 type erspan-destination
switch(config-erspan-dst)# source ip 9.1.1.2
switch(config-erspan-dst)# destination interface e14/29
switch(config-erspan-dst)# erspan-id 1
switch(config-erspan-dst)# vrf default
switch(config-erspan-dst)# no shut
switch(config-erspan-dst)# exit
switch(config)# show monitor session 2
switch# config t
switch(config)# interface e14/29
switch(config-if)# no shut
switch(config-if)# switchport
switch(config-if)# switchport monitor
switch(config-if)# exit
switch(config)# monitor session 2 type erspan-destination
switch(config-erspan-dst)# source ip 9.1.1.2
switch(config-erspan-dst)# destination interface e14/29
switch(config-erspan-dst)# erspan-id 1
switch(config-erspan-dst)# no shut
switch(config-erspan-dst)# exit
switch(config)# show monitor session 2
```

ERSPAN ACL の設定例

次に、ERSPAN ACL を設定する例を示します。

```
switch# configure terminal
switch(config)# ip access-list match_11_pkts
switch(config-acl)# permit ip 11.0.0.0 0.255.255.255 any
switch(config-acl)# exit
switch(config)# monitor session 1 type erspan-source
switch(config-erspan-src)# filter access-group match_11_pkts
```

ERSPAN SPAN-on-Drop セッションの設定例

次に、ERSPAN SPAN-on-Drop セッションを設定する例を示します。

```
switch# configure terminal
switch(config) # monitor session 47 type span-on-drop-erspan
switch(config-span-on-drop-erspan) # description span-on-drop-erspan-session_47
switch(config-span-on-drop-erspan) # source interface ethernet 1/3
switch(config-span-on-drop-erspan) # destination ip 10.1.1.1
switch(config-span-on-drop-erspan) # erspan-id 30
switch(config-span-on-drop-erspan) # ip ttl 245
switch(config-span-on-drop-erspan) # ip dscp 36
switch(config) # copy running-config startup-config
switch(config) #
```

ERSPAN SPAN-on-Latency セッションの設定例

次に、ERSPAN SPAN-on-Latency セッションを設定する例を示します。

```
switch# configure terminal
switch(config) # interface ethernet 1/1
switch(config-if) # packet latency threshold 530000000
switch(config) # monitor session 10 type span-on-latency-erspan
switch(config-span-on-latency-erspan) # description span-on-latency-erspan-session_10
switch(config-span-on-latency-erspan) # source interface ethernet 1/3
switch(config-span-on-latency-erspan) # destination ip 192.0.3.1
switch(config-span-on-latency-erspan) # erspan-id 30
switch(config-span-on-latency-erspan) # ip ttl 245
switch(config-span-on-latency-erspan) # ip dscp 36
switch(config-span-on-latency-erspan) # mtu 1500
switch(config-span-on-latency-erspan) # vrf default
switch(config) # copy running-config startup-config
switch(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
ERSPAN コマンド：コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト、使用上の注意事項、および例	ご使用プラットフォームの『*Cisco Nexus NX-OS System Management Command Reference*』。

第 18 章

NTP の設定

この章の内容は、次のとおりです。

- NTP の概要，245 ページ
- ライセンス要件，247 ページ
- NTP の前提条件，247 ページ
- NTP の注意事項と制約事項，247 ページ
- NTP のデフォルト設定，248 ページ
- NTP の設定，249 ページ
- NTP の設定確認，259 ページ
- NTP の設定例，260 ページ

NTP の概要

NTP サーバに関する情報

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

すべての NTP 通信は UTC を使用します。

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

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

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

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

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

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

タイム サーバとしての NTP

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

CFS を使用した NTP の配信

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

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

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

クロック マネージャ

クロックはさまざまなプロセス間で共有する必要のあるリソースです。

NTP や高精度時間プロトコル（PTP）といった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。

ハイ アベイラビリティ

NTP はステートレス リスタートをサポートします。リブート後またはスーパーバイザ スイッチオーバー後に、実行コンフィギュレーションが適用されます。

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。

ライセンス要件

製品	ライセンス要件
Cisco NX-OS	NTP にはライセンスは不要です。ライセンス パッケージに含まれていない機能はすべてCisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。NX-OS ライセンス方式の詳細については、『Cisco NX-OS Licensing Guide』を参照してください。

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。

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

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

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

NTP 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。

表 *31*：デフォルトの *NTP* パラメータ

パラメータ（Parameters）	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 ロギング	ディセーブル

NTP の設定

NTP のイネーブル化/ディセーブル化

はじめる前に

正しい VDC 内にいることを確認します。VDC を変更するには、**switchto vdc** コマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# [**no**] **feature ntp**	VDC で NTP をイネーブル/ディセーブルにします。NTP はデフォルトでイネーブルです。 （注） NTP は [**no**] **ntp enable** コマンドを使用してイネーブル/ディセーブルにします。
ステップ 3	switch(config)# **show ntp status**	（任意） NTP アプリケーションのステータスを表示します。
ステップ 4	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、NTP をディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# no feature ntp
```

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	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	[**no**] **ntp master** [*stratum*]	正規の NTP サーバとしてデバイスを設定します。 NTP クライアントがこれらの時間を同期するのと別の階層レベルを指定できます。指定できる範囲は 1 ～ 15 です。
ステップ 3	**show running-config ntp**	（任意） NTP コンフィギュレーションを表示します。
ステップ 4	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、正規の NTP サーバとして Cisco NX-OS デバイスを別の階層レベルで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 master 5
```

NTP サーバおよびピアの設定

NTP サーバおよびピアを設定できます。

はじめる前に

NTP サーバとそのピアの IP アドレスまたは 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	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# [**no**] **ntp server** {*ip-address* | *ipv6-address* | *dns-name*} [**key***key-id*]	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。

	コマンドまたはアクション	目的
	[**maxpoll***max-poll*] [**minpoll***min-poll*] [**prefer**] [**use-vrf***vrf-name*]	*key-id* 引数の範囲は 1 ～ 65535 です。 ピアをポーリングする最大および最小の間隔を設定するには、**maxpoll** および **minpoll** キーワードを使用します。*max-poll* および *min-poll* 引数の範囲は 4 ～ 16 秒で、デフォルト値はそれぞれ 6 秒と 4 秒です。 デバイスに対して対象の NTP サーバを優先にするには、**prefer keyword** キーワードを使用します。 指定された VRF を介して通信するように NTP サーバを設定するには、**use-vrf** キーワードを使用します。 *vrf-name* 引数として、default、management、または大文字と小文字を区別した 32 文字までの任意の英数字の文字列を使用できます。 （注） NTP サーバとの通信で使用するキーを設定する場合は、そのキーが、デバイス上の信頼できるキーとして存在していることを確認してください。
ステップ 3	switch(config)# [**no**] **ntp peer** {*ip-address* | *ipv6-address* | *dns-name*} [**key***key-id*] [**maxpoll***max-poll*] [**minpoll***min-poll*] [**prefer**] [**use-vrf***vrf-name*]	1 つのピアと 1 つのピア アソシエーションを形成します。複数のピア アソシエーションを指定できます。 NTP ピアとの通信で使用するキーを設定するには、**key** キーワードを使用します。*key-id* 引数の範囲は 1 ～ 65535 です。 ピアをポーリングする最大および最小の間隔を設定するには、**maxpoll** および **minpoll** キーワードを使用します。*max-poll* および *min-poll* 引数の範囲は 4 ～ 17 秒で、デフォルト値はそれぞれ 6 秒と 4 秒です。 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。 指定された VRF を介して通信するように NTP ピアを設定するには、**use-vrf** キーワードを使用します。*vrf-name* 引数として、**default**、**management**、または大文字と小文字を区別した 32 文字までの任意の英数字の文字列を使用できます。
ステップ 4	switch(config)# **show ntp peers**	（任意） 設定されたサーバおよびピアを表示します。 （注） ドメイン名が解決されるのは、DNS サーバが設定されている場合だけです。

	コマンドまたはアクション	目的
ステップ 5	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

NTP 認証の設定

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

はじめる前に

NTP サーバと NTP ピアの認証は、各 **ntp server** および **ntp peer** コマンドで key キーワードを使用して、ピア アソシエーションごとに設定されます。この手順で指定する予定の認証キーによって、すべての NTP サーバとピア アソシエーションが設定されていることを確認します。key キーワードを指定しない **ntp server** または **ntp peer** コマンドは、認証なしで動作を続行します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# [**no**] **ntp authentication-key***number***md5***md5-string*	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。
ステップ 3	switch(config)# **show ntp authentication-keys**	（任意） 設定済みの NTP 認証キーを表示します。
ステップ 4	switch(config)# [**no**] **ntp trusted-key***number*	1 つ以上のキー（ステップ 2 で定義されているもの）を指定します。デバイスが時刻源と同期するために、時刻源はこのキーを NTP パケット内に提供する必要があります。 Trusted Key の範囲は 1 ～ 65535 です。

	コマンドまたはアクション	目的
		このコマンドにより、デバイスが、信頼されていない時刻源と誤って同期する、ということが防止されます。
ステップ 5	switch(config)# **show ntp trusted-keys**	（任意） 設定済みの NTP の信頼されているキーを表示します。
ステップ 6	switch(config)# [**no**] **ntp authenticate**	NTP 認証機能をイネーブルまたはディセーブルにします。NTP認証はデフォルトでディセーブルになっています。
ステップ 7	switch(config)# **show ntp authentication-status**	（任意） NTP 認証の状況を表示します。
ステップ 8	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、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 10.1.1.1 key 42
switch(config)# ntp trusted-key 42
switch(config)# ntp authenticate
switch(config)# copy running-config startup-config
[##########################################] 100%
switch(config)#
```

NTP アクセス制限の設定

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

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# [**no**] **ntp access-group** {**peer** | **serve** | **serve-only** | **query-only**} *access-list-name*	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。 アクセス グループのオプションは、次の順序で制限の緩いものから厳しいものへとスキャンされます。ただし、ピアに設定された拒否 ACL ルールに NTP が一致した場合、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。 • **peer** キーワードは、デバイスが時刻要求と NTP 制御クエリーを受信し、アクセスリストで指定されているサーバと同期するようにします。 • **serve** キーワードは、アクセスリストに指定されているサーバからの時刻要求と NTP 制御クエリーをデバイスが受信できるようにしますが、指定されたサーバとは同期しないようにします。 • **serve-only** キーワードは、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。
ステップ 3	switch(config)# **show ntp access-groups**	（任意）NTP アクセス グループのコンフィギュレーションを表示します。
ステップ 4	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、アクセス グループ「accesslist1」からピアと同期できるようデバイスを設定する例を示します。

```
switch# configure terminal
switch(config)# ntp access-group peer accesslist1
switch(config)# show ntp access-groups
Access List Type
-----------------------------
```

```
accesslist1 Peer
switch(config)# copy running-config startup-config
[##########################################] 100%
switch(config)#
```

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	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	[**no**] **ntp source** *ip-address*	すべての NTP パケットにソース IP アドレスを設定します。*ip-address* には IPv4 または IPv6 形式を使用できます。

次に、NTP ソース IP アドレスに 192.0.2.2 を設定する例を示します。

```
switch# configure terminal
switch(config)# ntp source 192.0.2.2
```

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	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	[**no**] **ntp source-interface** *interface*	すべての NTP パケットに対してソースインターフェイスを設定します。次のリストに、*interface* として有効な値を示します。 • ethernet • loopback • mgmt • port-channel

	コマンドまたはアクション	目的
		• vlan

次に、NTP 送信元インターフェイスを設定する例を示します。

```
switch# configure terminal
switch(config)# ntp source-interface ethernet
```

NTP ロギングの設定

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# [**no**] **ntp logging**	重要な NTP イベントでシステム ログを生成することをイネーブルまたはディセーブルにします。NTP ロギングはデフォルトでディセーブルになっています。
ステップ 3	switch(config)# **show ntp logging-status**	（任意） NTP ロギングのコンフィギュレーション状況を表示します。
ステップ 4	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、重要な NTP イベントによってシステム ログを生成するよう、NTP ロギングをイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# ntp logging
switch(config)# copy running-config startup-config
[########################################] 100%
switch(config)#
```

NTP 用の CFS 配信のイネーブル化

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

はじめる前に

デバイスの CFS 配信をイネーブルにしていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# [**no**] **ntp distribute**	CFS を介して配信される NTP コンフィギュレーションのアップデートをデバイスが受信することを、イネーブルまたはディセーブルにします。
ステップ 3	switch(config)# **show ntp status**	（任意） NTP CFS の配信状況を表示します。
ステップ 4	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

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

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

NTP 設定変更のコミット

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **ntp commit**	ネットワーク内のすべての Cisco NX-OS デバイスに NTP コンフィギュレーションの変更を配信し、CFS ロックを解放します。このコマンドは、保留データベースに対して行われた変更によって、有効なデータベースを上書きします。

NTP 設定変更の廃棄

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **ntp abort**	保留データベースで NTP コンフィギュレーションの変更を破棄して、CFS ロックを解放します。このコマンドは、NTP コンフィギュレーションを起動したデバイスで使用します。

CFS セッション ロックの解放

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **clear ntp session**	保留データベースでNTPコンフィギュレーションの変更を破棄して、CFS ロックを解放します。

NTP の設定確認

コマンド	目的
show ntp access-groups	NTPアクセスグループのコンフィギュレーションを表示します。
show ntp authentication-keys	設定済みの NTP 認証キーを表示します。
show ntp authentication-status	NTP 認証の状況を表示します。
show ntp internal	内部の NTP 情報を表示します。
show ntp logging-status	NTP のロギング状況を表示します。
show ntp peer-status	すべての NTP サーバおよびピアのステータスを表示します。
show ntp peer	すべての NTP ピアを表示します。
show ntp pending	NTP用の一時CFSデータベースを表示します。
show ntp pending-diff	保留 CFS データベースと現行の NTP コンフィギュレーションの差異を表示します。
show ntp rts-update	RTS アップデートの状況を表示します。
show ntp session status	NTPCFS配信セッションの情報を表示します。
show ntp source	設定済みの NTP ソース IP アドレスを表示します。

コマンド	目的
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*} | **name** *peer-name*}}	NTP 統計情報を表示します。
show ntp status	NTP CFS の配信状況を表示します。
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 の設定例

NTP の設定例

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

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ntp server 192.0.2.105 key 42
switch(config)# ntp peer 192.0.2.105
switch(config)# show ntp peers
--------------------------------------------------
Peer IP Address Serv/Peer
--------------------------------------------------
192.0.2.100 Peer (configured)
192.0.2.105 Server (configured)
switch(config)# ntp authentication-key 42 md5 aNiceKey
switch(config)# show ntp authentication-keys
-----------------------------
Auth key MD5 String
-----------------------------
42 aNicekey
switch(config)# ntp trusted-key 42
switch(config)# show ntp trusted-keys
Trusted Keys:
42
switch(config)# ntp authenticate
switch(config)# show ntp authentication-status
Authentication enabled.
switch(config)# ntp logging
switch(config)# show ntp logging
NTP logging enabled.
switch(config)# copy running-config startup-config
[########################################] 100%
switch(config)#
```

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

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

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

第 19 章

EEM の設定

この章の内容は、次のとおりです。

- Embedded Event Manager について，263 ページ
- EEM ポリシー，264 ページ
- EEM イベント文，265 ページ
- EEM アクション文，266 ページ
- VSH スクリプト ポリシー，267 ページ
- EEM イベント相関，267 ページ
- EEM 仮想化サポート，268 ページ
- EEM のライセンス要件，268 ページ
- EEM の前提条件，268 ページ
- EEM の注意事項と制約事項，268 ページ
- EEM のデフォルト設定，269 ページ
- EEM の設定，269 ページ
- EEM 設定の確認，283 ページ
- EEM のコンフィギュレーション例，284 ページ

Embedded Event Manager について

Embedded Event Manager（EEM）はデバイス上で発生するイベントをモニタし、設定に基づいて各イベントの回復またはトラブルシューティングのためのアクションを実行します。

EEM は次の 3 種類の主要コンポーネントからなります。

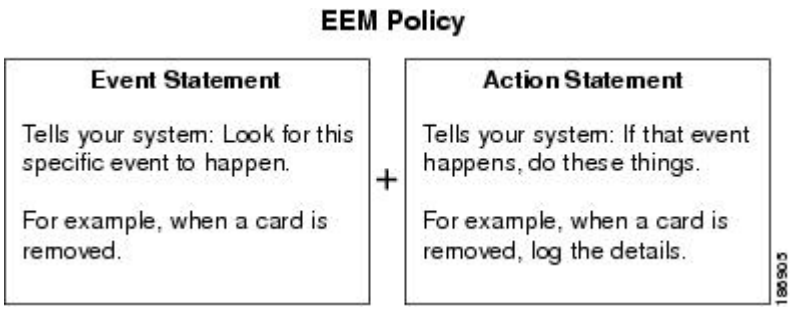
- イベント文：別の Cisco NX-OS コンポーネントからモニタし、アクション、回避策、または通知が必要になる可能性のあるイベント。
- アクション文：電子メールの送信、インターフェイスのディセーブル化など、イベントから回復するために EEM が実行できるアクション。
- ポリシー：イベントのトラブルシューティングまたはイベントからの回復を目的とした 1 つまたは複数のアクションとペアになったイベント。

EEM 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。

次の図に、EEM ポリシーの基本的な 2 種類の文を示します。

図 *2*：*EEM* ポリシー文



EEM ポリシーを設定するには、CLI または VSH スクリプトを使用します。

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。ユーザポリシーを設定する場合には、CLI によるユーザ ポリシーの定義，（270 ページ）を参照してください。

一部のシステムポリシーは上書きすることもできます。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。

上書きポリシーを設定する場合は、ポリシーの上書き，（277 ページ）を参照してください。

（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。

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。

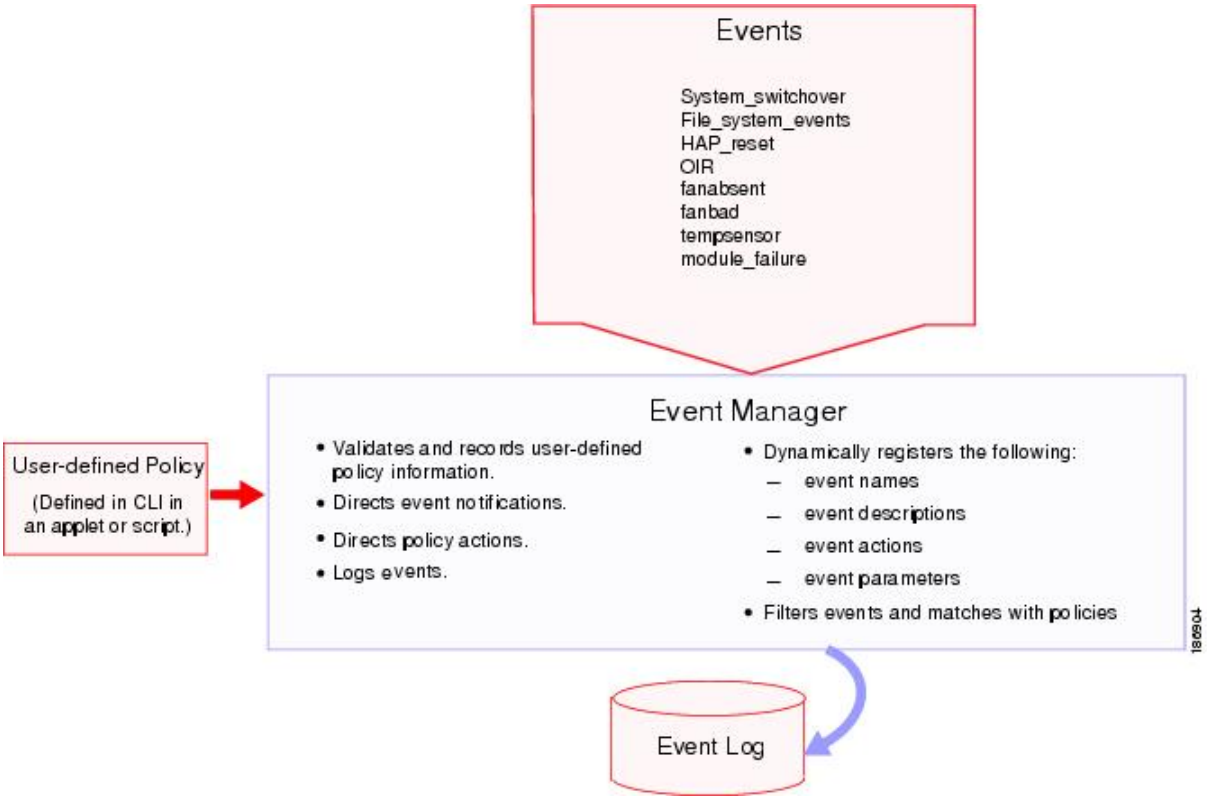
EEM イベント文

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。

次の図は、EEM によって処理されたイベントを示します。

図 3 : *EEM* の概要



イベント文では、ポリシー実行のトリガーになるイベントを指定します。複数イベントの設定の詳細については、EEM イベント相関, （267 ページ）を参照してください。

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。

EEM アクション文

アクション文は、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。
- デバイスのリロード。
- Syslog メッセージの生成。
- SNMP 通知の生成。
- システム ポリシー用デフォルト アクションの使用。

（注） 発生したイベントでデフォルトのアクションを処理できるようにする場合は、デフォルトのアクションを許可する EEM ポリシーを設定する必要があります。たとえば、match 文で CLI コマンドを照合する場合、EEM ポリシーに event-default アクション文を追加する必要があります。この文がないと、EEM では CLI コマンドを実行できません。

ユーザ ポリシーまたは上書きポリシーの中に、相互に否定したり、関連付けられたシステム ポリシーに悪影響を与えたりするようなアクション文がないかどうかを確認してください。

VSH スクリプト ポリシー

テキストエディタを使用し、VSHスクリプトでポリシーを作成することもできます。このようなポリシーにも、他のポリシーと同様、イベント文およびアクション文（複数可）を使用します。また、これらのポリシーでシステムポリシーを補うことも上書きすることもできます。VSHスクリプトポリシーを書き込んだ後、デバイスにコピーしてアクティブにします。VHSスクリプトでポリシーを設定する場合は、VSHスクリプトによるポリシーの定義,（276ページ）を参照してください。

EEM イベント相関

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、not）を使用し、カウントと時間を合わせて、カスタム アクションをトリガーするためのこれらイベントの組み合わせを定義できます。

（注） EEMイベント相関の設定方法の詳細については、CLIによるユーザ ポリシーの定義,（270ページ）を参照してください。

EEM 仮想化サポート

ログインした仮想デバイスコンテキスト（VDC）で、EEM を設定します。デフォルトでは、Cisco NX-OS はデフォルト VDC に配置します。モジュールベースのイベントに対応するポリシーを設定する場合は、この VDC を使用する必要があります。

すべての VDC ですべてのアクションまたはイベントを確認できるわけではありません。ポリシーを設定するには、network-admin または vdc-admin の権限が必要です。

EEM のライセンス要件

製品	ライセンス要件
Cisco NX-OS	EEM にはライセンスは不要です。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。NX-OS ライセンス方式の詳細については、『Cisco NX-OS Licensing Guide』を参照してください。

EEM の前提条件

EEM には次の前提条件があります。

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

EEM の注意事項と制約事項

EEM に関する設定時の注意事項および制約事項は、次のとおりです。

- 設定可能な EEM ポリシーの最大数は 500 です。
- ユーザ ポリシーまたは上書きポリシー内のアクション文が、相互に否定したり、関連付けられたシステム ポリシーに悪影響を与えたりするようなことがないようにする必要があります。
- 発生したイベントでデフォルトのアクションを処理できるようにする場合は、デフォルトのアクションを許可する EEM ポリシーを設定する必要があります。たとえば、match 文で CLI コマンドを照合する場合、EEM ポリシーに event-default アクション文を追加する必要があります。この文がないと、EEM では CLI コマンドを実行できません。
- イベント文が指定されていて、アクション文が指定されていない上書きポリシーを設定した場合、アクションは開始されません。また、障害も通知されません。

- 上書きポリシーにイベント文が含まれていないと、システム ポリシーで可能性のあるイベントがすべて上書きされます。
- 通常コマンドの表現の場合、すべてのキーワードを拡張する必要があり、アスタリスク（*）記号のみが引数の置換に使用できます。
- EEM イベント相関は 1 つのポリシーに最大 4 つのイベント文をサポートします。イベント タイプは同じでも別でもかまいませんが、サポートされるイベント タイプは、cli、カウンタ、モジュール、モジュール障害、oir、snmp、syslog、追跡だけです。
- 複数のイベント文が EEM ポリシーに存在する場合は、各イベント文に **tag** キーワードと一意な *tag* 引数が必要です。
- EEM イベント相関はシステムのデフォルト ポリシーを上書きしません。
- デフォルト アクション実行は、タグ付きのイベントで設定されているポリシーではサポートされません。

EEM のデフォルト設定

次の表に、EEM パラメータのデフォルト設定を示します。

表 *32* : デフォルトの *EEM* パラメータ

パラメータ（Parameters）	デフォルト
システム ポリシー	Active

EEM の設定

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。

はじめる前に

正しい VDC 内にいることを確認します。VDC を変更するには、**switchto vdc** コマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **event manager environment** *variable-name variable-value*	EEM 用の環境変数を作成します。*variable-name* は大文字と小文字を区別し、最大 29 の英数字を使用できます。*variable-value* には最大 39 文字の英数字を引用符で囲んで使用できます。
ステップ 3	switch(config)# **show event manager environment** {*variable-name* | **all**}	（任意） 設定した環境変数に関する情報を表示します。ストリングは引用符で囲みます。
ステップ 4	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、環境変数を定義する例を示します。

```
switch# configure terminal
switch(config)# event manager environment emailto "admin@anyplace.com"
switch(config)# show event manager environment all
switch(config)# copy running-config startup-config
```

CLI によるユーザ ポリシーの定義

CLI を使用したユーザ ポリシーを定義できます。

はじめる前に

正しい VDC 内にいることを確認します。VDC を変更するには、**switchto vdc** コマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **event manager applet** *applet-name*	EEM にアプレットを登録し、アプレット コンフィギュレーション モードを開始します。*applet-name*

	コマンドまたはアクション	目的
		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	switch(config-applet)# **description** *policy-description*	（任意） ポリシーの説明になるストリングを設定します。string には最大 80 文字の英数字を使用できます。ストリングは引用符で囲みます。
ステップ 4	switch(config-applet)# **event** *event-statement*	ポリシーのイベント文を設定します。イベント文の設定，（272 ページ）を参照してください。 イベント文が複数の場合は、ステップ 4 を繰り返します。
ステップ 5	switch(config-applet)# **tag** *tag* {**and** | **andnot** | **or**} *tag* [**and** | **andnot** | or {*tag*}] {**happens** *occurs* **in** *seconds*}	（任意） ポリシー内の複数のイベントを相互に関連付けます。 *occurs* 引数の範囲は 1 ～ 4294967295 です。*seconds* 引数の範囲は 0～4294967295 秒です。
ステップ 6	switch(config-applet)# **action** *number*[.*number2*] *action-statement*	ポリシーのアクション文を設定します。アクション文の設定，（274 ページ）を参照してください。 アクション文が複数の場合は、ステップ 6 を繰り返します。
ステップ 7	switch(config-applet)# **show event manager policy-state** *name* [**module** *module-id*]	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	switch(config-applet)# **copy running-config startup-config**	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、CLI を使用してユーザ ポリシーを定義する例を示します。

```
switch# configure terminal
switch(config)# event manager applet monitorShutdown
switch(config-applet)# description "Monitors interface shutdown."
switch(config-applet)# event cli match "shutdown"
switch(config-applet)# tag one or two happens 1 in 10000
switch(config-applet)# action 1.0 cli local show interface e 3/1
switch(config-applet)# show event manager policy-state monitorShutdown
switch(config-applet)# 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、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
event cli [**tag** *tag*] **match** *expression* [**count** *repeats* | **time** *seconds*] 例： switch(config-applet)# event cli match "shutdown"	正規表現と一致するコマンドが入力された場合に、イベントを発生させます。 **tag** *tag* キーワードと引数のペアは、複数のイベントがポリシーに含まれている場合、この特定のイベントを識別します。 *repeats* 引数の範囲は 1 ～ 65000 です。*seconds* 引数の範囲は 0 ～ 4294967295 秒です。0 は無制限を示します。 ストリングは引用符で囲みます。
event counter [**tag** *tag*] **name** *counter* **entry-val** *entry* **entry-op** {**eq** | **ge** | **gt** | **le** | **lt** |**ne**} [**exit-val** *exit* **exit-op** {**eq** | **ge** | **gt** | **le** | **lt** | **ne**}] 例： switch(config-applet)# event counter name mycounter entry-val 20 gt	カウンタが、開始演算子に基づいて開始のしきい値を超えた場合にイベントを発生させます。イベントはただちにリセットされます。任意で、カウンタが終了のしきい値を超えたあとでリセットされるように、イベントを設定できます。 **tag** *tag* キーワードと引数のペアは、複数のイベントがポリシーに含まれている場合、この特定のイベントを識別します。 *counter* name は大文字と小文字を区別し、最大 28 の英数字を使用できます。*entry* および *exit* の値の範囲は 0 ～ 2147483647 です。
event fanabsent [**fan** *number*] **time** *seconds* 例： switch(config-applet)# event fanabsent time 3000	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。
event fanbad [**fan** *number*] **time** *seconds* 例： switch(config-applet)# event fanbad time 3000	秒数で設定された時間を超えて、ファンが故障状態の場合に、イベントを発生させます。*number* の範囲はモジュールに依存します。*seconds* の範囲は 10 ～ 64000 です。

コマンド	目的
event oir [**tag** *tag*] {**fan** | **module** | **powersupply**} {**anyoir** | **insert** | **remove**} [*number*] 例： switch(config-applet)# event oir fan remove 4	設定されたデバイス構成要素（ファン、モジュール、または電源モジュール）がデバイスに取り付けられた場合、またはデバイスから取り外された場合に、イベントを発生させます。 **tag** *tag* キーワードと引数のペアは、複数のイベントがポリシーに含まれている場合、この特定のイベントを識別します。 任意で、ファン、モジュール、または電源モジュールの具体的な番号を設定できます。*number* の範囲は次のとおりです。 • ファン番号：モジュール依存 • モジュール番号：デバイス依存 • 電源モジュール番号：範囲は 1 ～ 3
event policy-default count *repeats* [**time** *seconds*] 例： switch(config-applet)# event policy-default count 3	システムポリシーで設定されているイベントを使用します。このオプションは、ポリシーを上書きする場合に使用します。 *repeats* の範囲は 1 ～ 65000 です。*seconds* の範囲は 0 ～ 4294967295 秒です。0 は無制限を示します。
event snmp [**tag** *tag*] **oid** *oid* **get-type** {**exact** | **next**} **entry-op** {**eq** | **ge** | **gt** | **le** | **lt** |**ne**} **entry-val** *entry* [**exit-comb** {**and** | **or**}] **exit-op** {**eq** | **ge** | **gt** | **le** | **lt** |**ne**} **exit-val** *exit* **exit-time** *time* **polling-interval** *interval* 例： switch(config-applet)# event snmp oid 1.3.6.1.2.1.31.1.1.1.6 get-type next entry-op lt 300 entry-val 0 exit-op eq 400 exit-time 30 polling-interval 300	SNMP OID が、開始演算子に基づいて開始のしきい値を超えた場合にイベントを発生させます。イベントはただちにリセットされます。任意で、カウンタが終了のしきい値を超えたあとでリセットされるように、イベントを設定できます。OID はドット付き10 進表記です。 **tag** *tag* キーワードと引数のペアは、複数のイベントがポリシーに含まれている場合、この特定のイベントを識別します。 *entry* および *exit* の値の範囲は 0 ～ 18446744073709551615 です。time の範囲は 0 ～ 2147483647 秒です。interval の範囲は 1 ～ 2147483647 秒です。
event storm-control 例： switch(config-applet)# event storm-control	ポート上のトラフィックが設定されたストーム制御しきい値を超えた場合に、イベントを発生させます。

コマンド	目的
event sysmgr memory [**module** *module-num*] **major** *major-percent* **minor** *minor-percent* **clear** *clear-percent* 例： switch(config-applet)# event sysmgr memory minor 80	指定したシステムマネージャのメモリのしきい値を超えた場合にイベントを発生させます。パーセンテージの範囲は 1 ～ 99 です。
event temperature [**module** *slot*] [**sensor** *number*] **threshold** {**any** | **major** | **minor**} 例： switch(config-applet)# event temperature module 2 threshold any	温度センサーが設定されたしきい値を超えた場合に、イベントを発生させます。sensor の範囲は 1 ～ 18 です。
event track [**tag** *tag*] *object-number* **state** {**any** | **down** | **up**} 例： switch(config-applet)# event track 1 state down	トラッキング対象オブジェクトが設定された状態になった場合に、イベントを発生させます。 **tag** *tag* キーワードと引数のペアは、複数のイベントがポリシーに含まれている場合、この特定のイベントを識別します。 *object-number* の範囲は 1 ～ 500 です。

アクション文の設定

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

コマンド	目的
action *number*[*.number2*] **cli** *command1* [*command2*...][**local**] 例： switch(config-applet)# action 1.0 cli “show interface e 3/1“	設定された CLI コマンドを実行します。任意で、イベントが発生したモジュール上でコマンドを実行できます。アクションラベルのフォーマットは number1.number2 です。 *number* は 16 桁までの任意の数値にできます。*number2* の範囲は 0 ～ 9 です。 ストリングは引用符で囲みます。

コマンド	目的
action *number*[*.number2*] **counter name** *counter* **value** *val* **op** {**dec** | **inc** | **nop** | **set**} 例： switch(config-applet)# action 2.0 counter name mycounter value 20 op inc	設定された値および操作でカウンタを変更します。アクション ラベルのフォーマットは number1.number2 です。 *number* は 16 桁までの任意の数値にできます。*number2* の範囲は 0 ～ 9 です。 counter name は大文字と小文字を区別し、最大 28 の英数字を使用できます。*val* には 0 ～ 2147483647 の整数または置換パラメータを指定できます。
action *number*[*.number2*] **event-default** 例： switch(config-applet)# action 1.0 event-default	関連付けられたイベントのデフォルトアクションを実行します。アクション ラベルのフォーマットは number1.number2 です。 *number* は 16 桁までの任意の数値にできます。number2 の範囲は 0 ～ 9 です。
action *number*[*.number2*] **policy-default** 例： switch(config-applet)# action 1.0 policy-default	上書きしているポリシーのデフォルトアクションを実行します。アクション ラベルのフォーマットは number1.number2 です。 *number* は 16 桁までの任意の数値にできます。*number2* の範囲は 0 ～ 9 です。
action *number*[*.number2*] **reload** [**module** *slot* [-*slot*]] 例： switch(config-applet)# action 1.0 reload module 3-5	1 つまたは複数のモジュールまたはシステム全体を強制的にリロードします。 *number* は 16 桁までの任意の数値にできます。*number2* の範囲は 0 ～ 9 です。
action *number*[*.number2*] **snmp-trap** {[**intdata1** *data* [**intdata2** *data*] [*strdata string*]} 例： switch(config-applet)# action 1.0 snmp-trap strdata "temperature problem"	設定されたデータを使用して SNMP トラップを送信します。*number* は 16 桁までの任意の数値にできます。*number2* の範囲は 0 ～ 9 です。 *data* 引数には、最大 80 桁の任意の数を指定できます。*string* には最大 80 文字の英数字を使用できます。 ストリングは引用符で囲みます。

コマンド	目的
action *number*[*.number2*] **syslog** [**priority** *prio-val*] **msg** *error-message* 例： switch(config-applet)# action 1.0 syslog priority notifications msg "cpu high"	設定されたプライオリティで、カスタマイズした syslog メッセージを送信します。*number* は 16 桁までの任意の数値にできます。*number2* の範囲は 0 ～ 9 です。 *error-message* には最大 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** コマンドを使用すると、CLI が一致するすべての EEM ポリシーで、CLI コマンドを実行できます。

VSH スクリプトによるポリシーの定義

VSH スクリプトを使用してポリシーを定義できます。

はじめる前に

正しい VDC 内にいることを確認します。VDC を変更するには、**switchto vdc** コマンドを使用します。

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 ファイルを次のシステム ディレクトリにコピーします。
`bootflash://eem/user_script_policies`

VSH スクリプト ポリシーの登録およびアクティブ化

VSH スクリプトで定義したポリシーを登録してアクティブにできます。

はじめる前に

正しい VDC 内にいることを確認します。VDC を変更するには、**switchto vdc** コマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **event manager policy** *policy-script*	EEM スクリプト ポリシーを登録してアクティブにします。*policy-script* は大文字と小文字を区別し、最大 29 文字の英数字を使用できます。
ステップ 3	switch(config)# **show event manager policy internal** *name*	（任意） 設定したポリシーに関する情報を表示します。
ステップ 4	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、VSH スクリプト ポリシーを登録してアクティブにする例を示します。

```
switch# configure terminal
switch(config)# event manager policy moduleScript
switch(config)# show event manager policy internal moduleScript
switch(config)# copy running-config startup-config
```

ポリシーの上書き

システム ポリシーは上書き可能です。

はじめる前に

正しい VDC 内にいることを確認します。VDC を変更するには、**switchto vdc** コマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	switch(config)# **show event manager policy-state** *system-policy*	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。
ステップ 3	switch(config)# **event manager applet** *applet-name* **override** *system-policy*	システム ポリシーを上書きし、アプレット コンフィギュレーション モードを開始します。*applet-name* は大文字と小文字を区別し、最大 29 文字の英数字を使用できます。*system-policy* は、既存のシステム ポリシーの 1 つにする必要があります。
ステップ 4	switch(config-applet)# **description** *policy-description*	（任意） ポリシーの説明になるストリングを設定します。string には最大 80 文字の英数字を使用できます。ストリングは引用符で囲みます。
ステップ 5	switch(config-applet)# **event** *event-statement*	ポリシーのイベント文を設定します。ページ14-10 の「イベント文の設定」を参照してください。
ステップ 6	switch(config-applet)# **action** *number action-statement*	ポリシーのアクション文を設定します。ページ 14-13 の「アクション文の設定」を参照してください。 アクション文が複数の場合は、ステップ 6 を繰り返します。
ステップ 7	switch(config-applet)# **show event manager policy-state** *name*	（任意） 設定したポリシーに関する情報を表示します。
ステップ 8	switch(config-applet)# **copy running-config startup-config**	この設定変更を保存します。

次の例に、ポリシーの上書き方法を示します。

```
switch# configure terminal
switch(config)# 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
switch(config)# event manager applet ethport override _ethpm_link_flap
switch(config-applet)# description "Overrides link flap policy"
switch(config-applet)# event policy-default count 2 time 1000
switch(config-applet)# action 1.0 syslog priority warnings msg "Link is flapping."
switch(config-applet)# show event manager policy-state ethport
switch(config-applet)# copy running-config startup-config
```

EEM パブリッシャとしての syslog の設定

スイッチからの syslog メッセージをモニタできます。

（注） syslog メッセージをモニタする検索文字列の最大数は 10 です。

はじめる前に

EEM が syslog による登録に利用可能であることを確認します。

syslog デーモンを設定して実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **event manager applet** *applet-name*	EEM にアプレットを登録し、アプレット コンフィギュレーション モードを開始します。
ステップ 3	switch(config)# **event syslog** [**tag** *tag*] {**occurs** *number* | **period** *seconds* | **pattern** *msg-text* | **priority** *priority*}	syslog メッセージを監視し、ポリシーの検索文字列に基づいてポリシーを呼び出します。 • **tag** *tag* キーワードと引数のペアは、複数のイベントがポリシーに含まれている場合、この特定のイベントを識別します。 • **occurs** *number* のキーワードと引数のペアは、発生回数を指定します。指定できる範囲は 1 ～ 65000 です。 • **period** *seconds* のキーワードと引数のペアは、イベントの発生間隔を指定します。範囲は 1 ～ 4294967295 です。 • **pattern** *msg-text* のキーワードと引数のペアは、一致する正規表現を指定します。パターンには、文字テキスト、環境変数、またはこの 2 つの組み合わせを含めることができます。文字列に空白が含まれる場合は引用符で囲みます。 • **priority** *priority* のキーワードと引数のペアは、syslog メッセージのプライオリティを指定します。このキーワードを指定しないと、すべての Syslog メッセージのプライオリティ レベルが「情報レベル」に設定されます。

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

次に、EEM パブリッシャとして syslog を設定する例を示します。

```
switch# configure terminal
switch(config)# event manager applet abc
switch(config-applet)# event syslog occurs 10
switch(config-applet)# copy running-config startup-config
```

Tcl スクリプト トリガーのための CLI を使用したユーザ ポリシーの定義

はじめる前に

EEM ポリシーを介してトリガーされる Tcl スクリプトをスイッチのブートフラッシュにコピーします。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **event manager applet** *applet-name*	EEM にアプレットを登録し、アプレット コンフィギュレーション モードを開始します。*applet-name* は大文字と小文字を区別し、最大 29 文字の英数字を使用できます。
ステップ 3	switch(config-applet)# **description** *policy-description*	（任意） ポリシーの説明になるストリングを設定します。string には最大 80 文字の英数字を使用できます。ストリングは引用符で囲みます。
ステップ 4	switch(config-applet)# **event** *event-statement*	ポリシーのイベント文を設定します。イベント文の設定，（272 ページ）を参照してください。 イベント文が複数の場合は、ステップ 4 を繰り返します。

	コマンドまたはアクション	目的
ステップ 5	switch(config-applet)# **tag** *tag* {**and** | **andnot** | **or**} *tag* [**and** | **andnot** | or {*tag*}] {**happens** *occurs* **in** *seconds*}	（任意） ポリシー内の複数のイベントを相互に関連付けます。 *occurs* 引数の範囲は 1 ～ 4294967295 です。*seconds* 引数の範囲は 0～4294967295 秒です。
ステップ 6	switch(config-applet)# **action** *number*[.*number2*] *action-statementtcl-filename*	ポリシーのアクション文を設定します。アクション文の設定，（274 ページ）を参照してください。 アクション文が複数の場合は、ステップ 6 を繰り返します。
ステップ 7	switch(config-applet)# **show event manager policy-state** *name* [**module** *module-id*]	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	switch(config-applet)# **copy running-config startup-config**	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。

Tcl サンプル ファイル（Vlan.tcl）。ブートフラッシュにこのファイルをコピーします。ファイルを実行すると、VLAN 99 を作成し、その名前を指定します。

```
set i 1
while {$i<100} {
cli configure terminal
cli vlan $i
cli name VLAN$i
cli no shutdown
cli exit
incr i
}
```

次に、CLI を使用してポリシーを定義し、イベントがトリガーされた場合アクション ステートメントを使用して Tcl スクリプトを起動する例を示します。

```
switch# configure terminal
switch(config)# event manager applet TCL
switch(config-applet)# description "Triggers TCL Script"
switch(config-applet)# event cli match "shutdown"
switch(config-applet)# action 1.0 cli local tclsh VLAN.tcl
switch(config-applet)# copy running-config startup-config
```

Python スクリプト トリガーのための CLI を使用したユーザ ポリシーの定義

はじめる前に

EEM ポリシーを介してトリガーされる Python スクリプトをスイッチのブートフラッシュにコピーします。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **event manager applet** *applet-name*	EEM にアプレットを登録し、アプレットコンフィギュレーションモードを開始します。*applet-name* は大文字と小文字を区別し、最大 29 文字の英数字を使用できます。
ステップ 3	switch(config-applet)# **description** *policy-description*	（任意） ポリシーの説明になるストリングを設定します。string には最大 80 文字の英数字を使用できます。ストリングは引用符で囲みます。
ステップ 4	switch(config-applet)# **event** *event-statement*	ポリシーのイベント文を設定します。イベント文の設定，（272 ページ）を参照してください。 イベント文が複数の場合は、ステップ 4 を繰り返します。
ステップ 5	switch(config-applet)# **tag** *tag* {**and** | **andnot** | **or**} *tag* [**and** | **andnot** | or {*tag*}] {**happens** *occurs* **in** *seconds*}	（任意） ポリシー内の複数のイベントを相互に関連付けます。 *occurs* 引数の範囲は 1 ～ 4294967295 です。*seconds* 引数の範囲は 0～4294967295 秒です。
ステップ 6	switch(config-applet)# **action** *number*[.*number2*] *action-statementpython-filename*	ポリシーのアクション文を設定します。アクション文の設定，（274 ページ）を参照してください。 アクション文が複数の場合は、ステップ 6 を繰り返します。
ステップ 7	switch(config-applet)# **show event manager policy-state** *name* [**module** *module-id*]	設定したポリシーの状態に関する情報を表示します。

	コマンドまたはアクション	目的
ステップ 8	switch(config-applet)# **copy running-config startup-config**	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

サンプル Python ファイル（Python.py）。ブートフラッシュにこのファイルをコピーします。

```
import re
import cisco
cisco.cli ("show interface eth 1/1-32 transceiver detail >> bootflash:link_flap.txt")
```

次に、CLI を使用してポリシーを定義し、イベントがトリガーされた場合アクション ステートメントを使用して Python スクリプトを起動する例を示します。

```
switch# configure terminal
switch(config)# event manager applet PYTHON
switch(config-applet)# description "Triggers PYTHON Script"
switch(config-applet)# event cli match "shutdown"
switch(config-applet)# action 1.0 cli local python bootflash:Python.py
switch(config-applet)# copy running-config startup-config
```

EEM 設定の確認

EEM の設定情報を表示するには、次のコマンドのいずれかを入力します。

コマンド	目的
show event manager environment [*variable-name* | **all**]	イベントマネージャの環境変数に関する情報を表示します。
show event manager event-types [*event* | **all** | **module** *slot*]	イベント マネージャのイベント タイプに関する情報を表示します。
show event manager history events [**detail**] [**maximum** *num-events*] [**severity** {**catastrophic** | **minor** | **moderate** | **severe**}]	すべてのポリシーについて、イベント履歴を表示します。
show event manager policy internal *[policy-name]* [**inactive**]	設定したポリシーに関する情報を表示します。
show event manager policy-state *policy-name*	しきい値を含め、ポリシーの状態に関する情報を表示します。
show event manager script system [*policy-name* | **all**]	スクリプト ポリシーに関する情報を表示します。

コマンド	目的
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 のコンフィギュレーション例

__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。

```
switch# configure terminal
switch(config)# event manager applet ethport override __ethpm_link_flap
switch(config-applet)# event policy-default count 2 time 1000
switch(config-applet)# action 1 cli conf t
switch(config-applet)# action 2 cli int et1/1
switch(config-applet)# action 3 cli no shut
```

次に、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、CLI コマンドを実行できるが、SNMP 通知をトリガーする EEM ポリシーを作成する例を示します。

```
switch# configure terminal
switch(config)# event manager applet TEST
switch(config-applet)# event cli match "conf t"
switch(config-applet)# action 1.0 snmp-trap strdata "Configuration change"
switch(config-applet)# 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。

```
switch# configure terminal
switch(config)# event manager applet eem-correlate
switch(config-applet)# event syslog tag one pattern "copy bootflash:.* running-config.*"
switch(config-applet)# event syslog tag two pattern "copy run start"
switch(config-applet)# event syslog tag three pattern "hello"
switch(config-applet)# tag one or two or three happens 1 in 120
switch(config-applet)# action 1.0 reload module 1
```

第 20 章

OpenFlow の設定

この章の内容は、次のとおりです。

- OpenFlow について，285 ページ
- OpenFlow の制約事項，286 ページ
- サポートされるインターフェイス タイプ，286 ページ
- サポートされないインターフェイス タイプ，286 ページ
- サポートされるインターフェイス モード，286 ページ
- サポートされる match フィールド，287 ページ
- サポートされるアクション，287 ページ
- フロー数の拡張，288 ページ
- パイプラインのサポート，288 ページ
- OpenFlow の前提条件，288 ページ
- OpenFlow 仮想サービスのセットアップ，290 ページ
- OpenFlow のイネーブル化，290 ページ
- OpenFlow スイッチの設定，291 ページ
- OpenFlow の確認，293 ページ

OpenFlow について

OpenFlow は Open Networking Foundation（ONF）の仕様で、機能を学習し、フロー コントロールのエントリおよび要求の統計情報を追加、削除するための、フローベースの転送インフラストラクチャ（L2-L4 イーサネット スイッチ モデル）および標準化されたアプリケーションのプログラム インターフェイス（プロトコル定義）を定義します。OpenFlow では、セキュアなチャネルを介して、スイッチのフォワーディング機能を方向付けすることができます。

Cisco ONE Platform Kit を使用すると、シスコのネットワーキング インフラストラクチャ上にある、または隣接しているシスコの内部および外部のサードパーティアプリケーションをホストすることができます。また、管理された一貫性のある方法で、ネットワーキング サービスへプログラムでアクセスすることができます。シスコのルータまたはスイッチ上でアプリケーションをホストした場合、アプリケーションは仮想マシンまたはコンテナ内で実行されます。

OpenFlow の制約事項

Cisco Nexus 5500 および Cisco Nexus 6000 スイッチは、レイヤ 2 の宛先 MAC アドレスを書き換えるための OpenFlow アクションをサポートしていません。したがって、Topology Independent Forwarding や Latency Optimized Forwarding などの XNC コントローラの使用例は、Cisco Nexus 5500 および Cisco Nexus 6000 スイッチでは正しく機能しないことがあります。

サポートされるインターフェイス タイプ

次に、サポートされるインターフェイス タイプの一覧を示します。

- 通常のレイヤ 2 の物理ポート（switchport）
- レイヤ 2 のポート チャネル

サポートされないインターフェイス タイプ

次に、サポートされないインターフェイス タイプの一覧を示します。

- レイヤ 3 ポート（スイッチポートなし）
- ファブリック エクステンダ ポート
- 仮想ポート チャネル（VPC）ポート
- レイヤ 3 ポート チャネル

サポートされるインターフェイス モード

次に、サポートされるインターフェイス モードの一覧を示します。

- Access port
- トランク ポート

サポートされる match フィールド

次に、サポートされる match フィールドの一覧を示します。

- レイヤ 2 ヘッダー
  - Ethertype
  - VLAN ID
  - VLAN 優先度（PCP）
  - 送信元 MAC アドレス
  - 宛先 MAC アドレス
- レイヤ 3 ヘッダー
  - 送信元 IP アドレス
  - 宛先 IP アドレス
  - レイヤ 4 プロトコル
  - Diffserv コード ポイント（DSCP）
- レイヤ 4 ヘッダー
  - 送信元ポート
  - 宛先ポート
- Ingress Interface

サポートされるアクション

次に、サポートされるアクションの一覧を示します。

- パケットを 1 つの出力ポートにリダイレクトする
- パケットを複数の出力ポートにリダイレクトする
- 出力で VLAN タグ（vlan rewrite）を設定する
- 出力で VLAN タグを削除する
- データパス パケットを OpenFlow コントローラへ転換する
- パケットをドロップします。

フロー数の拡張

- Cisco Nexus デバイスは、合計で最大 65535 のフローをサポートします。デバイスは、最大 3500 の ACL テーブルのフローと 62K の MAC テーブル フローの組み合わせをサポートします。
- Cisco Nexus デバイスは、アクションがコントローラへのパントの場合に、最大 □□ のフローをサポートします。

パイプラインのサポート

OpenFlow ポリシーは、ACL テーブルと MAC テーブルに適用できます。OpenFlow は「パイプライン」の概念を利用してテーブルを関連付けます。Cisco Nexus デバイスは、201 と 202 の 2 つのパイプラインをサポートしています。openflow エージェントの論理スイッチ設定で **pipeline***id* コマンドを入力して、201 と 202 のパイプラインを切り替えることができます。

- パイプライン 201
  - すべてのフローが ACL テーブルに追加されます。例：ACL TCAM。
  - リダイレクトまたはドロップとしてのアクションによる ACL テーブル フローは、ACL-TCAM の IFACL リージョンにインストールされます。
  - コントローラへのパントアクションによる ACL テーブル フローは、ACL-TCAM の SIP リージョンにインストールされます。
- パイプライン 202
  - フローは ACL テーブル（ACL TCAM）と MAC テーブル（STM テーブル）の両方に追加できます。
  - 一致基準が L2-dest-mac および VLAN のみのフローは、MAC テーブルにインストールされます。残りのフローは ACL テーブルにインストールされます。
  - MAC テーブルでサポートされるアクションは、ポートへのリダクレクト、およびドロップです。
  - MAC テーブルは、ACL テーブルより高位のスケール番号をサポートします。

OpenFlow の前提条件

OpenFlow エージェントでは、トポロジ検出とフローのインストールをサポートするように、OpenFlow 特定のコマンドで Cisco Nexus デバイスを設定する必要があります。Cisco Nexus デバイスは、startup-config ファイルのデフォルト コマンドが起動時に実行されるように、ハイブリッド

モードで動作します。これにより、望ましくない影響を受けることがあるため、変更する必要があります。

（注） これらの必要なコマンドを変更または無効にした場合、予期しないシステム動作が発生することがあります。

VLAN の作成

OpenFlow コントローラのスイッチで必要な VLAN を作成するために、次のコマンドを使用します。このコマンドにより、VLAN データベースに OpenFlow 特定の VLAN が作成されます。

`vlan x[-y]`

ハイブリッドな Ships-In-Night モードで動作している場合でも、OpenFlow 制御のポートと通常のポート間では VLAN を分離することをお勧めします。トラフィックのリークを防ぐために、OpenFlow ポートと非 OpenFlow ポート間で VLAN を共有しないように注意する必要があります。

インターフェイス レベルの設定

他のスイッチに接続しているインターフェイスが、スパンされたトラフィックを受信するようにするために、インターフェイスはアナライザに接続され、OpenFlow をサポートするように設定されます。**interface ethernet** コマンドは、パーサーをインターフェイス サブモードに変更します。インターフェイス上で OpenFlow のサポートを可能にする **mode openflow** コマンドを入力する前に、次のコマンドが必要です。

- **switchport mode trunk**
- **switchport trunk allowed vlan x-y**

Cisco Nexus デバイスで strip-vlan 機能を動作させるには、ネイティブ VLAN でトランク ポートを設定する必要があります。

Cisco One コントローラは、OpenFlow 対応ポートのトポロジ検出を実行することができます。トランク ポートでのトポロジ検出を可能にするには、トランク ポート上でネイティブ VLAN を設定する必要があります。

switchport trunk native vlan z

インターフェイスが OpenFlow 論理スイッチに追加されると、インターフェイスには次のコマンドが暗黙的に適用されます。

- **mode openflow**
- **spanning-tree bpdufilter enable**
- **no lldp transmit**

OpenFlowに対するテンプレート ベースの TCAM カービング

Cisco Nexus デバイスは、テンプレート ベース TCAM カービングをサポートしています。デバイスで OpenFlow を設定するには、テンプレート ベースの TCAM カービングのコマンドを使用して、TCAM カービングのリージョンに対していくつかの変更を行う必要があります。

OpenFlow ポリシーで高位のスケール番号をサポートするには、TCAM の IFACL リージョンを適宜に再カービングする必要があります。最大フロー スケールに TCAM カービングを適用するには、次のコマンドを入力します。

```
switch(config)# hardware profile tcam resource template openflow
switch(config-tcam-templ)# vacl 64
switch(config-tcam-templ)# ifacl 3520
switch(config-tcam-templ)# qos 128
switch(config-tcam-templ)# rbacl 64
switch(config-tcam-templ)# span 64
switch(config)# hardware profile tcam resource service-template openflow
```

TCAM カービングを検証するには、次のコマンドを入力します。**show hardware profile tcam resource template***tmplt-name*

（注） TCAM カービングの設定では、Cisco Nexus デバイスの再ロードが必要です。

OpenFlow 仮想サービスのセットアップ

仮想サービス マネージャを使用して、OpenFlow エージェント アプリケーションをコンテナ上で仮想サービスとして実行することができます。OpenFlow の仮想サービスをセットアップするには、次の作業を行います。

- アプリケーションの OVA パッケージをシステムにダウンロードします。
- 指定した仮想サービスの OVA パッケージをインストールします。次に例を示します。

  ```
  switch#virtual-service install name openflow-agent package file-url
  ```

- 仮想サービスを設定し、アクティブにします。次に例を示します。

  ```
  switch(config)#virtual-service openflow-agent
  switch(config-virt-serv)#activate
  ```

仮想サービスにインストールされているソフトウェア パッケージをアップグレードするには、**virtual-service upgrade name** *application-name* **package** *file-url* コマンドを使用します。

（注） アクティブな仮想サービスはアップグレードできません。

仮想サービスにインストールされているソフトウェア パッケージを削除するには、**virtual-service uninstall name** *application-name* コマンドを使用します。

（注） アクティブな仮想サービスは削除できません。

OpenFlow のイネーブル化

OpenFlow の機能をイネーブルにするには、**hardware profile openflow** コマンドを入力し、OpenFlow エージェントに必要なハードウェア リソースを割り当てます。スイッチのリロード後に **hardware**

profile コマンドを使用して、OpenFlow 機能に対して ACL Feature Manager（AFM）および Forwarding Manager（FWM）モジュールを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **hardware profile openflow**	OpenFlow エージェントに必要なハードウェア リソースを割り当てます。
ステップ 3	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て、リブートおよびリスタート後も変更が永続的に保存されるようにします。
ステップ 4	switch#**reload**	スイッチにオペレーティング システムをリロードします。

OpenFlow スイッチの設定

設定を有効にするには、スイッチで OpenFlow をイネーブルにする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**OpenFlow** 例： `switch(config)# openflow`	OpenFlow コンフィギュレーション モードを開始します。
ステップ 3	**switch***switch-number* 例： `switch(config-ofa)# switch 1`	OpenFlow の論理スイッチを指定し、OpenFlow のスイッチ 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	**pipeline {201|202}** 例： `switch(config-ofa-switch)# pipeline 201`	パイプライン モードを指定します。 OpenFlow ポリシーは、ACL テーブルと MAC テーブルに適用できます。Cisco Nexus デバイスは、201 と 202 の 2 つのパイプラインをサポー

	コマンドまたはアクション	目的
		トします。このコマンドにより、サポートされているパイプラインモードを切り替えることができます。
ステップ 5	**controlleripv4***ipv4-address* **port***port-number***vrf***vrf-name***security** {**none** | **tls**} 例： `switch(config-ofa-switch)# controller ipv4 192.0.2.10 port 6653 vrf mnagement security none`	指定された VRF を介してコントローラとの接続を確立します。 TLS をディセーブルまたはイネーブルにできます。
ステップ 6	**of-port interface***interface-typeslot / port* 例： `switch(config-ofa-switch)# interface ethernet 2/5`	OpenFlow の論理スイッチへインターフェイスを追加します。
ステップ 7	**default-miss cascade** {**drop** | **controller** | **normal**} 例： `switch(config-ofa-switch)# default-miss cascade normal`	スイッチの hybrid-normal モードをイネーブルにします。OpenFlow エージェントを hybrid-normal モードから punt-to-controller モードに変更するには、**default-miss cascade controller** コマンドを使用します。OpenFlow エージェントを hybrid-normal モードから default-drop モードに変更するには、**default-miss cascade drop** コマンドを使用します。
ステップ 8	**max-backoff***back-off-time* 例： `switch(config-ofa-switch)# max-backoff 7`	OpenFlow コントローラの最大バックオフ タイマーを設定します。デフォルト値は 8 秒です。
ステップ 9	**probe-internal***interval-time* 例： `switch(config-ofa-switch)# probe-interval 6`	OpenFlow コントローラ プローブのインターバルタイマーを設定します。デフォルト値は 5 秒です。
ステップ 10	**exit** 例： `switch(config-ofa-switch)# exit`	OpenFlow スイッチ コンフィギュレーション モードを終了します。
ステップ 11	**exit** 例： `switch(config-ofa)# exit`	OpenFlow コンフィギュレーション モードを終了します。

OpenFlow の確認

次のいずれかのコマンドを使用して、設定を確認します。

コマンド	目的
show running-config | section openflow	OpenFlow 実行コンフィギュレーション情報を表示します。
show running-config interface ethernet*slot*/*port*	特定のイーサネットインターフェイスの実行コンフィギュレーションを表示します。
show openflow *openflow-agent* **switch** *number* **controllers**	コントローラへの OpenFlow エージェントの接続情報を表示します。
show openflow *openflow-agent* **switch** *number* **flows**	OpenFlow エージェント フローに関する情報を表示します。
show openflow *openflow-agent* **switch** *number* **ports**	OpenFlow エージェント ポートのステータスに関する情報を表示します。

第 21 章

NetFlow の設定

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

- NetFlow の概要，295 ページ
- フロー レコード，296 ページ
- Flow Exporter，296 ページ
- NetFlow の照合キー，297 ページ
- NetFlow の collect パラメータ，299 ページ
- サンプリングされた NetFlow，300 ページ
- NetFlow の注意事項と制約事項，300 ページ
- NetFlow の設定方法，301 ページ
- NetFlow 設定の確認，310 ページ
- NetFlow のモニタリング，311 ページ
- NetFlow の設定例，311 ページ

NetFlow の概要

NetFlow ではフローを使用して、アカウンティング、ネットワーク モニタリング、およびネットワーク プランニングに関連する統計情報を提供します。フローは送信元インターフェイス（または VLAN）に届く単方向のパケット ストリームで、キーの値は同じです。キーは、パケット内のフィールドを識別する値です。フローを作成するには、フロー レコードを使用して、フロー固有のキーを定義します。

Cisco NX-OS は、Traditional Netflow と Flexible NetFlow の両方をサポートします。

Traditional NetFlow では、エクスポートされるすべてのキーとフィールドが固定でなければなりません。Traditional Netflow は IPv4 フローのみをサポートしています。フローを定義するために使用するキーを選択できます。それぞれの一意のフローはキャッシュされ、いくつかの統計情報はフロー用に収集されます。

Flexible NetFlow によって、機能強化されたネットワーク異常とセキュリティの検出が可能になります。フレクシブル NetFlow 機能を使用すると、大量の定義済みフィールドの集合からキーを選択することで、そのアプリケーションに最適なフロー レコードを定義できます。

1 つのフローと見なされるパケットでは、すべてのキー値が一致している必要があります。フローは、設定したエクスポート レコードバージョンに基づいて、関係のある他のフィールドを集めることもあります。フローは NetFlow キャッシュに格納されます。

フロー レコードによってフロー用に収集するデータのタイプが決まります。フロー モニタはフロー レコードおよびフロー エクスポータを NetFlow キャッシュ情報と結合します。

Cisco NX-OS は NetFlow 統計情報をサンプル モードで収集します。これは、インターフェイスまたはサブインターフェイス上のパケットが、設定したレートで分析されることを意味します。

フロー レコード

フロー レコードでは、フロー内のパケットを識別するために NetFlow で使用するキーとともに、NetFlow がフローについて収集する関連フィールドを定義します。キーと関連フィールドを任意の組み合わせで指定して、フロー レコードを定義できます。Cisco NX-OS は、様々なキー セットをサポートしています。フロー レコードでは、フロー単位で収集するカウンタのタイプも定義します。32 ビットまたは 64 ビットのパケット カウンタまたはバイト カウンタを設定できます。キー フィールドは、match キーワードで指定されます。対象フィールドとカウンタは match キーワードで指定されます。

Cisco NX-OS では、フロー レコードの作成時に次の match フィールドをデフォルトとして使用できます。

- match interface input
- match interface output
- match flow direction

Flow Exporter

フロー エクスポータでは、NetFlow エクスポート パケットに関して、ネットワーク層およびトランスポート層の詳細を指定します。フロー エクスポータで設定できる情報は次のとおりです。

- エクスポートの宛先 IPv4 または IPv6 アドレス
- 送信元インターフェイス
- UDP ポート番号（コレクタが NetFlow パケットをリスニングするところ）
- エクスポート フォーマット

（注） NetFlow エクスポート パケットでは、送信元インターフェイスに割り当てられた IP アドレスを使用します。送信元インターフェイスに IP アドレスが割り当てられていない場合、フローエクスポータはアクティブになりません。

Cisco NX-OS は、タイムアウトが発生するたびに UDP フレームを使用してデータをリモート コレクタへエクスポートします。デフォルトでは、フロー タイムアウト値は 15 秒に設定されています。

NetFlow の照合キー

フローを識別するために、フロー レコードの一部として 1 つ以上の照合キーを選択できます。

NetFlow は、フローを識別するために次の照合キーをサポートしています。

- IPv4 の送信元アドレスおよび IPv4 宛先アドレス
- IPv6 の送信元アドレスおよび IPv6 宛先アドレス
- IPv6 フロー ラベル
- IPv6 オプション
- TOS フィールド
- レイヤ 4 プロトコル
- レイヤ 4 送信元ポートおよび宛先ポート

次の照合キーがレイヤ 2 NetFlow に提供されています。

- MAC の送信元アドレスおよび宛先アドレス
- Ethertype
- VLAN

match パラメータの指定

フロー レコードごとに、次の match パラメータを 1 つ以上設定する必要があります。

コマンド	目的
match ip {**protocol** | **tos**} 例： `switch(config-flow-record)# match ip protocol`	IP プロトコルまたは ToS フィールドをキーとして指定します。 （注） レイヤ 4 ポートデータをエクスポートするには、**match transport destination-port** コマンドおよび **match ip protocol** コマンドが必要です。**show hardware flow ip** コマンドの出力にデータが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およびエクスポートされません。
match ipv4 {**destination address** | **source address**} 例： `switch(config-flow-record)# match ipv4 destination address`	IPv4 送信元または宛先アドレスをキーとして指定します。
match ipv6 {**destination address** | **source address** | **flow-label** | **opitons** } 例： `switch(config-flow-record)# match ipv6 flow label`	IPv6 キーを指定します。
match transport {**destination-port** | **source-port**} 例： `switch(config-flow-record)# match transport destination-port`	トランスポート送信元または宛先ポートをキーとして指定します。 （注） レイヤ 4 ポートデータをエクスポートするには、**match transport destination-port** コマンドおよび **match ip protocol** コマンドが必要です。**show hardware flow ip** コマンドの出力にデータが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およびエクスポートされません。
match datalink {**mac source-address** | **mac destination-address** | **ethertype** | **vlan**} 例： `switch(config-flow-record)# match datalink ethertype`	レイヤ 2 属性をキーとして指定します。

NetFlow の collect パラメータ

NetFlow は、次のパラメータを収集し、バージョン 5（Traditional NetFlow）またはバージョン 9（Flexible NetFlow）形式で値をエクスポートできます。

（注） これらのフィールドの中には、Traditional NetFlow 形式で使用できないものがあります。

- レイヤ 3 バイト数（任意で 64 ビット値）
- パケット数（任意で 64 ビット値）
- フロー方向
- フロー サンプラー ID
- インターフェイス タイプ（入力、出力、または両方）
- 最初または最後のパケットのシステム稼動時間
- TCP フラグ

collect パラメータの指定

フロー レコードごとに、次の collect パラメータを 1 つ以上設定する必要があります。

コマンド	目的

collect counter {**bytes** | **packets**} [**long**]
例：
`switch(config-flow-record)#`
`switch(config-flow-record)# collect counter packets`
	フローからパケットベースまたはバイト カウンタを収集します。任意で、64 ビット カウンタを使用することを指定できます。

collect flow sampler id 例： `switch(config-flow-record)# collect flow sampler`	フローに使用するサンプラの ID を収集します。
collect timestampsys-uptime {**first** | **last**} 例： `switch(config-flow-record)# collect timestamp sys-uptime last`	フローの先頭または最終パケットに関するシステム稼働時間を収集します。
collect transporttcpflags 例： `switch(config-flow-record)# collect transport tcp flags`	フローのパケットに対応する TCP トランスポート層フラグを収集します。

コマンド	目的
collect ip version 例： `switch(config-flow-record)# collect ip version`	フローの IP バージョンを収集します。

サンプリングされた NetFlow

Cisco NX-OS はサンプリングされた NetFlow をサポートします。この機能は、インターフェイスの着信パケットをサンプリングします。パケットはサンプリングされ、その後フローを作成するために適性確認されます。サンプリングされた NetFlow は、フローを作成するパケット数およびフロー数を制限することで、コレクタに送信されるエクスポート データの量を削減します。これは、フローが、転送エンジン上ではなく、ライン カードまたは外部デバイス上で作成された場合に重要です。

サポートされるサンプリング モードは M out of N（M:N）です。M 個のパケットがサンプリングのために N 個のパケットからランダムに選択され、これらのパケットのみがフローを作成することができます。Cisco Nexus 6000 シリーズの最小サンプリング レートは 1:64 K パケットです。次の表は、サンプリング レートが 1:64 K パケットに設定された場合の、異なるポート タイプに対する異なるパケット レートを示しています。

ポート速度	1:64 K サンプリング パケット レートを使用したパケット数
1 ギガビット	23
10 ギガビット	230
40 ギガビット	920

（注） 上の表の値は、64 バイト サイズのパケットに適用されます。パケットのサイズによって値は異なります。

NetFlow の注意事項と制約事項

NetFlow に関する設定時の注意事項および制約事項は、次のとおりです。

- M:N を使用するサンプラ モードでは、N は 2 の累乗にする必要があります。たとえば 1024、2048、または 4096 です。
- 送信元インターフェイスを設定する必要があります。送信元インターフェイスを設定しなかった場合、フロー エクスポータはディセーブル ステートのままです。

- NetFlow と SPAN の両方を同じインターフェイス上に設定すると、SPAN 設定のみが適用され、NetFlow 設定は無視されます。
- フロー モニタごとに、有効なレコード名を設定する必要があります。
- NetFlow でサポートされているエントリの最大数は 512,000 です。
- モニタに適用されるレコードのフィールドは変更できません
- モニタに適用されるサンプラのサンプリング モード値は変更できません
- NetFlow が SVI と VLAN の両方について設定されている場合、SVI NetFlow では、ルーティングされたパケットのみが更新されます。
- NetFlow は CPU の負荷が高くなる原因となることがあります。コントロールプレーンの問題を回避するために、次の制限が適用されます。
  - NetFlow は、入力方向でのみ設定できます。
  - CPU に到達する NetFlow パケットは ASIC でポリシングされません。
- 入力レイヤ 2 の NetFlow は、次のタイプのインターフェイスでサポートされます。
  - レイヤ 2 スイッチ インターフェイス/ポート チャネル
  - FEX インターフェイス
- 入力レイヤ 3 の NetFlow は、次のタイプのインターフェイスでサポートされます。
  - レイヤ 3 インターフェイス/ポート チャネル
  - レイヤ 3 サブインターフェース/ポート チャネル サブインターフェース
  - SVI
- 入力ブリッジ型 NetFlow は VLAN 上でサポートされます。

NetFlow の設定方法

スイッチで NetFlow を設定するには、次の手順を実行します。

- 対象のキー フィールドおよび非キー フィールドを指定して、フロー レコードを定義します。
- エクスポート形式、プロトコル、宛先、およびその他のパラメータを指定して、1 つまたは複数のフロー エクスポータを定義します。
- 上記のフロー レコードおよびフローエクスポータに基づいて、フローモニタを定義します。
- 指定されたサンプリング方法で、インターフェイスにフロー モニタを適用します。

NetFlow 機能のイネーブル化

フローを設定するには、先に NetFlow をグローバルでイネーブルにしておく必要があります。

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	**feature netflow** 例： `switch(config)# feature netflow`	NetFlow 機能をイネーブルにします。

フロー レコードの作成

はじめる前に

正しい VDC 内にいることを確認します。VDC を変更するには、**switchto vdc** コマンドを使用します。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure 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 IPv4Flow`	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。
ステップ 3	**description***string* 例： `switch(config-flow-record)# description Ipv4flow`	このフロー レコードについて説明します。

	コマンドまたはアクション	目的
ステップ 4	**match***type* 例： `switch(config-flow-record)# match transport destination-port`	照合キーを指定します。
ステップ 5	**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。
ステップ 6	**exit** 例： `switch(config-flow-record)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

フロー エクスポータの作成

フロー エクスポータの設定では、フローに対するエクスポート パラメータを定義し、リモート NetFlow コレクタへの到達可能性情報を指定します。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**flow exporter***name* 例： `switch(config)# flow exporter flow-exporter-one`	フローエクスポータを作成し、フローエクスポータ コンフィギュレーション モードを開始します。フローエクスポータ名を最大 63 文字の英数字で入力できます。

	コマンドまたはアクション	目的
ステップ 3	**destination** { **ipv4-address** | **ipv6-address**} [**use-vrf***name*] 例： `switch(config-flow-exporter)# destination 192.0.2.1`	このフロー エクスポータの宛先 IPv4 または IPv6 アドレスを設定します。任意で、NetFlow コレクタに到達するために使用する VRF を設定できます。VRF 名には最大 32 文字の英数字を入力できます。
ステップ 4	**sourceinterface-type***name/port* 例： `switch(config-flow-exporter)# source ethernet 2/1`	設定された宛先で NetFlow コネクタに到達するために使用するインターフェイスを指定します。
ステップ 5	**description***string* 例： `switch(config-flow-exporter)# description exportversion9`	（任意） （任意）このフローエクスポータについて説明します。説明には最大63 文字の英数字を入力できます。
ステップ 6	**dscp***value* 例： `switch(config-flow-exporter)# dscp 0`	（任意） （任意）DSCP（DiffServ コードポイント）値を指定します。範囲は 0 ～ 63 です。
ステップ 7	**transport udp***port* 例： `switch(config-flow-exporter)# transport udp 200`	（任意） （任意）NetFlow コレクタに到達するために使用する UDP ポートを指定します。範囲は 0 ～ 65535 です。 （注） UDP ポートを指定しない場合は、9995 がデフォルトとして選択されます。
ステップ 8	**version** {**5** | **9**} 例： `switch(config-flow-exporter)# version 9`	NetFlow エクスポート バージョンを指定します。フローエクスポータのバージョン 9 コンフィギュレーション サブモードを開始するには、バージョン 9 を選択します。
ステップ 9	**option** {**exporter-stats** | **interface-table** | **sampler-table**} **timeout***seconds* 例： `switch(config-flow-exporter-version-9)# option exporter-stats timeout 1200`	（任意） フローエクスポータの統計情報再送信タイマーを設定します。値の範囲は 1 ～ 86400 秒です。

	コマンドまたはアクション	目的
ステップ 10	**templatedatatimeout***seconds* 例： `switch(config-flow-exporter-version-9)# template data timeout 1200`	（任意） テンプレートデータ再送信タイマーを設定します。値の範囲は1～86400秒です。
ステップ 11	**exit** 例： `switch(config-flow-exporter-version-9)# exit`	フロー エクスポータ コンフィギュレーション モードに戻ります。
ステップ 12	**exit** 例： `switch(config-flow-exporter)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 13	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。

フロー モニタの作成

フロー モニタを作成して、フロー レコードおよびフロー エクスポータと関連付けることができます。1 つのモニタに属しているすべてのフローは、様々なフィールド上で照合するために関連するフロー レコードを使用します。データは指定されたフローエクスポータにエクスポートされます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal switch(config)#`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**flow monitor***name* 例： `switch(config)# flow monitor flow-monitor-one`	フロー モニタを作成し、フロー モニタ コンフィギュレーション モードを開始します。フロー モニタ名を最大 63 文字の英数字で入力できます。

	コマンドまたはアクション	目的
ステップ 3	**description***string* 例： `switch(config-flow-monitor)# description IPv4Monitor`	（任意） このフローモニタについて説明します。説明には最大 63 文字の英数字を入力できます。
ステップ 4	**exporter***name* 例： `switch(config-flow-monitor)# export v9`	（任意） フローエクスポータとこのフローモニタを関連付けます。エクスポータ名には最大63文字の英数字を入力できます。
ステップ 5	**record** {*name***netflow-original** | **netflow protocol-port** | **netflow** {**ipv4** | **ipv6**} {**original-input** | **original-output**}} 例： `switch(config-flow-monitor)# record IPv4Flow`	フローレコードを指定したフローモニタと関連付けます。レコード名には最大63文字の英数字を入力できます。
ステップ 6	**exit** 例： `switch(config-flow-monitor)# exit`	グローバルコンフィギュレーションモードに戻ります。
ステップ 7	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。

サンプラーの作成

フローサンプラーを作成し、フローに対して NetFlow サンプリングレートを定義することができます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal switch(config)#`	グローバルコンフィギュレーションモードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**sampler***name* 例： `switch(config)# sampler testsampler`	サンプラーを作成し、サンプラー コンフィギュレーション モードを開始します。フロー サンプラー名を最大 63 文字の英数字で入力できます。
ステップ 3	**description***string* 例： `switch(config-flow-sampler)# description samples`	（任意） （任意）このサンプラーについて説明します。説明には最大63 文字の英数字を入力できます。
ステップ 4	**mode***sample-number***out-of***packet-number* 例： `switch(config-flow-sampler)# mode 1 out-of 128`	受信パケット数あたりの取得サンプル数を定義します。sample-number の範囲は 1 ～ 64 で、packet-number の範囲は 1 ～ 65536 です。
ステップ 5	**exit** 例： `switch(config-flow-sampler)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

インターフェイスへのフロー モニタの適用

（注） 出力インターフェイスにはフロー モニタを適用できません。入力 NetFlow のみサポートされています。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**interface***interface-typeslot/port* 例： `switch(config)# interface ethernet 2/1`	インターフェイス コンフィギュレーション モードを開始します。インターフェイス タイプには、イーサネット（サブインターフェイスを含む）、ポート チャネル、または VLAN インターフェイスを使用できます。
ステップ 3	**ip flow monitor***name***inputsampler***name* 例： `switch(config-if)# ip flow monitor testmonitor input sampler testsampler`	入力パケットのインターフェイスに、IPv4 フロー モニタおよびサンプラを関連付けます。フロー モニタ名およびサンプラ名を最大 63 文字の英数字で入力できます。
ステップ 4	**ipv6 flow monitor***name***inputsampler***name* 例： `switch(config-if)# ipv6 flow monitor testmonitorv6 input sampler testsamplerv6`	入力パケットのインターフェイスに、IPv6 フロー モニタおよびサンプラを関連付けます。フロー モニタ名およびサンプラ名を最大 63 文字の英数字で入力できます。
ステップ 5	**layer2-switched flow monitor***name***inputsampler***name* 例： `switch(config-if)# layer2-switched flow monitor testmonitorl2 input sampler testsamplerl2`	入力パケットのインターフェイスに、レイヤ 2 スイッチ フローモニタとサンプラを関連付けます。フローモニタ名およびサンプラ名を最大63文字の英数字で入力できます。
ステップ 6	**exit** 例： `switch(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

VLAN 上でのブリッジ型 NetFlow の設定

VLAN にフロー モニタおよびサンプラを適用できます。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**vlan configuration***vlan-id* 例： `switch(config)# vlan configuration 30`	VLAN コンフィギュレーション モードを開始します。vlan-id の範囲は 1 ～ 3967、または 4048 ～ 4093 です。 （注） VLAN コンフィギュレーション モードでは、作成とは無関係に VLAN を設定できます。これは、VTP クライアントのサポートに必要です。
ステップ 3	{**ipipv6**} **flow monitor***name***inputsampler***name* 例： `switch(config-vlan-config)# ip flow monitor testmonitor input sampler testsampler`	入力パケットの VLAN にフロー モニタおよびサンプラを関連付けます。フロー モニタ名およびサンプラ名を最大 63 文字の英数字で入力できます。
ステップ 4	**exit** 例： `switch(config-vlan-config)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

NetFlow タイムアウトの設定

任意で、システム内のすべてのフローに適用されるグローバルな NetFlow タイムアウトを設定できます。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**flow timeout***seconds* 例： `switch(config)# flow timeout 30`	フラッシュタイムアウト値を秒単位で設定します。範囲は 5 ～ 60 秒です。
ステップ 3	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

NetFlow 設定の確認

NetFlow の設定を表示するには、次のいずれかの作業を行います。

コマンド	目的
show flow exporter [*name*]	NetFlow のフロー エクスポータ情報と統計情報を表示します。フロー エクスポータ名を最大 63 文字の英数字で入力できます。
show flow interface [*interface-type slot/port*]	NetFlow インターフェイスに関する情報を表示します。
show flow record [*name*]	NetFlow のフロー レコード情報を表示します。フロー レコード名を最大 63 文字の英数字で入力できます。
show flow record netflow layer2-switched input	レイヤ 2 NetFlow コンフィギュレーションの情報を表示します。
show flow timeout	NetFlow タイムアウト情報を表示します。

コマンド	目的
show sampler [*name*]	NetFlow サンプラに関する情報を表示します。 サンプラ名には最大 63 文字の英数字を入力できます。
show hardware ip flow	NetFlow ハードウェア IP フローに関する情報を表示します。
show running-config netflow	現在のデバイス上の NetFlow 設定を表示します。

NetFlow のモニタリング

NetFlow の統計情報を表示するには、**show flow exporter** コマンドを使用します。NetFlow フローエクスポータの統計情報を消去するには、**clear flow exporter** コマンドを使用します。

NetFlow の設定例

例：フローの作成と適用

フローを作成し、そのフローをインターフェイスへ適用する方法の例を示します。

```
feature netflow
flow exporter ee
 version 9
flow record rr
 match ipv4 source address
 match ipv4 destination address
 collect counter bytes
 collect counter packets
flow monitor foo
 record rr
 exporter ee
sampler testsampler
 mode 1 out-of 65536
interface Ethernet2/45
 ip flow monitor foo input sampler testsampler
 ip address 10.20.1.1/24
 no switchport
```

例：NetFlow エクスポータの設定

次に、IPv4 に対して NetFlow エクスポータを設定する例を示します。

```
flow exporter pw
  destination 172.20.101.87 use-vrf management
  transport udp 3000
  source mgmt0
```

```
  version 9
flow record pw
  match ipv4 source address
  match ipv4 destination address
  match ip protocol
  match ip tos
  match transport source-port
  match transport destination-port
  collect counter bytes long
  collect counter packets long
  collect timestamp sys-uptime first
  collect timestamp sys-uptime last
  collect ip version
sampler testsampler
 mode 1 out-of 65536
flow monitor pw
  record pw
  exporter pw
interface Ethernet2/9
  ip flow monitor pw input sampler testsampler
```

第 22 章

GIRの設定（Cisco NX-OS Release 7.3(0)N1(1)）

この章の内容は、次のとおりです。

- GIR について，313 ページ
- GIR の注意事項および制約事項，320 ページ
- カスタムのメンテナンス モードおよびカスタムの通常モードのプロファイルの設定，321 ページ
- スナップショットの作成，322 ページ
- スナップショットへの show コマンドの追加，324 ページ
- スナップショット セクションのダンプ，325 ページ
- メンテナンス モードの開始，326 ページ
- 通常モードへの復帰，330 ページ
- メンテナンス プロファイルの削除，331 ページ
- GIR の設定例，331 ページ
- GIR の確認，339 ページ
- GIR の機能の履歴，342 ページ

GIR について

グレースフル挿入と削除（GIR）を使用して、デバッグやアップグレードを実行するためにスイッチをメンテナンス モードにすることができます。スイッチのメンテナンスが完了したら、スイッチを通常モードに戻すことができます。

スイッチをメンテナンス モードにすると、すべてのプロトコルがネットワークから分離されます。通常モードに復元されると、すべてのプロトコルが復帰します。

Cisco NX-OS Release 7.1(0)N1(1) で GIR のデフォルト モードは **shutdown** です。スイッチがメンテナンス モードになると、すべてのプロトコルは正常に停止し、すべての物理ポートがシャットダウンします。通常モードに復元されると、すべてのプロトコルとポートが復帰します。次のプロトコルがサポートされています。

- Border Gateway Protocol（BGP）
- BGPv6
- Enhanced Interior Gateway Routing Protocol（EIGRP）
- EIGRPv6
- Intermediate System-to-Intermediate System（ISIS）
- ISISv6
- Open Shortest Path First（OSPF）
- OSPFv3
- RIP

また、次のものもサポートされます。

- バーチャル ポート チャネル（vPC）と vPC+
- インターフェイス
- FabricPath

Cisco NX-OS Release 7.3(0)N1(1) 以降の GIR のデフォルト モードは **isolate** です。すべての有効なプロトコルをメンテナンス モードにするには、**system mode maintenance** コマンドを使用します。スイッチは、**isolate** コマンドを使用して、プロトコルをネットワークから分離します。その後、スイッチはネットワークから分離されますが、シャットダウンされません。スイッチがネットワークから分離されているとき、ピア スイッチとのネイバーシップを維持するために、ルーティングプロトコルがスイッチで実行され続けます。**isolate** コマンドは、プロトコル インスタンスに適用されます。次のプロトコルに適用できます。

- Border Gateway Protocol（BGP）
- BGPv6
- Enhanced Interior Gateway Routing Protocol（EIGRP）
- EIGRPv6
- Intermediate System-to-Intermediate System（ISIS）
- ISISv6
- Open Shortest Path First（OSPF）
- OSPFv3
- FabricPath（スパイン スイッチのみに適用可能）

（注）

- **system mode maintenance shutdown** コマンドを使用して、Cisco NX-OS Release 7.1(0)N1(1) の場合と同様に GIR で **shutdown** モードを使用できます。
- カスタム プロファイルが設定されていて Cisco NX-OS Release 7.3(1)N1(1) イメージを実行しているスイッチをメンテナンス モードをサポートしない他の Cisco NX-OS リリースにコールド ブートすると、書き込み/消去/リロード後に同じコンフィギュレーション ファイルを使用できません。
- 通常モードでは、プロトコルがメンテナンス モードで処理される順序とは逆の順序でプロトコルの処理が実行されます。同様に、メンテナンス モードでは、プロトコルが通常モードで処理される順序とは逆の順序でプロトコルの処理が実行されます。

メンテナンス プロファイル

メンテナンス プロファイルには、グレースフル削除中またはグレースフル挿入中に順番に適用される一連のコマンドが含まれています。

デフォルトでは、すべての有効なプロトコルは、グレースフル削除中に分離され、グレースフル挿入時に復元されます。プロトコルは、定義済みの順序で分離および復元されます。

スイッチは、次のプロファイルをサポートしています。

- メンテナンスモードプロファイル：スイッチがメンテナンスモードになったときに、グレースフル削除中に実行されるすべてのコマンドが含まれます。
- 通常モードプロファイル：スイッチが通常モードに戻ったときに、グレースフル挿入中に実行されるすべてのコマンドが含まれます。

システム生成プロファイル

特定のコンフィギュレーション コマンドを使用して、メンテナンス モード プロファイルまたは通常モードプロファイルを生成できます。**system mode maintenance** コマンドを使用するとメンテナンス モード プロファイルが生成され、**no system mode maintenance** コマンドを使用すると通常モード プロファイルが生成されます。

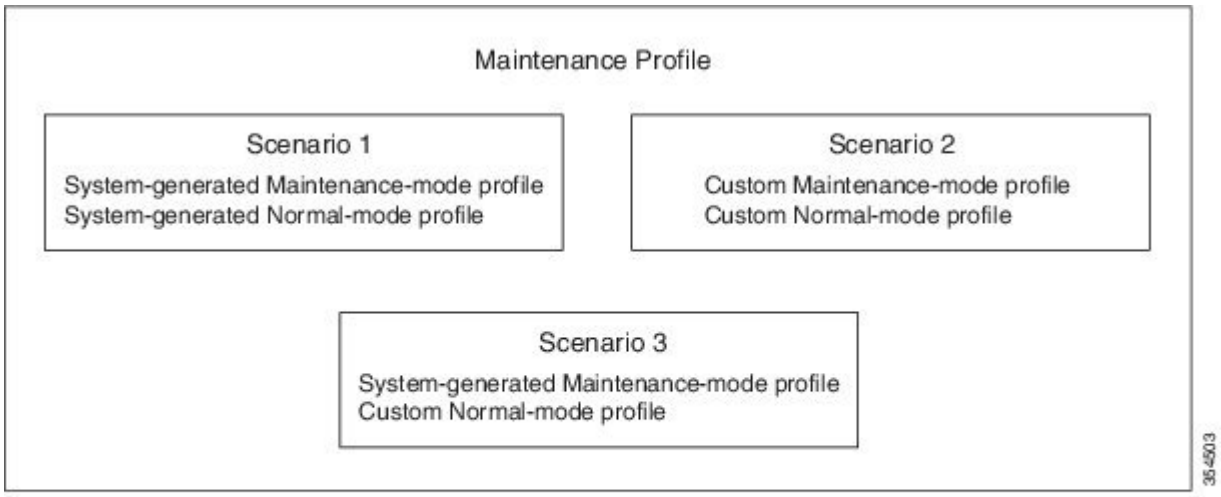
カスタム プロファイル

グレースフル削除中またはグレースフル挿入中に適用できるコンフィギュレーション コマンドを使用して、カスタムのメンテナンス モード プロファイルまたは通常モード プロファイルを作成し、プロトコルを個別に分離、シャットダウン、復元（または追加の設定を実行）できます。システム生成プロファイルでは必要な設定が提供されない場合、または既存のシステム生成プロファイルまたはカスタム プロファイルを拡張して導入に固有の追加機能が含まれるようにする必要がある場合、カスタム プロファイルを使用できます。必要なコマンドを含むカスタムのメンテナンス モード プロファイルを設定するには **configure maintenance profile maintenance-mode** コマンド

を使用し、必要なコマンドを含むカスタムの通常モード プロファイルを設定するには **configure maintenance profile normal-mode** コマンドを使用します。

システム生成プロファイルはカスタム プロファイルを上書きします（逆も同様です）。システム生成のメンテナンス モード プロファイルとカスタムのメンテナンス モード プロファイルのいずれか一方を一度に使用できます。同様に、システム生成の通常モード プロファイルとカスタムの通常モード プロファイルのいずれか一方を一度に使用できます。シナリオを次の図に示します。

図 *4*：メンテナンス プロファイルのシナリオ



（注） シナリオ 1 または 2 の使用を推奨します。

計画外のメンテナンス

重大な障害によりスイッチをリロードする際に、スイッチを計画外のメンテナンス モードにすることができます。シングル スーパーバイザのスイッチでは、**system mode maintenance on-reload reset-reason** コマンドを使用してリセット理由 CLI を設定し、重大な障害によりスイッチをリロードした後でスイッチをメンテナンスモードにすることができます。デュアル スーパーバイザのスイッチでは、スイッチの重大な障害があるときに SUP のスイッチオーバーが発生し、スイッチはメンテナンスモードになりません。スタートアップ コンフィギュレーション内に存在するメンテナンス モード プロファイルは、スイッチが計画外のメンテナンス モードになるときに適用されます。スタートアップ コンフィギュレーション内にメンテナンス モード プロファイルがない場合、スイッチが計画外のメンテナンス モードになるときにシステム生成のメンテナンス モード プロファイルが作成されて適用されます。

メンテナンス モードのタイマー

指定した分だけスイッチをメンテナンスモードのままにするには、メンテナンスモードを開始する前に **system mode maintenance timeout** コマンドを使用します。スイッチがメンテナンス モードのときにこのコマンドを使用して、スイッチをメンテナンス モードにする分数を変更することもできます。タイマーはその時点から新しいタイマー値で再起動します。設定された時間が経過すると、**no system mode maintenance mode** コマンドを使用しなくても、スイッチは自動的に通常モードに復帰します。タイマーを無効にするには、**no system mode maintenance timeout** コマンドを使用します。

Snapshot

選択した機能の実行中状態をキャプチャしたり、永続ストレージ メディアに保存したりするには、**snapshot** コマンドを使用します。

スナップショットを使用すると、スイッチをメンテナンス モードにする前の状態と通常モードに復帰した後の状態を比較できます。スナップショット プロセスは、次の 3 つの部分で構成されます。

- 事前に選択したスイッチの一部機能の状態のスナップショットを作成し、永続ストレージメディアに保存する。
- さまざまな時間間隔で取得したスナップショットを一覧にして、管理する。
- スナップショットを比較して、各機能の概要と詳細を表示する。

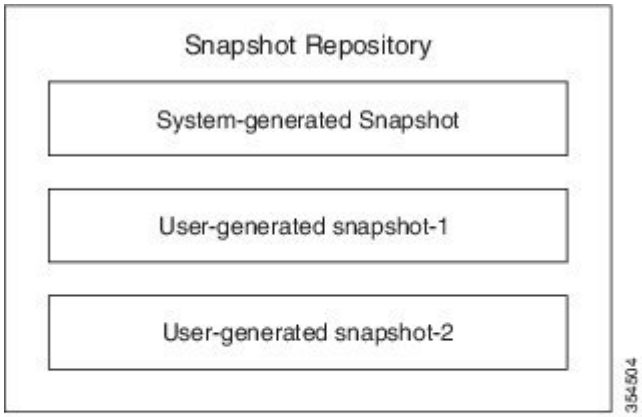
スナップショットには、次の 2 つのタイプがあります。

- システム生成のスナップショット：**[no] system mode maintenance** コマンドを使用すると、システムによって生成されます。メンテナンス モードに移行する直前に、before_maintenance スナップショットがシステムによって生成されます。通常モードに移行する直前に、after_maintenance スナップショットが作成されます。**[no] system mode maintenance** コマンドを使用する際、古いスナップショットは上書きされます。システム生成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。
- ユーザ生成のスナップショット：ユーザ生成のスナップショットを作成するには、**snapshot create** *name description* コマンドを使用します。ユーザ生成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。

特定のシナリオでは、ハードウェア プログラミング中にシステム生成の after_maintenance スナップショットが作成されることがあります。このような場合、システムがハードウェア プログラミングを完了していて安定状態にあるときに、ユーザ生成のスナップショットを作成することを推奨します。その後、新しい after_maintenance スナップショットと before_maintenance スナップショットを比較できます。

システム生成およびユーザ生成のスナップショットは、スナップショット リポジトリに保存されます。

図 5：スナップショット リポジトリ



次の表にスナップショット セクションと対応する show コマンドを示します。

セクションの名前	対応する **show** コマンド
bgp-sessions	show bgp sessions vrf all
eigrp	show ip eigrp topology summary
eigrpv6	show ipv6 eigrp topology summary
interface	show interface
ospf	show ip ospf vrf all
ospfv3	show ipv6 ospfv3 vrf all
isis	show isis database detail vrf all
rip	show ip rip vrf all
route-summary	show ip route summary vrf all
routev6-summary	show ipv6 route summary vrf all
vpc	show vpc

FIB 保留の抑制

Forwarding Information Base（FIB）保留の抑制機能では、Border Gateway Protocol-Routing Information Base（BGP-RIB）および Enhanced Interior Gateway Routing Protocol-Routing Information Base（EIGRP-RIB）フィードバック メカニズムを使用して、ネットワークにおける初期のルート アドバタイズメントと後続のパケット損失を防ぎます。このメカニズムはデフォルトで有効であり、ルートがネイバーにアドバタイズされる前にローカルに組み込まれるようになります。

BGP と EIGRP は RIB からのフィードバックを待ちます。このフィードバックには、EIGRP または BGP によって RIB に組み込まれたルートが、EIGRP または BGP がネイバーにアップデートを送信する前に FIB に組み込まれたことが示されています。EIGRP または BGP がアップデートを送信するのは、FIB が組み込んだバージョン以下のバージョンのルートだけです。この選択的アップデートにより、EIGRP または BGP が初期アップデートを送信しなくなります。その結果、スイッチのリロードやライン カードのリロード後、データ プレーンがプログラミングされる前であっても、またはスイッチがメンテナンス モードから通常モードに移行する際に、トラフィックを招きます。

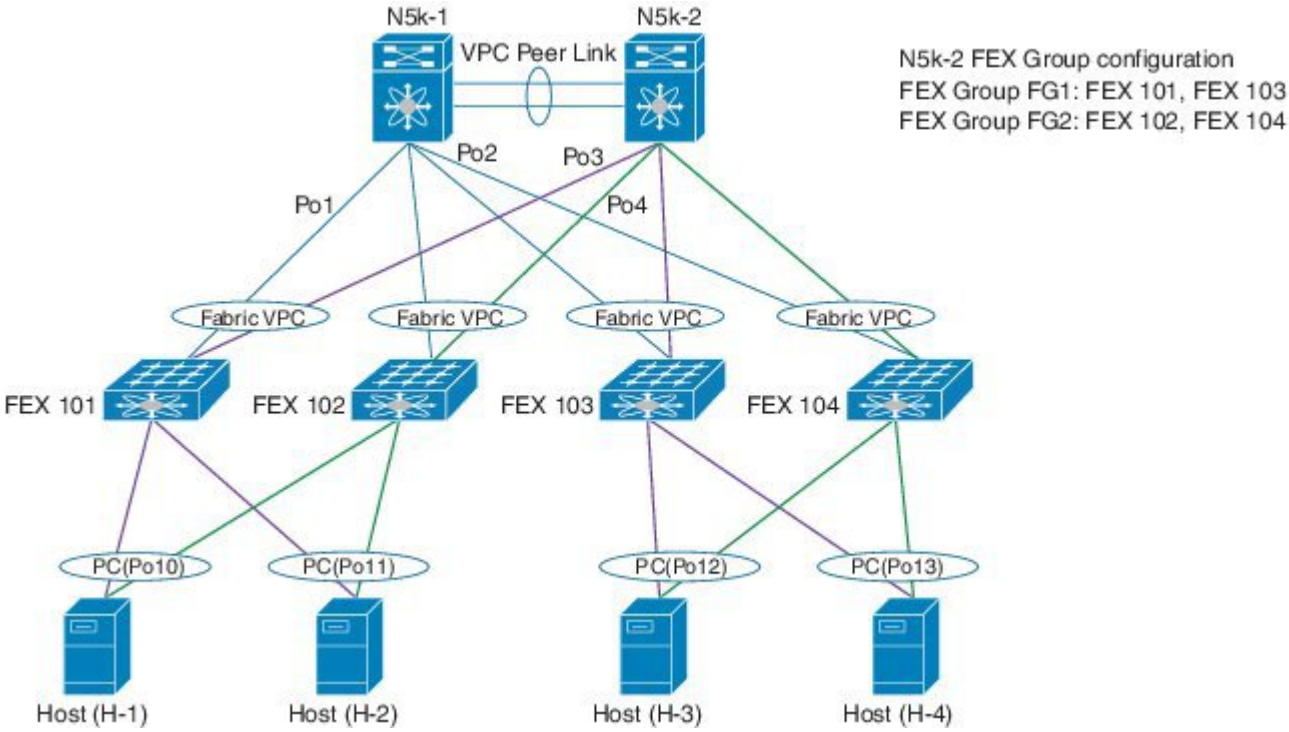
FEX グループの GIR 機能

GIR を使用して、デュアルホーム vPC トポロジの Cisco Nexus 5000、5500、および 6000 シリーズスイッチおよび接続された FEX のメンテナンスとソフトウェア アップグレードを実行できます。FEX グループは、FEX の論理グループです。FEX グループは、FEX の起動または停止の手順を最適化するために追加されました。

VPC ドメインに FG1 と FG2 という 2 つの FEX グループがあるようなシナリオを考えてみます（下図を参照）。すべてのホストが冗長接続されていて、1 つは FG1 内のいずれかの FEX に接続され、もう 1 つは FG2 内のいずれかの FEX に接続されているとします。「セカンダリ」スイッチをメンテナンス モードにする前に、FG1 を停止して FG1 内のすべての FEX でイメージの新しいバージョンに強制アップグレードし、「プライマリ」スイッチへの接続を確立します。「プライマリ」

スイッチへの接続が確立されたら、FG2 内の FEX を停止してから、「セカンダリ」スイッチをメンテナンス モードにします。

図 *6*：トポロジの例



（注） FEX グループを作成するには、**fex-group** *name* コマンドを使用します。FEX グループで FEX を追加または削除するには、**fex** *range* コマンドを使用します。FEX グループをシャットダウンするには、**system fex-group** *name* **shutdown** コマンドを使用します。FEX グループを起動するには、**no system fex-group** *name* **shutdown** コマンドを使用します。

GIR の注意事項および制約事項

- カスタム メンテナンス プロファイルは、自動またはシステム生成のプロファイルでサポートされないカスタムのトポロジおよびプロトコルに使用する必要があります。
- メンテナンスを開始する前に、メンテナンス モードになった後でスイッチがデータ トラフィックを招かないことを確認します。スイッチでデータ トラフィックがないことを確認するためにカウンタと統計情報を使用できます。
- カスタム プロファイルを使用するときにカスタム プロファイルがシステム生成のプロファイルによって上書きされないようにする場合は、**system mode maintenance always-use-custom-profile** コマンドを使用します。

- スナップショット情報は、デュアル スーパーバイザ システムのスタンバイ スーパーバイザに自動的にコピーされません。
- 一部のトポロジや設定では、GIR がアプリケーション トラフィックの損失ゼロを実現できないことがあります。
- Cisco NX-OS Release 7.3(0)N1(1) 以降では、**configure profile [maintenance-mode | normal-mode] type admin** コマンドの使用は推奨されません。**configure maintenance profile [maintenance-mode | normal-mode]** コマンドを使用することを強く推奨します。
- メンテナンス モードでは、In-Service Software Upgrade（ISSU）または In-Service Software Downgrade（ISSD）を実行できません。

カスタムのメンテナンス モードおよびカスタムの通常モードの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コンフィギュレーション コマンドを使用して、メンテナンス モード プロファイルまたは通常モード プロファイルを作成できます。メンテナンスモード操作時にはカスタムプロファイルが常に使用されるようにするため、カスタムのメンテナンスモードプロファイルおよびカスタムの通常モードプロファイルの設定後に **system mode maintenance always-use-custom-profile** コマンドを使用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	switch# **configure maintenance profile** [**maintenance-mode** | **normal-mode**]	メンテナンス モード プロファイルまたは通常モード プロファイルのコンフィギュレーション セッションを開始します。 （注） 設定しているプロトコルに応じて、プロトコルを停止する適切なコマンドを入力します。
ステップ 2	switch# **end**	メンテナンス モード プロファイルを閉じます。

次に、カスタムのメンテナンス モード プロファイルを作成する例を示します。

```
switch# configure maintenance profile maintenance-mode
Please configure 'system mode maintenance always-use-custom-profile' if you want to use
custom profile always for maintenance mode.
Enter configuration commands, one per line. End with CNTL/Z.
switch(config-mm-profile)# router bgp 100
switch(config-mm-profile-router)# isolate
switch(config-mm-profile-router)# exit
switch(config-mm-profile)# sleep instance 1 10
switch(config-mm-profile)# interface ethernet 1/1
switch(config-mm-profile-if-verify)# shutdown
switch(config-mm-profile-if-verify)# end
```

```
Exit maintenance profile mode.
```

次に、カスタムの通常モード プロファイルを作成する例を示します。

```
switch# configure maintenance profile normal-mode
Please configure 'system mode maintenance always-use-custom-profile' if you want to use
custom profile always for maintenance mode.
Enter configuration commands, one per line. End with CNTL/Z.
switch(config-mm-profile)# interface ethernet 1/1
switch(config-mm-profile-if-verify)# no shutdown
switch(config-mm-profile-if-verify)# exit
switch(config-mm-profile)# sleep instance 1 20
switch(config-mm-profile)# router bgp 100
switch(config-mm-profile-router)# no isolate
switch(config-mm-profile-router)# end
Exit maintenance profile mode.
```

```
switch# show maintenance profile
[Normal Mode]
interface Ethernet1/1
no shutdown
sleep instance 1 20
router bgp 100
no isolate
[Maintenance Mode]
router bgp 100
isolate
sleep instance 1 20
interface Ethernet1/1
shutdown
```

スナップショットの作成

選択した機能の実行状態のスナップショットを作成できます。スナップショットを作成する場合、定義済みの一連の show コマンドが実行され、出力が保存されます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **snapshot create***name description*	スナップショットを作成します。*name* 変数は最大 64 文字です。*description* 変数は最大 256 文字です。 すべてのスナップショットまたは特定のスナップショットを削除するには、**snapshot delete** {**all** | *snapshot-name*} コマンドを使用します。
ステップ 2	switch# **show snapshots**	（任意） スイッチ上に存在するスナップショットを表示します。
ステップ 3	switch# **show snapshots compare***snapshot-name-1 snapshot-name-2* [**summary**]	（任意） 2 つのスナップショットの比較を表示します。**summary** キーワードは、2 つのスナップショット間の全体的な変更を確認するのに十分な情報のみ表示します。

	コマンドまたはアクション	目的

次に、スナップショットを作成する例を示します。

```
switch# snapshot create before_maint taken before maint
Executing 'show interface'... Done
Executing 'show ip route summary vrf all'... Done
Executing 'show ipv6 route summary vrf all'... Done
Executing 'show bgp sessions vrf all'... Done
Executing 'show ip eigrp topology summary'... Done
Executing 'show ipv6 eigrp topology summary'... Done
Executing 'show vpc'... Done
Executing 'show ip ospf vrf all'... Done
Feature 'ospfv3' not enabled, skipping...
Executing 'show isis database detail vrf all'... Done
Executing 'show ip rip vrf all'... Done
Executing user-specified 'show ip route detail vrf all'... Done
Snapshot 'before_maint' created
```

次に、スイッチ上に存在するスナップショットを表示する例を示します。

```
switch# show snapshots
Snapshot Name           Time                           Description
-------------------------------------------------------------------------------
before_maint            Wed Oct 14 10:56:50 2015       taken before maint
```

次に、2 つのスナップショットの比較を表示する例を示します。

```
switch# show snapshots compare before_maintenance after_maintenance summary
================================================================================
Feature changed                       before_maintenance after_maintenance
================================================================================
basic summary
   # of interfaces                          50                50
   # of vlans                               0                 0
   # of ipv4 routes  vrf default            13                13
   # of ipv4 paths   vrf default            13                13
   # of ipv4 routes  vrf management         14                14
   # of ipv4 paths   vrf management         14                14
   # of ipv6 routes  vrf default            3                 3
   # of ipv6 paths   vrf default            3                 3

interfaces
   # of eth interfaces                      48                48
   # of eth interfaces up                   1                 1
   # of eth interfaces down                 47                47
   # of eth interfaces other                0                 0

   # of vlan interfaces                     0                 0
   # of vlan interfaces up                  0                 0
   # of vlan interfaces down                0                 0
   # of vlan interfaces other               0                 0
```

次に、スナップショットを削除する例を示します。

```
switch# snapshot delete before_maint
switch# show snapshots
Snapshot Name           Time                           Description
-------------------------------------------------------------------------------
```

スナップショットへの show コマンドの追加

スナップショットでキャプチャされる追加の **show** コマンドを指定できます。それらの **show** コマンドは、ユーザ指定のスナップショット セクションで定義されます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **snapshot section add***section "show-command" row-id element-key1* [*element-key2*]	ユーザ指定のセクションをスナップショットに追加します。*section* 変数は、**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。 **show** コマンドは、引用符で囲む必要があります。**show** 以外のコマンドは拒否されます。 *row-id* 引数では、**show** コマンドの XML 出力の各行エントリのタグを指定します。*element-key1* および *element-key2* 引数では、行エントリ間を区別するために使用されるタグを指定します。ほとんどの場合、行エントリ間を区別するために指定する必要があるのは *element-key1* 引数だけです。 （注） スナップショットからユーザ指定のセクションを削除するには、**snapshot section delete***section* セクション コマンドを使用します。
ステップ 2	switch# **show snapshots sections**	（任意） ユーザ指定のスナップショット セクションを表示します。

次に、**show ip route detail vrf all** コマンドをスナップショットに追加する例を示します。

```
switch# snapshot section add v4route "show ip route detail vrf all" ROW_prefix ipprefix
switch# show snapshots sections
user-specified snapshot sections
--------------------------------
[v4route]
show command: show ip route detail vrf all
row id: ROW_prefix
key1: ipprefix
key2: -
```

次に、**show ipv6 route detail vrf all** コマンドをスナップショットに追加する例を示します。

```
switch# snapshot section add routev6 "show ipv6 route detail vrf all" ROW_prefix ipprefix
added section "routev6"

switch# show snapshots sections
user-specified snapshot sections
--------------------------------
[routev6]
show command: show ipv6 route detail vrf all
```

```
row id: ROW_prefix
key1: ipprefix
key2: -
```

次に、ユーザ指定のスナップショット セクションを削除する例を示します。

```
switch# snapshot section delete v4route
deleted section ”v4route"

switch# show snapshots sections
user-specified snapshot sections
--------------------------------
none
```

次に、**show ip route detail vrf all** コマンドの XML 出力例を示します。

```
switch(config)# show ip route detail vrf all | xml
<?xml version="1.0" encoding="ISO-8859-1"?>
<nf:rpc-reply xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns="http://w
ww.cisco.com/nxos:7.3.0.N1.1.:urib">
 <nf:data>
  <show>
   <ip>
       <__readonly__>
         <TABLE_vrf>
          <ROW_vrf>
           <vrf-name-out>default</vrf-name-out>
           <TABLE_addrf>
            <ROW_addrf>
             <addrf>ipv4</addrf>
             <TABLE_prefix>
              <ROW_prefix>
               <ipprefix>0.0.0.0/32</ipprefix>
               <ucast-nhops>1</ucast-nhops>
               <mcast-nhops>0</mcast-nhops>
               <attached>false</attached>
              … <snip>
              </ROW_prefix>
```

スナップショット セクションのダンプ

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **show snapshots dump***snapshot-name*	生成されたスナップショットのさまざまなセクションの内容を表示します。

次に、生成されたスナップショットのさまざまなセクションの内容をダンプする例を示します。

```
switch# show snapshots dump new
File:  interface.xml        Snapshot:  new
==============================================================================
<?xml version="1.0" encoding="ISO-8859-1"?>
<nf:rpc-reply xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns="http://w
ww.cisco.com/nxos:7.3.0.N1.1.:if_manager">
 <nf:data>
  <show>
   <interface>
    <__readonly__>
```

```
<TABLE_interface>
 <ROW_interface>
  <interface>mgmt0</interface>
  <state>up</state>
  <admin_state>up</admin_state>
  <eth_hw_desc>GigabitEthernet</eth_hw_desc>
  <eth_hw_addr>5cfc.666d.3b34</eth_hw_addr>
  <eth_bia_addr>5cfc.666d.3b34</eth_bia_addr>
  <eth_ip_addr>5.24.100.101</eth_ip_addr>
  <eth_ip_mask>16</eth_ip_mask>
  <eth_ip_prefix>5.24.0.0</eth_ip_prefix>
  <eth_mtu>1500</eth_mtu>
… <snip> …
```

メンテナンス モードの開始

system mode maintenance コマンドを使用する代わりにカスタムのプロファイルを作成する場合は、「カスタムのメンテナンス モードおよびカスタムの通常モードのプロファイルの設定」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	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **system mode maintenance** [**shutdown** | **timeout***value* | **on-reload reset-reason***reason* | **dont-generate-profile** | **always-use-custom-profile**]	すべての有効なプロトコルをメンテナンス モードにします（**isolate** コマンドを使用）。 **dont-generate-profile** および **shutdown** オプションを使用して、スイッチをメンテナンス モードにします。 • **dont-generate-profile**：有効なプロトコルの動的な検索が回避され、メンテナンス モード プロファイルに設定されているコマンドが実行されます。カスタムのメンテナンス モードプロファイルでコマンドを実行する場合は、このオプションを使用します。 • **shutdown**：すべてのプロトコル、および管理インターフェイスを除くインターフェイスをシャットダウンします（**shutdown** コマンドを使用）。このオプションを指定すると中断が発生しますが、デフォルト（**isolate** コマンドを使用）の場合、中断は発生しません。 **on-reload reset-reason**, **timeout** および **always-use-custom-profile** オプションは、メンテナンスモードパラメータを設定するために使用しますが、スイッチをメンテナンスモードにしません。 • **timeout***value*：指定した分数の間、スイッチをメンテナンス モードのままにします。範囲は 5 ～ 65535 です。タイム

	コマンドまたはアクション	目的
		アウト値は少なくとも60分に設定することを推奨します。設定した時間が経過すると、スイッチは自動的に通常モードに戻ります。**no system mode maintenance timeout** コマンドは、タイマーを無効にします。 • **on-reload reset-reason***reason*：指定されているシステム クラッシュが発生した場合、スイッチは自動的にメンテナンス モードで起動します。**no system mode maintenance on-reload reset-reason** コマンドを使用すると、システム クラッシュ時にスイッチがメンテナンスモードで起動するのを回避できます。メンテナンスモードのリセット理由は次のとおりです。 • HW_ERROR：ハードウェア エラー • SVC_FAILURE：重大なサービス障害 • KERN_FAILURE：カーネル パニック • WDOG_TIMEOUT：ウォッチドッグ タイムアウト • FATAL_ERROR：致命的なエラー • MANUAL_RELOAD：手動リロード • MAINTENANCE：スイッチがリロード前にすでにメンテナンス モードになっていたために、メンテナンス モードでスイッチをリロードします。 • MATCH_ANY：上記のいずれかの理由 • ANY_OTHER：上記で指定されていないいずれかのリロード理由。 続行を促すプロンプトが表示されます。続行する場合は y、プロセスを終了する場合は n を入力します。 （注） リセット理由を設定し、スタートアップ コンフィギュレーションに保存することを推奨します。これにより、スイッチが何らかの理由でリロードした後、スイッチはメンテナンスモードになることができます。 • **always-use-custom-profile**：既存のカスタムのメンテナンス モード プロファイルを適用し、自動生成のメンテナンス モードプロファイルが作成されないようにする場合は、このオプションを使用します。このオプションでは、**system mode maintenance** コマンドを使用して指定しなかった場合でも、dont-generate-profile オプションが強制的に使用され

	コマンドまたはアクション	目的
		ます。このオプションを使用するときは、shutdown オプションを使用できません。
ステップ 3	switch# **show system mode**	（任意） 現在のシステムモードを表示します。このコマンドは、スイッチがメンテナンスモードにあるときにメンテナンスモードのタイマーの現在の状態も表示します。

次に、**system mode maintenance** コマンドを使用してすべてのプロトコルをメンテナンスモードにする例を示します。

```
switch# configure terminal
switch(config)# system mode maintenance
Following configuration will be applied:

router bgp 100
  isolate
router ospf 100
  isolate
router isis 100
  isolate

Do you want to continue (y/n)? [no] y

Generating a snapshot before going into maintenance mode

Starting to apply commands...

Applying : router bgp 100
Applying :   isolate
Applying : router ospf 100
Applying :   isolate
Applying : router isis 100
Applying :   isolate

Maintenance mode operation successful.
```

次に、スイッチのすべてのプロトコルおよびインターフェイスをシャットダウンする例を示します。

```
switch# configure terminal
switch(config)# system mode maintenance shutdown
Following configuration will be applied:

router bgp 64581
  shutdown
router eigrp p2
  shutdown
  address-family ipv6 unicast
    shutdown
router eigrp 0
  shutdown
  address-family ipv6 unicast
    shutdown
router ospf 200
  shutdown
router isis 70
  shutdown
```

```
vpc domain 2
  shutdown
system interface shutdown

NOTE: 'system interface shutdown' will shutdown all interfaces excluding mgmt 0
Do you want to continue (yes/no)? [no] yes

Generating a snapshot before going into maintenance mode

Starting to apply commands...

Applying : router bgp 64581
Applying :   shutdown
Applying : router eigrp p2
Applying :   shutdown
Applying :   address-family ipv6 unicast
Applying :     shutdown
Applying : router eigrp 0
Applying :   shutdown
Applying :   address-family ipv6 unicast
Applying :     shutdown
Applying : router ospf 200
Applying :   shutdown
Applying : router isis 70
Applying :   shutdown
Applying : vpc domain 2
Applying :   shutdown2016 Jan 15 11:10:36.080386 CP-BL26-N7K-1A %$ VDC-1 %$
%VPC-2-VPC_SHUTDOWN: vPC shutdown status is ON

Applying : system interface shutdown

Maintenance mode operation successful.
switch(config)# 2016 Jan 15 11:10:42.057678 CP-BL26-N7K-1A %$ VDC-1 %$ %MMODE-2-MODE_CHANGED:
 System changed to "maintenance" mode.
2016 Jan 15 11:10:42.058167 CP-BL26-N7K-1A %$ VDC-1 %$ %MMODE-2-MODE_CHANGE_WARN: System
will be moved to "normal" mode in 5 minutes
```

次に、指定した分数の間、スイッチをメンテナンス モードのままにする例を示します。

```
switch# configure terminal
switch (config)# system mode maintenance timeout 25

switch# show system mode
System Mode: Maintenance
Maintenance Mode Timer: 24 minutes 55 seconds remaining
```

次に、致命的なエラーが発生した場合に、スイッチを自動的にメンテナンス モードで起動する例を示します。

```
switch# configure terminal
switch(config)# system mode maintenance on-reload reset-reason fatal_error
```

次に、以前作成したメンテナンス モード プロファイルを使用してスイッチをメンテナンス モードにする例を示します。

```
switch# configure terminal
switch(config)# system mode maintenance dont-generate-profile

Following configuration will be applied:

router bgp 100
  isolate
sleep instance 1 10
interface Ethernet1/1
  shutdown

Do you want to continue (y/n)? [no] y

Generating a snapshot before going into maintenance mode
```

```
Starting to apply commands...

Applying : router bgp 100
Applying :   isolate
Applying : sleep instance 1 10
Applying : interface Ethernet1/1
Applying :   shutdown

Maintenance mode operation successful.
```

次に、既存のカスタムのメンテナンス モード プロファイルを適用し、自動生成のメンテナンス モード プロファイルが作成されないようにする例を示します。

```
switch# configure terminal
switch(config)# system mode maintenance always-use-custom-profile
```

通常モードへの復帰

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch# **no system mode maintenance** [**dont-generate-profile**]	以前に作成した通常モード プロファイル ファイル、または動的に作成した通常モード プロファイル ファイルを実行します。**dont-generate-profile** オプションは、通常モード メンテナンス プロファイルの作成を抑制し、既存の通常モード メンテナンス プロファイルの再利用を防ぎます。 続行を促すプロンプトが表示されます。続行する場合は **y**、プロセスを終了する場合は **n** を入力します。 （注） 大規模な設定では、一定のインターバルの後にインターフェイスが起動します。

次に、メンテナンス モードから通常モードに戻る例を示します。

```
switch# configure terminal
switch(config)# no system mode maintenance
Following configuration will be applied:

interface Ethernet1/1
  no shutdown
sleep instance 1 20
router bgp 100
  no isolate

Do you want to continue (y/n)? [no] yes

Starting to apply commands...

Applying : interface Ethernet1/1
Applying :   no shutdown
```

```
Applying : sleep instance 1 20
Applying : router bgp 100
Applying :   no isolate

Maintenance mode operation successful.

Generating Current Snapshot

Please use 'show snapshots compare before_maintenance after_maintenance' to check the health
 of the system
switch(config)#


switch(config)# show system mode
System Mode: Normal
```

メンテナンス プロファイルの削除

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch# **no configure maintenance profile** {**normal-mode** | **maintenance-mode**}	通常モードまたはメンテナンス モードのプロファイルを削除します。

次に、メンテナンス プロファイルを削除する例を示します。

```
switch# configure terminal
switch(config)# no configure maintenance profile maintenance-mode
```

GIR の設定例

次に、カスタムのメンテナンス モード プロファイルを作成する例を示します。

```
switch# configure maintenance profile maintenance-mode
Please configure 'system mode maintenance always-use-custom-profile' if you want to use
custom
profile always for maintenance mode.
Enter configuration commands, one per line. End with CNTL/Z.
switch(config-mm-profile)# router bgp 100
switch(config-mm-profile-router)# isolate
switch(config-mm-profile-router)# exit
switch(config-mm-profile)# sleep instance 1 10
switch(config-mm-profile)# interface ethernet 1/1
switch(config-mm-profile-if-verify)# shutdown
switch(config-mm-profile-if-verify)# end
Exit maintenance profile mode.
```

次に、カスタムの通常モード プロファイルを作成する例を示します。

```
switch# configure maintenance profile normal-mode
Please configure 'system mode maintenance always-use-custom-profile' if you want to use
```

```
custom
profile always for maintenance mode.
Enter configuration commands, one per line. End with CNTL/Z.
switch(config-mm-profile)# interface ethernet 1/1
switch(config-mm-profile-if-verify)# no shutdown
switch(config-mm-profile-if-verify)# exit
switch(config-mm-profile)# sleep instance 1 20
switch(config-mm-profile)# router bgp 100
switch(config-mm-profile-router)# no isolate
switch(config-mm-profile-router)# end
Exit maintenance profile mode.
```

次に、IPv6プロトコル用にカスタムのメンテナンスモードおよび通常モードプロファイルを作成する例を示します。

```
switch# configure terminal
switch(config)# configure maintenance profile maintenance-mode
Please configure 'system mode maintenance always-use-custom-profile' if you want to use
custom
profile always for maintenance mode.
switch(config-mm-profile)# router ospfv3 ospf_ipv6
switch(config-mm-profile-router)# shutdown
switch(config-mm-profile-router)# exit
switch(config-mm-profile)# router eigrp 660
switch(config-mm-profile-router)# address-family ipv6 unicast
switch(config-mm-profile-router-af)# shutdown
switch(config-mm-profile-router-af)# exit
switch(config-mm-profile)# router isis isp
switch(config-mm-profile-router)# set-overload-bit always
switch(config-mm-profile-router)# address-family ipv6 unicast
switch(config-mm-profile-router-af)# shutdown
switch(config-mm-profile-router-af)# exit


switch# configure terminal
switch(config)# configure maintenance profile normal-mode
Please configure 'system mode maintenance always-use-custom-profile' if you want to use
custom
profile always for maintenance mode.
switch(config-mm-profile)# router isis isp
switch(config-mm-profile-router)# no set-overload-bit always
switch(config-mm-profile-router)# address-family ipv6 unicast
switch(config-mm-profile-router-af)# no shutdown
switch(config-mm-profile-router-af)# exit
switch(config-mm-profile)# router eigrp 660
switch(config-mm-profile-router)# address-family ipv6 unicast
switch(config-mm-profile-router-af)# no shutdown
switch(config-mm-profile-router-af)# exit
switch(config-mm-profile)# router ospfv3 ospf_ipv6
switch(config-mm-profile-router)# no shutdown
switch(config-mm-profile-router)# exit


switch# show maintenance profile
[Normal mode]
router isis isp
  no set-overload-bit always
  address-family ipv6 unicast
   no shutdown
router eigrp 660
  address-family ipv6 unicast
   no shutdown
router ospfv3 ospf_ipv6
   no shutdown
[Maintenance Mode]
router ospfv3 ospf_ipv6
  shutdown
router eigrp 660
  address-family ipv6 unicast
   shutdown
router isis isp
```

```
  set-overload-bit always
  address-family ipv6 unicast
   shutdown
```

次に、VPC 用にカスタムのメンテナンス モード プロファイルおよびカスタムの通常モード プロファイルを作成する例を示します。

```
switch# configure terminal
switch(config)# configure maintenance profile maintenance-mode
switch(config-mm-profile)# router bgp 100
switch(config-mm-profile-router)# isolate
switch(config-mm-profile-router)# exit
switch(config-mm-profile)# interface port channel 5
switch(config-mm-profile-if-verify)# vpc orphan port suspend
switch(config-mm-profile-if-verify)# exit
switch(config-mm-profile)# interface port channel 6
switch(config-mm-profile-if-verify)# vpc orphan port
suspend switch(config-mm-profile-if-verify)# exit
switch(config-mm-profile)# sleep instance 1 5
switch(config-mm-profile)# vpc domain 1
switch(config-mm-profile-vpc-domain)# shutdown


switch# configure terminal
switch(config)# configure maintenance profile normal-mode
switch(config-mm-profile)# vpc domain 1
switch(config-mm-profile-vpc-domain)# no shutdown
switch(config-mm-profile-vpc-domain)# exit
switch(config-mm-profile)# sleep instance 1 60
switch(config-mm-profile)# interface port channel 5
switch(config-mm-profile-if-verify)# no vpc orphan port suspend
switch(config-mm-profile-if-verify)# exit
switch(config-mm-profile)# interface port channel 6
switch(config-mm-profile-if-verify)# no vpc orphan port suspend
switch(config-mm-profile-if-verify)# exit
switch(config-mm-profile)# router bgp 100
switch(config-mm-profile-router)# no isolate


switch# show maintenance profile
[Normal Mode]
vpc domain 1
  no shutdown
sleep instance 1 60
interface port-channel 5
  no vpc orphan-port suspend
interface port-channel 6
  no vpc orphan-port suspend router
bgp 100
  no isolate

[Maintenance Mode]
router bgp 100
  isolate
interface port-channel 5 vpc
  orphan-port suspend
interface port-channel 6 vpc
  orphan-port suspend
sleep instance 1 5
  vpc domain 1 shutdown
```

次に、**isolate** コマンドを使用してすべてのプロトコルをメンテナンス モードにする例を示します。

```
switch(config)# system mode maintenance

Following configuration will be applied:

router bgp 100
  isolate
```

```
router ospf 100
  isolate
router isis 100
  isolate

Do you want to continue (y/n)? [no] y

Generating a snapshot before going into maintenance mode

Starting to apply commands...

Applying : router bgp 100
Applying :   isolate
Applying : router ospf 100
Applying :   isolate
Applying : router isis 100
Applying :   isolate

Maintenance mode operation successful.
```

次に、スイッチのすべてのプロトコルおよびインターフェイスをシャットダウンする例を示します。

```
switch# configure terminal
switch(config)# system mode maintenance shutdown

Following configuration will be applied:

router bgp 64581
  shutdown
router eigrp p2
  shutdown
  address-family ipv6 unicast
    shutdown
router eigrp 0
  shutdown
  address-family ipv6 unicast
    shutdown
router ospf 200
  shutdown
router isis 70
  shutdown
vpc domain 2
  shutdown
system interface shutdown

NOTE: 'system interface shutdown' will shutdown all interfaces excluding mgmt 0
Do you want to continue (yes/no)? [no] yes

Generating a snapshot before going into maintenance mode

Starting to apply commands...

Applying : router bgp 64581
Applying :   shutdown
Applying : router eigrp p2
Applying :   shutdown
Applying :   address-family ipv6 unicast
Applying :     shutdown
Applying : router eigrp 0
Applying :   shutdown
Applying :   address-family ipv6 unicast
Applying :     shutdown
Applying : router ospf 200
Applying :   shutdown
Applying : router isis 70
Applying :   shutdown
Applying : vpc domain 2
Applying :   shutdown2016 Jan 15 11:10:36.080386 CP-BL26-N7K-1A %$ VDC-1 %$
%VPC-2-VPC_SHUTDOWN: vPC shutdown status is ON
```

```
Applying : system interface shutdown

Maintenance mode operation successful.
switch(config)# 2016 Jan 15 11:10:42.057678 CP-BL26-N7K-1A %$ VDC-1 %$ %MMODE-2-MODE_CHANGED:
 System changed to "maintenance" mode.
2016 Jan 15 11:10:42.058167 CP-BL26-N7K-1A %$ VDC-1 %$ %MMODE-2-MODE_CHANGE_WARN: System
will be moved to "normal" mode in 5 minutes
```

次に、メンテナンス モードから通常モードに戻る例を示します。

```
switch# configure terminal
switch(config)# no system mode maintenance dont-generate-profile

Following configuration will be applied:
interface Ethernet1/1
  no shutdown
  sleep instance 1 20
router bgp 100
  no isolate
Do you want to continue (y/n)? [no] yes
Starting to apply commands...
Applying : interface Ethernet1/1
Applying :   no shutdown
Applying : sleep instance 1 20
Applying : router bgp 100
Applying :   no isolate
Maintenance mode operation successful.
Generating Current Snapshot
Please use 'show snapshots compare before_maintenance after_maintenance' to check the
health of the system
```

次に、FabricPath 用にカスタムのメンテナンス モードおよび通常モード プロファイルを作成する例を示します。

```
switch# configure maintenance profile maintenance-mode
Enter configuration commands, one per line. End with CNTL/Z.
switch(config-mm-profile)# fabricpath domain default
switch(config-mm-profile-fabricpath-isis)# set-overload-bit always
switch(config-mm-profile-fabricpath-isis)# end
Exit maintenance profile mode.
switch#

switch# configure maintenance profile normal-mode
Enter configuration commands, one per line. End with CNTL/Z.
switch(config-mm-profile)# fabricpath domain default
switch(config-mm-profile-fabricpath-isis)# no set-overload-bit always
switch(config-mm-profile-fabricpath-isis)# end
Exit maintenance profile mode.
switch#


switch# show maintenance profile
[Normal Mode]
fabricpath domain default
  no set-overload-bit always
[Maintenance Mode]
fabricpath domain default
  set-overload-bit always
```

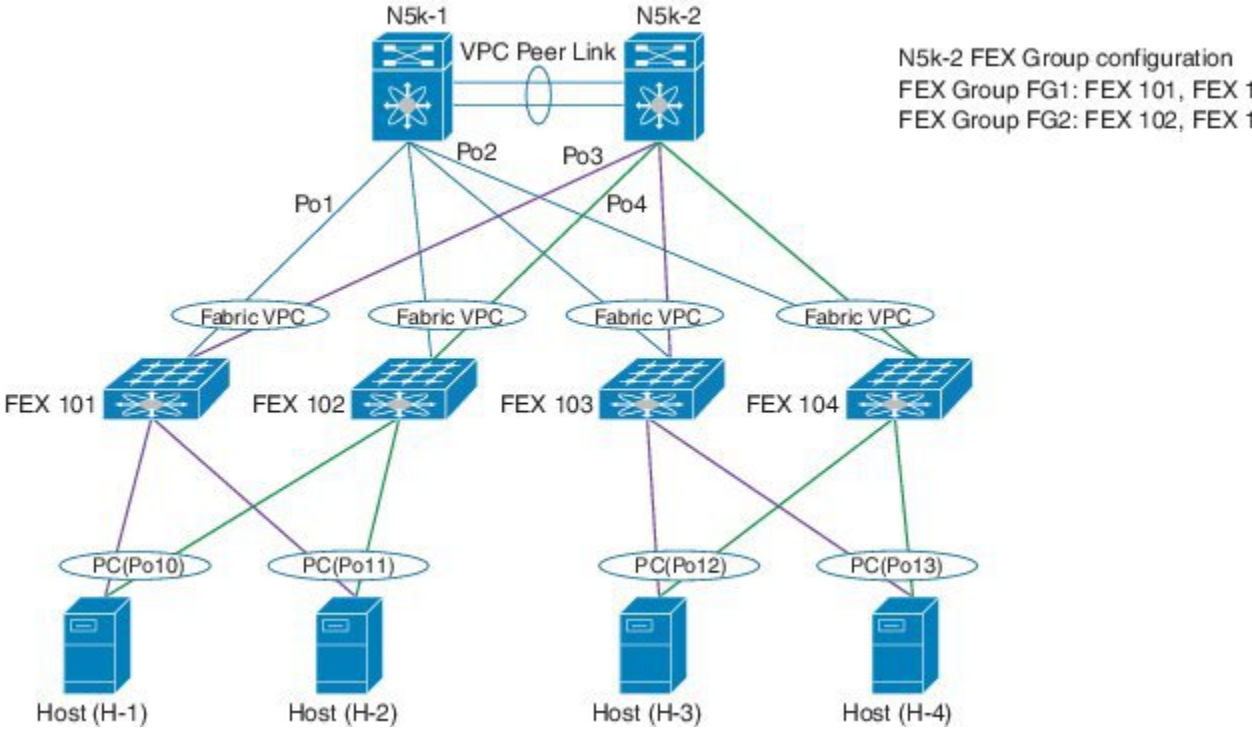
次に、バーチャル ポート チャネル（vPC）用にカスタムのメンテナンス モードおよび通常モード プロファイルを作成する例を示します。

```
switch# configure maintenance profile maintenance-mode
Enter configuration commands, one per line. End with CNTL/Z.
switch(config-mm-profile)# vpc domain 1
switch(config-mm-profile-vpc-domain)# shutdown
switch(config-mm-profile-vpc-domain)# exit
switch(config-mm-profile)# system interface shutdown
switch(config-mm-profile)# end
```

```
Exit maintenance profile mode.
switch#


switch# configure maintenance profile normal-mode
Enter configuration commands, one per line. End with CNTL/Z.
switch(config-mm-profile)# vpc domain 1
switch(config-mm-profile-vpc-domain)# no shutdown
switch(config-mm-profile-vpc-domain)# exit
switch(config-mm-profile)# no system interface shutdown
switch(config-mm-profile)# end
Exit maintenance profile mode.
switch#



switch# show maintenance profile
[Normal Mode]
vpc domain 1
  no shutdown
no system interface shutdown
[Maintenance Mode]
vpc domain 1
  shutdown
system interface shutdown
```

（注） FEX グループを作成するには、**fex-group** *name* コマンドを使用します。FEX グループで FEX を追加または削除するには、**fex** *range* コマンドを使用します。FEX グループをシャットダウンするには、**system fex-group** *name* **shutdown** コマンドを使用します。FEX グループを起動するには、**no system fex-group** *name* **shutdown** コマンドを使用します。

次に、FEX を使用して vPC をアップグレードするためのメンテナンス モード プロファイルおよび通常モード プロファイルを作成する例を示します（以下のトポロジを参照）。



N5K-1 configuration:

```
switch# configure terminal
switch(config)# configure maintenance profile maintenance-mode
switch(config-mm-profile)# vpc domain 1
switch(config-mm-profile-vpc-domain)# shutdown
switch(config-mm-profile)# system interface shutdown
switch# configure terminal
switch(config)# configure maintenance profile normal-mode
switch(config-mm-profile)# no system interface shutdown
switch(config-mm-profile)# vpc domain 1
switch(config-mm-profile-vpc-domain)# no shutdown
```

N5K-2 configuration:

```
switch# configure terminal
switch(config)# configure maintenance profile maintenance-mode
switch(config-mm-profile)# system fex-group fg1 shutdown
switch(config-mm-profile)# sleep 900
switch(config-mm-profile)# system fex-group fg2 shutdown
switch(config-mm-profile)# vpc domain 1
switch(config-mm-profile-vpc-domain)# shutdown
switch(config-mm-profile-vpc-domain)# exit
switch(config-mm-profile)# system interface shutdown

switch# configure terminal
switch(config)# configure maintenance profile normal-mode
switch(config-mm-profile)# no system interface shutdown
switch(config-mm-profile)# vpc domain 1
switch(config-mm-profile-vpc-domain)# no shutdown
switch(config-mm-profile-vpc-domain)#  exit
switch(config-mm-profile)# no system fex-group fg2 shutdown
switch(config-mm-profile)# no system fex-group fg1 shutdown
```

次に、vPC VLAN トラフィックを伝送するポートチャネルまたは通常の L2 イーサネットインターフェイス（vPC ピア リンクを除く）が存在していて、対応するスイッチ仮想インターフェイス

（SVI）の状態がこれらのインターフェイスによって制御されるべきではないときに使用されるコンフィギュレーションを示します。

```
Port-channel configuration
switch(config)# interface port-channel3
switch(config-if)# description "L2-Cross Link eth3/3 eth4/3 eth5/3 eth6/3"
switch(config-if)# switchport
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk allowed vlan 1101-1500
switch(config-if)# spanning-tree port type network
switch(config-if)# lacp min-links 2
switch(config-if)# switchport autostate exclude vlan 1101-1500


L2 Ethernet configuration
switch(config)# interface ethernet 3/3
switch(config-if)# switchport
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk allowed vlan 1101-1500
switch(config-if)# switchport autostate exclude vlan 1101-1500
```

Border Gateway Protocol（BGP）の **isolate** モードは直接ルートを撤回しないため、BGP での redistribute direct コンフィギュレーションはトラフィックを招きます。次に、**route-map** コマンドを使用して BGP が **isolate** モードで直接ルートを撤回できるようにする例を示します。

ポリシー設定

タグ 200 設定を持つ SVI を除外するには、メンテナンス モードで **route-map my-rmap-deny** を使用します。

```
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
```

タグ 200 設定を持つ SVI を含めるには、通常モードで **route-map my-rmap-permit** を使用します。

```
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）設定

```
switch(config)# interface loopback 200
switch(config-if)# ip address 192.0.2.100/8 tag 200
switch(config)# interface vlan 2
switch(config-if)# ip address 192.0.2.108/8 tag 200
....
switch(config)# interface vlan 3
switch(config-if)# ip address 192.0.2.102/8 tag 200
```

BGP の設定

```
switch(config)# feature bgp
switch(config)# router bgp 100
switch(config-router)# neighbor 192.0.2.100
....
```

メンテナンス モード プロファイル

```
switch# configure maintenance profile maintenance-mode
switch(config-mm-profile)# router bgp 200
switch(config-mm-profile-router)# address-family ipv4 unicast
switch(config-mm-profile-router-af)# redistribute direct route-map my-rmap-deny
switch(config-mm-profile-router-af)# exit
```

```
switch(config-mm-profile)# sleep instance 1 10
```

通常モード プロファイル

```
switch# configure maintenance profile normal-mode
switch(config-mm-profile)# router bgp 100
switch(config-mm-profile-router)# address-family ipv4 unicast
switch(config-mm-profile-router-af)# redistribute direct route-map my-rmap-permit
switch(config-mm-profile-router-af)# exit
switch(config-mm-profile)# sleep instance 1 20
```

GIR の確認

設定を確認するには、次のコマンドを使用します。

コマンド	目的
show interface brief	インターフェイスの要約情報を表示します。
show maintenance on-reload reset-reason	スイッチがメンテナンスモードで起動されることになる、リセット理由を表示します。
show maintenance profile [maintenance-mode | normal-mode]	メンテナンスモードまたは通常モードプロファイルの詳細を表示します。
show maintenance timeout	メンテナンスモードのタイムアウト期間を表示します。この期間後、スイッチは自動的に通常モードに戻ります。
show tech-support mmode	シスコのテクニカルサポート向けにメンテナンス モードの情報を表示します。
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*	生成されたスナップショットのさまざまなセクションの内容を表示します。

コマンド	目的
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。このコマンドは、スイッチがメンテナンスモードにあるときにメンテナンスモードのタイマーの現在の状態も表示します。

プロトコル レベルでの GIR の確認

BGP（メンテナンス モード）

メンテナンス モードで BGP のステータスを表示するには、**show bgp process** コマンドを使用します。

```
switch# show bgp process

BGP Process Information
BGP Process ID                  : 11725
BGP Protocol Started, reason:  : configuration
BGP Protocol Tag                : 100
BGP Protocol State          : Running (Isolate)
BGP MMODE                   : Initialized
BGP Memory State                : OK
BGP asformat                    : asplain

BGP attributes information
Number of attribute entries     : 1
HWM of attribute entries        : 1
Bytes used by entries           : 100
Entries pending delete          : 0
HWM of entries pending delete   : 0
BGP paths per attribute HWM     : 3
BGP AS path entries             : 0
Bytes used by AS path entries   : 0
```

プログラムされている BGP IPv4 と IPv6 プレフィックスの数、およびプログラムされていない BGP IPv4 および IPv6 プレフィクスの数を表示するには、**show bgp internal all statistics** コマンドを使用します。

```
BGP internal statistics information for VRF default, address family IPv4 Unicast
  Total prefixes in BGP Table: 3
  Total prefixes pending programming in HW: 0
BGP internal statistics information for VRF default, address family IPv6 Unicast
  Total prefixes in BGP Table: 0
  Total prefixes pending programming in HW: 0
```

EIGRP（メンテナンス モード）

メンテナンス モードで EIGRP のステータスを表示するには、**show ip eigrp** コマンドを使用します。

```
switch# show ip eigrp
IP-EIGRP AS 100 ID 30.1.1.1 VRF default
  Process-tag: 100
```

```
  Instance Number: 1
  Status: running (isolate)
  Authentication mode: none
  Authentication key-chain: none
  Metric weights: K1=1 K2=0 K3=1 K4=0 K5=0
  IP proto: 88 Multicast group: 224.0.0.10
  Int distance: 90 Ext distance: 170
  Max paths: 8
  Number of EIGRP interfaces: 1 (0 loopbacks)
  Number of EIGRP passive interfaces: 0
  Number of EIGRP peers: 1
  Redistributing:
    direct route-map passall
    static route-map passall
  Graceful-Restart: Enabled
  Stub-Routing: Disabled
  NSF converge time limit/expiries: 120/0
  NSF route-hold time limit/expiries: 240/6
  NSF signal time limit/expiries: 20/0
  Redistributed max-prefix: Disabled
  MMODE: Initialized
  Suppress-FIB-Pending Configured
```

ISIS（メンテナンス モード）

メンテナンス モードで ISIS のステータスを表示するには、**show isis protocol** コマンドを使用します。

```
switch# show isis protocol
ISIS process : 100
 Instance number :  1
 UUID: 1090519320
 Process ID 6969
VRF: default
  System ID : 0300.0000.0004  IS-Type : L2
  SAP : 412  Queue Handle : 16
  Maximum LSP MTU: 1492
  Stateful HA enabled
  Graceful Restart enabled. State: Inactive
  Last graceful restart status : none
  Start-Mode Complete
  BFD IPv4 is globally disabled for ISIS process: 100
  BFD IPv6 is globally disabled for ISIS process: 100
  Topology-mode is base
  Metric-style : advertise(wide), accept(narrow, wide)
  Area address(es) :
    10
  Process is up and running (isolate)
  VRF ID: 1
  Stale routes during non-graceful controlled restart
  Interfaces supported by IS-IS :
    Ethernet1/2
```

OSPF（メンテナンス モード）

メンテナンス モードで OSPF のステータスを表示するには、**show ip ospf internal** コマンドを使用します。

```
switch# show ip ospf internal

ospf 100
ospf process tag 100
ospf process instance number 1
ospf process uuid 1090519321
ospf process linux pid 6968
ospf process state running (isolate)
System uptime 6d06h
SUP uptime 2 6d06h
```

```
Server up : L3VM|IFMGR|RPM|AM|CLIS|URIB|U6RIB|IP|IPv6|SNMP|MMODE
Server required  : L3VM|IFMGR|RPM|AM|CLIS|URIB|IP|SNMP
Server registered: L3VM|IFMGR|RPM|AM|CLIS|URIB|IP|SNMP|MMODE
Server optional  : MMODE

Early hello : OFF
Force write PSS: FALSE
OSPF mts pkt sap 324
OSPF mts base sap 320
```

GIR の機能の履歴

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

機能名	リリース	情報
グレースフル挿入と削除（GIR）	7.3(0)N1(1)	GIR のデフォルト モードは isolate です。計画外のメンテナンス、メンテナンス モードのタイマー、FIB 保留の抑制、スナップショットへの show コマンドの追加、スナップショット セクションのダンプなどをサポートします。
グレースフル挿入と削除（GIR）	7.1(0)N1(1)	この機能が導入されました。GIR のデフォルト モードは shutdown です。「GIR の設定（Cisco NX-OS Release 7.1(0)N1(1)）」を参照してください。

第 23 章

GIRの設定（Cisco NX-OS Release 7.1(0)N1(1)）

この章の内容は、次のとおりです。

- GIR について，343 ページ
- GIR の注意事項および制約事項，344 ページ
- GIR サイクルの実行，344 ページ
- 通常モード プロファイル ファイルの設定，345 ページ
- スナップショットの作成，346 ページ
- メンテナンス モードの開始，347 ページ
- 通常モードへの復帰，348 ページ
- メンテナンス モード プロファイル ファイルの設定，348 ページ
- GIR の確認，350 ページ

GIR について

グレースフル挿入と削除（GIR）を使用して、デバッグやアップグレードを実行するためにスイッチをネットワークから分離できます。スイッチのメンテナンスが完了したら、スイッチを通常モードに戻すことができます。

スイッチがメンテナンス モードになると、すべてのプロトコルは正常に停止し、すべての物理ポートがシャットダウンします。通常モードに復元されると、すべてのプロトコルとポートが復帰します。

次のプロトコルがサポートされています。

- Border Gateway Protocol（BGP）
- BGPv6
- Enhanced Interior Gateway Routing Protocol（EIGRP）

- EIGRPv6
- Intermediate System-to-Intermediate System（ISIS）
- Open Shortest Path First（OSPF）
- OSPFv3

また、次のものもサポートされます。

- バーチャル ポート チャネル（vPC）
- インターフェイス
- FabricPath

スイッチをメンテナンス モードにする前に自分でメンテナンス モード プロファイル ファイルを作成することも、**[no] system mode maintenance** コマンドを入力するときにシステムによってメンテナンス モード プロファイル ファイルを作成することもできます。

選択した機能の実行中状態をキャプチャしたり、永続ストレージ メディアに保存したりするには、**snapshot** コマンドを使用します。

スナップショットは、スイッチをメンテナンス モードにする前の状態と通常モードに復帰した後の状態を比較するのに便利です。スナップショット プロセスは、次の 3 つの部分で構成されます。

- 事前に選択したスイッチの一部機能の状態のスナップショットを作成し、永続ストレージメディアに保存する。
- さまざまな時間間隔で取得したスナップショットを一覧にして、管理する。
- スナップショットを比較して、各機能の概要と詳細を表示する。

GIR の注意事項および制約事項

グレースフル挿入と削除（GIR）には、次の注意事項と制約事項があります。

- メンテナンス モードまたは通常モードのプロファイル ファイルを作成するには、それぞれ **config profile maintenance-mode type admin** および **config profile normal-mode type admin** コマンドを使用します。

GIR サイクルの実行

手順

ステップ 1 （任意） メンテナンス モード プロファイル ファイルを作成します。
メンテナンス モード プロファイル ファイルの設定, （348 ページ）を参照してください。

ステップ 2　（任意） 通常モード プロファイル ファイルを作成します。
通常モード プロファイル ファイルの設定，（345 ページ）を参照してください。

ステップ 3　メンテナンス モードを開始する前にスナップショットを作成します。
スナップショットの作成，（346 ページ）を参照してください。

ステップ 4　スイッチをメンテナンス モードにします。
メンテナンス モードの開始，（347 ページ） を参照してください。

ステップ 5　（任意） **copy running-config startup-config** コマンドを入力します。

ステップ 6　スイッチを通常モードに戻します。
通常モードへの復帰，（348 ページ）を参照してください。

ステップ 7　通常モードに戻った後で、スナップショットを作成します。
スナップショットの作成，（346 ページ）を参照してください。

通常モード プロファイル ファイルの設定

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **configure profile normal-mode type admin**	通常モードプロファイルファイルのコンフィギュレーション セッションを開始します。 （注） 設定しているプロトコルに応じて、プロトコルを起動する適切なコマンドを入力する必要があります。
ステップ 3	switch# **end**	通常モード プロファイル ファイルを閉じます。

次に、通常モード プロファイル ファイルを作成する例を示します。

```
switch# configure terminal
switch(config)# configure profile normal-mode type admin
switch(config-profile)# router ospf 100
switch(config-profile-router)# no shutdown
switch(config-profile-router)# exit
switch(config-profile)# router eigrp 101
switch(config-profile-router)# no shutdown
switch(config-profile-router)# exit
switch(config-profile)# router isis 102
switch(config-profile-router)# no shutdown
switch(config-profile-router)# no set-overload-bit always
switch(config-profile-router)# exit
```

```
switch(config-profile)# router bgp 103
switch(config-profile-router)# no shutdown
switch(config-profile-router)# exit
switch(config-profile)# vpc domain 20
switch(config-profile-router)# no shutdown
switch(config-profile-router)# exit
switch(config-profile)# no system interface shutdown
switch(config-profile)# end
Exit configure profile mode.
switch#
```

次に、通常モードのカスタム プロファイル ファイルを作成する例を示します。

```
switch# configure terminal
switch(config)# configure profile normal-mode type admin
switch(config-profile)# router bgp 65501
switch(config-profile-router)# no shutdown
switch(config-profile-router)# exit
switch(config-profile)# router eigrp 100
switch(config-profile-router)# no shutdown
switch(config-profile-router)# exit
switch(config-profile)# address-family ipv6 unicast
switch(config-profile)# no shutdown
switch(config-profile)# router eigrp 600
switch(config-profile-router)# no shutdown
switch(config-profile-router)# exit
switch(config-profile)# address-family ipv6 unicast
switch(config-profile-router)# no shutdown
switch(config-profile-router)# exit
switch(config-profile)# router ospf 100
switch(config-profile-router)# no shutdown
switch(config-profile-router)# exit
switch(config-profile)# router ospfv3 ospf_ipv6
switch(config-profile-router)# no shutdown
switch(config-profile-router)# exit
switch(config-profile)# router isis isp
switch(config-profile-router)# no set-overload-bit always
switch(config-profile-router)# exit
switch(config-profile)# vpc domain 2
switch(config-profile-router)# no shutdown
switch(config-profile-router)# exit
switch(config-profile)# no system interface shutdown
switch(config-profile)# end
Exit configure profile mode.
switch#
```

スナップショットの作成

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **snapshot create***namedescription*	スナップショットを作成します。*name* 変数は最大 64 文字です。*description* 変数は最大 256 文字です。

次に、スナップショットを作成する例を示します。

```
switch# snapshot create snap1 For documentation purposes.
Executing show interface... Done
```

```
Executing show bgp sessions vrf all... Done
Executing show ip eigrp topology summary... Done
Executing show ipv6 eigrp topology summary... Done
Executing show vpc... Done
Executing show ip ospf vrf all... Done
Feature 'ospfv3' not enabled, skipping...
Executing show isis vrf all... Done
Snapshot 'snap1' created
switch#
```

メンテナンス モードの開始

はじめる前に

system mode maintenance コマンドを使用する代わりにカスタムのプロファイルを作成する場合は、メンテナンス モード プロファイル ファイルの設定，（348 ページ）を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **system mode maintenance** [**dont-generate-profile**]	以前に作成したメンテナンス モード プロファイル ファイルを実行するか、またはメンテナンスモードプロファイル ファイルを動的に作成します。**dont-generate-profile** オプションは、メンテナンス モード プロファイル ファイルの作成を抑制します。 （注） 続行を促すプロンプトが表示されます。続行する場合は y、プロセスを終了する場合は n を入力します。

スイッチはメンテナンス モードになります。

（注） メンテナンス モードでは、In-Service Software Downgrade（ISSD）を実行できません。

次に、以前作成したメンテナンス モード プロファイル ファイルを使用してスイッチをメンテナンス モードにする例を示します。

```
switch# configure terminal
switch(config)# system mode maintenance dont-generate-profile
Do you want to continue (y/n)? [n] y

Progressing.............................................Done.

System mode operation completed successfully
switch(config)#
```

通常モードへの復帰

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **no system mode maintenance** [**dont-generate-profile**]	以前に作成した通常モード プロファイル ファイル、または動的に作成した通常モード プロファイル ファイルを実行します。**dont-generate-profile** オプションは、通常モード プロファイル ファイルの作成を抑制します。 （注） 続行を促すプロンプトが表示されます。続行する場合は y、プロセスを終了する場合は n を入力します。 スイッチは通常モードになります。

次に、メンテナンス モードから通常モードに戻る例を示します。

```
switch# configure terminal
switch(config)# no system mode maintenance dont-generate-profile
Do you want to continue (y/n)? [n] y

Progressing................Done.

System mode operation completed successfully

switch(config)#
```

メンテナンス モード プロファイル ファイルの設定

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバルコンフィギュレーションモードを開始します。
ステップ 2	switch(config)# **configure profile maintenance-mode type admin**	メンテナンス モード プロファイル ファイルのコンフィギュレーション セッションを開始します。 （注） 設定しているプロトコルに応じて、プロトコルを停止する適切なコマンドを入力する必要があります。

	コマンドまたはアクション	目的
ステップ 3	switch# **end**	メンテナンス モード プロファイル ファイルを閉じます。

次に、メンテナンス モード プロファイル ファイルを作成する例を示します。

```
switch# configure terminal
switch(config)# configure profile maintenance-mode type admin
switch(config-profile)# router ospf 100
switch(config-profile-router)# shutdown
switch(config-profile-router)# exit
switch(config-profile)# router eigrp 101
switch(config-profile-router)# shutdown
switch(config-profile-router)# exit
switch(config-profile)# router isis 102
switch(config-profile-router)# shutdown
switch(config-profile-router)# set-overload-bit always
switch(config-profile-router)# exit
switch(config-profile)# router bgp 103
switch(config-profile-router)# shutdown
switch(config-profile-router)# exit
switch(config-profile)# vpc domain 20
switch(config-profile-router)# shutdown
switch(config-profile-router)# exit
switch(config-profile)# system interface shutdown
switch(config-profile)# end
Exit configure profile mode.
switch#
```

次に、メンテナンス モードのカスタム プロファイル ファイルを作成する例を示します。

```
switch# configure terminal
switch(config)# configure profile maintenance-mode type admin
switch(config-profile)# router bgp 65501
switch(config-profile-router)# shutdown
switch(config-profile-router)# exit
switch(config-profile)# address-family ipv6 unicast
switch(config-profile)# shutdown
switch(config-profile)# router eigrp 600
switch(config-profile-router)# shutdown
switch(config-profile-router)# exit
switch(config-profile)# address-family ipv6 unicast
switch(config-profile-router)# shutdown
switch(config-profile-router)# exit
switch(config-profile)# router ospf 100
switch(config-profile-router)# shutdown
switch(config-profile-router)# exit
switch(config-profile)# router ospfv3 ospf_ipv6
switch(config-profile-router)# shutdown
switch(config-profile-router)# exit
switch(config-profile)# router isis isp
switch(config-profile-router)# set-overload-bit always
switch(config-profile-router)# exit
switch(config-profile)# vpc domain 2
switch(config-profile-router)# shutdown
switch(config-profile-router)# exit
switch(config-profile)# system interface shutdown
switch(config-profile)# end
Exit configure profile mode.
switch#
```

次に、IPv6プロトコル用にメンテナンスモードプロファイルファイルを作成する例を示します。

```
switch# configure terminal
switch(config)# configure profile maintenance-mode type admin
switch(config-profile)# router ospfv3 ospf_ipv6
switch(config-profile-router)# shutdown
switch(config-profile-router)# exit
switch(config-profile)# router eigrp 660
switch(config-profile-router)# address-family ipv6 unicast
switch(config-profile-router-af)# shutdown
switch(config-profile-router-af)# exit
switch(config-profile-router)# router isis isp
switch(config-profile-router)# set-overload-bit always
switch(config-profile-router)# exit
switch(config-profile)# router bgp 655551
switch(config-profile)# address-family ipv6 unicast
switch(config-profile-router)# shutdown
switch(config-profile-router)# exit
switch(config-profile)#
```

GIR の確認

次のいずれかのコマンドを使用して、設定を確認します。

コマンド	目的
show system mode	現在のシステム モードを表示します。
show interface brief	インターフェイスの要約情報を表示します。
show snapshots*before-maintenance-mode description*	スイッチ上に存在するスナップショットを表示します。
show config-profile*name*	設定プロファイル ファイルの詳細を表示します。

show system mode コマンド

```
switch# show system mode
System Mode : Maintenance
```

show interface brief コマンド

```
switch# show interface brief

--------------------------------------------------------------------------------
Ehternet       VLAN     Type Mode   Status  Reason                Speed   Port
Interface                                                                  Ch #
--------------------------------------------------------------------------------
Eth1/1         - -      eth  routed  down    sysIntfShut           10G(D) - -
Eth1/2         - -      eth  routed  down    sysIntfShut           10G(D) - -
Eth1/3         - -      eth  routed  down    sysIntfShut           10G(D) - -
Eth1/4         - -      eth  routed  down    sysIntfShut           10G(D) - -
Eth1/5         - -      eth  routed  down    sysIntfShut           10G(D) - -
Eth1/6         - -      eth  routed  down    sysIntfShut           10G(D) - -
Eth1/7         - -      eth  routed  down    SFP not inserted      10G(D) - -
Eth1/8         - -      eth  routed  down    SFP not inserted      10G(D) - -
```

```
Eth1/9          - -      eth  routed  down   SFP not inserted      10G(D) - -
Eth1/10         - -      eth  routed  down   SFP not inserted      10G(D) - -
Eth1/12         - -      eth  routed  down   SFP not inserted      10G(D) - -
Eth1/13         - -      eth  routed  down   SFP not inserted      10G(D) - -
Eth1/14         - -      eth  routed  down   SFP not inserted      10G(D) - -
Eth1/15         - -      eth  routed  down   SFP not inserted      10G(D) - -
Eth1/16         - -      eth  routed  down   SFP not inserted      10G(D) - -

--------------------------------------------------------------------------------
Port-channel  VLAN    Type Mode    Status  Reason                   Speed   Protocol
Interface
--------------------------------------------------------------------------------
Po1           1       eth  access  down    No operational members   auto(I)  none
Po100         1       eth  access  down    No operational members   auto(I)  none

--------------------------------------------------------------------------------
Port     VRF         Status IP Address                              Speed    MTU
--------------------------------------------------------------------------------
mgmt0    - -         up     192.0.0.1                               1000     1500
switch#
```

show snapshots コマンド

```
switch# show snapshots
Snapshot Name
-----------------------------------------------------------------------------------------
snapshot_before_maintenance      Wed Sep 10 20:19:31 2014      system-internal-snapshot
snapshot_after_maintenance       Wed Sep 10 20:29:54 2014      system-internal-snapshot
snap1                            Wed Sep 10 20:36:15 2014      For testing
```

show config-profile コマンド

```
switch# show config-profile

config-profile maintenance-mode type admin
  router ospf 100
   shutdown
  router eigrp 101
   shutdown
  router isis 102
   set-overload-bit always
  router bgp 103
   shutdown
  vpc domain 20
   shutdown
  system interface shutdown exclude fex-fabric

config-profile normal-mode type admin
  router ospf 100
   no shutdown
  router eigrp 101
   no shutdown
  router isis 102
   no set-overload-bit always
  router bgp 103
   no shutdown
  vpc domain 20
   no shutdown
  no system interface shutdown
```

第 24 章

クラスベース QoS MIB

この章の内容は、次のとおりです。

- クラスベース QoS MIB，353 ページ

クラスベース QoS MIB

クラスベース QoS MIB（cbQoSMIB）機能は、クラスマップとポリシーマップの設定と統計情報の取得を可能にする Simple Network Management Protocol（SNMP）MIB を提供します。

クラスベース QoS MIB について

CoPP と QoS ポリシーは、クラスベース QoS MIB（cbQoSMIB）をサポートしました。cbQoSMIB はモジュラ QoS CLI（MQC）の設定と統計情報へのアクセスを提供する SNMP MIB です。

次の cbQoSMIB テーブルは、QoS ポリシーと CoPP によってサポートされます。

- cbQosClassMapCfg
- cbQosMatchStmtCfg
- cbQosPoliceStats
- cbQosPolicyMapCfg
- cbQosPoliceCfg

次の cbQoSMIB テーブルは、QoS ポリシーによってサポートされます。

- cbQosInterfacePolicy
- cbQosObjects
- cbQosQueueingCfg
- cbQosServicePolicy
- cbQosSetCfg

cbQoSMIB のテーブルと要素の詳細は、次の URL で入手できます。http://tools.cisco.com/Support/SNMP/do/BrowseOID.do?local=en&translate=Translate&objectInput=1.3.6.1.4.1.9.9.166

クラスベース QoS MIB のライセンス要件

この機能には、ライセンスは必要ありません。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。NX-OS ライセンス方式の詳細については、『Cisco NX-OS Licensing Guide』を参照してください。

QoS ポリシーの設定

次の設定は、QoS ポリシーを設定する一般的な例です。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config) # **snmp-server community** *com-name* **rw**	SNMPv1 または SNMPv2c 用に Simple Network Management Protocol（SNMP）のコミュニティを作成します。
ステップ 3	switch(config) # **snmp-server community** *com-name* **rw**	SNMPv1 または SNMPv2c 用に Simple Network Management Protocol（SNMP）のコミュニティを作成します。
ステップ 4	switch(config) # **class-map type qos match-all** *class-map-name*	クラス マップのコンポーネント タイプ qos を指定し、クラスマップ タイプ qos 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	switch(config-cmap-qos) # **description** *text*	クラスマップの記述を追加します。
ステップ 6	switch(config-cmap-qos) # **match cos** *cos-list*	タイプ qos クラス マップのサービス クラス（CoS）値を使用してトラフィックのクラスを定義します。
ステップ 7	switch(config-cmap-qos) # **exit**	クラスマップ タイプ qos コンフィギュレーション モードを終了します。
ステップ 8	switch(config) # **policy-map type qos** *qos-policy-map-name*	タイプ qos ポリシーマップを指定し、ポリシーマップ qos 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 9	switch(config-pmap-qos) # **description** *text*	ポリシーマップの記述を設定します。
ステップ 10	switch(config-pmap-qos) # **class** *class-map-name*	クラスマップのサービス ポリシーを設定します。
ステップ 11	switch(config-pmap-c-qos) # **set qos-group** *qos-group-value*	次に、タイプ qos ポリシーマップのトラフィックのクラスに QoS グループ ID を割り当てます。
ステップ 12	switch(config-pmap-c-qos) # **exit**	ポリシーマップ タイプ qos クラス コンフィギュレーション モードを終了します。
ステップ 13	switch(config-pmap-qos) # **exit**	ポリシーマップ qos コンフィギュレーション モードを終了します。
ステップ 14	switch(config) # **interface** *type number*	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 15	switch(config-if) # **service-policy type qos input** *policy-map-name*	サービスポリシーマップを前述のインターフェイスに着信するパケットに適用します。
ステップ 16	switch(config-if) # **exit**	インターフェイスコンフィギュレーションモードを終了します。
ステップ 17	switch(config) # **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。

次に、スイッチで QoS ポリシーを設定する例を示します。

（注） これは、QoS ポリシーを設定する一般的な例です。

```
switch# configure terminal
switch(config)# snmp-server community public rw
switch(config)# snmp-server community private rw
switch(config)# class-map type qos match-all cmcos
switch(config-cmap-qos) # description qos cmap to match cos
switch(config-cmap-qos) # match cos 5
switch(config) # policy-map type qos p1
switch(config-pmap-qos) # description qos pmap1
switch(config-pmap-qos) # class cmcos
switch(config-pmap-c-qos) # set qos-group 3
switch(config-pmap-c-qos) # exit
switch(config-pmap-qos) # exit
switch(config) # interface ethernet 1/1
switch(config-if) # service-policy type qos input p1
```

クラスベース QoS MIB の設定と統計情報の表示

手順

	コマンドまたはアクション	目的
ステップ 1	$ **snmpwalk -v2c -c** *ip-address oid*	クラスマップおよびポリシーマップの設定と統計情報を表示します。 （注） SNMP 対応サーバで **snmpwalk** コマンドを使用します。

次に、クラス マップおよびポリシー マップの設定と統計情報を表示する例を示します。

（注） 次の出力例は、上記の設定に対応します。デフォルトですべての CoPP 設定を使用できます。

```
$ snmpwalk -v2c -c public 10.193.53.92 1.3.6.1.4.1.9.9.166.1

Interface Policy Table (QoS only table) - corresponding to the service policy applied on
eth1/1

CISCO-CLASS-BASED-QOS-MIB::cbQosIfType.285212673 = INTEGER: mainInterface(1)
CISCO-CLASS-BASED-QOS-MIB::cbQosPolicyDirection.285212673 = INTEGER: input(1)
CISCO-CLASS-BASED-QOS-MIB::cbQosIfIndex.285212673 = INTEGER: 436207616
CISCO-CLASS-BASED-QOS-MIB::cbQosVlanIndex.285212673 = Gauge32: 1

Service Policy Table (QoS only table) - corresponding to the service policy applied on
eth1/1

CISCO-CLASS-BASED-QOS-MIB::cbQosIFPolicyIndex.436207616.input = Gauge32: 285212673

Objects Table (QoS only table) corresponding to the policy-map, class-map, match & set
Statements

CISCO-CLASS-BASED-QOS-MIB::cbQosConfigIndex.285212673.285212673 = Gauge32: 285212823
CISCO-CLASS-BASED-QOS-MIB::cbQosConfigIndex.285212673.285212674 = Gauge32: 285212821
CISCO-CLASS-BASED-QOS-MIB::cbQosConfigIndex.285212673.285212675 = Gauge32: 285212822
CISCO-CLASS-BASED-QOS-MIB::cbQosConfigIndex.285212673.285212676 = Gauge32: 285212825

CISCO-CLASS-BASED-QOS-MIB::cbQosObjectsType.285212673.285212673 = INTEGER: policymap(1)
CISCO-CLASS-BASED-QOS-MIB::cbQosObjectsType.285212673.285212674 = INTEGER: classmap(2)
CISCO-CLASS-BASED-QOS-MIB::cbQosObjectsType.285212673.285212675 = INTEGER: matchStatement(3)
CISCO-CLASS-BASED-QOS-MIB::cbQosObjectsType.285212673.285212676 = INTEGER: set(8)

CISCO-CLASS-BASED-QOS-MIB::cbQosParentObjectsIndex.285212673.285212673 = Gauge32: 0
CISCO-CLASS-BASED-QOS-MIB::cbQosParentObjectsIndex.285212673.285212674 = Gauge32: 285212673
CISCO-CLASS-BASED-QOS-MIB::cbQosParentObjectsIndex.285212673.285212675 = Gauge32: 285212674
CISCO-CLASS-BASED-QOS-MIB::cbQosParentObjectsIndex.285212673.285212676 = Gauge32: 285212674

Policy Map Table corresponding to the policy-map configured above & the default CoPP
policy-map

CISCO-CLASS-BASED-QOS-MIB::cbQosPolicyMapName.285212823 = STRING: p1
CISCO-CLASS-BASED-QOS-MIB::cbQosPolicyMapName.721420364 = STRING: copp-system-policy-default
CISCO-CLASS-BASED-QOS-MIB::cbQosPolicyMapDesc.285212823 = STRING: qos pmap 1
CISCO-CLASS-BASED-QOS-MIB::cbQosPolicyMapDesc.721420364 = STRING: Control Plane Service
Policy

Class Map Table corresponding to the class-map configured above & one default CoPP class-map
```

```
CISCO-CLASS-BASED-QOS-MIB::cbQosCMName.285212821 = STRING: cmcos
CISCO-CLASS-BASED-QOS-MIB::cbQosCMName.721420290 = STRING: copp-system-class-igmp
CISCO-CLASS-BASED-QOS-MIB::cbQosCMDesc.285212821 = STRING: qos cmap to Match cos
CISCO-CLASS-BASED-QOS-MIB::cbQosCMDesc.721420290 = STRING: copp-system-class-igmp
CISCO-CLASS-BASED-QOS-MIB::cbQosCMInfo.285212821 = INTEGER: matchAll(2)
CISCO-CLASS-BASED-QOS-MIB::cbQosCMInfo.721420290 = INTEGER: matchAny(3)

Match Stmt Table corresponding to the match statement configured above & one match statement
from default CoPP configuration

CISCO-CLASS-BASED-QOS-MIB::cbQosMatchStmtName.285212822 = STRING: match cos 5
CISCO-CLASS-BASED-QOS-MIB::cbQosMatchStmtName.721420291 = STRING: protocol IGMP
CISCO-CLASS-BASED-QOS-MIB::cbQosMatchStmtInfo.285212822 = INTEGER: none(1)
CISCO-CLASS-BASED-QOS-MIB::cbQosMatchStmtInfo.721420291 = INTEGER: none(1)

Queueing Config Table(QoS only table, taken from default QoS policies)

CISCO-CLASS-BASED-QOS-MIB::cbQosQueueingCfgBandwidth.301990019 = INTEGER: 100
CISCO-CLASS-BASED-QOS-MIB::cbQosQueueingCfgBandwidthUnits.301990019 = INTEGER: percentage(2)
CISCO-CLASS-BASED-QOS-MIB::cbQosQueueingCfgPriorityEnabled.301990019 = INTEGER: false(2)
CISCO-CLASS-BASED-QOS-MIB::cbQosQueueingCfgQLimitUnits.301990019 = INTEGER: 0
CISCO-CLASS-BASED-QOS-MIB::cbQosQueueingCfgAggregateQLimit.301990019 = Gauge32: 0

Set Action Table (QoS only table) corresponding to the set statement configured above

CISCO-CLASS-BASED-QOS-MIB::cbQosSetCfgQosGroupValue.285212825 = INTEGER: 3

Policing Config Table(no QoS config, displays only CoPP statistics)

CISCO-CLASS-BASED-QOS-MIB::cbQosPoliceCfgBurstSize.721420365 = Gauge32: 65535 Octets
CISCO-CLASS-BASED-QOS-MIB::cbQosPoliceCfgConformAction.721420365 = INTEGER: transmit(1)
CISCO-CLASS-BASED-QOS-MIB::cbQosPoliceCfgViolateAction.721420365 = INTEGER: drop(5)
CISCO-CLASS-BASED-QOS-MIB::cbQosPoliceCfgRate64.721420365 = Counter64: 1048576 bits/second
CISCO-CLASS-BASED-QOS-MIB::cbQosPoliceCfgRateType.721420365 = INTEGER: bps(1)
CISCO-CLASS-BASED-QOS-MIB::cbQosPoliceCfgConditional.721420365 = INTEGER: false(2)

Policing Stats Table(no QoS config, displays only CoPP statistics)

CISCO-CLASS-BASED-QOS-MIB::cbQosPoliceConformedByte64.721420364.721420365 = Counter64: 1144
Octets
CISCO-CLASS-BASED-QOS-MIB::cbQosPoliceViolatedByte64.721420364.721420365 = Counter64: 0
Octets
```

クラスベース QoS MIB のその他の参考資料

ここでは、クラスベース QoS MIB に関連するその他の情報について説明します。

関連資料

関連項目	マニュアル タイトル
ライセンス	『Cisco NX-OS Licensing Guide』
コマンド リファレンス	『Cisco Nexus 5000 Series NX-OS QoS Command Reference』 『Cisco Nexus 5000 Series NX-OS System Management Command Reference』

クラスベース QoS MIB の機能の履歴

表 *33* : クラスベース *QoS MIB* の機能の履歴

機能名	リリース	機能情報
クラスベース QoS MIB	7.1(1) N1(1)	この機能が導入されました。

索 引

A

ACL 200, 221
　ERSPAN 221
　SPAN 200
ACL のロギング 125
　インターフェイスへの適用 125
ACL フィルタリング 209
　SPAN 209
ACL ロギング キャッシュ 124
　設定 124
ACL ログ 126
　一致レベル 126

C

cache 124
　ロギング 124
　　設定 124
Call Home の通知 153
　syslog の XML 形式 153
　syslog のフル テキスト形式 153
CFS 44, 50, 58, 64, 65, 67
　NTP コンフィギュレーションの配信 64
　RADIUS コンフィギュレーションの配信 65
　Smart Call Home コンフィギュレーションの配信 58
　TACACS+ コンフィギュレーションの配信 67
　ユーザ ロール コンフィギュレーションの配信 67
　ロック済みセッションのクリア 50
　制限事項 44
　注意事項 44
collect パラメータ 299
　Netflow 299

E

ERSPAN 217, 218, 219, 220, 221, 222, 226, 229, 232, 233, 236, 237, 242, 243, 244
　ACL 221, 243
　　設定例 243
　destination 243
　　設定例 243
　ERSPAN SPAN-on-Drop セッション 236
　source 242
　　設定例 242
　sources 219
　SPAN-on-drop 221
　SPAN-on-Drop 244
　　設定例 244
　SPAN-on-Latency 221, 237, 244
　　設定例 244
　truncated 220, 232, 243
　　設定例 243
　タイプ 219
　デフォルト パラメータ 226
　ハイ アベイラビリティ 221
　モニタ対象トラフィック 218
　ライセンス要件 221
　宛先 220
　宛先セッション 233
　　ERSPAN の設定 233
　宛先セッションの設定 233
　概要 217
　関連資料 244
　前提条件 222
　送信元セッション 226, 229
　　ERSPAN の設定 226, 229
　送信元セッションの設定 226, 229
ERSPAN セッション 242
　設定例 242

F

flow record 296
Netflow 296

G

GOLD 診断 101, 102, 103
runtime 101
ヘルス モニタリング 102
拡張モジュール 103
設定 103

I

ID 134
シリアル ID 134

L

linkDown 通知 186
linkUp 通知 186

M

mgmt0 インターフェイス 125
ACL のロギング 125

N

Netflow 295, 296, 297, 299
collect パラメータ 299
flow record 296
照合キー 297
説明 295
定義 295
NetFlow 296, 297, 299, 300, 302, 303, 305, 306, 307, 308, 309
collect パラメータ 299
match パラメータ 297
sampler 300
timeouts 309
VLAN でのブリッジ 308
フロー エクスポータ 296
フロー エクスポータの作成 303
フロー サンプラーの作成 306
NetFlow *(続き)*
フロー モニタ インターフェイス 307
フロー モニタの作成 305
フロー レコードの作成 302
注意事項と制約事項 300
NTP コンフィギュレーション 64
CFS を使用して配信 64

O

OpenFlow 286, 287, 288, 290, 291, 293
イネーブル化 290
サポートされないインターフェイス タイプ 286
サポートされる match フィールド 287
サポートされるアクション 287
サポートされるインターフェイス タイプ 286
サポートされるインターフェイス モード 286
スイッチの設定 291
仮想サービス 290
確認 293
制限事項 286
前提条件 288

P

PTP 69, 70, 71, 72, 73, 75
process 71
インターフェイス、設定 75
グローバル設定 73
クロック管理 71
NTP 71
デバイス タイプ 70
デフォルト設定 73
概要 69
注意事項と制約事項 72

R

RADIUS コンフィギュレーション 65
CFS を使用して配信 65
RBAC 79, 80, 81, 84, 86, 88, 90, 92, 93
ユーザ アカウント、設定 86
ユーザ アカウントの制限事項 84
ユーザ ロール 79
ユーザ ロール VLAN ポリシー、変更 92
ユーザ ロール VSAN ポリシー、変更 92

RBAC *(続き)*
ユーザ ロールおよびルール、設定 88
ルール 81
確認 93
機能グループ、作成 90
registering 141, 276
smart call home 141
VSH スクリプト ポリシー 276

S

sampler 300
NetFlow 300
SAN 管理者、ユーザ ロール 80
SAN 管理者ユーザ、設定 87
RBAC 87
Session Manager 95, 96, 97, 98
ACL セッションの設定例 98
セッションのコミット 97
セッションの確認 97
セッションの廃棄 98
セッションの保存 98
制限事項 96
設定の確認 98
説明 95
注意事項 96
show コマンドの追加、アラート グループ 147
smart call home 147
smart call home 129, 130, 131, 139, 140, 141, 143, 144, 146, 147, 148, 149, 150, 151, 152
registering 141
show コマンドの追加、アラート グループ 147
アラート グループ 131
アラート グループのアソシエート 146
デフォルト設定 140
メッセージ フォーマット オプション 130
宛先プロファイル 130
宛先プロファイル、作成 143
宛先プロファイル、変更 144
確認 152
重複メッセージ抑制、ディセーブル化 150, 151
設定のテスト 151
説明 129
前提条件 140
担当者情報、設定 141
注意事項と制約事項 139
定期的なインベントリ通知 149
電子メールの詳細、設定 148
Smart Call Home コンフィギュレーション 58
CFS を使用して配信 58
Smart Call Home のメッセージ 130, 133
フォーマット オプション 130
レベルの設定 133
SNMP 169, 170, 172, 173, 174, 175, 176, 177, 180, 181, 182, 189
CLI を使用したユーザの同期 173
アクセス グループ 174
インバンド アクセス 182
グループ ベースのアクセス 174
セキュリティ モデル 172
ディセーブル化 189
デフォルト設定 174
トラップ通知 170
バージョン 3 のセキュリティ機能 170
メッセージの暗号化 176
ユーザ ベースのセキュリティ 172
SNMP 172
ユーザの設定 175
ライセンス 174
機能の概要 169
注意事項と制約事項 174
通知レシーバ 177
発信元インターフェイス 180, 181
要求のフィルタリング 177
SNMP notifications 179
VRF に基づくフィルタリング 179
SNMP のデフォルト設定 174
SNMP 通知レシーバ 179
VRF による設定 179
SNMP 要求のフィルタリング 177
SNMP（簡易ネットワーク管理プロトコル） 171
バージョン 171
SNMPv3 170, 176
セキュリティ機能 170
複数のロールの割り当て 176
SPAN 198, 199, 200, 204, 205, 207, 208, 209, 210, 211, 213, 215, 216
ACL 200, 216
設定例 216
ACL フィルタリング 209
SPAN-on-drop 200
SPAN-on-Drop セッション 210
SPAN-on-Latency 200, 211, 216
設定例 216
イーサネット宛先ポート、設定 205
セッションのアクティブ化 213
モニタリングの送信元 198
宛先 199

SPAN *(続き)*
宛先ポート、特性 199
作成、セッションの削除 204
出力送信元 198
情報の表示 215
説明、設定 208
送信元ポート、設定 207
特性、送信元ポート 198
入力送信元 198
複数の宛先 200
SPAN 送信元 198
ingress 198
出力 198
SPAN-on-drop 200, 221
ERSPAN 221
SPAN 200
SPAN-on-Latency 200, 221
ERSPAN 221
SPAN 200
syslog 116, 126
ACL ログの一致レベル 126
設定 116

T

TACACS+ コンフィギュレーション 67
CFS を使用して配信 67

U

users 79
説明 79

V

VRF 179
SNMP 通知のフィルタリング 179
SNMP 通知レシーバの設定 179
VSH スクリプト ポリシー 267

あ

アクション文の設定 274
アクティブ化 276
VSH スクリプト ポリシー 276
アラート グループ 131
smart call home 131
アラート グループのアソシエート 146
smart call home 146

い

イーサネット宛先ポート、設定 205
SPAN 205
イネーブル化 249, 257, 290
NTP 249
NTP 用 CFS 配信 257
OpenFlow 290
イベント文の設定 272
インターフェイス、設定 75
PTP 75

く

クリア 50, 128
ACL ログ 128
ロック済みセッション 50
クロック管理 71
PTP 71

こ

コミット 257
NTP 設定変更 257

さ

サーバ ID 134
説明 134

し

システム メッセージ ロギングの設定 109
デフォルト 109
システム メッセージのログ 107, 109
ライセンス 109
概要 107
注意事項と制約事項 109

シリアル ID 134
説明 134

す

スイッチ プロファイル 13, 27, 28, 31, 32, 33, 34
バッファ、表示 27, 34
リブート後のコンフィギュレーションの同期 28
確認とコミット、表示 33
実行コンフィギュレーション、表示 31
注意事項と制約事項 13
例、ローカルとピアの同期 32, 34
スイッチ プロファイル バッファ、表示 27, 34
スイッチド ポート アナライザ 198

せ

セッションのアクティブ化 213
SPAN 213
セッションの実行 97

て

ディスカーディング 258
NTP 設定変更 258
ディセーブル化 249
NTP 249
デバイス ID 134
Call Home の形式 134
デフォルト パラメータ 226
ERSPAN 226
デフォルト設定 98, 140, 248, 269
NTP 用 248
smart call home 140
ロールバック 98
組み込みイベント マネージャ（EEM） 269

と

トラップ通知 170

は

ハードウェア プロファイル 290
OpenFlow 290
ハイ アベイラビリティ 72
PTP 72
ハイ アベイラビリティ 72
パイプラインのサポート 288
パスワード要件 85

ふ

ファシリティ メッセージのロギング 113
設定 113
フロー エクスポータ 296
NetFlow 296
フロー数の拡張 288

へ

ヘルス モニタリング診断 102
情報 102

め

メッセージの暗号化 176
SNMP 176

も

モジュール メッセージのロギング 113
設定 113
モジュールの事前プロビジョニング 37
概要 37

ゆ

ユーザ アカウント 85, 86, 93
パスワード 85
確認 93
注意事項と制約事項 86
ユーザ アカウントの制限事項 84
RBAC 84

ユーザ ポリシーの定義 280, 282
CLI を使用した Python スクリプトのトリガー 282
CLI を使用した Tcl スクリプトのトリガー 280
ユーザ ロール 79
RBAC 79
ユーザ ロール VLAN ポリシー、変更 92
RBAC 92
ユーザ ロール VSAN ポリシー、変更 92
ユーザ ロール コンフィギュレーション 67
CFS を使用して配信 67
ユーザ ロール、RBAC 80
SAN 管理者 80
ユーザ ロールおよびルール、作成 88
RBAC 88

ら

ライセンス 72, 109, 174
PTP 72
ライセンス 72
SNMP 174
システム メッセージのログ 109
ライセンス要件 221
ERSPAN 221
ランタイム診断 101
情報 101

り

リブート後のコンフィギュレーションの同期 28
スイッチ プロファイル 28

る

ルール 81
RBAC 81

ろ

ロール 79
認証 79
ロールバック 95, 96, 98
チェック ポイントのコピー 95
チェックポイント コピーの作成 96
チェックポイント ファイルの削除 96
チェックポイント ファイルへの復帰 96
デフォルト設定 98
ハイ アベイラビリティ 95
ロールバックの実装 96
制限事項 96
設定の確認 98
設定例 96
説明 95
注意事項 96
ロギング 113, 126
ACL ログの一致レベル 126
ファシリティ メッセージ 113
モジュール メッセージ 113
ロギング キャッシュ 124
設定 124
ロック済みセッション 50
クリア 50