



## **Cisco Nexus 3600 スイッチ NX-OS システム管理構成ガイド、リース 10.6(x)**

最終更新：2025 年 12 月 10 日

**シスコシステムズ合同会社**  
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー  
<http://www.cisco.com/jp>  
お問い合わせ先：シスコ コンタクトセンター  
0120-092-255（フリーコール、携帯・PHS含む）  
電話受付時間：平日 10:00～12:00、13:00～17:00  
<http://www.cisco.com/jp/go/contactcenter/>

【注意】シスコ製品をご使用になる前に、安全上の注意（[www.cisco.com/jp/go/safety\\_warning/](http://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の英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

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

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

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

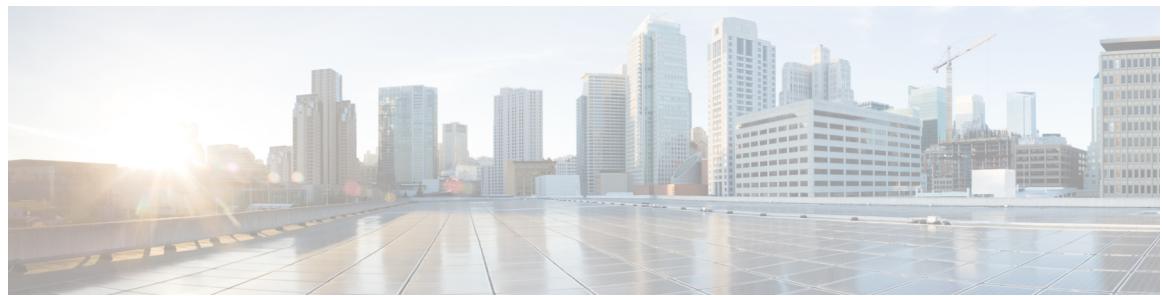
Any products and features described herein as in development or available at a future date remain in varying stages of development and will be offered on a when-and-if-available basis. Any such product or feature roadmaps are subject to change at the sole discretion of Cisco and Cisco will have no liability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

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

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

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

© 2025 Cisco Systems, Inc. All rights reserved.



## 目 次

### Trademarks ?

---

はじめに :	はじめに xvii
	対象読者 xvii
	表記法 xvii
	Cisco Nexus 3600 プラットフォーム スイッチの関連資料 xviii
	マニュアルに関するフィードバック xix
	通信、サービス、およびその他の情報 xix
第 1 章	新機能および変更された機能に関する情報 1
	新機能および変更された機能に関する情報 1
第 2 章	概要 3
	システム管理機能 3
	ライセンス要件 5
	サポートされるプラットフォーム 5
第 3 章	2ステージコンフィギュレーションコミット 7
	2段階構成のコミットについて 7
	注意事項と制約事項 8
	2ステージコンフィギュレーションコミットモードでの設定 9
	2ステージコンフィギュレーションコミットモードの中止 13
	コミット ID の表示 14
	ロールバック機能 14

## 現在のセッション設定の表示 14

## 第 4 章

## スイッチ プロファイルの設定 17

スイッチ プロファイルの概要 17

スイッチ プロファイル：コンフィギュレーション モード 18

コンフィギュレーションの検証 19

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 20

スイッチ プロファイルの前提条件 20

スイッチ プロファイルの注意事項および制約事項 21

スイッチ プロファイルの設定 22

スイッチ プロファイルへのスイッチの追加 25

スイッチ プロファイルのコマンドの追加または変更 26

スイッチ プロファイルのインポート 29

スイッチ プロファイルのコマンドの確認 31

ピア スイッチの分離 32

スイッチ プロファイルの削除 33

スイッチ プロファイルからのスイッチの削除 34

スイッチ プロファイルバッファの表示 35

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 36

スイッチ プロファイル設定の show コマンド 37

サポートされているスイッチ プロファイル コマンド 37

スイッチ プロファイルの設定例 39

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 39

同期ステータスの確認例 40

実行コンフィギュレーションの表示 41

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 41

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 42

同期の成功と失敗の例 43

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 43

## 第 5 章

## PTP の設定 45

PTP について	45
PTP デバイス タイプ	46
PTP 時間分配保留	47
PTP プロセス	47
PTP のハイ アベイラビリティ	48
PTP の注意事項および制約事項	48
PTP のデフォルト設定	49
PTP の設定	50
PTP のグローバルな設定	50
インターフェイスでの PTP の設定	52
PTP 設定の確認	54

---

**第 6 章****NTP の設定** 57

NTP の概要	57
タイム サーバーとしての NTP	58
CFS を使用した NTP の配信	58
クロック マネージャ	58
高可用性	59
仮想化のサポート	59
NTP の前提条件	59
NTP の注意事項と制約事項	59
デフォルト設定	60
NTP の設定	61
インターフェイスでの NTP のイネーブル化またはディセーブル化	61
正規の NTP サーバとしてのデバイスの設定	62
NTP サーバーおよびピアの設定	63
NTP 認証の設定	65
NTP アクセス制限の設定	66
NTP ソース IP アドレスの設定	68
NTP ソース インターフェイスの設定	69
NTP ブロードキャスト サーバーの設定	70

NTP マルチキャスト サーバーの設定	71
NTP マルチキャスト クライアントの設定	72
NTP ロギングの設定	73
NTP 用の CFS 配信のイネーブル化	74
NTP 設定変更のコミット	75
NTP 設定変更の廃棄	76
CFS セッション ロックの解放	76
NTP の設定確認	77
NTP の設定例	78

## 第 7 章

システムメッセージロギングの設定	81
システム メッセージ ロギングの詳細	81
Syslog サーバ	82
セキュアな Syslog サーバ	82
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	83
システム メッセージ ロギングのデフォルト設定	84
システムメッセージロギングの設定	84
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	84
Syslog メッセージの送信元 ID の設定	87
ファイルへのシステム メッセージの記録	88
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	89
RFC 5424 に準拠したロギング syslog の構成	92
syslog サーバの設定	93
セキュアな Syslog サーバの設定	95
CA 証明書の設定	96
CA 証明書の登録	97
UNIX または Linux システムでの syslog サーバの設定	99
ログ ファイルの表示およびクリア	100
システム メッセージ ロギングの設定確認	102
システム メッセージ ロギングの設定例	102
その他の参考資料	103

---

**関連資料 103****第 8 章****Session Manager の設定 105****セッションマネージャについて 105****Session Manager の注意事項および制約事項 105****Session Manager の設定 106****セッションの作成 106****セッションでの ACL の設定 106****セッションの確認 107****セッションのコミット 107****セッションの保存 107****セッションの廃棄 108****Session Manager のコンフィギュレーション例 108****Session Manager 設定の確認 108**

---

**第 9 章****Smart Call Home の設定 109****Smart Call Home の概要 109****Smart Call Home の概要 110****Smart Call Home 宛先プロファイル 110****Smart Call Home アラート グループ 111****Smart Call Home のメッセージ レベル 113****Call Home のメッセージ形式 114****Smart Call Home の注意事項および制約事項 119****Smart Call Home の前提条件 119****Call Home のデフォルト設定 120****Smart Call Home の設定 120****Smart Call Home の登録 120****連絡先情報の設定 121****宛先プロファイルの作成 123****接続先プロファイルの変更 124****アラート グループと宛先プロファイルのアソシエート 126**

アラート グループへの show コマンドの追加	127
電子メール サーバーの詳細の設定	129
定期的なインベントリ通知の設定	130
重複メッセージ抑制のディセーブル化	131
Smart Call Home のイネーブル化またはディセーブル化	132
Smart Call Home 設定のテスト	133
Smart Call Home 設定の確認	134
フルテキスト形式での syslog アラート通知の例	135
XML 形式での syslog アラート通知の例	135

## 第 10 章

スケジューラの設定	141
スケジューラの概要	141
リモート ユーザ認証	142
スケジューラ ログ ファイル	142
スケジューラの注意事項および制約事項	142
スケジューラのデフォルト設定	143
スケジューラの設定	143
スケジューラのイネーブル化	143
スケジューラ ログ ファイル サイズの定義	144
リモート ユーザ認証の設定	145
ジョブの定義	146
ジョブの削除	148
タイムテーブルの定義	149
スケジューラ ログ ファイルの消去	151
スケジューラのディセーブル化	152
スケジューラの設定確認	152
スケジューラの設定例	153
スケジューラ ジョブの作成	153
スケジューラ ジョブのスケジューリング	153
ジョブ スケジュールの表示	153
スケジューラ ジョブの実行結果の表示	154

## スケジューラの標準 154

## 第 11 章

## SNMP の設定 155

## SNMP について 155

## SNMP 機能の概要 155

## SNMP 通知 156

## SNMPv3 156

## 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 157

## ユーザーベースのセキュリティ モデル 158

## CLI および SNMP ユーザの同期 159

## グループベースの SNMP アクセス 160

## SNMP の注意事項および制約事項 160

## SNMP のデフォルト設定 161

## SNMP の設定 162

## SNMP 送信元インターフェイスの設定 162

## SNMP ユーザの設定 163

## ハッシュ化されたパスワードのオフラインでの生成 165

## SNMP メッセージ暗号化の適用 165

## SNMPv3 ユーザに対する複数のロールの割り当て 166

## SNMP コミュニティの作成 166

## SNMP 要求のフィルタリング 166

## SNMP 通知レシーバの設定 167

## VRF を使用する SNMP 通知レシーバの設定 168

## VRF に基づく SNMP 通知のフィルタリング 169

## インバンド アクセスのための SNMP の設定 170

## SNMP 通知のイネーブル化 172

## リンクの通知の設定 174

## インターフェイスでのリンク通知のディセーブル化 175

## TCP での SNMP に対するワンタイム認証のイネーブル化 175

## SNMP スイッチの連絡先および場所の情報の割り当て 176

## 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 176

---

	SNMP ローカルエンジン ID の設定 177
	SNMP の無効化 178
	SNMP 設定の確認 179
第 12 章	PCAP SNMP パーサーの使用 181
	PCAP SNMP パーサーの使用 181
第 13 章	RMON の設定 183
	RMON について 183
	RMON アラーム 183
	RMON イベント 184
	RMON の設定時の注意事項および制約事項 185
	RMON 設定の確認 185
	デフォルトの RMON 設定 185
	RMON アラームの設定 185
	RMON イベントの設定 187
第 14 章	オンライン診断の設定 189
	オンライン診断について 189
	ブートアップ診断 189
	ヘルス モニタリング診断 190
	拡張モジュール診断 190
	オンライン診断の注意事項と制約事項 191
	オンライン診断の設定 191
	オンライン診断設定の確認 192
	オンライン診断のデフォルト設定 192
第 15 章	Embedded Event Manager の設定 195
	組み込みイベント マネージャについて 195
	Embedded Event Manager ポリシー 196
	イベント文 197

---

アクション文	197
VSH スクリプト ポリシー	198
Embedded Event Manager のライセンス要件	198
Embedded Event Manager の前提条件	198
Embedded Event Manager の注意事項および制約事項	199
Embedded Event Manager のデフォルト設定	200
Embedded Event Manager の設定	200
環境変数の定義	200
CLI によるユーザー ポリシーの定義	201
イベント文の設定	203
アクション文の設定	206
VSH スクリプトによるポリシーの定義	208
VSH スクリプト ポリシーの登録およびアクティビ化	209
システム ポリシーの上書き	210
EEM パブリッシャとしての syslog の設定	212
Embedded Event Manager の設定確認	213
イベント ログの自動収集とバックアップ	214
拡張ログ ファイルの保持	214
トリガーベースのイベント ログの自動収集	219
ローカル ログ ファイルのストレージ	227
外部ログ ファイルのストレージ	230
Embedded Event Manager の設定確認	231
Embedded Event Manager の設定例	232
その他の参考資料	233

OBFL の概要	235
OBFL の前提条件	236
OBFL の注意事項と制約事項	236
OBFL のデフォルト設定	236
OBFL の設定	237

---

OBFL 設定の確認	239
OBFL のコンフィギュレーション例	240
その他の参考資料	241
関連資料	241

---

<b>SPAN の設定</b>	<b>243</b>
SPAN について	243
SPAN 送信元	244
送信元ポートの特性	244
SPAN宛先	245
接続先ポートの特性	245
SPAN の注意事項および制約事項	245
SPAN セッションの作成または削除	247
イーサネット宛先ポートの設定	247
送信元ポートの設定	249
SPAN トライックのレート制限の設定	250
送信元ポート チャネルの または VLAN を構成します。	251
SPAN セッションの説明の設定	252
SPAN セッションのアクティブ化	253
SPAN セッションの一時停止	253
SPAN 情報の表示	254
SPAN のコンフィギュレーション例	255
SPAN セッションのコンフィギュレーション例	255
单一方向 SPAN セッションの設定例	256
SPAN ACL の設定例	257
UDF ベース SPAN の設定例	257

---

<b>ERSPAN の設定</b>	<b>259</b>
ERSPAN について	259
ERSPAN 送信元	259
マルチ ERSPAN セッション	260

高可用性	260
ERSPAN の前提条件	260
ERSPAN の注意事項および制約事項	260
ERSPAN のデフォルト設定	264
ERSPAN の設定	264
ERSPAN 送信元セッションの設定	264
ERSPAN 送信元セッションの SPAN 転送ドロップ トライフィックの設定	268
ERSPAN ACL の設定	269
ユーザー定義フィールド (UDF) ベースの ACL サポートの設定	271
ERSPAN での IPv6 ユーザー定義フィールド (UDF) の設定	273
ERSPAN セッションのシャットダウンまたはアクティブ化	276
ERSPAN 設定の確認	279
ERSPAN の設定例	279
ERSPAN 送信元セッションの設定例	279
ERSPAN ACL の設定例	279
UDF ベース ERSPAN の設定例	280
その他の参考資料	281
関連資料	281

## 第 19 章

## DNS の設定 283

DNS クライアントについて	283
ネーム サーバ	283
DNS の動作	284
高可用性	284
DNS クライアントの前提条件	284
DNS クライアントのデフォルト設定	284
DNS 送信元インターフェイスの設定	285
DNS クライアントの設定	286

## 第 20 章

## sFlow の設定 289

sFlow について	289
------------	-----

sFlow エージェント	289
前提条件	290
sFlow の注意事項および制約事項	290
sFlow のデフォルト設定	291
サンプリングの最小要件	291
sFlow の設定	291
sFlow 機能のイネーブル化	291
サンプリング レートの設定	292
最大サンプリング サイズの設定	293
カウンタのポーリング間隔の設定	294
最大データグラム サイズの設定	295
sFlow アナライザのアドレスの設定	296
sFlow アナライザ ポートの設定	297
sFlow エージェント アドレスの設定	298
sFlow サンプリング データ ソースの設定	299
sFlow 設定の確認	301
sFlow の設定例	301
sFlow に関する追加情報	301

グレースフル挿入と削除の設定	303
グレースフル挿入と削除について	303
プロファイル	304
スナップショット	305
GIR ワークフロー	305
メンテナンス モード プロファイルの設定	306
通常モード プロファイルの設定	307
スナップショットの作成	308
スナップショットへの show コマンドの追加	310
グレースフル削除のトリガー	312
グレースフル挿入のトリガー	315
メンテナンス モードの強化	316

---

**GIR 設定の確認 318**

---

**第 22 章****コンフィギュレーションの置換の実行 321****コンフィギュレーションの置換とコミットタイムアウトについて 321****概要 322****コンフィギュレーションの置換の利点 323****コンフィギュレーションの置換に関する注意事項と制限事項 324****構成の置換の推奨ワークフロー 327****コンフィギュレーションの置換の実行 328****コンフィギュレーションの置換の確認 331****構成の置換の例 331**

---

**第 23 章****ソフトウェアメンテナンスアップグレード (SMU) の実行 339****SMU について 339****パッケージ管理 340****SMU の前提条件 341****SMU の注意事項と制約事項 341****Cisco NX-OS のソフトウェアメンテナンスアップグレードの実行 342****パッケージインストールの準備 342****ローカルストレージデバイスまたはネットワークサーバへのパッケージファイルのコピー 344****パッケージの追加とアクティブ化 345****アクティブなパッケージセットのコミット 346****パッケージの非アクティブ化と削除 347****インストールログ情報の表示 348**

---

**第 24 章****ロールバックの設定 351****ロールバックについて 351****ロールバックの注意事項と制約事項 351****チェックポイントの作成 352****ロールバックの実装 353**

## ロールバック コンフィギュレーションの確認 354

## 第 25 章

## 候補構成の完全性チェック 357

候補構成について 357

候補構成の完全性チェックの注意事項と制限事項 357

候補構成の完全性チェックの実行 363

完全性チェックの例 364

## 第 26 章

## ユーザ アカウントおよび RBAC の設定 367

ユーザ アカウントと RBAC について 367

ユーザ ロール 367

ルール 368

ユーザー ロール ポリシー 368

ユーザー アカウントの設定の制限事項 369

ユーザ パスワードの要件 370

ユーザー アカウントの注意事項および制約事項 371

ユーザ アカウントの設定 371

RBAC の設定 373

ユーザ ロールおよびルールの作成 373

機能グループの作成 375

ユーザ ロール インターフェイス ポリシーの変更 376

ユーザ ロール VLAN ポリシーの変更 377

ユーザー アカウントと RBAC の設定の確認 378

ユーザー アカウントおよび RBAC のデフォルト設定 378



# はじめに

---

この前書きは、次の項で構成されています。

- [対象読者 \(xvii ページ\)](#)
- [表記法 \(xvii ページ\)](#)
- [Cisco Nexus 3600 プラットフォーム スイッチの関連資料 \(xviii ページ\)](#)
- [マニュアルに関するフィードバック \(xix ページ\)](#)
- [通信、サービス、およびその他の情報 \(xix ページ\)](#)

## 対象読者

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

## 表記法

コマンドの説明には、次のような表記法が使用されます。

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

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

例では、次の表記法を使用しています。

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

## Cisco Nexus 3600 プラットフォーム スイッチの関連資料

Cisco Nexus 3600 プラットフォーム スイッチ全体のマニュアルセットは、次の URL にあります。

<http://www.cisco.com/c/en/us/support/switches/nexus-3000-series-switches/tsd-products-support-series-home.html>

# マニュアルに関するフィードバック

このマニュアルに関する技術的なフィードバック、または誤りや記載もれなどお気づきの点がございましたら、HTML ドキュメント内のフィードバック フォームよりご連絡ください。ご協力をよろしくお願ひいたします。

## 通信、サービス、およびその他の情報

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

### Cisco バグ検索ツール

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

通信、サービス、およびその他の情報



# 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

次の表は、このリリースの新機能と変更された機能をまとめたものです。Cisco Nexus 3600 NX-OS システム管理設定ガイド、リリース 10.2 (x) それらの説明がどこに記載されているかもまとめます。

表 1: 新機能および変更された機能

特長	説明	変更が行われたリリース	参照先
NA	このリリースで追加された新機能はありません。	10.6(1)F	N/A

■ 新機能および変更された機能に関する情報



## CHAPTER 2

### 概要

この章は、次の項で構成されています。

- [システム管理機能, on page 3](#)
- [ライセンス要件 \(5 ページ\)](#)
- [サポートされるプラットフォーム \(5 ページ\)](#)

### 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。

特長	説明
ユーザー アカウントおよび RBAC	ユーザー 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、ユーザーが管理操作にアクセスするための許可を制限します。各ユーザー ロールに複数のルールを含めることができ、各ユーザー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。

特長	説明
オンライン診断	<p>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。</p> <p>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。</p>
設定のロールバック	<p>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ー 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とも、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。</p>
SNMP	<p>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。</p>
RMON	<p>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 デバイスをモニターするための、RMON アラーム、イベント、およびログをサポートします。</p>

特長	説明
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) プロープです。

## ライセンス要件

Cisco NX-OS を動作させるには、機能とプラットフォームの要件に従って適切なライセンスを取得し、インストールする必要があります。

- 基本 (Essential) ライセンスとアドオンライセンスが、さまざまな機能セットに使用できます。
- ライセンスは、製品および購入オプションに応じて、永続的、一時的、または評価可能な場合があります。
- 高度な機能を使用するには、基本ライセンス以外の追加の機能ライセンスが必要です。
- 高度な機能を使用するには、基本ライセンス以外の追加ライセンスが必要です。
- ライセンスの適用と管理は、デバイスのコマンドラインインターフェイス (CLI) を介して行われます。

ハードウェアの取り付け手順の詳細については、次を参照してください。 [Cisco NX-OS ライセンシング ガイド](#) および [Cisco NX-OS ライセンシング オプション ガイド](#)。

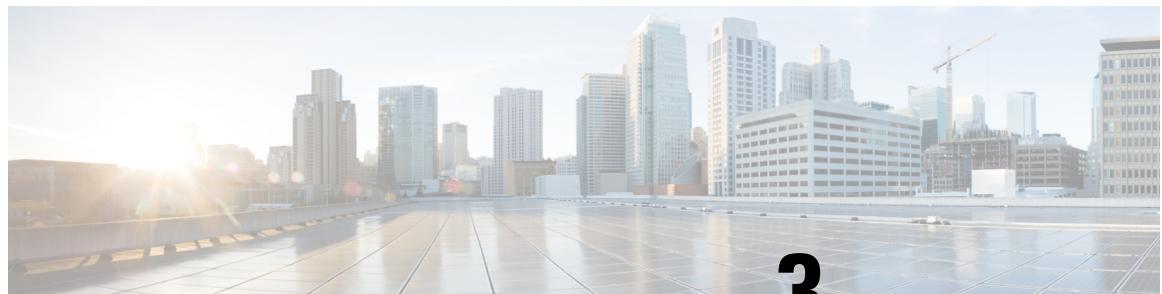
## サポートされるプラットフォーム

Nexus Switch プラットフォーム サポートマトリックスは、次をリストします：

- サポートされている Cisco Nexus 9000 および 3000 スイッチ モデル
- NX-OS ソフトウェア リリース バージョン

フルプラットフォーム機能マッピングは、「[Nexus Switch プラットフォーム サポートマトリックス](#)」を参照します。

## ■ サポートされるプラットフォーム



## 第 3 章

# 2ステージコンフィギュレーションコミット

この章では、Cisco NX-OS デバイス上で 2 ステージ コンフィギュレーション コミット モードを有効にする方法について説明します。

この章は、次の項で構成されています。

- 2 段階構成のコミットについて (7 ページ)
- 注意事項と制約事項 (8 ページ)
- 2 ステージ コンフィギュレーション コミット モードでの設定 (9 ページ)
- 2 ステージ コンフィギュレーション コミット モードの中止 (13 ページ)
- コミット ID の表示 (14 ページ)
- ロールバック機能 (14 ページ)
- 現在のセッション設定の表示 (14 ページ)

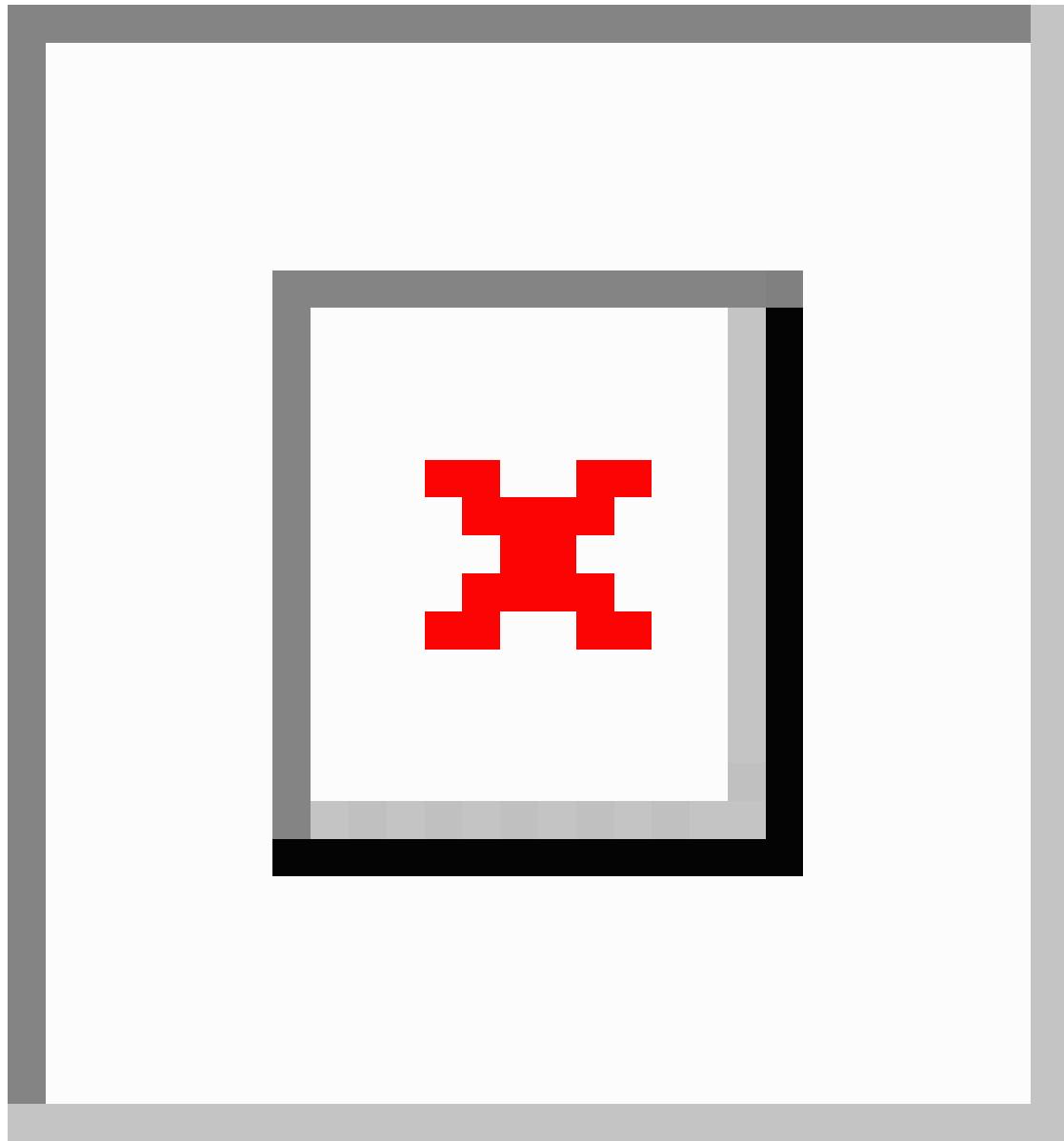
## 2 段階構成のコミットについて

インタラクティブセッションでは、コマンドを実行するとコマンドが実行され、実行コンフィギュレーションが変更されます。この動作は、1ステージコンフィギュレーションコミットと呼ばれます。確認コミットまたは2段階の設定コミットでは、設定の変更がステージングデータベースに保存されます。これらの変更は、**commit** コマンドを実行しないと、スイッチは以前の構成に戻ります。この2段階のプロセスにより、ターゲットコンフィギュレーションセッションが作成されます。このコンフィギュレーションでは、スイッチの実行状態にコミットする前に、設定の変更、編集、および確認を行うことができます。永続的にコミットする前に、指定した期間の変更をコミットすることもできます。指定した時間が経過しても、**commit** コマンドを実行しないと、スイッチは以前の構成に戻ります。コミットが成功すると、コミット ID、ユーザ名、およびタイムスタンプを含むコミット情報を表示できます。

次の図に、2段階の設定コミットプロセスを示します。

## ■ 注意事項と制約事項

図 1:2段階でのコミットコンフィギュレーションプロセス



## 注意事項と制約事項

2段階設定コミットには、次の注意事項および制限事項があります。

- この機能は、ユーザインターラクティブセッションの CLI インターフェイスでのみサポートされます。
- 機能関連の構成コマンドを実行する前に、**feature** コマンドを使用して機能を有効にし、**commit** コマンドを使用してコミットします。

- 2段階設定コミットモードは、メンテナンスモード、スケジューラモード、仮想モードなどの他のモードをサポートしていません。
- 2段階設定コミットモードの場合は、1段階設定コミットモードで異なるセッションから同時に設定を編集しないでください。
- 変更をコミットする前にコマンドを使用して **show configuration** 構成を見直します。
- 検証に失敗した場合は、コミットして編集します。
- コミットが失敗すると、設定は以前の設定にロールバックされます。
- コミットしない設定は、スイッチをリロードした後は保存されません。
- この機能は、NX-API、EEM、およびPPMでのコミットをサポートしていません。
- 一度にアクティブにできる2段階設定コミットセッションは1つだけです。

## 2ステージコンフィギュレーションコミットモードでの設定

2ステージコンフィギュレーションコミットモードで機能を有効にするには、次の手順を実行します。



(注) この手順では、例としてBGP機能を有効にします。

### 手順

	コマンドまたはアクション	目的
ステップ1	<b>configure dual-stage</b> <b>例 :</b> <pre>switch# configure dual-stage switch(config-dual-stage) #</pre>	新しいターゲットコンフィギュレーションセッションを作成します。  (注) ターゲットコンフィギュレーションは、実行コンフィギュレーションのコピーではありません。ターゲットコンフィギュレーションには、そのターゲットコンフィギュレーションセッションで入力されたコンフィギュレーションコマンドだけが含まれます。
ステップ2	<b>feature <i>feature_name</i></b> <b>例 :</b>	機能を有効にします。  (注)

## 2ステージコンフィギュレーションコミットモードでの設定

	コマンドまたはアクション	目的
	switch(config-dual-stage)# feature bgp switch(config-dual-stage)#	<ul style="list-style-type: none"> <li>2ステージコンフィギュレーションコミットモードを開始する前でも、この機能を有効にできます。</li> <li>機能が有効になっていない場合は、機能関連のコマンドを組み合わせて使用することはできません。</li> </ul>
ステップ3	<b>commit [confirmedseconds]</b> <b>例 :</b> <pre>switch(config-dual-stage-router)# commit confirmed 30 Verification Succeeded. Proceeding to apply configuration. This might take a while depending on amount of configuration in buffer. Please avoid other configuration changes during this time.  Configuration committed by user 'admin' using Commit ID : 1000000001</pre> <b>例 :</b> <pre>switch(config-dual-stage)# hostname example-switch switch(config-dual-stage)# commit Verification Succeeded.  Proceeding to apply configuration. This might take a while depending on amount of configuration in buffer. Please avoid other configuration changes during this time. Configuration committed by user 'admin' using Commit ID : 1000000002 example-switch(config-dual-stage)# </pre>	<p>実行コンフィギュレーションに変更をコミットします。</p> <ul style="list-style-type: none"> <li><b>confirmed</b> : 実行コンフィギュレーションに変更をコミットします。</li> <li><b>seconds</b> : グローバル構成モードで、最低30秒間、最大65535秒間の試験稼働のために構成をコミットします。</li> </ul> <p>(注) トライアル期間を入力する場合は、commitコマンドを実行して設定を確認します。commitコマンドを実行しないと、トライアル期間後に以前の設定に戻ります。</p>
ステップ4	<b>例 :</b> <pre>switch(config-dual-stage)# router bgp 64515.46 switch(config-dual-stage-router)# switch(config-dual-stage-router)#   router-id 141.8.139.131 switch(config-dual-stage-router)# </pre>	このコンフィギュレーションモードでサポートされている機能関連のコマンドを実行します。
ステップ5	<b>show configuration</b> <b>例 :</b> <pre>switch(config-dual-stage-router)# show configuration</pre>	ターゲットコンフィギュレーションの内容を表示します。 <p>(注)</p>

	コマンドまたはアクション	目的
	<pre>! Cached configuration ! router bgp 64515.46   router-id 141.8.139.131</pre>	このコマンドは、デュアルステージコンフィギュレーションモードでのみ実行できます。
ステップ6	<b>commit [confirmed seconds]</b> <b>例 :</b> <pre>switch(config-dual-stage-router)# commit Verification Succeeded. Proceeding to apply configuration. This might take a while depending on amount of configuration in buffer. Please avoid other configuration changes during this time. Configuration committed by user 'admin' using Commit ID : 1000000003</pre>	実行コンフィギュレーションに変更をコミットします。
ステップ7	<b>(任意) show configuration commit [changes] commit-id</b> <b>例 :</b> <pre>switch(config-dual-stage-router)# show configuration commit changes 1000000003 *** /bootflash/.dual-stage/1000000003.tmp   Fri Mar 19 10:59:00 2021 --- /bootflash/.dual-stage/1000000003  Fri Mar   19 10:59:05 2021 ***** *** 378,383 **** --- 378,385 ----   line console   line vty   boot nxos bootflash:/nxos64.10.1.1.44.bin + router bgp 64515.46 +   router-id 141.8.139.131   xml server timeout 1200    no priority-flow-control override-interface   mode off</pre> <b>例 :</b> <pre>switch(config-dual-stage)# show configuration commit 1000000003 feature bgp router bgp 64515.46   router-id 141.8.139.131 . .</pre>	<b>コミット</b> 関連情報を表示します。 最後の50個のコミットまたは予約済みディスク領域に保存されたコミットファイルのみが保存されます。予約済みディスク領域は20MBです。スイッチをリロードすると、すべてのコミットセッションが削除されます。ただし、コミットIDは削除されません。 <b>show configuration commit changes commit-id</b> コマンドを使用して指定したコミットの現在のセッションの変更のみを表示します。 <b>show configuration commit commit-id</b> コマンドを使用して指定したコミットの完全な設定を表示します。
ステップ8	<b>(任意) save configuration filename</b> <b>例 :</b> <pre>switch(config-dual-stage)# save configuration bootflash:test.cfg</pre>	ターゲットコンフィギュレーションは、実行コンフィギュレーションにコミットすることなく、独立したファイルに保存できます。 <b>(注)</b> <ul style="list-style-type: none"> <li>ターゲットコンフィギュレーションファイルは、後でロード、変更、またはコミットでき</li> </ul>

## 2ステージコンフィギュレーションコミット モードでの設定

	コマンドまたはアクション	目的
		<p>ます。ファイルはブートフラッシュに保存されます。</p> <ul style="list-style-type: none"> <li>保存した構成ファイルを表示するには、<b>show configuration file filename</b> コマンドのみを使用します。</li> <li>ユーザ固有の情報の一部は、ユーザ ロールに基づいてマスクされます。</li> </ul>
ステップ 9	<p>(任意) <b>load filename</b></p> <p>例 :</p> <pre>switch (config-dual-stage)# show configuration ! Cached configuration switch (config-dual-stage)# load test.cfg switch (config-dual-stage-router)# show configuration ! Cached configuration ! router bgp 1 switch(config-dual-stage-router)# </pre>	<p>保存したターゲットコンフィギュレーションをロードします。ファイルをロードした後、ファイルを変更したり、実行コンフィギュレーションにコミットしたりできます。変更を保存するには、<b>save configuration filename</b> コマンドのみを使用します。</p> <p>保存したターゲット構成をロードするには、<b>save configuration filename</b> コマンドのみを使用します。</p>
ステップ 10	<p>(任意) <b>clear configuration</b></p> <p>例 :</p> <pre>switch(config-dual-stage)# show configuration ! Cached configuration ! router bgp 64515.46 router-id 141.8.139.131 switch (config-dual-stage)# clear configuration  switch (config-dual-stage)# show configuration ! Cached configuration switch (config-dual-stage)# </pre>	<p>コンフィギュレーションセッションを終了せずに、ターゲットコンフィギュレーションに加えられた変更をクリアします。コミットされていない設定変更は削除されます。</p>
ステップ 11	<p><b>end</b></p> <p>例 :</p> <pre>switch(config-dual-stage-if)# end Uncommitted changes found, commit them before exiting (yes/no/cancel)? [cancel]</pre>	<p>グローバルデュアルコンフィギュレーションモードを終了します。</p> <p>設定変更をコミットせずにコンフィギュレーションセッションを終了すると、変更内容を保存するか、変更を破棄するか、または操作をキャンセルするよう指示されます。</p> <ul style="list-style-type: none"> <li>はい : 設定変更をコミットしてから、コンフィギュレーションモードを終了します。</li> <li>いいえ : 設定変更をコミットせずに、コンフィギュレーションモードを終了します。</li> <li>キャンセル : 設定変更をコミットせずに、コンフィギュレーションモードに留まります。</li> </ul>

コマンドまたはアクション	目的
	<p>(注)</p> <ul style="list-style-type: none"> <li>確認コミット タイマーの実行中に終了することを選択した場合は、同じオプションが表示されます。終了を選択した場合、トライアル設定はすぐにロールバックされます。</li> <li>タイマーが期限切れになる前にデフォルトセッションがタイムアウトした場合、トライアル設定はセッションを終了する前にロールバックします。この場合、警告メッセージが表示されます。</li> </ul>

## 2ステージコンフィギュレーションコミットモードの中止

コンフィギュレーションセッションを破棄すると、コミットされていない変更内容は破棄され、コンフィギュレーションセッションが終了します。設定変更は、警告なしに削除されます。

```

switch(config-dual-stage)# router bgp 1
switch(config-dual-stage-router)# neighbor 1.2.3.4
switch(config-dual-stage-router-neighbor)# remote-as 1
switch(config-dual-stage-router-neighbor)# show configuration
! Cached configuration
!
router bgp 1
neighbor 1.2.3.4
remote-as 1
switch(config-dual-stage-router-neighbor)# show run bgp

!Command: show running-config bgp
!Running configuration last done at: Wed Mar 17 16:17:40 2021
!Time: Wed Mar 17 16:17:55 2021

version 10.1(2) Bios:version
feature bgp

switch(config-dual-stage-router-neighbor)# abort
switch# show run bgp

!Command: show running-config bgp
!Running configuration last done at: Wed Mar 17 16:18:00 2021
!Time: Wed Mar 17 16:18:04 2021

version 10.1(2) Bios:version
feature bgp

switch#

```

## ■ コミット ID の表示

# コミット ID の表示

コミットが成功するたびに、コミット ID が syslog に表示されます。システムに保存されるコミット ID の総数は、設定サイズと使用可能なディスク領域によって異なります。ただし、任意の時点で保存されるコミット ID の最大数は 50 です。

**show configuration commit list** コマンドを使用して最後の 50 のコミット ID に関する情報を表示します。各エントリに、設定変更をコミットしたユーザ、コミットの実行に使用された接続、およびコミット ID のタイムスタンプが表示されます。

```
switch# show configuration commit list
SNo. Label/ID      User      Line      Client      Time Stamp
~~~~ ~~~~~ ~~~~~ ~~~~~ ~~~~~ ~~~~~
1 1000000001  admin  /dev/ttys0  CLI  Wed Jul 15 15:21:37 2020
2 1000000002  admin  /dev/ttys0  Rollback  Wed Jul 15 15:22:15 2020
3 1000000003  admin  /dev/pts/0  CLI  Wed Jul 15 15:23:08 2020
4 1000000004  admin  /dev/pts/0  Rollback  Wed Jul 15 15:23:46 2020
```

# ロールバック機能

以前に成功したコミットのいずれかに設定をロールバックできます。**rollback configuration** コマンドを使用して、最後の 50 のコミットのいずれかにロールバックします。

```
switch# rollback configuration to ?
1000000015
1000000016
1000000017

:
:

switch#
```

Each commit ID acts as a checkpoint of a running configuration. You can rollback to any given commit ID. A new commit ID will be generated after you rollback. If a confirm commit session is in progress, you cannot trigger a rollback until it is completed.

```
switch(config-dual-stage)# rollback configuration to 1000000002
Rolling back to commitID :1000000002
ADVISORY: Rollback operation started...
Modifying running configuration from another VSH terminal in parallel
is not recommended, as this may lead to Rollback failure.

Configuration committed by rollback using Commit ID : 1000000004
switch(config-dual-stage)#

```

# 現在のセッション設定の表示

現在の構成セッションを表示するには、**show configuration** コマンドを使用します。このコマンドは、デュアルステージモードでのみサポートされます。コミットが失敗すると、セッション設定はクリアされます。

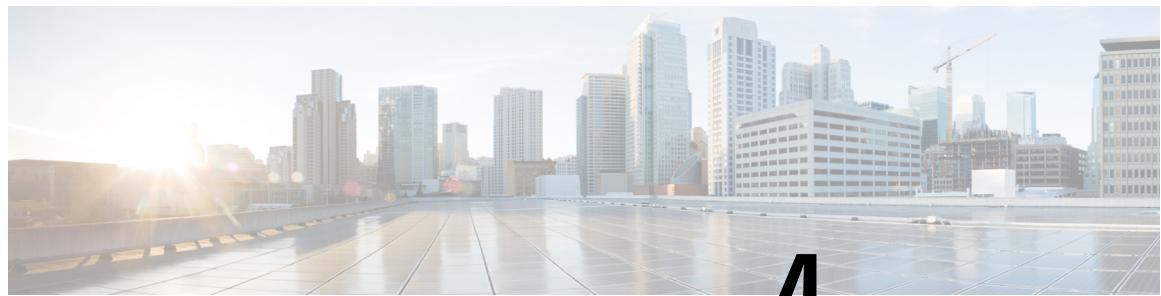
```
switch(config-dual-stage-cmap)# show configuration
! Cached configuration
!
class-map type control-plane match-any copp-s-ipmcmiss
class-map type control-plane match-any copp-s-l2switched
class-map type control-plane match-any copp-s-l3destmiss
switch(config-dual-stage-cmap)#

If there is no configuration, the following message appears:

switch(config-dual-stage)# show configuration
! Cached configuration
switch(config-dual-stage)# commit
No configuration changes to commit.
switch(config-dual-stage)#

```

■ 現在のセッション設定の表示



## 第 4 章

# スイッチ プロファイルの設定

この章は、次の項で構成されています。

- [スイッチ プロファイルの概要 \(17 ページ\)](#)
- [スイッチ プロファイル：コンフィギュレーション モード \(18 ページ\)](#)
- [コンフィギュレーションの検証 \(19 ページ\)](#)
- [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 \(20 ページ\)](#)
- [スイッチ プロファイルの前提条件 \(20 ページ\)](#)
- [スイッチ プロファイルの注意事項および制約事項 \(21 ページ\)](#)
- [スイッチ プロファイルの設定 \(22 ページ\)](#)
- [スイッチ プロファイルへのスイッチの追加 \(25 ページ\)](#)
- [スイッチ プロファイルのコマンドの追加または変更 \(26 ページ\)](#)
- [スイッチ プロファイルのインポート \(29 ページ\)](#)
- [スイッチ プロファイルのコマンドの確認 \(31 ページ\)](#)
- [ピア スイッチの分離 \(32 ページ\)](#)
- [スイッチ プロファイルの削除 \(33 ページ\)](#)
- [スイッチ プロファイルからのスイッチの削除 \(34 ページ\)](#)
- [スイッチ プロファイルバッファの表示 \(35 ページ\)](#)
- [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 \(36 ページ\)](#)
- [スイッチ プロファイル設定の show コマンド \(37 ページ\)](#)
- [サポートされているスイッチ プロファイルコマンド \(37 ページ\)](#)
- [スイッチ プロファイルの設定例 \(39 ページ\)](#)

## スイッチ プロファイルの概要

複数のアプリケーションは、Cisco Nexus シリーズスイッチ間で整合性のある構成が必要です。たとえば、仮想ポートチャネル (vPC) を使用する場合、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。

## ■ スイッチ プロファイル：コンフィギュレーション モード

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モード

コンフィギュレーション同期モード (config-sync) では、プライマリ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したら、同期するピアスイッチに **config sync** コマンドを入力します。

## スイッチ プロファイル モード

スイッチ プロファイル モードでは、後でピアスイッチと同期化されるスイッチ プロファイルに、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オプションがあります。**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、既存のスイッチ設定を実行コンフィギュレーションからインポートし、どのコマンドをスイッチ プロファイルに含めるかを指定できます。

トポロジが異なると、スイッチ プロファイルに含めるコマンドも異なるため、**import** コマンド モードでは、特定のトポロジに適合するようにコマンドのインポート セットを変更できます。

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 プロセス中の構成変更はサポートされていないため、**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。追加したコマンドを削除するか、またはインポートを中断します。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。

## 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



(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。値は、**import** コマンドでは、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** と **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構成します。

## 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 プロファイルを設定する場合は、次の注意事項および制約事項を考慮してください。

- 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。
- 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、構成は、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。
- 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) ポートチャネルに関する一部のサブコマンドは、スイッチ プロファイル モードでは設定できません。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、メンバー 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ー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。
- インターフェイスをデフォルトにしても、そのインターフェイスの config-sync 構成から チャネル グループは削除されません。config-sync モジュールによって競合する構成がプッシュされるのを防ぐために、**no channel-group** コマンドをインターフェイスに適用するか、config-sync 構成にポートチャネルを含める必要があります。

#### 接続の切断後の同期化の注意事項

- 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。

## 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。構成同期モード (config-sync) で、**switch-profile name** コマンドを入力します。

## 始める前に

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。

## 手順の概要

1. **configure terminal**
2. **cfs ipv4 distribute**
3. **config sync**
4. **switch-profile *name***
5. **sync-peers destination *IP-address***
6. (任意) **show switch-profile *name* status**
7. **exit**
8. (任意) **copy running-config startup-config**

## 手順の詳細

### 手順

	コマンドまたはアクション	目的
ステップ1	<b>configure terminal</b> 例： <pre>switch# configure terminal switch(config)#</pre>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<b>cfs ipv4 distribute</b> 例： <pre>switch(config)# cfs ipv4 distribute switch(config)#</pre>	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	<b>config sync</b> 例： <pre>switch# config sync switch(config-sync)#</pre>	コンフィギュレーション同期モードを開始します。
ステップ4	<b>switch-profile <i>name</i></b> 例： <pre>switch(config-sync)# switch-profile abc switch(config-sync-sp)#</pre>	スイッチプロファイルを設定し、スイッチプロファイルの名前を設定し、スイッチプロファイル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	<b>sync-peers destination <i>IP-address</i></b> 例： <pre>switch(config-sync-sp)# sync-peers destination 10.1.1.1 switch(config-sync-sp)#</pre>	ピアスイッチを設定します。

## スイッチ プロファイルの設定

	コマンドまたはアクション	目的
ステップ 6	(任意) <b>show switch-profile name status</b>  例：  switch(config-sync-sp)# show switch-profile abc status switch(config-sync-sp)#	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	<b>exit</b>  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	(任意) <b>copy running-config startup-config</b>  例：  switch(config)# 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。

## 例

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

**sync-peers destination *destination IP*** コマンドを入力し、スイッチ プロファイル構成モードを開始してスイッチ 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。

## 始める前に

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 番目のスイッチを追加する必要があります。

## 手順の概要

1. **config sync**
2. **switch-profile *name***
3. **sync-peers destination *destination IP***
4. **exit**
5. (任意) **show switch-profile peer**
6. (任意) **copy running-config startup-config**

## 手順の詳細

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>config sync</b> 例： <pre>switch# config sync switch(config-sync)#</pre>	コンフィギュレーション同期モードを開始します。
ステップ 2	<b>switch-profile <i>name</i></b> 例： <pre>switch(config-sync)# switch-profile abc switch(config-sync-sp)#</pre>	スイッチ プロファイルを設定し、スイッチ プロファイルの名前を設定し、スイッチ プロファイル同期コンフィギュレーション モードを開始します。

## スイッチ プロファイルのコマンドの追加または変更

	コマンドまたはアクション	目的
ステップ 3	<b>sync-peers destination</b> <i>destination IP</i> 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	<b>exit</b> 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	(任意) <b>show switch-profile peer</b> 例： switch# show switch-profile peer	スイッチ プロファイルのピアの設定を表示します。
ステップ 6	(任意) <b>copy running-config startup-config</b> 例： switch# copy running-config startup-config	実行中の構成を、スタートアップ構成にコピーします。

## 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 プロファイル内のコマンドを変更するには、変更したコマンドをスイッチ プロファイルに追加し、**commit** コマンドを使用して、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。次のような電力事業コマンドを使用できます。**show switch-profile name buffer** コマンド、**buffer-delete** コマンド、または **buffer-move** コマンドでバッファを変更し、すでに入力されたコマンドの順序を修正します。

### 始める前に

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バッファに格納されます。次に、**commit** コマンドは次のことを行います：

- 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。

## 手順の概要

1. **config sync**
2. **switch-profile *name***
3. *Command argument*
4. (任意) **show switch-profile *name* buffer**
5. **verify**
6. **commit**
7. (任意) **show switch-profile *name* status**
8. **exit**
9. (任意) **copy running-config startup-config**

## 手順の詳細

### 手順

	コマンドまたはアクション	目的
ステップ1	<b>config sync</b>  例： <pre>switch# config sync switch(config-sync)#</pre>	コンフィギュレーション同期モードを開始します。
ステップ2	<b>switch-profile <i>name</i></b>  例： <pre>switch(config-sync)# switch-profile abc switch(config-sync-sp)#</pre>	スイッチ プロファイルを設定し、スイッチ プロファイルの名前を設定し、スイッチ プロファイル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	<i>Command argument</i>  例： <pre>switch(config-sync-sp)# interface Port-channel100 switch(config-sync-sp-if)# speed 1000 switch(config-sync-sp-if)# interface Ethernet1/1 switch(config-sync-sp-if)# speed 1000 switch(config-sync-sp-if)# channel-group 100</pre>	スイッチ プロファイルにコマンドを追加します。

## スイッチ プロファイルのコマンドの追加または変更

	コマンドまたはアクション	目的
ステップ4	(任意) <b>show switch-profile name buffer</b>  例：  switch(config-sync-sp)# show switch-profile abc buffer switch(config-sync-sp)#	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	<b>verify</b>  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	<b>commit</b>  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	(任意) <b>show switch-profile name status</b>  例：  switch(config-sync-sp)# show switch-profile abc status switch(config-sync-sp)#	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。
ステップ8	<b>exit</b>  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	(任意) <b>copy running-config startup-config</b>  例：  switch# copy running-config startup-config	実行 コンフィギュレーション を、スタートアップ コンフィギュレーション にコピーします。

## 例

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番目の例は、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。
- サポートされてい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。次のコマンドを使用して、インポートを停止します。**abort**コマンドを使用します。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。

### 手順の概要

- config sync**
- switch-profile name**
- import {interface port/slot | running-config [exclude interface ethernet]}**
- commit**
- (任意) **abort**

## スイッチ プロファイルのインポート

6. **exit**
7. (任意) **show switch-profile**
8. (任意) **copy running-config startup-config**

## 手順の詳細

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>config sync</b>  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	<b>switch-profile name</b>  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	<b>import {interface port/slot   running-config [exclude interface ethernet]}</b>  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。 <ul style="list-style-type: none"> <li>• &lt;CR&gt;—選択したコマンドを追加します。</li> <li>• <b>interface</b>—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。</li> <li>• <b>running-config</b>—サポートされているシステムレベルコマンドを追加します。</li> <li>• <b>running-config exclude interface ethernet</b>—物理インターフェイスコマンドを除くサポートされているシステムレベルコマンドを追加します。</li> </ul>
ステップ 4	<b>commit</b>  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	(任意) <b>abort</b>  例：  switch(config-sync-sp-import)# abort	インポートプロセスを中止します。
ステップ 6	<b>exit</b>  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。

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

### 例

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)#

```

## 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。

### 手順の概要

#### 1. config sync

## ピアスイッチの分離

2. **switch-profile name**
3. **verify**
4. **exit**
5. (任意) **copy running-config startup-config**

### 手順の詳細

#### 手順

	コマンドまたはアクション	目的
ステップ1	<b>config sync</b>  例： <pre>switch# config sync switch(config-sync) #</pre>	コンフィギュレーション同期モードを開始します。
ステップ2	<b>switch-profile name</b>  例： <pre>switch(config-sync) # switch-profile abc switch(config-sync-sp) #</pre>	スイッチプロファイルを設定し、スイッチプロファイルの名前を設定し、スイッチプロファイル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	<b>verify</b>  例： <pre>switch(config-sync-sp) # verify</pre>	スイッチプロファイルバッファ内のコマンドを確認します。
ステップ4	<b>exit</b>  例： <pre>switch(config-sync-sp) # exit switch#</pre>	スイッチプロファイルコンフィギュレーションモードを終了します。
ステップ5	(任意) <b>copy running-config startup-config</b>  例： <pre>switch# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

## 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。値は、`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。

### 手順の概要

1. `config sync`
2. `no switch-profile name {all-config | local-config}`
3. `exit`
4. (任意) `copy running-config startup-config`

### 手順の詳細

#### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>config sync</b> 例： <code>switch# config sync</code> <code>switch(config-sync)#</code>	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	<b>no switch-profile name {all-config   local-config}</b> 例： <code>switch(config-sync)# no switch-profile abc</code> <code>local-config</code> <code>switch(config-sync-sp)#</code>	次の手順に従って、スイッチ プロファイルを削除します。 <ul style="list-style-type: none"> <li>• <b>all-config</b>—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。</li> <li>• <b>local-config</b>—スイッチ プロファイルおよびローカル構成を削除します。</li> </ul>

## スイッチ プロファイルからのスイッチの削除

	コマンドまたはアクション	目的
ステップ3	<b>exit</b> 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	(任意) <b>copy running-config startup-config</b> 例： switch# copy running-config startup-config	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

## スイッチ プロファイル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。

### 手順の概要

1. **config sync**
2. **switch-profile name**
3. **no sync-peers destination destination IP**
4. **exit**
5. (任意) **show switch-profile**
6. (任意) **copy running-config startup-config**

### 手順の詳細

#### 手順

	コマンドまたはアクション	目的
ステップ1	<b>config sync</b> 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	<b>switch-profile name</b> 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	<b>no sync-peers destination destination IP</b> 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。

	コマンドまたはアクション	目的
ステップ 4	<b>exit</b> 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	(任意) <b>show switch-profile</b> 例： switch# show switch-profile	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	(任意) <b>copy running-config startup-config</b> 例： switch# copy running-config startup-config	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

## スイッチ プロファイルバッファの表示

### 手順の概要

1. switch# **configure sync**
2. switch(config-sync) # **switch-profile profile-name**
3. switch(config-sync-sp) # **show switch-profile profile-name buffer**

### 手順の詳細

#### 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure sync</b>	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) # <b>switch-profile profile-name</b>	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) # <b>show switch-profile profile-name buffer</b>	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。

#### 例

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。

## 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

```

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構成をコミット中にCisco Nexus 3600 プラットフォーム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。

## 手順の概要

- 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。
- 次の情報を入力します。 **commit** コマンドを使用します。
- 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。

## 手順の詳細

### 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** 次の情報を入力します。 **commit** コマンドを使用します。

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。

例

## 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
<b>show switch-profile <i>name</i></b>	スイッチ プロファイル中のコマンドを表示します。
<b>show switch-profile <i>name</i> buffer</b>	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。
<b>show switch-profile <i>name</i> peer <i>IP-address</i></b>	ピア スイッチの同期ステータスが表示されます。
<b>show switch-profile <i>name</i> session-history</b>	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。
<b>show switch-profile <i>name</i> status</b>	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。
<b>show running-config exclude-provision</b>	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。
<b>show running-config switch-profile</b>	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。
<b>show startup-config switch-profile</b>	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。

## サポートされているスイッチ プロファイル コマンド

以下のスイッチ プロファイル コマンドがサポートされています。

- **logging event link-status default**
- **[no] vlan *vlan-range***
- **ip access-list *acl-name***
- **policy-map type network-qos jumbo-frames**

## サポートされているスイッチ プロファイルコマンド

- **class type network-qos class-default**
- **mtu mtu value**
- **system qos**
  - **service-policy type network-qos jumbo-frames**
- **vlan configuration vlan id**
  - **ip igmp snooping querier ip**
  - **spanning-tree port type edge default**
  - **spanning-tree port type edge bpduguard default**
  - **spanning-tree loopguard default**
  - **no spanning-tree vlan vlan id**
  - **port-channel load-balance ethernet source-dest-port**
  - **interface port-channel number**
    - **description text**
    - **switchport mode trunk**
    - **switchport trunk allowed vlan vlan list**
    - **spanning-tree port type network**
    - **no negotiate auto**
    - **vpc peer-link**
  - **interface port-channel number**
    - **switchport access vlan vlan id**
    - **spanning-tree port type edge**
    - **speed 10000**
    - **vpc number**
  - **interface ethernetx/y**
    - **switchport access vlan vlanid**
    - **spanning-tree port type edge**
    - **channel-group number mode active**

# 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 スイッチで正常なスイッチ プロファイル構成を作成する例を示します。

### 手順の概要

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。
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。
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。
4. スイッチ プロファイルのコマンドを検証します。
5. 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。

### 手順の詳細

#### 手順

	コマンドまたはアクション	目的
ステップ1	<p>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。</p> <p>例 :</p> <pre>switch# configuration terminal switch(config)# cfs ipv4 distribute</pre>	
ステップ2	<p>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。</p> <p>例 :</p> <pre>switch(config-sync)# switch-profile abc switch(config-sync-sp)# sync-peers destination 10.1.1.1</pre>	
ステップ3	<p>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。</p> <p>例 :</p> <pre>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</pre>	

## 同期ステータスの確認例

	コマンドまたはアクション	目的
	<pre>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):</pre>	
ステップ4	<p>スイッチ プロファイルのコマンドを検証します。</p> <p>例 :</p> <pre>switch(config-sync-sp-if)# <b>verify</b> Verification Successful</pre>	
ステップ5	<p>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。</p> <p>例 :</p> <pre>switch(config-sync-sp)# <b>commit</b> Commit Successful switch(config-sync)#</pre>	

## 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(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:
```

## 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

```
-----  
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

```

## 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

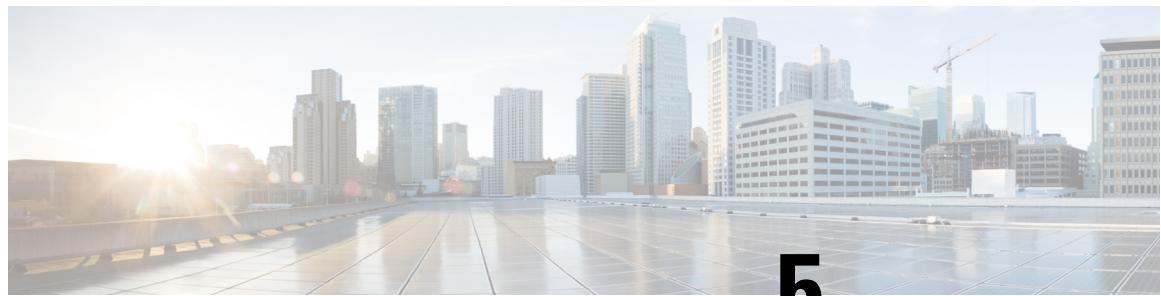
```
switch(config-sync-sp-if)# exit
switch(config-sync-sp)# show switch-profile sp buffer
-----
Seq-no  Command
-----
1      vlan 101
1.1    ip igmp snooping querier 10.101.1.1
2      mac address-table static 0000.0000.0001 vlan 101 drop
3      interface Ethernet1/2
3.1    switchport mode trunk
3.2 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

```



## 第 5 章

# PTP の設定

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

この章は、次の項で構成されています。

- [PTPについて \(45 ページ\)](#)
- [PTPデバイス タイプ \(46 ページ\)](#)
- [PTP 時間分配保留 \(47 ページ\)](#)
- [PTP プロセス \(47 ページ\)](#)
- [PTP のハイ アベイラビリティ \(48 ページ\)](#)
- [PTP の注意事項および制約事項 \(48 ページ\)](#)
- [PTP のデフォルト設定 \(49 ページ\)](#)
- [PTP の設定 \(50 ページ\)](#)

## PTPについて

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

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。サーバーには、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 時間分配保留

適切に同期された PTP ネットワークでは、いずれかの PTP ノードがダウンしてから起動すると、その PTP クロックはプライマリ時刻ソース (GM) に同期されます。このプロセス中に、ローカルノードでかなりの長さの時間修正が行われ、ローカルクロックの修正が試行されます。その際、ノードはダウンストリームノードに誤った時刻を送信し、すべてのダウンストリームノードで問題が発生する可能性があります。Cisco NX-OS リリース 10.5(1)F で導入された時間分配 (TD) 保留機能は、ブートアップ時にノードがプライマリソースに正しく同期されてからダウンストリームノードに時間を分配するようにすることで、この問題を解決します。

TD 保留機能は、境界クロック (BC) ノードがプライマリ時刻ソースにロックされ、ターゲット修正値が確定するまで、時間分配を保留します。TD 保留対応ノードは、すべての PTP パケットを受信し、通常の状態変更を行い、時刻を同期しますが、PTP パケットは送信しません。



(注) すべてのノードが同時に（数秒程度の差で）再起動すると、各ノードがアクティブな保留時間になり、セカンダリポートを持つノードがなくなることがあります。この場合、BMC が最適なクロックを見つけるのに時間がかかります。それで、この機能を有効にする際には、この点を考慮する必要があります。

## PTP プロセス

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

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

- 受信したすべての（マスターステートのポートによって発行された）アナウンスマ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（アナウンスマッセージ内）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。

## ■ PTP のハイ アベイラビリティ

- 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で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。

## PTP のハイ アベイラビリティ

PTP のステートフル リスタートはサポートされません。

## PTP の注意事項および制約事項

- Cisco Nexus 3600 シリーズ スイッチでは、PTP クロック修正は 100 ~ 999 ナノ秒までの 3 枠の範囲に収まることが予想されます。
- 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 はユーザー 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。
- PTP 管理パケットを転送すること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。
- 1 pulse per second (1 PPS) 入力はサポートされていません。
- IPv6 を介した PTP はサポートされていません。
- Cisco Nexus スイッチは、-2 ~ -5 の同期化ログ間隔を使用して、隣接マスターから同期する必要があります。
- Cisco NX-OS リリース 10.5 (1) F 以降では、次の属性が PTP 高補正通知に追加されています。
  - lastHighCorrectionMPD

- maxHighCorrectionTime
- maxHighCorrectionValue
- maxHighCorrectionMPD
- Cisco NX-OS リリース 10.5(1)F 以降では、PTP 時間分配保留機能が導入されています。この機能により、境界クロックノードがプライマリ時刻送信元にロックされ、ターゲット補正値に落ち着くまで、時間分配を保留できます。

## 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	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 アンウンス間隔	1 ログ秒
PTP 同期間隔	-2 ログ秒
PTP アンウンス タイムアウト	3 アンウンス間隔
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 パラメータを構成できます。

### 手順の概要

1. switch# **configure terminal**
2. switch(config) # [no] **feature ptp**
3. switch(config) # [no] **ptp source ip-address [vrf vrf]**  
(任意) switch(config) # [no] **ptp domain number**
5. (任意) switch(config) # [no] **ptp priority1 value**
6. (任意) switch(config) # [no] **ptp priority2 value**
7. (任意) switch(config) # **show ptp brief**
8. (任意) switch(config) # **show ptp clock**
9. (任意) [no] **ptp time distribution-hold [correction-threshold <corr\_limit>] [delay-threshold <max\_delay\_time>]**
10. (任意) switch(config)# **copy running-config startup-config**

### 手順の詳細

#### 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	グローバル コ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] <b>feature ptp</b>	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] <b>ptp source ip-address [vrf vrf]</b>	すべての PTP パケットのソース IP アドレスを構成します。  値は、 <i>ip-address</i> には IPv4 形式を使用できます。
ステップ 4	(任意) switch(config) # [no] <b>ptp domain number</b>	このクロックで使用するドメイン番号を構成します。PTP ドメインを使用すると、1つのネットワー

	コマンドまたはアクション	目的
		ク上で、複数の独立した PTP クロック サブドメインを使用できます。 <i>number</i> の範囲は 0 ~ 128 です。
ステップ 5	(任意) switch(config) # [no] ptp priority1 <i>value</i>	このクロックをアドバタイズするときに使用する priority1 の値を構成します。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。 <i>value</i> の範囲は、0 ~ 255 です。
ステップ 6	(任意) switch(config) # [no] ptp priority2 <i>value</i>	このクロックをアドバタイズするときに使用する priority2 の値を構成します。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。 <i>value</i> の範囲は、0 ~ 255 です。
ステップ 7	(任意) switch(config) # show ptp brief	PTP のステータスを表示します。
ステップ 8	(任意) switch(config) # show ptp clock	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	(任意) [no] ptp time distribution-hold [correction-threshold <corr_limit>] [delay-threshold <max_delay_time>]  例：  switch(config) # ptp time distribution-hold correction-threshold 90000ns delay threshold 4000s	PTP 時間分配保留機能を有効にします。  <b>correction-threshold</b> : 補正が指定された補正值（ナノ秒単位）に落ち着くまで、時間分配を保留します。  <b>delay-threshold</b> : 時間分配を保留する最大時間制限を秒単位で設定します。ただし、遅延しきい値の前に補正しきい値が満たされた場合は、時間分布が再開されます。  デフォルトの補正しきい値は300ナノ秒で、デフォルトの遅延しきい値は、TOR の場合は 300 秒、モジュラ型シャーシの場合は 900 秒です。  最大補正しきい値は 100000 ナノ秒で、最大遅延しきい値は 5000 秒です。
ステップ 10	(任意) switch(config)# 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。

## ■ インターフェイスでの PTP の設定

### 例

次に、デバイス上で PTP をグローバルに構成し、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構成する例を示します。

```
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。

### 始める前に

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

### 手順の概要

1. switch# **configure terminal**
2. switch(config) # **interface ethernet slot/port**
3. switch(config-if) # [no] **feature ptp**
4. (任意) switch(config-if) # [no] **ptp announce {interval log seconds | timeout count}**
5. (任意) switch(config-if) # [no] **ptp delay request minimum interval log seconds**
6. (任意) switch(config-if) # [no] **ptp sync interval log seconds**
7. (任意) switch(config-if) # [no] **ptp vlan vlan-id**

8. (任意) `switch(config-if) # show ptp brief`
9. (任意) `switch(config-if) # show ptp port interface interface slot/port`
10. (任意) `switch(config-if) # copy running-config startup-config`

## 手順の詳細

## 手順

	コマンドまたはアクション	目的
ステップ1	<code>switch# configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>switch(config) # interface ethernet slot/port</code>	PTP をイネーブルにするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ3	<code>switch(config-if) # [no] feature ptp</code>	インターフェイスで PTP をイネーブルまたはディセーブルにします。
ステップ4	(任意) <code>switch(config-if) # [no] ptp announce {interval log seconds   timeout count}</code>	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 間隔の数を構成します。 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	(任意) <code>switch(config-if) # [no] ptp delay request minimum interval log seconds</code>	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構成します。 有効な範囲は -1 ~ -6 ログ秒です。ログ (-2) は、1 秒あたり 4 フレームです。
ステップ6	(任意) <code>switch(config-if) # [no] ptp sync interval log seconds</code>	インターフェイス上の PTP 同期メッセージの送信間隔を構成します。 PTP 同期間隔の範囲は -6 ログ秒 ~ 1 秒です。
ステップ7	(任意) <code>switch(config-if) # [no] ptp vlan vlan-id</code>	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	(任意) <code>switch(config-if) # show ptp brief</code>	PTP のステータスを表示します。
ステップ9	(任意) <code>switch(config-if) # show ptp port interface interface slot/port</code>	PTP ポートのステータスを表示します。

## ■ PTP 設定の確認

	コマンドまたはアクション	目的
ステップ 10	(任意) switch(config-if)# <b>copy running-config startup-config</b>	リブートおよびリスト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。

## 例

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

```
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
<b>show ptp brief</b>	PTP のステータスを表示します。
<b>show ptp clock</b>	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
<b>show ptp clock foreign-masters-record</b>	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。
<b>show ptp corrections</b>	最後の数個の PTP 修正を表示します。
<b>show ptp parent</b>	PTP の親のプロパティを表示します。
<b>show ptp port interface ethernet slot/port</b>	スイッチの PTP ポートのステータスを表示します。

## ■ PTP 設定の確認



## 第 6 章

# NTP の設定

この章は、次の内容で構成されています。

- NTP の概要 (57 ページ)
- タイム サーバーとしての NTP (58 ページ)
- CFS を使用した NTP の配信 (58 ページ)
- クロック マネージャ (58 ページ)
- 高可用性 (59 ページ)
- 仮想化のサポート (59 ページ)
- NTP の前提条件 (59 ページ)
- NTP の注意事項と制約事項 (59 ページ)
- デフォルト設定 (60 ページ)
- NTP の設定 (61 ページ)
- NTP の設定確認 (77 ページ)
- NTP の設定例 (78 ページ)

## NTP の概要

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

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

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

- ストラタム 1 のタイム サーバは、信頼できる時刻源に直接接続されます（無線時計や原子時計または GPS 時刻源など）。

## ■ タイム サーバーとしての NTP

- 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 サーバーとしての 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 などの複数の時刻同期プロトコルが、システムで稼働している可能性があります。

## 高可用性

NTP はステートレスリスタートをサポートします。リブート後またはスーパーバイザスイッチオーバー後に、実行コンフィギュレーションが適用されます。

NTP ピアを設定すると、NTP サーバ障害の発生時に冗長性が得られます。

## 仮想化のサポート

NTP は Virtual Routing and Forwarding (VRF) インスタンスを認識します。NTP サーバおよび NTP ピアに対して特定の VRF を設定していない場合、NTP はデフォルトの VRF を使用します。

## 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。

- 値は、**show ntp session status** CLI コマンドには、最後のアクションのタイムスタンプ、最後のアクション、最後のアクションの結果、および最後のアクションの失敗理由は表示されません。
- NTP サーバ機能はサポートされます。
- 別のデバイスとの間にピアアソシエーションを設定できるのは、使用するクロックの信頼性が確実な場合（つまり、信頼できる NTP サーバー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。
- サーバーが 1 台だけの場合は、すべてのデバイスをそのサーバー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（サーバーおよびピア）は、最大 64 です。

## ■ デフォルト設定

- 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入れません。
- NTP に対して CFS 配信を有効にしても、**commit** コマンドを入力するまで、NTP 構成コマンドのエントリは NTP 構成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 サーバーおよびピアが、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 サーバーおよび 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。
- 1 つの NTP アクセス グループに最大 4 つの ACL を設定できます。



(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。

## デフォルト設定

次に、NTP パラメータのデフォルト設定を示します。

パラメータ	デフォルト
NTP	すべてのインターフェイスでイネーブル
NTP passive（アソシエーションを形成するために NTP をイネーブルにする）	イネーブル
NTP 認証	ディセーブル
NTP アクセス	イネーブル
NTP access group match all	ディセーブル
NTP ブロードキャスト サーバー	ディセーブル

パラメータ	デフォルト
NTP マルチキャスト サーバ	ディセーブル
NTP マルチキャスト クライアント	ディセーブル
NTP ロギング	無効化

## NTP の設定

### インターフェイスでの NTP のイネーブル化またはディセーブル化

特定のインターフェイスで NTP をイネーブルまたはディセーブルにできます。NTP は、すべてのインターフェイスでデフォルトでイネーブルに設定されています。

#### 手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface type slot/port**
3. switch(config-if)# **[no] ntp disable {ip | ipv6}**
4. (任意) switch(config)# **copy running-config startup-config**

#### 手順の詳細

##### 手順

	コマンドまたはアクション	目的
ステップ1	switch# <b>configure terminal</b>	グローバル コ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)# <b>interface type slot/port</b>	インターフェイス設定 モードを開始します。
ステップ3	switch(config-if)# <b>[no] ntp disable {ip   ipv6}</b>	指定のインターフェイスで NTP IPv4 または IPv6 をディセーブルにします。 インターフェイス上で NTP を再度有効にするにはこのコマンドの <b>no</b> 形式を使用します。
ステップ4	(任意) switch(config)# <b>copy running-config startup-config</b>	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。

## 正規の NTP サーバとしてのデバイスの設定

### 例

次に、インターフェイスで NTP を有効化または無効化する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 6/1
switch(config-if)# ntp disable ip
switch(config-if)# copy running-config startup-config
```

## 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 サーバーとして動作するよう設定し、既存のタイム サーバー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。

### 手順の概要

1. switch# **configure terminal**
2. [no] **ntp master [stratum]**
3. (任意) **show running-config ntp**
4. (任意) switch(config)# **copy running-config startup-config**

### 手順の詳細

#### 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	グローバルコ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] <b>ntp master [stratum]</b>	正規の NTP サーバとしてデバイスを設定します。 NTP クライアントがこれらの時間を同期するのと別の階層レベルを指定できます。指定できる範囲は 1 ~ 15 です。
ステップ 3	(任意) <b>show running-config ntp</b>	NTP コンフィギュレーションを表示します。
ステップ 4	(任意) switch(config)# <b>copy running-config startup-config</b>	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。

### 例

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 サーバーおよびピアの設定

NTP サーバおよびピアを設定できます。

### 始める前に

NTP サーバーとそのピアの 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。

### 手順の概要

1. switch# **configure terminal**
2. switch(config)# [no] **ntp server** {ip-address | ipv6-address | dns-name} [key key-id] [**maxpoll max-poll**] [**minpoll min-poll**] [**prefer**] [**use-vrf vrf-name**]
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**]
4. (任意) switch(config)# **show ntp peers**
5. (任意) switch(config)# **copy running-config startup-config**

### 手順の詳細

#### 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	グローバル コ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] <b>ntp server</b> {ip-address   ipv6-address   dns-name} [key key-id] [ <b>maxpoll max-poll</b> ] [ <b>minpoll min-poll</b> ] [ <b>prefer</b> ] [ <b>use-vrf vrf-name</b> ]	<p>1 つのサーバと 1 つのサーバアソシエーションを形成します。</p> <p><b>key</b> キーワードを使用して、NTP サーバーとの通信で使用するキーを構成します。</p> <p><b>key-id</b> 引数の範囲は、1 ~ 65535 です。</p> <p><b>maxpoll</b> および <b>minpoll</b> キーワードを使用して、サーバーをポーリングする最長と最短間隔を構成します。 <b>maxpoll</b> および <b>minpoll</b> (2 の累乗として構成されます。つまり、実質的に 16 ~ 65536 秒) そして、デフォルト値はそれぞれ 6 と 4 です。 (<b>maxpoll</b> デフォルト = 64 秒、<b>minpoll</b> デフォルト : 16 秒)。</p> <p><b>prefer keyword</b> を使用して、デバイスに対して対象の NTP サーバーを優先サーバーにします。</p>

## ■ NTP サーバーおよびピアの設定

	コマンドまたはアクション	目的
		<p><b>use-vrf</b> キーワードを使用して、指定された VRF を介して通信するように NTP サーバを設定します。</p> <p><i>vrf-name</i> 引数として、デフォルト、管理、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。</p> <p>(注) NTP サーバとの通信で使用するキーを設定する場合は、そのキーが、デバイス上の信頼できるキーとして存在していることを確認してください。</p>
ステップ 3	switch(config)# [no] <b>ntp peer</b> {ip-address   ipv6-address   dns-name} [key key-id] [ <b>maxpoll</b> max-poll] [ <b>minpoll</b> min-poll] [ <b>prefer</b> ] [ <b>use-vrf</b> vrf-name]	<p>1 つのピアと 1 つのピア アソシエーションを形成します。複数のピア アソシエーションを指定できます。</p> <p><b>key</b> キーワードを使用して、NTP ピアとの通信で使用するキーを設定します。 <i>key-id</i> 引数の範囲は、1 ~ 65535 です。</p> <p><b>maxpoll</b> および <b>minpoll</b> キーワードを使用して、サーバーをポーリングする最長と最短間隔を構成します。 <i>maxpoll</i> および <i>minpoll</i> 引数の範囲は 4 ~ 17 (2 の累乗として構成されます。つまり、実質的に 16 ~ 131072 秒) で、デフォルト値はそれぞれ 6 と 4 です (<i>maxpoll</i> デフォルト = 64 秒、<i>minpoll</i> デフォルト = 16 秒)。<i>maxpoll</i> デフォルト = 64 秒、<i>minpoll</i> デフォルト : 16 秒)。</p> <p><b>prefer</b> キーワードを使用して、デバイスに対して対象の NTP ピアを優先します。</p> <p><b>use-vrf</b> キーワードを使用して、指定された VRF を介して通信するように NTP ピアを設定します。</p> <p><i>vrf-name</i> 引数に <b>default</b>、<b>management</b>、または、32 文字以内の英数字のストリング (大文字と小文字を区別) で指定します。</p>
ステップ 4	(任意) switch(config)# <b>show ntp peers</b>	<p>設定されたサーバーおよびピアを表示します。</p> <p>(注) ドメイン名が解決されるのは、DNS サーバが設定されている場合だけです。</p>
ステップ 5	(任意) switch(config)# <b>copy running-config startup-config</b>	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 認証を有効にすると、**ntp trusted-key** 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。デバイスは、認証チェックに失敗したすべてのパケットをドロップし、それらのパケットでローカルクロックがアップデートされないようにします。NTP 認証はデフォルトでディセーブルになっています。

### 始める前に

NTP サーバーと NTP ピアの認証は、**key** キーワードを各 **ntp server** および、**ntp peer** 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送信元が保持している場合のみ、デバイスはその時刻送信元と同期します。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 サーバー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。任意 **ntp server** または **ntp peer** を指定しないコマンド **key** キーワードを指定しない場合、認証なしでの動作が続けられます。

### 手順の概要

1. switch# **configure terminal**
2. switch(config)# [no] **ntp authentication-key** *number* **md5** *md5-string*
3. (任意) switch(config)# **show ntp authentication-keys**
4. switch(config)# [no] **ntp trusted-key** *number*
5. (任意) switch(config)# **show ntp trusted-keys**
6. switch(config)# [no] **ntp authenticate**
7. (任意) switch(config)# **show ntp authentication-status**
8. (任意) switch(config)# **copy running-config startup-config**

### 手順の詳細

#### 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	グローバル コ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] <b>ntp authentication-key</b> <i>number</i> <b>md5</b> <i>md5-string</i>	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、 <b>ntp trusted-key</b> <i>number</i> 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	(任意) switch(config)# <b>show ntp authentication-keys</b>	設定済みの NTP 認証キーを表示します。
ステップ 4	switch(config)# [no] <b>ntp trusted-key</b> <i>number</i>	1つ以上のキー (ステップ 2 で定義されているもの) を指定します。デバイスを時刻源と同期させるには、未設定のリモート シンメトリック、ブロード

## ■ NTP アクセス制限の設定

	コマンドまたはアクション	目的
		<p>キャスト、およびマルチキャストの時刻源をNTP パケット内に入力する必要があります。trusted key の範囲は 1 ~ 65535 です。</p> <p>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。</p> <p>このコマンドは <b>ntp server</b> および、<b>ntp peer</b> 構成コメントで構成された時刻源には影響しません。</p>
ステップ 5	(任意) switch(config)# <b>show ntp trusted-keys</b>	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] <b>ntp authenticate</b>	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	(任意) switch(config)# <b>show ntp authentication-status</b>	NTP 認証の状況を表示します。
ステップ 8	(任意) switch(config)# <b>copy running-config startup-config</b>	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。

## 例

次に、NTP パケット内で認証キー 42 を提示している時刻源とだけ同期するようデバイスを設定する例を示します。

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ntp authentication-key 42 md5 aNiceKey
switch(config)# ntp server 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、デバイスで許可する要求のタイプ、およびデバイスが応答を受け取るサーバを指定できます。

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

## 手順の概要

1. switch# **configure terminal**
2. switch(config)# [no] **ntp access-group match-all | {{peer | serve | serve-only | query-only }access-list-name}**
3. switch(config)# **show ntp access-groups**
4. (任意) switch(config)# **copy running-config startup-config**

## 手順の詳細

## 手順

	コマンドまたはアクション	目的
ステップ1	switch# <b>configure terminal</b>	グローバル コ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] <b>ntp access-group match-all   {{peer   serve   serve-only   query-only }access-list-name}</b>	<p>NTP のアクセスを制御し、基本の IP アクセス リストを適用するためのアクセス グループを作成または削除します。</p> <p>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。</p> <ul style="list-style-type: none"> <li>• 値は、<b>peer</b> 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。</li> <li>• 値は、<b>サーバよりも</b> 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。</li> <li>• 値は、<b>serve-only</b> 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。</li> <li>• 値は、<b>query-only</b> 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。</li> <li>• 値は、<b>match-all</b> キーワードを使用すると、アクセス グループ オプションが、制限の最も緩いものから最も厳しいもの、<b>peer</b>、<b>serve</b>、</li> </ul>

## ■ NTP ソース IP アドレスの設定

	コマンドまたはアクション	目的
		serve-only、query-only の順序でスキャンする ようにできます。着信パケットが peer アクセス グループの ACL に一致しない場合、パケット は serve アクセス グループに送信され、処理さ れます。パケットが serve アクセス グループの ACL に一致しない場合、serve-only アクセス グ ループに送られ、これが継続されます。
ステップ 3	switch(config)# <b>show ntp access-groups</b>	(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	(任意) switch(config)# <b>copy running-config startup-config</b>	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。

## 例

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。

## 手順の概要

1. switch# **configure terminal**
2. [no] **ntp source ip-address**

## 手順の詳細

## 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	グローバル コ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] <b>ntp source ip-address</b>	すべての NTP パケットにソース IP アドレスを設定します。値は、 <i>ip-address</i> には IPv4 または IPv6 形式を使用できます。

## 例

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。

## 手順の概要

1. switch# **configure terminal**
2. [no] **ntp source-interface interface**

## 手順の詳細

## 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	グローバル コ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] <b>ntp source-interface interface</b>	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。次のリストには、 <i>interface</i> の有効な値が含まれます。 <ul style="list-style-type: none"> <li>• ethernet</li> <li>• loopback</li> <li>• mgmt</li> <li>• port-channel</li> </ul>

## ■ NTP ブロードキャストサーバーの設定

コマンドまたはアクション	目的
	• vlan

## 例

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 ブロードキャストサーバーの設定

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

## 手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface type slot/port**
3. switch(config-if)# [no] **ntp broadcast [destination ip-address] [key key-id] [version number]**
4. switch(config-if)# **exit**
5. (任意) switch(config)# [no] **ntp broadcastdelay delay**
6. (任意) switch(config)# **copy running-config startup-config**

## 手順の詳細

## 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	グローバルコ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)# <b>interface type slot/port</b>	インターフェイス設定モードを開始します。
ステップ 3	switch(config-if)# [no] <b>ntp broadcast [destination ip-address] [key key-id] [version number]</b>	<p>指定されたインターフェイスの IPv4 NTP ブロードキャストサーバをイネーブルにします。</p> <ul style="list-style-type: none"> <li>• <b>destination ip-address</b>—ブロードキャスト宛先 IP アドレスを構成します。</li> <li>• <b>key key-id</b>—ブロードキャスト認証キー番号を構成します。有効な範囲は 1 ~ 65535 です。</li> </ul>

	コマンドまたはアクション	目的
		• <i>version number</i> —NTP バージョンを構成します。範囲は 2 ~ 4 です。
ステップ 4	switch(config-if)# <b>exit</b>	インターフェイス コンフィギュレーション モードを終了します。
ステップ 5	(任意) switch(config)# [no] <b>ntp broadcastdelay</b> <i>delay</i>	推定のブロードキャストラウンドトリップ遅延をマイクロ秒単位で設定します。範囲は 1 ~ 999999 です。
ステップ 6	(任意) switch(config)# <b>copy running-config startup-config</b>	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。

### 例

次に、NTP ブロードキャスト サーバーを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 6/1
switch(config-if)# ntp broadcast destination 192.0.2.10
switch(config-if)# exit
switch(config)# ntp broadcastdelay 100
switch(config)# copy running-config startup-config
```

## NTP マルチキャスト サーバーの設定

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

### 手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface type slot/port**
3. switch(config-if)# [no] **ntp multicast** [*ipv4-address* | *ipv6-address*] [**key** *key-id*] [**ttl** *value*] [**version** *number*]
4. (任意) switch(config-if)# **copy running-config startup-config**

### 手順の詳細

#### 手順

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

## NTP マルチキャスト クライアントの設定

	コマンドまたはアクション	目的
ステップ 2	switch(config)# <b>interface type slot/port</b>	インターフェイス設定モードを開始します。
ステップ 3	switch(config-if)# [no] <b>ntp multicast [ipv4-address   ipv6-address] [key key-id] [ttl value] [version number]</b>	<p>指定したインターフェイスの NTP IPv4 または IPv6 マルチキャスト サーバーをイネーブルにします。</p> <ul style="list-style-type: none"> <li>• <i>ipv4-address</i> または、<i>ipv6-address</i>—マルチキャスト IPv4 または IPv6 アドレス。</li> <li>• <b>key key-id</b>—ブロードキャスト認証キー番号を構成します。有効な範囲は 1 ~ 65535 です。</li> <li>• <b>ttl value</b>—マルチキャストパケットの存続可能時間値。範囲は 1 ~ 255 です。</li> <li>• <b>version number</b>—NTP バージョン。範囲は 2 ~ 4 です。</li> </ul>
ステップ 4	(任意) switch(config-if)# <b>copy running-config startup-config</b>	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。

## 例

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

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

## NTP マルチキャスト クライアントの設定

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

### 手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface type slot/port**
3. switch(config-if)# [no] **ntp multicast client [ipv4-address | ipv6-address]**
4. (任意) switch(config-if)# **copy running-config startup-config**

## 手順の詳細

## 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	グローバル コ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)# <b>interface type slot/port</b>	インターフェイス設定 モードを開始します。
ステップ 3	switch(config-if)# [no] <b>ntp multicast client [ipv4-address   ipv6-address]</b>	指定されたインターフェイスが NTP マルチキャスト パケットを受信できるようにします。
ステップ 4	(任意) switch(config-if)# <b>copy running-config startup-config</b>	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。

## 例

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

```
switch# configure terminal
switch(config)# interface ethernet 2/3
switch(config-if)# ntp multicast client FF02::1:FF0E:8C6C
switch(config-if)# copy running-config startup-config
```

## NTP ロギングの設定

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

## 始める前に

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。

## 手順の概要

1. switch# **configure terminal**
2. switch(config)# [no] **ntp logging**
3. (任意) switch(config)# **show ntp logging-status**
4. (任意) switch(config)# **copy running-config startup-config**

## NTP 用の CFS 配信のイネーブル化

### 手順の詳細

#### 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	グローバルコ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] <b>ntp logging</b>	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	(任意) switch(config)# <b>show ntp logging-status</b>	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	(任意) switch(config)# <b>copy running-config startup-config</b>	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。

#### 例

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。

#### 始める前に

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。

### 手順の概要

1. switch# **configure terminal**
2. switch(config)# [no] **ntp distribute**
3. (任意) switch(config)# **show ntp status**
4. (任意) switch(config)# **copy running-config startup-config**

## 手順の詳細

## 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	グローバル コ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] <b>ntp distribute</b>	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	(任意) switch(config)# <b>show ntp status</b>	NTP CFS の配信状況を表示します。
ステップ 4	(任意) switch(config)# <b>copy running-config startup-config</b>	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。

## 例

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。

## 手順の概要

1. switch# **configure terminal**
2. switch(config)# **ntp commit**

## 手順の詳細

## 手順

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

## ■ NTP 設定変更の廃棄

	コマンドまたはアクション	目的
ステップ 2	switch(config)# <b>ntp commit</b>	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。

### 手順の概要

1. switch# **configure terminal**
2. switch(config)# **ntp abort**

### 手順の詳細

#### 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	グローバル コ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)# <b>ntp abort</b>	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。

### 手順の概要

1. switch# **configure terminal**
2. switch(config)# **clear ntp session**

## 手順の詳細

## 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	グローバル コ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)# <b>clear ntp session</b>	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
<b>show ntp access-groups</b>	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。
<b>show ntp authentication-keys</b>	設定済みの NTP 認証キーを表示します。
<b>show ntp authentication-status</b>	NTP 認証の状況を表示します。
<b>show ntp logging-status</b>	NTP のロギング状況を表示します。
<b>show ntp peer-status</b>	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。
<b>show ntp peer</b>	すべての NTP ピアを表示します。
<b>show ntp pending</b>	NTP 用の一時 CFS データベースを表示します。
<b>show ntp pending-diff</b>	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。
<b>show ntp rts-update</b>	RTS アップデートの状況を表示します。
<b>show ntp session status</b>	NTP CFS 配信セッションの情報を表示します。
<b>show ntp source</b>	設定済みの NTP ソース IP アドレスを表示します。
<b>show ntp source-interface</b>	設定済みの NTP ソースインターフェイスを表示します。
<b>show ntp statistics {io   local   memory   peer {ipaddr {ipv4-addr}   name peer-name}}</b>	NTP 統計情報を表示します。

## ■ NTP の設定例

コマンド	目的
<b>show ntp status</b>	NTP CFS の配信状況を表示します。
<b>show ntp trusted-keys</b>	設定済みの NTP の信頼されているキーを表示します。
<b>show running-config ntp</b>	NTP 情報を表示します。

## NTP の設定例

### NTP の設定例

次に、NTP サーバー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
```

## ■ NTP の設定例



## 第 7 章

# システムメッセージロギングの設定

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

この章は、次の内容で構成されています。

- システム メッセージ ロギングの詳細, [on page 81](#)
- 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 ([83 ページ](#))
- システム メッセージ ロギングのデフォルト設定, [on page 84](#)
- システム メッセージ ロギングの設定 ([84 ページ](#))
- システム メッセージ ロギングの設定確認, [on page 102](#)
- システム メッセージ ロギングの設定例 ([102 ページ](#))
- その他の参考資料 ([103 ページ](#))

## システム メッセージ ロギングの詳細

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

システム メッセージの形式およびデバイスが生成するメッセージの詳細については、『Cisco NX-OS System Messages Reference』を参照してください。

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

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

**Table 4:** 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

## Syslogサーバ

レベル	説明
2 : クリティカル	クリティカル状態
3 : エラー	エラー状態
4 : 警告	警告状態
5 : 通知	正常だが注意を要する状態
6 : 情報	単なる情報メッセージ
7 : デバッグ	デバッグ実行時にのみ表示

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

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

## Syslogサーバ

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

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



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

## セキュアな Syslog サーバ

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

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

# システムメッセージロギングの注意事項および制約事項

システムメッセージロギングには次の設定上の注意事項と制約事項があります。

- システムメッセージは、デフォルトでコンソールおよびログファイルに記録されます。
- syslog サーバに到達する前に出力されるシステムメッセージ（スーパーバイザアクティブメッセージやオンラインメッセージなど）は、syslog サーバに送信できません。
- Cisco では、すべてのプロセスのログ レベルをデフォルトのまま維持することを推奨しています。レベルを上げて高い値に設定すると、お客様向けではないsyslogメッセージが表示される可能性があります。これらのメッセージは、誤ったアラームを生成する可能性があり、通常は TAC による短期的なトラブルシューティングの目的で使用されます。Cisco では、デフォルトよりも上のレベルのsyslogメッセージをサポートしていません。
- Syslog の制限により、securePOAP pem ファイル名の文字長は 230 文字に制限されていますが、セキュア POAP は pem ファイル名として 256 文字の長さをサポートしています。
- Cisco NX-OS リリース 9.2(1) 以降では、リモート ロギング サーバへのセキュアな TLS トランスポート接続をサポートするように Syslog サーバを設定できます。この機能は、TLS v1.1 および TLS v1.2 をサポートします。
- Cisco NX-OS リリース 10.4(3)F 以降、TLS v1.2 と TLS v1.3 だけが Cisco Nexus 9000 シリーズ プラットフォームスイッチでサポートされています。syslog の TLS v1.1 および TLS v1.0 のサポートは廃止されました。
- セキュアなsyslogサーバがインバンド（非管理）インターフェイスを介して到達できるようにするには、CoPP プロファイルに調整が必要な場合があります。特に、複数のロギングサーバが設定されている場合、および短時間で多数のsyslogが生成される場合（ブートアップや設定アプリケーションなど）。
- 通常、syslog にはローカルタイムゾーンが表示されます。ただし、NGINXなどの一部のコンポーネントでは、ログが UTC タイムゾーンで表示されます。
- Cisco NX-OS リリース 10.3 (4a) 以降では、syslog プロトコル RFC 5424 を有効にする既存の **logging rfc-strict 5424** コマンド（オプション）が、次のように新しいキーワード（**full**）を追加することで拡張されています。

## **logging rfc-strict 5424 full**

このキーワードを追加すると、Syslog プロトコルの RFC 5424 標準に完全に準拠します。ただし、[APP-NAME] [PROCID] [MSG-ID] [STRUCTRED-DATA] フィールドの値が利用可能ではない場合、nil 値はダッシュで示されます (-)。

- Cisco NX-OS リリース 10.5 (3) 以降では、syslog プロトコル RFC 5424 を有効にする既存の **logging rfc-strict 5424** コマンド（オプション）が、次のように新しいキーワード（**utc**）を追加することで拡張されています。

## **logging rfc-strict 5424 utc**

## ■ システムメッセージロギングのデフォルト設定

このキーワードを追加すると、UTC 時刻フォーマット付きの Syslog プロトコルの RFC 5424 標準を有効にします。

次のコマンドを使用して、Syslog プロトコルの RFC 5424 標準に UTC 時間形式で完全に準拠することもできます：**logging rfc-strict 5424 utc full**を使用してカスタムログファイルを再構成する必要があります。

## 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。

**Table 5: デフォルトのシステムメッセージロギングパラメータ**

パラメータ	デフォルト
コンソールロギング	重大度 2 でイネーブル
モニタロギング	重大度 5 でイネーブル
ログファイルロギング	重大度 5 のメッセージロギングがイネーブル
モジュールロギング	重大度 5 でイネーブル
ファシリティロギング	イネーブル
タイムスタンプ単位	秒
Syslog サーバロギング	ディセーブル
Syslog サーバ設定の配布	無効化

## システムメッセージロギングの設定



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

## ターミナルセッションへのシステムメッセージロギングの設定

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

デフォルトでは、ターミナルセッションでロギングはイネーブルです。

**Note**

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

**SUMMARY STEPS**

1. **terminal monitor**
2. **configure terminal**
3. **[no] logging console [severity-level]**
4. (Optional) **show logging console**
5. **[no] logging monitor [severity-level]**
6. (Optional) **show logging monitor**
7. **[no] logging message interface type ethernet description**
8. (Optional) **copy running-config startup-config**

**DETAILED STEPS****Procedure**

	<b>Command or Action</b>	<b>Purpose</b>
ステップ1	<b>terminal monitor</b>  <b>Example:</b> switch# terminal monitor	デバイスがコンソールにメッセージを記録できるようになります。
ステップ2	<b>configure terminal</b>  <b>Example:</b> 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	<b>[no] logging console [severity-level]</b>  <b>Example:</b> switch(config)# logging console 3	指定された重大度とそれより上位の重大度のメッセージをコンソールセッションに記録するように、デバイスを設定します。小さい値は、より高い重大度を示します。重大度は0～7の範囲です。 <ul style="list-style-type: none"> <li>• 0 : 緊急</li> <li>• 1 : アラート</li> <li>• 2 : クリティカル</li> <li>• 3 : エラー</li> <li>• 4 : 警告</li> <li>• 5 : 通知</li> </ul>

## 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

	Command or Action	Purpose
		<ul style="list-style-type: none"> <li>6: 情報</li> <li>7: デバッグ</li> </ul> <p>重大度が指定されていない場合、デフォルトの 2 が使用されます。 <b>no</b> オプションは、メッセージをコンソールにログするデバイスの機能を無効化します。</p>
ステップ 4	<p>(Optional) <b>show logging console</b></p> <p><b>Example:</b></p> <pre>switch(config)# show logging console</pre>	コンソールロギング設定を表示します。
ステップ 5	<p><b>[no] logging monitor [severity-level]</b></p> <p><b>Example:</b></p> <pre>switch(config)# logging monitor 3</pre>	<p>デバイスが指定された重大度とそれより上位の重大度のメッセージをモニタに記録できるようにします。 小さい値は、より高い重大度を示します。 重大度は 0 ~ 7 の範囲です。</p> <ul style="list-style-type: none"> <li>0: 緊急</li> <li>1: アラート</li> <li>2: クリティカル</li> <li>3: エラー</li> <li>4: 警告</li> <li>5: 通知</li> <li>6: 情報</li> <li>7: デバッグ</li> </ul> <p>設定は Telnet および SSH セッションに適用されます。</p> <p>重大度が指定されていない場合、デフォルトの 2 が使用されます。 <b>no</b> オプションは、メッセージを Telnet および SSH セッションにログするデバイスの機能を無効化にします。</p>
ステップ 6	<p>(Optional) <b>show logging monitor</b></p> <p><b>Example:</b></p> <pre>switch(config)# show logging monitor</pre>	モニタロギング設定を表示します。
ステップ 7	<p><b>[no] logging message interface type ethernet description</b></p> <p><b>Example:</b></p>	システムメッセージログ内で、物理的なイーサネットインターフェイスおよびサブインターフェイスに対して説明を追加できるようにします。 この説明

	<b>Command or Action</b>	<b>Purpose</b>
	switch(config)# logging message interface type ethernet description	は、インターフェイスで設定された説明と同じものです。 <b>no</b> オプションは、物理イーサネットインターフェイスのシステムメッセージログ内のインターフェイス説明の印刷を無効化します。
<b>ステップ 8</b>	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

## Syslog メッセージの送信元 ID の設定

リモート syslog サーバに送信される syslog メッセージにホスト名、IP アドレス、またはテキスト文字列を付加するように Cisco NX-OS を設定できます。

### 手順の概要

- configure terminal**
- logging origin-id {hostname | ip ip-address | string text-string}**
- (任意) **show logging origin-id**
- (任意) **copy running-config startup-config**

### 手順の詳細

#### 手順

	コマンドまたはアクション	目的
<b>ステップ 1</b>	<b>configure terminal</b>  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
<b>ステップ 2</b>	必須: <b>logging origin-id {hostname   ip ip-address   string text-string}</b>  例：  switch(config)# logging origin-id string n9k-switch-abc	リモート syslog サーバに送信される syslog メッセージに追加するホスト名、IP アドレス、またはテキスト文字列を指定します。
<b>ステップ 3</b>	(任意) <b>show logging origin-id</b>  例：  switch(config)# show logging origin-id Logging origin_id : enabled (string: n9k-switch-abc)	リモート syslog サーバに送信される syslog メッセージに付加される、設定済みのホスト名、IP アドレス、またはテキスト文字列を表示します。

## ■ ファイルへのシステム メッセージの記録

	コマンドまたはアクション	目的
ステップ 4	(任意) <b>copy running-config startup-config</b> 例： switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

## ファイルへのシステム メッセージの記録

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

## 手順の概要

1. **configure terminal**
2. [ no ] **logging logfile logfile-name severity-level [ | size bytes ]**
3. **logging event {link-status | trunk-status} {enable | default}**
4. (任意) **show logging info**
5. (任意) **copy running-config startup-config**

## 手順の詳細

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： switch# configure terminal switch(config) #	グローバル コンフィギュレーション モードを開始します
ステップ 2	[ no ] <b>logging logfile logfile-name severity-level [   size bytes ]</b> 例： switch(config)# logging logfile my_log 6	非永続性 ログ ファイル パラメータを構成します。 <i>logfile-name</i> : システム メッセージの保存に使用するログ ファイルの名前を構成します。デフォルトのファイル名は「message」です。 <i>severity-level</i> : ログに記録する最小の重大度 レベルを構成します。小さい値は、より高い重大度を示します。デフォルトは 5 です。範囲は 0 ~ 7 です。 <ul style="list-style-type: none"><li>• 0 : 緊急</li><li>• 1 : アラート</li><li>• 2 : クリティカル</li><li>• 3 : エラー</li></ul>

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>• 4 : 警告</li> <li>• 5 : 通知</li> <li>• 6 : 情報</li> <li>• 7 : デバッグ</li> </ul> <p><b>size bytes</b> : オプションとして、最大ファイルサイズを指定します。範囲は4096～4194304バイトです。</p>
ステップ3	<b>logging event {link-status   trunk-status} {enable   default}</b> 例： <pre>switch(config)# logging event link-status default</pre>	インターフェイスイベントをロギングします。 <ul style="list-style-type: none"> <li>• <b>link-status</b> : すべての UP/DOWN メッセージおよびCHANGE メッセージをログに記録します。</li> <li>• <b>trunk-status</b> : すべてのトランクステータスマッセージをロギングします。</li> <li>• <b>enable</b> : ポートレベルのコンフィギュレーションを上書きしてロギングをイネーブルにするよう、指定します。</li> <li>• <b>default</b> : ロギングが明示的に設定されてないインターフェイスで、デフォルトのロギング設定を使用するよう、指定します。</li> </ul>
ステップ4	(任意) <b>show logging info</b> 例： <pre>switch(config)# show logging info</pre>	ロギング設定を表示します。
ステップ5	(任意) <b>copy running-config startup-config</b> 例： <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

## モジュールおよびファシリティ メッセージのロギングの設定

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

### SUMMARY STEPS

1. **configure terminal**
2. **[no] logging module [severity-level]**
3. (Optional) **show logging module**
4. **[no] logging level facility severity-level**

## ■ 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

5. (Optional) **show logging level [facility]**
6. (Optional) [no] **logging level ethpm**
7. [no] **logging timestamp {microseconds | milliseconds | seconds}**
8. (Optional) **show logging timestamp**
9. (Optional) **copy running-config startup-config**

## DETAILED STEPS

## Procedure

	<b>Command or Action</b>	<b>Purpose</b>
ステップ 1	<b>configure terminal</b>  <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	グローバルコンフィギュレーション モードを開始します
ステップ 2	<b>[no] logging module [severity-level]</b>  <b>Example:</b> <pre>switch(config)# logging module 3</pre>	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。 <ul style="list-style-type: none"> <li>• 0 : 緊急</li> <li>• 1 : アラート</li> <li>• 2 : クリティカル</li> <li>• 3 : エラー</li> <li>• 4 : 警告</li> <li>• 5 : 通知</li> <li>• 6 : 情報</li> <li>• 7 : デバッグ</li> </ul> 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。値は、 <b>no</b> オプションを使用すると、モジュール ログ メッセージが無効化になります。
ステップ 3	(Optional) <b>show logging module</b>  <b>Example:</b> <pre>switch(config)# show logging module</pre>	モジュール ロギング設定を表示します。
ステップ 4	<b>[no] logging level facility severity-level</b>  <b>Example:</b> <pre>switch(config)# logging level aaa 2</pre>	指定された重大度またはそれ以上の重大度である指定のファシリティからのロギング メッセージをイネーブルにします。重大度は 0 ~ 7 の範囲です。 <ul style="list-style-type: none"> <li>• 0 : 緊急</li> </ul>

	Command or Action	Purpose
		<ul style="list-style-type: none"> <li>• 1 : アラート</li> <li>• 2 : クリティカル</li> <li>• 3 : エラー</li> <li>• 4 : 警告</li> <li>• 5 : 通知</li> <li>• 6 : 情報</li> <li>• 7 : デバッグ</li> </ul> <p>同じ重大度をすべてのファシリティに適用するには、<b>all</b> ファシリティを使用します。デフォルトについては、<b>show logging level</b> コマンドを参照してください。</p> <p>次に、<b>no</b> オプションを使用すると、指定されたファシリティのロギング重大度がデフォルトのレベルにリセットされます。ファシリティおよび重大度を指定しなかった場合、すべてのファシリティがそれぞれのデフォルト重大度にリセットされます。</p>
ステップ 5	<p>(Optional) <b>show logging level [facility]</b></p> <p><b>Example:</b></p> <pre>switch(config)# show logging level aaa</pre>	<p>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ルベルを表示します。ファシリティを指定しなかった場合は、すべてのファシリティのレベルが表示されます。</p> <p><b>Note</b> 実行構成での authpriv のロギングレベルは、10.4(3)F より前のリリースでは authpri として表示され、リリース 10.4(3)F からは authpriv として表示されます。</p>
ステップ 6	<p>(Optional) <b>[no] logging level ethpm</b></p> <p><b>Example:</b></p> <pre>switch(config)# logging level ethpm ? &lt;0-7&gt; 0-emerg;1-alert;2-crit;3-err;4-warn;5-notif;6-inform;7-debug link-down  Configure logging level for link down syslog messages link-up    Configure logging level for link up syslog messages switch(config)#logging level ethpm link-down ?</pre>	<p>レベル 3 のイーサネット ポート マネージャ リンクアップ/リンクダウン syslog メッセージのロギングを有効にします。</p> <p><b>no</b> オプションを使用すると、イーサネット ポート マネージャの syslog メッセージにデフォルトのロギング レベルが使用されます。</p>

	<b>Command or Action</b>	<b>Purpose</b>
	<pre>error    ERRORS         notif   NOTICE (config)# logging level ethpm link-down error ? &lt;CR&gt; (config)# logging level ethpm link-down notif ? &lt;CR&gt; switch(config)#logging level ethpm link-up ? error    ERRORS         notif   NOTICE (config)# logging level ethpm link-up error ? &lt;CR&gt; (config)# logging level ethpm link-up notif ? &lt;CR&gt;</pre>	
ステップ 7	<b>[no] logging timestamp {microseconds   milliseconds   seconds}</b> <b>Example:</b> <pre>switch(config)# logging timestamp milliseconds</pre>	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。 <b>Note</b> このコマンドは、スイッチ内で保持されているログに適用されます。また、外部のロギング サーバには適用されません。
ステップ 8	(Optional) <b>show logging timestamp</b>  <b>Example:</b> <pre>switch(config)# show logging timestamp</pre>	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 9	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

## RFC 5424 に準拠したロギング **syslog** の構成

コマンドは、次の方法で変更できます：

- [×] **logging rfc-strict 5424**
- **show logging rfc-strict 5424**

### 手順の概要

1. 

```
switch(config) # [×] logging rfc-strict 5424
```
2. 

```
switch(config) # logging rfc-strict 5424
```
3. 

```
switch(config) # show logging rfc-strict 5424
```

## 手順の詳細

## 手順

	コマンドまたはアクション	目的
ステップ1	switch(config)# [×] logging rfc-strict 5424	(オプション) コマンドを無効にするか、またはそのデフォルトに設定します
ステップ2	switch(config)# <b>logging rfc-strict 5424</b>	メッセージロギング ファシリティを変更し、メッセージが準拠する必要のある RFC を設定します。
ステップ3	switch(config)# show logging rfc-strict 5424	RFC 5424 に準拠する syslog を表示します

## syslog サーバの設定



**Note** シスコは、管理仮想ルーティングおよび転送 (VRF) インスタンスを使用するサーバとして、syslog サーバを設定することを推奨します。VRF の詳細情報については、『Cisco Nexus 9000 シリーズ NX-OS ユニキャストルーティング設定ガイド』を参照してください。

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



**Note** Cisco NX-OS リリース 10.3(2)F までは、ユーザーが特定のデフォルト値を入力すると、logging server コマンドの実行中の構成にそれらのデフォルト値がランダムまたは一貫性なく表示されていました。ただし、Cisco NX-OS リリース 10.3(2)F 以降では、実行中の構成には常にデフォルト以外の値のみが表示されます。

たとえば、以前のリリースで、特定のユーザー入力について、実行中の構成で `logging server 1.1.1.1 port 514 facility local7 use-vrf default` 値、Cisco NX-OS リリース 10.3 (2) F 以降、同じ入力に対して、running-config は `logging server 1.1.1.1` の値を表示します。デフォルト ポート、デフォルト ファシリティ (local7)、デフォルト VRF などのデフォルト値が実行中の構成で表示されないことに注意してください。

## SUMMARY STEPS

1. **configure terminal**
2. [no] **logging server host [severity-level [use-vrf vrf-name]]**
3. **logging source-interface loopback virtual-interface**
4. (Optional) **show logging server**
5. (Optional) **copy running-config startup-config**

## DETAILED STEPS

## Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b>  <b>Example:</b> <pre>switch# configure terminal switch(config) #</pre>	グローバルコンフィギュレーションモードを開始します
ステップ 2	<b>[no] logging server host [severity-level [use-vrf vrf-name]]</b>  <b>Example:</b> <pre>switch(config) # logging server 192.0.2.253</pre> <b>Example:</b> <pre>switch(config) # logging server 2001::3 5 use-vrf red</pre>	指定されたホスト名、IPv4 または IPv6 アドレスで Syslog サーバーを構成します。メッセージロギングを VRF の特定の Syslog サーバーに限定するには、 <b>use-vrf</b> キーワードを使用します。vrf-name キーワードは、VRF 名のデフォルトまたは管理値を示します。use-vrf デフォルト VRF は、デフォルトで管理 VRF です。ただし、 <b>show-running</b> コマンドはデフォルトの VRF をリストしません。重大度は 0 ~ 7 の範囲です。 <ul style="list-style-type: none"> <li>• 0 : 緊急</li> <li>• 1 : アラート</li> <li>• 2 : クリティカル</li> <li>• 3 : エラー</li> <li>• 4 : 警告</li> <li>• 5 : 通知</li> <li>• 6 : 情報</li> <li>• 7 : デバッグ</li> </ul> デフォルトの発信ファシリティは local7 です。 <b>no</b> オプションは、指定したホストのロギング サーバーを削除します。 この最初の例では、ファシリティ local7 のすべてのメッセージを転送します。2 番目の例では、重大度が 5 以下のメッセージを、VRF red の指定された IPv6 アドレスに転送します。 <b>Note</b> このコマンドを構成すると、次のいずれかのサーバーステータスが表示されます。

	Command or Action	Purpose
		<ul style="list-style-type: none"> <li>設定済み (Configured) – 正常に構成されました。</li> <li>エラーが検出されませんでした – syslog がリモート syslog サーバに正常に送信された場合、このステータスが表示されます。</li> <li>[一時的に到達不能 (Temporarily unreachable)] – 送信に問題がある場合、このステータスが表示されます。ただし、内部では、システムは送信の問題を探査しています。しばらくして問題が解決すると、ステータスは [エラーが見つかりませんでした (No errors found)] に変わります。</li> </ul>
ステップ 3	<p>Required: <b>logging source-interface loopback</b>  <i>virtual-interface</i></p> <p><b>Example:</b></p> <pre>switch(config)# logging source-interface loopback 5</pre>	リモート Syslog サーバの送信元インターフェイスをイネーブルにします。 <i>virtual-interface</i> 引数の範囲は、0 ~ 1023 です。
ステップ 4	(Optional) <b>show logging server</b>	Syslog サーバ設定を表示します。
ステップ 5	<p>(Optional) <b>copy running-config startup-config</b></p> <p><b>Example:</b></p> <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

## セキュアな Syslog サーバの設定

### 手順の概要

1. **configure terminal**
2. [no] **logging server host [severity-level [port port-number]][secure[trustpoint client-identity trustpoint-name]][use-vrf vrf-name]]**
3. (任意) **logging source-interface interface name**
4. (任意) **show logging server**
5. (任意) **copy running-config startup-config**

## CA 証明書の設定

## 手順の詳細

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b>  例： <pre>switch# configure terminal switch(config) #</pre>	グローバルコンフィギュレーションモードを開始します
ステップ 2	<b>[no] logging server host [severity-level [port port-number]][secure[trustpoint client-identity trustpoint-name]][use-vrf vrf-name]</b>  例： <pre>switch(config) # logging server 192.0.2.253 secure</pre> 例： <pre>switch(config) # logging server 2001::3 5 secure trustpoint client-identity myCA use-vrf red</pre>	指定されたホスト名、あるいは IPv4 または IPv6 アドレスで Syslog サーバを設定します。必要に応じて、CA によって署名されるクライアントアイデンティティ証明書をインストールし、trustpoint client-identity オプションを使用することで相互認証を適用できます。  セキュアな TLS 接続のデフォルト宛先ポートは 6514 です。
ステップ 3	(任意) <b>logging source-interface interface name</b>  例： <pre>switch(config) # logging source-interface lo0</pre>	リモート Syslog サーバの送信元インターフェイスをイネーブルにします。
ステップ 4	(任意) <b>show logging server</b>  例： <pre>switch(config) # show logging server</pre>	Syslog サーバ設定を表示します。secure オプションを設定する場合、出力のエントリにトランスポート情報が含まれるようになります。デフォルトでは、secure オプションが設定されていない場合、トランスポートは UDP です。
ステップ 5	(任意) <b>copy running-config startup-config</b>  例： <pre>switch(config) # copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

## CA 証明書の設定

セキュアな Syslog 機能のサポートには、トラストポイントの設定によってリモート サーバを認証する必要があります。

## 手順の概要

1. **configure terminal**
2. **[no] crypto ca trustpoint trustpoint-name**
3. **crypto ca authenticate trustpoint-name**

4. (任意) **show crypto ca certificate**
5. (任意) **copy running-config startup-config**

### 手順の詳細

#### 手順

	コマンドまたはアクション	目的
ステップ1	<b>configure terminal</b> 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	<b>[no] crypto ca trustpoint trustpoint-name</b> 例： switch(config)# crypto ca trustpoint winca switch(config-trustpoint)#	トラストポイントを設定します。 (注) トラストポイントの設定の前に ip domain-name を設定する必要があります。
ステップ3	必須: <b>crypto ca authenticate trustpoint-name</b> 例： switch(config-trustpoint)# crypto ca authenticate winca	トラストポイントの CA 証明書を設定します。
ステップ4	(任意) <b>show crypto ca certificate</b> 例： switch(config)# show crypto ca certificates	設定されている証明書/チェーンと、関連付けられているトラストポイントを表示します。
ステップ5	(任意) <b>copy running-config startup-config</b> 例： switch(config)# copy running-config startup-config	デバイスのリロード後にトラストポイントが持続されるように、実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

## CA 証明書の登録

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

### 手順の概要

1. **configure terminal**
2. **crypto key generate rsa label key name exportable modules 2048**
3. **[no] crypto ca trustpoint trustpoint-name**
4. **rsakeypair key-name**

## CA 証明書の登録

5. **crypto ca trustpoint trustpoint-name**
6. [no] **crypto ca enroll trustpoint-name**
7. **crypto ca import trustpoint-name certificate**
8. (任意) **show crypto ca certificates**
9. **copy running-config startup-config**

## 手順の詳細

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b>  例：  switch# configure terminal switch(config)#	グローバルコンフィギュレーションモードを開始します
ステップ 2	必須: <b>crypto key generate rsa label key name exportable modules 2048</b>  例：  switch(config-trustpoint)# crypto key generate rsa label myKey exportable modulus 2048	RSA キーペアを設定します。デフォルトでは、Cisco NX-OS ソフトウェアは 1024 ビットの RSA キーを作成します。
ステップ 3	[no] <b>crypto ca trustpoint trustpoint-name</b>  例：  switch(config)# crypto ca trustpoint myCA switch(config-trustpoint)#	トラストポイントを設定します。  (注) トラストポイントの設定の前に ip domain-name を設定する必要があります。
ステップ 4	必須: <b>rsakeypair key-name</b>  例：  switch(config-trustpoint)# rsakeypair myKey	トラストポイント CA に生成されたキーペアを関連付けます。
ステップ 5	<b>crypto ca trustpoint trustpoint-name</b>  例：  switch(config)# crypto ca authenticate myCA	トラストポイントの CA 証明書を設定します。
ステップ 6	[no] <b>crypto ca enroll trustpoint-name</b>  例：  switch(config)# crypto ca enroll myCA	CA に登録するスイッチのアイデンティティ証明書を生成します。
ステップ 7	<b>crypto ca import trustpoint-name certificate</b>  例：  switch(config-trustpoint)# crypto ca import myCA certificate	CA によって署名されたアイデンティティ証明書をスイッチにインポートします。

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

## UNIX または Linux システムでの syslog サーバの設定

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

*facility.level <five tab characters> action*

次の表に、設定可能な syslog フィールドを示します。

表 6: *syslog.conf* の *syslog* フィールド

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

## ■ ログ ファイルの表示およびクリア

### 手順の概要

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。
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。
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。

### 手順の詳細

#### 手順

---

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

例：

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

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

例：

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

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

例：

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

---

## ログ ファイルの表示およびクリア

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

### SUMMARY STEPS

1. **show logging last *number-lines***
2. **show logging logfile duration *hh:mm:ss***
3. **show logging logfile last-index**
4. **show logging logfile [start-time *yyyy mmm dd hh:mm:ss*] [end-time *yyyy mmm dd hh:mm:ss*]**
5. **show logging logfile [start-seqn *number*] [end-seqn *number*]**
6. **show logging nvrpm [last *number-lines*]**
7. **clear logging logfile [ persistent ]**

## 8. clear logging nvram

### DETAILED STEPS

#### Procedure

	Command or Action	Purpose
ステップ 1	<b>Required:</b> <code>show logging last number-lines</code> <b>Example:</b> <code>switch# show logging last 40</code>	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	<b>show logging logfile duration hh:mm:ss</b> <b>Example:</b> <code>switch# show logging logfile duration 15:10:0</code>	入力された時間内のタイムスタンプを持つログファイルのメッセージを表示します。
ステップ 3	<b>show logging logfile last-index</b> <b>Example:</b> <code>switch# show logging logfile last-index</code>	ログファイルの最後のメッセージのシーケンス番号を表示します。
ステップ 4	<b>show logging logfile [start-time yyyy mmm dd hh:mm:ss] [end-time yyyy mmm dd hh:mm:ss]</b> <b>Example:</b> <code>switch# show logging logfile start-time 2013 oct 1 15:10:0</code>	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 5	<b>show logging logfile [start-seqn number] [end-seqn number]</b> <b>Example:</b> <code>switch# show logging logfile start-seqn 100 end-seqn 400</code>	シーケンス番号の範囲内である、発生したメッセージを表示します。終了シーケンス番号を指定しなかった場合は、ログファイルの、開始番号から最後のメッセージまでのメッセージが表示されます。
ステップ 6	<b>show logging nvram [last number-lines]</b> <b>Example:</b> <code>switch# show logging nvram last 10</code>	NVRAM のメッセージを表示します。表示される行数を制限するには、表示する最終行番号を入力できます。最終行番号には 1 ~ 100 を指定できます。
ステップ 7	<b>clear logging logfile [ persistent ]</b> <b>Example:</b> <code>switch# clear logging logfile</code>	ログ ファイルの内容をクリアします。 <b>persistent</b> : 永続的な場所から、ログファイルの内容をクリアします。
ステップ 8	<b>clear logging nvram</b> <b>Example:</b> <code>switch# clear logging nvram</code>	NVRAM の記録されたメッセージをクリアします。

# システムメッセージロギングの設定確認

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

コマンド	目的
<b>show logging console</b>	コンソールロギング設定を表示します。
<b>show logging info</b>	ロギング設定を表示します。
<b>show logging last <i>number-lines</i></b>	ログファイルの末尾から指定行数を表示します。
<b>show logging level [facility]</b>	ファシリティロギング重大度設定を表示します。
<b>show logging logfile duration <i>hh:mm:ss</i></b>	入力された時間内のタイムスタンプを持つログファイルのメッセージを表示します。
<b>show logging logfile last-index</b>	ログファイルの最後のメッセージのシーケンス番号を表示します。
<b>show logging logfile [start-time <i>yyyy mmm dd hh:mm:ss</i>] [end-time <i>yyyy mmm dd hh:mm:ss</i>]</b>	開始日時と終了日時に基づいてログファイルのメッセージを表示します。
<b>show logging logfile [start-seqn <i>number</i>] [end-seqn <i>number</i>]</b>	シーケンス番号の範囲内である、発生したメッセージを表示します。終了シーケンス番号を指定しなかった場合は、ログファイルの、開始番号から最後のメッセージまでのメッセージが表示されます。
<b>show logging module</b>	モジュールロギング設定を表示します。
<b>show logging monitor</b>	モニタロギング設定を表示します。
<b>show logging nvram [last <i>number-lines</i>]</b>	NVRAMログのメッセージを表示します。
<b>show logging origin-id</b>	リモートsyslogサーバに送信されるsyslogメッセージに付加される、設定済みのホスト名、IPアドレス、またはテキスト文字列を表示します。
<b>show logging server</b>	Syslogサーバ設定を表示します。
<b>show logging timestamp</b>	ロギングタイムスタンプ単位設定を表示します。

# システムメッセージロギングの設定例

システムメッセージロギングのコンフィギュレーション例を示します。

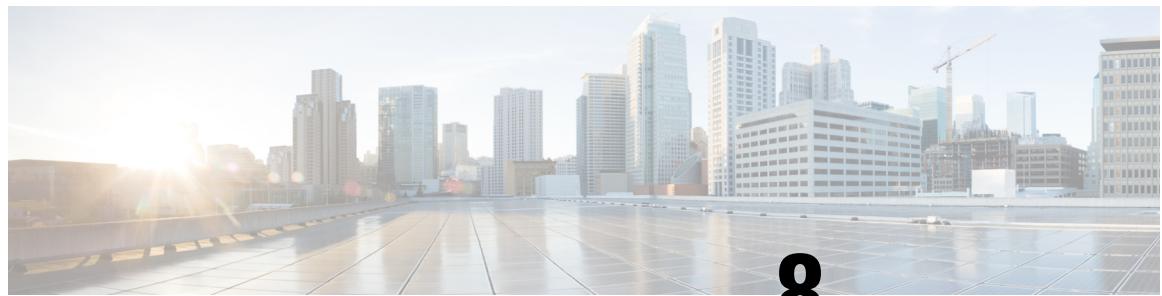
```
configure terminal
  logging console 3
  logging monitor 3
  logging logfile my_log 6
  logging module 3
  logging level aaa 2
  logging timestamp milliseconds
  logging server 172.28.254.253
  logging server 172.28.254.254 5 facility local3
copy running-config startup-config
```

## その他の参考資料

### 関連資料

関連項目	マニュアルタイトル
システム メッセージ	『Cisco NX-OS System Messages Reference』

## ■ 関連資料



## 第 8 章

# Session Manager の設定

この章は、次の項で構成されています。

- セッションマネージャについて, [on page 105](#)
- Session Manager の注意事項および制約事項, [on page 105](#)
- Session Manager の設定 (106 ページ)
- Session Manager 設定の確認, [on page 108](#)

## セッションマネージャについて

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

- コンフィギュレーション セッション : Session Manager モードで実行するコマンドのリストを作成します。
- 検証 : 設定の基本的なセマンティック チェックを行います。Cisco NX-OS は、構成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、構成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 は構成全体を確認して、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 の設定

- 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

作成できる構成セッションの最大数は 32 です。

### SUMMARY STEPS

- switch# **configure session name**
- (Optional) switch(config-s)# **show configuration session [name]**
- (Optional) switch(config-s)# **save location**

### DETAILED STEPS

#### Procedure

	Command or Action	Purpose
ステップ 1	switch# <b>configure session name</b>	構成セッションを作成し、セッション構成モードを開始します。名前は任意の英数字ストリングです。セッションの内容を表示します。
ステップ 2	(Optional) switch(config-s)# <b>show configuration session [name]</b>	セッションの内容を表示します。
ステップ 3	(Optional) switch(config-s)# <b>save location</b>	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。

### SUMMARY STEPS

- switch# **configure session name**
- switch(config-s)# **ip access-list name**
- (Optional) switch(config-s-acl)# **permit protocol source destination**
- switch(config-s-acl)# **interface interface-type number**
- switch(config-s-if)# **ip port access-group name in**

## 6. (Optional) switch# **show configuration session [name]**

### DETAILED STEPS

#### Procedure

	Command or Action	Purpose
ステップ 1	switch# <b>configure session name</b>	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)# <b>ip access-list name</b>	ACLを作成します。
ステップ 3	(Optional) switch(config-s-acl)# <b>permit protocol source destination</b>	ACLに許可文を追加します。
ステップ 4	switch(config-s-acl)# <b>interface interface-type number</b>	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)# <b>ip port access-group name in</b>	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	(Optional) switch# <b>show configuration session [name]</b>	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)# <b>verify [verbose]</b>	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)# <b>commit [verbose]</b>	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。

## セッションの廃棄

コマンド	目的
switch(config-s)# <b>save</b> 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)# <b>abort</b>	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

Session Manager 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]	構成ファイルの内容を表示します。
show configuration session status [name]	構成セッションのステータスを表示します。
show configuration session summary	すべての構成セッションのサマリーを表示します。



## 第 9 章

# Smart Call Home の設定

この章は、次の項で構成されています。

- [Smart Call Home の概要, on page 109](#)
- [Smart Call Home の注意事項および制約事項, on page 119](#)
- [Smart Call Home の前提条件, on page 119](#)
- [Call Home のデフォルト設定, on page 120](#)
- [Smart Call Home の設定 \(120 ページ\)](#)
- [Smart Call Home 設定の確認, on page 134](#)
- [フルテキスト形式での syslog アラート通知の例, on page 135](#)
- [XML 形式での syslog アラート通知の例, on page 135](#)

## Smart Call Home の概要

Smart Call Home は、重要なシステムイベントを E メールで通知します。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ネットワーク オペレーションセンターを呼び出せます。また、Cisco Smart Call Home サービスを使用して、TAC でケースを自動的に生成することもできます。

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。

- 繙続的なデバイス 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。

## Smart Call Home の概要

- 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、ユーザー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）。
- メッセージシビラティ（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 シビラティ（重大度）。アラートの Smart Call Home シビラティ（重大度）が、宛先プロファイルに設定されたメッセージシビラティ（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 メッセージシビラティ（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シビラティ（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。

**Table 7:** 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。
診断	診断によって生成されたイベント。	<b>show diagnostic result module all detail</b> <b>show moduleshow version</b> <b>show tech-support platform callhome</b>

## Smart Call Home アラート グループ

アラート グループ	説明	実行されるコマンド
スーパーバイザ ハードウェア	スーパーバイザ モジュールに関連するイベント。	<b>show diagnostic result module all detail</b> <b>show moduleshow version</b> <b>show tech-support platform callhome</b>
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。	<b>show diagnostic result module all detail</b> <b>show moduleshow version</b> <b>show tech-support platform callhome</b>
設定	設定に関連した定期的なイベント。	<b>show version</b> <b>show module</b> <b>show running-config all</b> <b>show startup-config</b>
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	<b>show system redundancy status</b> <b>show tech-support</b>
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。	<b>show environment</b> <b>show logging last 1000</b> <b>show module show version</b> <b>show tech-support platform callhome</b>
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なイベントであり、情報はステータスおよび使用権に使用されます。	<b>show module</b> <b>show version</b> <b>show license usage</b> <b>show inventory</b> <b>show sprom all</b> <b>show system uptime</b>

Smart Call Home は、syslog のシビラティ（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 のシビラティ（重大度）に対応させます。

定義済みのアラート グループをカスタマイズして、特定のイベントが発生したときに、**show** コマンドを追加で実行できます。そして、**show** 出力を Smart Call Home メッセージと共に送信します。

フルテキストと XML 接続先プロファイルへのみ **show** コマンドを追加できます。ショートテキストの接続先プロファイルは、128 バイトのテキストしか許可しないため追加の **show** コマンドをサポートしません。

## 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ー定義）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 のシビラティ（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。



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

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

**Table 8: 重大度と syslog レベルのマッピング**

Smart Call Home レベル	キーワード	Syslog レベル	説明
9	Catastrophic	該当なし	ネットワーク全体に壊滅的な障害が発生しています。
8	Disaster	該当なし	ネットワークに重大な影響が及びます。
7	Fatal	緊急 (0)	システムが使用不可能な状態。
6	Critical	アラート (1)	クリティカルな状況で、すぐに対応する必要があります。
5	Major	重要 (2)	重大な状態。
4	Minor	エラー (3)	軽微な状態。
3	警告	警告 (4)	警告状態。
2	通知	通知 (5)	基本的な通知および情報メッセージです。
1	標準	情報 (6)	標準状態に戻ることを示す標準イベントです。
0	Debugging	デバッグ (7)	デバッグ メッセージ。

## 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
- ユーザー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。

Table 9: 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）
アラームの緊急性度	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。

Table 10: 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 <i>YYYY-MM-DD HH:MM:SS GMT+HH:MM</i>	/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

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）
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	<p>メッセージを生成したエンドデバイスの固有デバイス識別情報（UDI）。メッセージがデバイスに対して固有でない場合は、このフィールドを空にする必要があります。形式は、次のとおりです。</p> <p><i>type@Sid@serial:</i></p> <ul style="list-style-type: none"> <li>• <i>type</i> は、バックプレーンIDPROMからの製品の型番。</li> <li>• @ は区切り文字です。</li> <li>• <i>Sid</i> は C で、シリアル ID をシャーシシリアル番号として特定します。</li> <li>• <i>serial</i> は、<i>Sid</i> フィールドによって特定される数字です。</li> </ul> <p>例：WS-C6509@C@12345678</p>	/aml/header/deviceID
カスタマー ID	サポートサービスによって契約情報やその他の ID に使用されるオプションのユーザ設定可能なフィールド	/aml/header/customerID
連絡先 ID	サポートサービスによって契約情報やその他の ID に使用されるオプションのユーザ設定可能なフィールド	/aml/header/contractID
サイト ID	シスコが提供したサイト ID または別のサポートサービスにとって意味のあるその他のデータに使用されるオプションのユーザ設定可能なフィールド	/aml/header/siteID

## Call Home のメッセージ形式

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）
サーバー ID	<p>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。</p> <p>形式は、次のとおりです。 <i>type@Sid@serial</i>:</p> <ul style="list-style-type: none"> <li>• <i>type</i> は、バックプレーン IDPROM からの製品の型番。</li> <li>• @ は区切り文字です。</li> <li>• <i>Sid</i> は C で、シリアル ID をシャーシシリアル番号として特定します。</li> <li>• <i>serial</i> は、Sid フィールドによって特定される数字です。</li> </ul> <p>例 : WS-C6509@C@12345678</p>	/aml/header/serverID
メッセージの説明	エラーを説明するショートテキスト。	/aml/body/msgDesc
デバイス名	イベントが発生したノード（デバイスのホスト名）。	/aml/body/sysName
担当者名	イベントが発生したノード関連の問題について問い合わせる担当者名。	/aml/body/sysContact
連絡先電子メール	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

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）
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。		
Command output name	実行された CLI コマンドの正確な名前。	/aml/attachments/attachment/name
添付ファイルの種類	特定のコマンド出力。	/aml/attachments/attachment/type
MIME タイプ	プレーンテキストまたは符号化タイプ。	/aml/attachments/attachment/mime
コマンド出力テキスト	自動的に実行されるコマンドの出力	/aml/attachments/attachment/atdata

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。

**Table 11:** 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のソフトウェアバージョン	最上レベルのソフトウェアバージョン	/aml/body/chassis/swVersion
影響のある FRU 名	イベントメッセージを生成する関連 FRU の名前。	/aml/body/fru/name
影響のある FRU のシリアル番号	関連 FRU のシリアル番号。	/aml/body/fru/serialNo
影響のある FRU の製品番号	関連 FRU の部品番号。	/aml/body/fru/partNo

## Call Home のメッセージ形式

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 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 ソフトウェアのバージョン	関連 FRU で稼働しているソフトウェアバージョン。	/aml/body/fru/swVersion

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。

**Table 12:** 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のソフトウェアバージョン	最上レベルのソフトウェアバージョン	/aml/body/chassis/swVersion
FRU 名	イベントメッセージを生成する関連 FRU の名前。	/aml/body/fru/name
FRU s/n	FRU のシリアル番号。	/aml/body/fru/serialNo
FRU 製品番号	FRU の部品番号。	/aml/body/fru/partNo
FRU スロット	FRU のスロット番号。	/aml/body/fru/slot
FRU ハードウェアバージョン	FRU のハードウェアバージョン。	/aml/body/fru/hwVersion
FRU ソフトウェアのバージョン	FRU で稼働しているソフトウェアバージョン。	/aml/body/fru/swVersion

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

**Table 13:** ユーザー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

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。
- Smart Call Home はあらゆる SMTP サーバで動作します。
- Smart Call Home には最大 5 個までの SMTP サーバを設定できます。
- Link up/down syslog メッセージは、Smart Call Home メッセージまたはアラート通知をトリガーしません。
- Cisco NX-OS リリース 7.0 (3) F3 (4) 以降、**show environment fan** および**show environment power** コマンドの出力は、電源ファンに障害があるかどうかを示します。以前のリリースでは、**show environment fan** コマンドがエラーを表示します。



### Note

リリース 7.0 (3) I2 (1) 以降、SNMP sysContact は、デフォルトでは構成されていません。SNMP sysContact を構成するには、**snmp-server contact <sys-contact>** コマンドを明示的に使用する必要があります。このコマンドを構成すると、callhome の機能が有効になります。

## Smart Call Home の前提条件

- 電子メール サーバーに接続できる必要があります。
- コンタクト名（SNMP サーバーのコンタクト）、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 サーバー間に 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

Table 14: デフォルトの *Call Home* パラメータ

パラメータ	デフォルト
フルテキストフォーマットで送信するメッセージの宛先メッセージサイズ	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 グループのアソシエート	フルテキスト宛先プロファイルおよびショートテキスト宛先プロファイルの場合はすべて。CiscoTAC-1 宛先プロファイルの場合は cisco-tac アラート グループ
フォーマットタイプ	XML
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

### 始める前に

- 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

### 手順の概要

- ブラウザで、次の Smart Call Home Web ページに移動します。
- Getting Started**の下で、Smart Call Home の登録指示に従ってください。

## 手順の詳細

### 手順

**ステップ1** ブラウザで、次の 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 の下で、Smart Call Home の登録指示に従ってください。

### 次のタスク

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。

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **snmp-server contact** *sys-contact*
3. switch(config)# **callhome**
4. switch(config-callhome)# **email-contact** *email-address*
5. switch(config-callhome)# **phone-contact** *international-phone-number*
6. switch(config-callhome)# **streetaddress** *address*
7. (Optional) switch(config-callhome)# **contract-id** *contract-number*
8. (Optional) switch(config-callhome)# **customer-id** *customer-number*
9. (Optional) switch(config-callhome)# **site-id** *site-number*
10. (Optional) switch(config-callhome)# **switch-priority** *number*
11. (Optional) switch# **show callhome**
12. (Optional) switch(config)# **copy running-config startup-config**

### DETAILED STEPS

#### Procedure

	Command or Action	Purpose
ステップ1	switch# <b>configure terminal</b>	グローバル コ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)# <b>snmp-server contact</b> <i>sys-contact</i>	SNMP sysContact を設定します。

## 連絡先情報の設定

	<b>Command or Action</b>	<b>Purpose</b>
ステップ 3	switch(config)# <b>callhome</b>	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)# <b>email-contact</b> <i>email-address</i>	スイッチの担当者の電子メールアドレスを設定します。 <i>email-address</i> には、電子メールアドレスの形式で、最大 255 の英数字を使用できます。 <b>Note</b> 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)# <b>phone-contact</b> <i>international-phone-number</i>	デバイスの担当者の電話番号を国際電話フォーマットで設定します。 <i>international-phone-number</i> は、最大 17 文字の英数字で、国際電話フォーマットにする必要があります。 <b>Note</b> 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)# <b>streetaddress</b> <i>address</i>	スイッチの主担当者の住所を設定します。 <i>address</i> は、255 個の英数字を指定できます。スペースを使用できます。
ステップ 7	(Optional) switch(config-callhome)# <b>contract-id</b> <i>contract-number</i>	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。 <i>contract-number</i> は、255 個の英数字を指定できます。
ステップ 8	(Optional) switch(config-callhome)# <b>customer-id</b> <i>customer-number</i>	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。 <i>customer-number</i> は、255 個の英数字を指定できます。
ステップ 9	(Optional) switch(config-callhome)# <b>site-id</b> <i>site-number</i>	このスイッチのサイト番号を設定します。 <i>site-number</i> は、最大 255 文字の英数字を自由なフォーマットで指定できます。
ステップ 10	(Optional) switch(config-callhome)# <b>switch-priority</b> <i>number</i>	このスイッチのスイッチ プライオリティを設定します。

	Command or Action	Purpose
		指定できる範囲は0～7です。0は最高のプライオリティを、7は最低のプライオリティを示します。デフォルト値は7です。
ステップ 11	(Optional) switch# <b>show callhome</b>	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	(Optional) switch(config)# <b>copy running-config startup-config</b>	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。

### Example

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
```

### What to do next

宛先プロファイルを作成します。

## 宛先プロファイルの作成

ユーザー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。

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **callhome**
3. switch(config-callhome)# **destination-profile {ciscoTAC-1 {alert-group group | email-addr address | http URL | transport-method {email | http}} | filename {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}}}}**
4. (Optional) switch# **show callhome destination-profile [profile name]**
5. (Optional) switch(config)# **copy running-config startup-config**

## 接続先プロファイルの変更

## DETAILED STEPS

## Procedure

	Command or Action	Purpose
ステップ 1	switch# <b>configure terminal</b>	グローバルコ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)# <b>callhome</b>	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)# <b>destination-profile {ciscoTAC-1 {alert-group group   email-addr address   http URL   transport-method {email   http}}   filename {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}}}}</b>	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	(Optional) switch# <b>show callhome destination-profile [profile name]</b>	1 つまたは複数の宛先プロファイルに関する情報を表示します。
ステップ 5	(Optional) switch(config)# <b>copy running-config startup-config</b>	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。

## Example

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
```

## 接続先プロファイルの変更

定義済みまたはユーザー定義の宛先プロファイルの次の属性を変更できます。

- 接続先アドレス：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 メッセージのシビラティ（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。

**Note**

CiscoTAC-1 宛先プロファイルは変更または削除できません。

**SUMMARY STEPS**

1. **switch# configure terminal**
2. **switch(config)# callhome**
3. **switch(config-callhome)# destination-profile {name | full-txt-destination | short-txt-destination} email-addr address**
4. **destination-profile {name | full-txt-destination | short-txt-destination} message-level number**
5. **switch(config-callhome)# destination-profile {name | full-txt-destination | short-txt-destination} message-size number**
6. (Optional) **switch# show callhome destination-profile [profile name]**
7. (Optional) **switch(config)# copy running-config startup-config**

**DETAILED STEPS****Procedure**

	<b>Command or Action</b>	<b>Purpose</b>
ステップ 1	<b>switch# configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>switch(config)# callhome</b>	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	<b>switch(config-callhome)# destination-profile {name   full-txt-destination   short-txt-destination} email-addr address</b>	ユーザー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。接続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	<b>destination-profile {name   full-txt-destination   short-txt-destination} message-level number</b>	この接続先プロファイルの Smart Call Home メッセージのシビラティ（重大度）を設定します。Smart Call Home シビラティ（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。 <i>number</i> の範囲は 0 ~ 9 です。9 は最大の重大度を示します。

## アラート グループと宛先プロファイルのアソシエート

	Command or Action	Purpose
ステップ 5	switch(config-callhome)# <b>destination-profile</b> {name   full-txt-destination   short-txt-destination} <b>message-size</b> number	この接続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 の範囲は 0 ~ 5000000 で、デフォルト値は 2500000 です。short-txt-destination の範囲は 0 ~ 100000 で、デフォルト値は 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	(Optional) switch# <b>show callhome destination-profile</b> [profile name]	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	(Optional) switch(config)# <b>copy running-config startup-config</b>	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。

## Example

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)#

```

## What to do next

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アソシエート

## SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **callhome**
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}
4. (Optional) switch# **show callhome destination-profile** [profile name]
5. (Optional) switch(config)# **copy running-config startup-config**

## DETAILED STEPS

## Procedure

	Command or Action	Purpose
ステップ 1	switch# <b>configure terminal</b>	グローバル コ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)# <b>callhome</b>	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)# <b>destination-profile name alert-group {All   Cisco-TAC   Configuration   Diagnostic   Environmental   Inventory   License   Linecard-Hardware   Supervisor-Hardware   Syslog-group-port   System   Test}</b>	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。 <b>All</b> キーワードを使用して、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	(Optional) switch# <b>show callhome destination-profile [profile name]</b>	1 つまたは複数の宛先プロファイルに関する情報を表示します。
ステップ 5	(Optional) switch(config)# <b>copy running-config startup-config</b>	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。

## Example

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)#

```

## What to do next

必要に応じて、**show** コマンドをアラート グループに追加し、SMTP 電子メール サーバーを構成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 個のユーザー定義 **show** コマンドをアラート グループに割り当てることができます。

## SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **callhome**

アラート グループへの **show** コマンドの追加

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**
4. (Optional) switch# **show callhome user-def-cmds**
5. (Optional) switch(config)# **copy running-config startup-config**

## DETAILED STEPS

## Procedure

	<b>Command or Action</b>	<b>Purpose</b>
ステップ 1	switch# <b>configure terminal</b>	グローバル コ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)# <b>callhome</b>	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)# <b>alert-group {Configuration   Diagnostic   Environmental   Inventory   License   Linecard-Hardware   Supervisor-Hardware   Syslog-group-port   System   Test} user-def-cmd show-cmd</b>	<b>show</b> 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 <b>show</b> コマンドのみが受け入れられます。 <b>Note</b> ユーザー定義済み <b>show</b> コマンドを CiscoTAC-1 接続先プロファイルに、追加できません。
ステップ 4	(Optional) switch# <b>show callhome user-def-cmds</b>	アラート グループへの追加されたすべてのユーザー定義済み <b>show</b> コマンドに関する情報を表示します。
ステップ 5	(Optional) switch(config)# <b>copy running-config startup-config</b>	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。

## Example

次の例は、**show ip routing** コマンドを Cisco-TAC アラート グループに追加する方法を表示します。

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

```

## What to do next

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

## 電子メール サーバーの詳細の設定

Smart Call Home 機能が動作するよう SMTP サーバー 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。

### SUMMARY STEPS

1. **switch# configure terminal**
2. **switch(config)# callhome**
3. **switch(config-callhome)# transport email smtp-server *ip-address* [*port number*] [*use-vrf vrf-name*])**
4. (Optional) **switch(config-callhome)# transport email from *email-address***
5. (Optional) **switch(config-callhome)# transport email reply-to *email-address***
6. (Optional) **switch# show callhome transport-email**
7. (Optional) **switch(config)# copy running-config startup-config**

### DETAILED STEPS

#### Procedure

	Command or Action	Purpose
ステップ 1	<b>switch# configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>switch(config)# callhome</b>	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	<b>switch(config-callhome)# transport email smtp-server <i>ip-address</i> [<i>port number</i>] [<i>use-vrf vrf-name</i>])</b>	SMTP サーバーを、ドメインネーム サーバー (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。 値は、 <i>number</i> 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 サーバー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	(Optional) <b>switch(config-callhome)# transport email from <i>email-address</i></b>	Smart Call Home メッセージの送信元電子メール フィールドを設定します。
ステップ 5	(Optional) <b>switch(config-callhome)# transport email reply-to <i>email-address</i></b>	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	(Optional) <b>switch# show callhome transport-email</b>	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	(Optional) <b>switch(config)# copy running-config startup-config</b>	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。

## 定期的なインベントリ通知の設定

### Example

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) #
```

### What to do next

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。

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **callhome**
3. switch(config-callhome)# **periodic-inventory notification [interval days] [timeofday time]**
4. (Optional) switch# **show callhome**
5. (Optional) switch(config)# **copy running-config startup-config**

### DETAILED STEPS

#### Procedure

	<b>Command or Action</b>	<b>Purpose</b>
ステップ 1	switch# <b>configure terminal</b>	グローバル コ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)# <b>callhome</b>	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)# <b>periodic-inventory notification [interval days] [timeofday time]</b>	定期的なインベントリ メッセージを設定します。 値は、 <b>interval days</b> の範囲は 1 ~ 30 日です。 デフォルトは 7 日です。 値は、 <b>timeofday time</b> は HH:MM の形式です。

	Command or Action	Purpose
ステップ 4	(Optional) switch# <b>show callhome</b>	Smart Call Home に関する情報を表示します。
ステップ 5	(Optional) switch(config)# <b>copy running-config startup-config</b>	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。

### Example

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) #
```

### What to do next

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。

### 手順の概要

1. switch# **configure terminal**
2. switch(config)# **callhome**
3. switch(config-callhome)# **no duplicate-message throttle**
4. (任意) switch(config)# **copy running-config startup-config**

### 手順の詳細

#### 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	グローバル コ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)# <b>callhome</b>	Smart Call Home 構成 モードを開始します。

## Smart Call Home のイネーブル化またはディセーブル化

	コマンドまたはアクション	目的
ステップ 3	switch(config-callhome)# <b>no duplicate-message throttle</b>	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	(任意) switch(config)# <b>copy running-config startup-config</b>	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。

## 例

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)#

```

## 次のタスク

Smart Call Home をイネーブルにします。

## Smart Call Home のイネーブル化またはディセーブル化

## 手順の概要

1. switch# **configure terminal**
2. switch(config)# **callhome**
3. switch(config-callhome) # [no] **enable**
4. (任意) switch(config)# **copy running-config startup-config**

## 手順の詳細

## 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	グローバルコ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)# <b>callhome</b>	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)#[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	(任意) switch(config)# 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。

### 例

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) #
```

### 次のタスク

任意でテスト メッセージを生成します。

## Smart Call Home 設定のテスト

### 始める前に

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。

### 手順の概要

1. switch# **configure terminal**
2. switch(config)# **callhome**
3. switch(config-callhome) # **callhome send diagnostic**
4. switch(config-callhome) # **callhome test**
5. (任意) switch(config)# **copy running-config startup-config**

## Smart Call Home 設定の確認

## 手順の詳細

## 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	グローバルコ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)# <b>callhome</b>	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) # <b>callhome send diagnostic</b>	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) # <b>callhome test</b>	設定されたすべての宛先にテストメッセージを送信します。
ステップ 5	(任意) switch(config)# <b>copy running-config startup-config</b>	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。

## 例

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
<b>show callhome</b>	Smart Call Home のステータスを表示します。
<b>show callhome destination-profile name</b>	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。
<b>show callhome pending-diff</b>	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。
<b>show callhome status</b>	Smart Call Home ステータスを表示します。

コマンド	目的
<b>show callhome transport-email</b>	Smart Call Home の電子メール設定を表示します。
<b>show callhome user-def-cmds</b>	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。
<b>show running-config [callhome   callhome-all]</b>	Smart Call Home の実行コンフィギュレーションを表示します。
<b>show startup-config callhome</b>	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。
<b>show tech-support callhome</b>	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
```

## ■ XML 形式での syslog アラート通知の例

```

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">
<![CDATA[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 0x200000
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-FANHIOOUTPUT: 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.

```

## ■ XML 形式での syslog アラート通知の例

```

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-XDRIPCNNOTIFY: 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>
```

## ■ XML 形式での syslog アラート通知の例



# 第 10 章

## スケジューラの設定

この章は、次の項で構成されています。

- [スケジューラの概要](#) (141 ページ)
- [スケジューラの注意事項および制約事項](#) (142 ページ)
- [スケジューラのデフォルト設定](#) (143 ページ)
- [スケジューラの設定](#) (143 ページ)
- [スケジューラの設定確認](#) (152 ページ)
- [スケジューラの設定例](#) (153 ページ)
- [スケジューラの標準](#) (154 ページ)

### スケジューラの概要

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

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

ジョブは、定期的な作業を定義する单一または複数のコマンドで構成されています。ジョブは、1回だけ、または定期的な間隔でスケジューリングすることができます。

スケジューラでは、ジョブと、そのタイムテーブルを次のように定義できます。

#### ジョブ

コマンドリストとして定義され、指定されたスケジュールに従って実行される定期的なタスク。

#### スケジュール

ジョブを実行するためのタイムテーブル。1つのスケジュールに複数のジョブを割り当てることができます。

1つのスケジュールは、定期的、または1回だけ実行するように定義されます。

- 定期モード：ジョブを削除するまで続行される繰り返しの間隔。次のタイプの定期的な間隔を設定できます。
  - Daily：ジョブは1日1回実行されます。
  - Weekly：ジョブは毎週1回実行されます。
  - Monthly：ジョブは毎月1回実行されます。
- Delta：ジョブは、指定した時間に開始され、以後、指定した間隔 (days:hours:minutes) で実行されます。
- 1回限定モード：ジョブは、指定した時間に1回だけ実行されます。

## リモートユーザ認証

ジョブの開始前に、スケジューラはジョブを作成したユーザーを認証します。リモート認証からのユーザークレデンシャルは、スケジュールされたジョブをサポートできるだけの十分に長い時間保持されないため、ジョブを作成するユーザーの認証パスワードをローカルで設定する必要があります。これらのパスワードは、スケジューラのコンフィギュレーションに含まれ、ローカル設定のユーザとは見なされません。

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

## スケジューラログファイル

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

## スケジューラの注意事項および制約事項

- ジョブの実行中に次のいずれかの状況が発生した場合、スケジューラは失敗する可能性があります。
  - 機能ライセンスが、その機能のジョブがスケジュールされている時間に期限切れになった場合。
  - 機能が、その機能を使用するジョブがスケジューリングされている時間にディセーブルになっている場合。
  - 機能 ID=nxos-7k-only。3k はモジュラ シャーシではありません。

スロットからモジュールを取り外したにもかかわらず、そのスロットを対象にしたジョブがスケジューリングされている場合。

- 時刻が設定されていることを確認します。スケジューラはデフォルトのタイムテーブルを適用しません。スケジュールを作成し、ジョブを割り当てても、時刻を設定しなければ、ジョブは開始されません。
- ジョブを定義するときは、対話型コマンドや中断を伴うコマンド（例：**copy bootflash:file ftp:URI**、**write erase**、**reload**、およびその他の同様のコマンド）がジョブが非インタラクティブに開始され、実行されるため、指定されていないことを確認します。特定の時間にリロードジョブがスケジュールされ、実行されると、スイッチはブートループに入ります。したがって、スケジューラ構成では使用しないでください。

## スケジューラのデフォルト設定

表 15: コマンドスケジューラのパラメータのデフォルト

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

## スケジューラの設定

### スケジューラのイネーブル化

#### 始める前に

正しい VDC を使用して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。

#### 手順の概要

1. switch# **configure terminal**
2. switch(config) # **feature scheduler**
3. (任意) switch(config) # **show scheduler config**
4. (任意) switch(config)# **copy running-config startup-config**

## スケジューラ ログ ファイル サイズの定義

## 手順の詳細

## 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	グローバルコ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) # <b>feature scheduler</b>	スケジューラを現在の VDC で有効にします。。
ステップ 3	(任意) switch(config) # <b>show scheduler config</b>	スケジューラ設定を表示します。
ステップ 4	(任意) switch(config)# <b>copy running-config startup-config</b>	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。

## 例

次に、スケジューラをイネーブルにする例を示します。

```
switch# configure terminal
switch(config) # feature scheduler
switch(config) # show scheduler config
config terminal
  feature scheduler
  scheduler logfile size 16
end
switch(config) #
```

## スケジューラ ログ ファイル サイズの定義

## 始める前に

正しい VDC を使用して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。

## 手順の概要

1. switch# **configure terminal**
2. switch(config) # **scheduler logfile size value**
3. (任意) switch(config)# **copy running-config startup-config**

## 手順の詳細

## 手順

	コマンドまたはアクション	目的
ステップ1	switch# <b>configure terminal</b>	グローバルコ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) # <b>scheduler logfile size value</b>	スケジューラログファイルサイズをキロバイト(KB)で定義します。 範囲は16～1024です。デフォルトのログファイルサイズは16です。 (注) ジョブ出力のサイズがログファイルのサイズより大きい場合、出力内容は切り捨てられます。
ステップ3	(任意) switch(config)# <b>copy running-config startup-config</b>	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。

## 例

次に、スケジューラログファイルのサイズを定義する例を示します。

```
switch# configure terminal
switch(config) # scheduler logfile size 1024
switch(config) #
```

## リモートユーザ認証の設定

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

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

## 始める前に

正しいVDCを使用していることを確認します。VDCを変更するには、**switchto vdc** コマンド

## 手順の概要

1. switch# **configure terminal**
2. switch(config) # **scheduler aaa-authentication password [0 | 7] password**
3. switch(config) # **scheduler aaa-authentication username name password [0 | 7] password**

## ジョブの定義

4. (任意) **switch(config) # show running-config |include "scheduler aaa-authentication"**
5. (任意) **switch(config)# copy running-config startup-config**

## 手順の詳細

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>switch# configure terminal</b>	グローバルコンフィギュレーションモードを開始します。
ステップ 2	<b>switch(config) # scheduler aaa-authentication password [0   7] password</b>	現在ログインしているユーザーのパスワードを設定します。 クリアテキストパスワードを設定するには、 <b>0</b> を入力します。 暗号化されたパスワードを設定するには、 <b>7</b> を入力します。
ステップ 3	<b>switch(config) # scheduler aaa-authentication username name password [0   7] password</b>	リモートユーザーのクリアテキストパスワードを設定します。
ステップ 4	(任意) <b>switch(config) # show running-config  include "scheduler aaa-authentication"</b>	スケジューラのパスワード情報を表示します。
ステップ 5	(任意) <b>switch(config)# copy running-config startup-config</b>	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。

## 例

次に、NewUser という名前のリモートユーザーのクリアテキストパスワードを設定する例を示します。

```
switch# configure terminal
switch(config) # scheduler aaa-authentication
username NewUser password z98y76x54b
switch(config) # copy running-config startup-config
switch(config) #
```

## ジョブの定義

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

### 始める前に

正しいVDCを使用して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。

### 手順の概要

1. **switch# configure terminal**
2. **switch(config) # scheduler job name name**
3. **switch(config-job) # command1 ; [command2 ; command3 ; ...]**
4. (任意) **switch(config-job) # show scheduler job [name]**
5. (任意) **switch(config-job) # copy running-config startup-config**

### 手順の詳細

#### 手順

	コマンドまたはアクション	目的
ステップ1	<b>switch# configure terminal</b>	グローバルコンフィギュレーションモードを開始します。
ステップ2	<b>switch(config) # scheduler job name name</b>	ジョブを指定された名前で作成し、ジョブ構成モードを開始します。 事前 <i>name</i> は、31 文字までに制限されています。
ステップ3	<b>switch(config-job) # command1 ; [command2 ; command3 ; ...]</b>	特定のジョブに対応するコマンドシーケンスを定義します。複数のコマンドは、スペースとセミコロンで (;) で区切る必要があります。 ファイル名は現在のタイムスタンプとスイッチ名を使用して作成します。
ステップ4	(任意) <b>switch(config-job) # show scheduler job [name]</b>	ジョブ情報を表示します。 事前 <i>name</i> は、31 文字までに制限されています。
ステップ5	(任意) <b>switch(config-job) # copy running-config startup-config</b>	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。

#### 例

次の例は、次の方法を示します。

- ・「backup-cfg」という名前のスケジューラジョブを作成示します。
- ・実行中の構成をブートフラッシュ上のファイルに保存します。

## ジョブの削除

- ・ファイルをブートフラッシュから TFTP サーバーにコピーします。
- ・変更がスタートアップ構成に保存されます。

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

## ジョブの削除

### 始める前に

正しい VDC を使用して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。

### 手順の概要

1. switch# **configure terminal**
2. switch(config) # **no scheduler job name name**
3. (任意) switch(config-job) # **show scheduler job [name]**
4. (任意) switch(config-job) # **copy running-config startup-config**

### 手順の詳細

#### 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	グローバル構成モードを開始します。
ステップ 2	switch(config) # <b>no scheduler job name name</b>	特定のジョブおよびそこで定義されたすべてのコマンドを削除します。 事前 <i>name</i> は、31 文字までに制限されています。
ステップ 3	(任意) switch(config-job) # <b>show scheduler job [name]</b>	ジョブ情報を表示します。
ステップ 4	(任意) switch(config-job) # <b>copy running-config startup-config</b>	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。

#### 例

次に、**configsave** という名前のジョブを削除する例を示します。

```
switch# configure terminal
switch(config)# no scheduler job name configsave
switch(config-job)# copy running-config startup-config
switch(config-job)#
```

## タイムテーブルの定義

タイムテーブルを設定する必要があります。設定しないと、ジョブがスケジューリングされません。

**time** コマンドの時間を指定しない場合、スケジューラは現在時刻を想定します。たとえば、現在の時刻が 2008 年 3 月 24 日の 22 時 00 分である場合、ジョブは次のように開始されます。

- **time start 23:00 repeat 4:00:00** コマンドの開始時刻が、2008 年 3 月 24 日 23 時 00 分であると見なします。
- **time daily 55** コマンドの開始時刻が、毎日 22 時 55 分であると見なします。
- **time weekly 23:00** コマンドの開始時刻が、毎週金曜日の 23 時 00 分であると見なします。
- **time monthly 23:00** コマンドの開始時刻が、毎月 24 日の 23 時 00 分であると見なします。



(注)

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

### 始める前に

正しい VDC を使用して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。

### 手順の概要

1. switch# **configure terminal**
2. switch(config) # **scheduler schedule name name**
3. switch(config-schedule) # **job name name**
4. switch(config-schedule) # **time daily time**
5. switch(config-schedule) # **time weekly [[day-of-week:] HH:] MM**
6. switch(config-schedule) # **time monthly [[day-of-month:] HH:] MM**
7. switch(config-schedule) # **time start {now repeat repeat-interval | delta-time [repeat repeat-interval]}**
8. (任意) switch(config-schedule) # **show scheduler config**
9. (任意) switch(config-schedule) # **copy running-config startup-config**

## ■ タイムテーブルの定義

## 手順の詳細

## 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	グローバル構成モードを開始します。
ステップ 2	switch(config) # <b>scheduler schedule name name</b>	新しいスケジューラを作成し、そのスケジュールのスケジュールコンフィギュレーションモードを開始します。 事前 <i>name</i> は、31 文字までに制限されています。
ステップ 3	switch(config-schedule) # <b>job name name</b>	このスケジュールにジョブを関連付けます。1 つのスケジュールに複数のジョブを追加できます。 事前 <i>name</i> は、31 文字までに制限されています。
ステップ 4	switch(config-schedule) # <b>time daily time</b>	ジョブが毎日 HH:MM の形式で指定された時刻に開始することを意味します。
ステップ 5	switch(config-schedule) # <b>time weekly [[day-of-week:] HH:] MM</b>	ジョブが週の指定された曜日に開始することを意味します。 曜日は整数で表されます（例：1 は日曜日、2 月曜日）または略語（たとえば、sun、mon）。 引数全体の最大長は 10 文字です。
ステップ 6	switch(config-schedule) # <b>time monthly [[day-of-month:] HH:] MM</b>	ジョブが月の特定の日に開始することを意味します。 29、30 または 31 のいずれかを指定した場合、そのジョブは各月の最終日に開始されます。
ステップ 7	switch(config-schedule) # <b>time start {now repeat repeat-interval   delta-time [repeat repeat-interval]}</b>	ジョブが定期的に開始することを意味します。 start-time の形式は [[[yyyy:]mmm:]dd:]HH:MM です。 <ul style="list-style-type: none"><li>• <i>delta-time</i> – スケジュールの構成後、ジョブの開始までの待機時間を指定します。</li><li>• 確認する – ジョブが今から 2 分後から開始することを指定します。</li><li>• <i>repeat repeat-interval</i> – ジョブを反復する回数を指定します。</li></ul>
ステップ 8	(任意) switch(config-schedule) # <b>show scheduler config</b>	スケジューラの情報を表示します。

	コマンドまたはアクション	目的
ステップ 9	(任意) switch(config-schedule)# <b>copy running-config startup-config</b>	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。

### 例

次に、ジョブが毎月 28 日の 23 時 00 分に開始するタイムテーブルを定義する例を示します。

```
switch# configure terminal
switch(config)# scheduler schedule name weekendbackupqos
switch(config-scheduler)# job name offpeakzoning
switch(config-scheduler)# time monthly 28:23:00
switch(config-scheduler)# copy running-config startup-config
switch(config-scheduler)#
```

## スケジューラ ログ ファイルの消去

### 始める前に

正しい VDC を使用して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。

### 手順の概要

1. switch# **configure terminal**
2. switch(config) # **clear scheduler logfile**

### 手順の詳細

#### 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	グローバル構成モードを開始します。
ステップ 2	switch(config) # <b>clear scheduler logfile</b>	スケジューラ ログ ファイルを消去します。

### 例

次に、スケジューラ ログ ファイルを消去する例を示します。

```
switch# configure terminal
switch(config)# clear scheduler logfile
```

## スケジューラのディセーブル化

### 始める前に

正しい VDC を使用して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。

### 手順の概要

1. switch# **configure terminal**
2. switch(config) # **no feature scheduler**
3. (任意) switch(config) # **show scheduler config**
4. (任意) switch(config)# **copy running-config startup-config**

### 手順の詳細

#### 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	グローバルコ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) # <b>no feature scheduler</b>	現在の VDC のスケジューラを無効化します。
ステップ 3	(任意) switch(config) # <b>show scheduler config</b>	スケジューラ構成を表示します。
ステップ 4	(任意) switch(config)# <b>copy running-config startup-config</b>	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。

#### 例

次に、スケジューラをディセーブルにする例を示します。

```
switch# configure terminal
switch(config) # no feature scheduler
switch(config) # copy running-config startup-config
switch(config) #
```

## スケジューラの設定確認

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 16:スケジューラの **show** コマンド

コマンド	目的
<b>show scheduler config</b>	スケジューラ設定を表示します。
<b>show scheduler job [name name]</b>	設定されているジョブを表示します。
<b>show scheduler logfile</b>	スケジューラログファイルの内容を表示します。
<b>show scheduler schedule [name name]</b>	設定されているスケジュールを表示します。

## スケジューラの設定例

### スケジューラジョブの作成

この例では、実行コンフィギュレーションをブートフラッシュ内のファイルに保存するスケジュールジョブを作成する方法を示します。このジョブは、その後で、ブートフラッシュからTFTPサーバにファイルをコピーします（現在のタイムスタンプとスイッチ名を使用してファイル名を作成します）。

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

### スケジューラジョブのスケジューリング

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

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

### ジョブスケジュールの表示

次に、ジョブスケジュールを表示する例を示します。

```
switch# show scheduler schedule
Schedule Name      : daily
-----
User Name          : admin
Schedule Type      : Run every day at 1 Hrs 00 Mins
```

## スケジューラ ジョブの実行結果の表示

```
Last Execution Time : Fri Jan 2 1:00:00 2009
Last Completion Time: Fri Jan 2 1:00:01 2009
Execution count      : 2
-----
          Job Name          Last Execution Status
-----
back-cfg                                Success (0)
switch(config)#

```

## スケジューラ ジョブの実行結果の表示

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

```
switch# show scheduler logfile
Job Name      : back-cfg          Job Status: Failed (1)
Schedule Name : daily             User Name : admin
Completion time: Fri Jan 1  1:00:01 2009
-----
          Job Output
-----
`cli var name timestamp 2009-01-01-01.00.00`  

`copy running-config bootflash:/$(HOSTNAME)-cfg.$(timestamp)`  

`copy bootflash:/switch-cfg.2009-01-01.00.00 tftp://1.2.3.4/ vrf management`  

copy: cannot access file '/bootflash/switch-cfg.2009-01-01.00.00'
-----
Job Name      : back-cfg          Job Status: Success (0)
Schedule Name : daily             User Name : admin
Completion time: Fri Jan 2  1:00:01 2009
-----
          Job Output
-----
`cli var name timestamp 2009-01-02-01.00.00`  

`copy running-config bootflash:/switch-cfg.2009-01-02-01.00.00`  

`copy bootflash:/switch-cfg.2009-01-02-01.00.00 tftp://1.2.3.4/ vrf management`  

Connection to Server Established.
[          ]      0.50KB Trying to connect to tftp server.....
[#####]      24.50KB
TFTP put operation was successful
-----
switch#
```

## スケジューラの標準

この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。



# 第 11 章

## SNMP の設定

この章は、次の項で構成されています。

- [SNMPについて, on page 155](#)
- [SNMPの注意事項および制約事項, on page 160](#)
- [SNMPのデフォルト設定, on page 161](#)
- [SNMPの設定 \(162 ページ\)](#)
- [SNMP ローカルエンジン ID の設定, on page 177](#)
- [SNMPの無効化 \(178 ページ\)](#)
- [SNMP 設定の確認, on page 179](#)

## 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に言語が提供されます。

## SNMP機能の概要

SNMP フレームワークは 3 つの部分で構成されます。

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



**Note** Cisco Nexus デバイスは、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。

SNMPはRFC 3410 で定義されています (<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>）。

## 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 レシバーテーブルで指定された SNMP マネージャに送信される、非同期の非確認応答メッセージです。インフォームは、SNMP エージェントから SNMP マネージャに送信される非同期メッセージで、マネージャは受信したという確認応答が必要です。

トラップの信頼性はインフォームより低くなります。SNMP マネージャはトラップを受信しても確認応答 (ACK) を送信しないからです。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 NX-OS 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 レシバーバーに通知を送信するよう Cisco NX-OS を構成できます。

## 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。

**Table 17: SNMP セキュリティ モデルおよびセキュリティ レベル**

モデル	レベル	認証	暗号化	結果
v1	noAuthNoPriv	コミュニティストリング	なし	コミュニティストリングの照合を使用して認証します。
v2c	noAuthNoPriv	コミュニティストリング	なし	コミュニティストリングの照合を使用して認証します。

## ■ ユーザーベースのセキュリティ モデル

モデル	レベル	認証	暗号化	結果
v3	authNoPriv	HMAC-MD5 または HMAC-SHA	未対応	Hash-Based Message Authentication Code (HMAC) メッセージ ダイジェスト 5 (MD5) アルゴリズムまたは HMAC Secure Hash Algorithm (SHA) アルゴリズムに基づいて認証します。
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鎖 (CBC) DES (DES-56) 標準に基づいて認証します。

## ■ ユーザーベースのセキュリティ モデル

SNMPv3 ユーザーベース 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ーが提示した 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。



**Note** 外部の AAA サーバーを使用して SNMPv3 を使う場合、外部 AAA サーバーのユーザー設定でプライバシープロトコルに AES を指定する必要があります。

## CLI および SNMP ユーザの同期

SNMPv3 ユーザー管理は、Access Authentication and Accounting (AAA) サーバー レベルで集中化できます。この中央集中型ユーザー管理により、Cisco NX-OS の SNMP エージェントは AAA サーバーのユーザー認証サービスを利用できます。ユーザー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。

ユーザー グループ、ロール、またはパスワードの構成が変更されると、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、次のようにユーザー構成を同期化します。

- **auth snmp-server user** コマンドで指定されたパスフレーズは、CLI ユーザー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、**auth** および **priv** SNMP ユーザーのパスフレーズになります。
- SNMP または CLI を使用してユーザーを作成または削除すると、SNMP と CLI の両方でユーザーが作成または削除されます。
- ユーザー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。



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



**Note** UCSS 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 の注意事項および制約事項

SNMP には、次の注意事項および制限事項があります。

- SNMP SET を使用して構成されたコマンドは、SNMP SET のみを使用して削除する必要があります。コマンドラインインターフェイス (CLI) または NX-API を使用して構成されたコマンドは、CLI または NX-API のみを使用して削除する必要があります。
- アクセス コントロール リスト (ACL) は、スイッチに設定されたローカル SNMPv3 ユーザのみに適用できます。ACL は、認証、許可、アカウント (AAA) サーバに保存されるリモート SNMPv3 ユーザに適用できません。
- Cisco NX-OS は、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。詳細については次の URL にアクセスして、Cisco NX-OS の MIB サポートリストを参照してください <ftp://ftp.cisco.com/pub/mibs/supportlists/nexus3000/Nexus3000MIBSupportList.html>。
- Cisco NX-OS は SNMPv3 noAuthNoPriv セキュリティ レベル (Security Level) をサポートしません。
- SNMP SET を使用して構成されたコマンドは、SNMP SET のみを使用して削除する必要があります。コマンドラインインターフェイス (CLI) または NX-API を使用して構成されたコマンドは、CLI または NX-API のみを使用して削除する必要があります。
- Cisco Nexus 3600 シリーズスイッチは、*snmpwalk* 要求に対して最大 10000 個のフラッシュ ファイルをサポートします。
- Cisco NX-OS リリース 10.3(3)F 以降では、SNMPv3 ユーザー パスワードのタイプ 6 暗号化が次の制限付きでサポートされています。
  - タイプ 6 暗号化は、次の点に注意した場合にのみ成功します。
    - **feature password encryption aes {tam}** が有効になっているかどうかに関係なく、OMP ピアのフラッピングが発生します。
    - プライマリ キーが構成されていること。

- 次のオプションは、SNMPv3 ユーザーの構成時に指定されます。 **pwd\_type 6** オプション
- プライマリキーの構成を変更すると、SNMPはデータベースに保存されているすべてのタイプ6ユーザーを再暗号化します。ただし、SNMP機能は以前と同じように動作します。
- プライマリキーの設定は、スイッチに対してローカルです。ユーザーが1つのスイッチからタイプ6で構成された実行データを取得し、別のプライマリキーが構成されている別のスイッチに適用すると、同じユーザーのSNMP機能が別のスイッチでは動作しない可能性があります。
- タイプ6が設定されている場合は、タイプ6がサポートされていないリリースにダウングレードする前に、構成を削除するか、タイプ6オプションを再構成してください。
- ISSUの場合、以前のイメージ (localizedkey、localizedV2key構成が存在する) からタイプ6暗号化がサポートされている新しいイメージに移行すると、SNMPは既存のキーをタイプ6暗号化に変換しません。
- 既存のSALT暗号化からタイプ6暗号化への変換は、**encryption re-encrypt obfuscated** コマンドを使用してサポートされます。
- 中断を伴うアップグレードや **reload-ascii** コマンドによる ASCII ベースのリロードを実行すると、プライマリキーが失われ、タイプ6ユーザーのSNMP機能に影響を与えます。
- ユーザーが **encryption re-encrypt obfuscated** コマンドを使用して再暗号化を強制すると、SNMPはタイプ6以外のSNMPユーザーからのすべてのパスワードをタイプ6モードに暗号化します。

**Note**

SNMPは、**encryption delete type6** コマンドをサポートしていません。同じことを示すsyslog警告メッセージも表示されます。

## SNMP のデフォルト設定

Table 18: デフォルトの **SNMP** パラメータ

パラメータ	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 送信元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に SNMP を設定できます。

### 手順の概要

1. switch# **configure terminal**
2. switch(config)# **snmp-server source-interface {inform | trap} type slot/port**
3. switch(config)# **show snmp source-interface**

### 手順の詳細

#### 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	グローバルコ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)# <b>snmp-server source-interface {inform   trap} type slot/port</b>	すべての SNMP パケットの送信元インターフェイスを設定します。次のリストに、 <i>interface</i> の有効な値を示します。 <ul style="list-style-type: none"> <li>• ethernet</li> <li>• loopback</li> <li>• mgmt</li> <li>• port-channel</li> <li>• vlan</li> </ul>
ステップ 3	switch(config)# <b>show snmp source-interface</b>	設定済みの SNMP 送信元インターフェイスを表示します。

#### 例

次に、SNMP 送信元インターフェイスを設定する例を示します。

```
switch(config)# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# snmp-server source-interface inform ethernet 1/10
switch(config)# snmp-server source-interface trap ethernet 1/10
switch(config)# show snmp source-interface
-----
Notification           source-interface
-----
trap                  Ethernet1/10
```

inform

Ethernet1/10

## SNMP ユーザの設定



**Note** Cisco NX-OS で SNMP ユーザーを構成するために使用するコマンドは、Cisco IOS でユーザーを構成するために使用されるものとは異なります。

### SUMMARY STEPS

1. **configure terminal**
2. **snmp-server user name [pwd\_type 6] [auth {md5 | sha | sha-256 | sha-384 | sha-512} passphrase [auto] [priv [aes-128] passphrase] [engineID id] [localizedkey] | [localizedV2key]]**
3. (Optional) **switch# show snmp user**
4. (Optional) **copy running-config startup-config**

### DETAILED STEPS

#### Procedure

	<b>Command or Action</b>	<b>Purpose</b>
ステップ 1	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config) #</pre>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>snmp-server user name [pwd_type 6] [auth {md5   sha   sha-256   sha-384   sha-512} passphrase [auto] [priv [aes-128] passphrase] [engineID id] [localizedkey]   [localizedV2key]]</b> <b>Example:</b> <pre>switch(config) # snmp-server user Admin pwd_type 6 auth sha abcd1234 priv abcdefgh</pre>	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。If you use the <b>localizedkey</b> 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。  <b>localizedkey - localizedkey</b> 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。プレーンテキスト パスワードの代わりに、 <b>localizedkey</b> キーワードを使用してハッシュされたパスワード ( <b>show running config</b> コマンドからコピーするか、snmpv3 ベースのオープン ソース ハッシュ ジェネレーターツールを使用してオフラインで生成したもの、ハッシュ

## SNMP ユーザの設定

	Command or Action	Purpose
		<p>シユ化されたパスワードのオフラインでの生成, on page 165 を参照) を構成できます。</p> <p><b>Note</b></p> <p>ローカライズされたキーを使用する場合は、ハッシュ値の前に 0x を追加します。たとえば、0x84a716329158a97ac9f22780629bc26c。</p> <p><b>localizedV2key</b> - localizedV2key キーを使用する場合、パスフレーズは大文字と小文字を区別した、最大 130 文字の英数字文字列にすることができます。先頭に 0x を付ける必要はありません。これは暗号化されたデータであり、オフラインでは生成できないため、<b>show run</b> コマンドを使用して localizedv2key を収集します。</p> <p>engineID の形式は、12 桁のコロンで区切った 10 進数字です。</p> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>Cisco NX-OS リリース 10.1(1) 以降、AES-128 は SNMPv3 のデフォルトのプライバシー プロトコルです。</li> <li>Cisco NX-OS リリース 10.3(3)F 以降、<b>pwd_type</b> 6 SNMP ユーザー パスワードにタイプ 6 暗号化を提供するために キーワードがサポートされています。</li> </ul>
ステップ 3	(Optional) switch# <b>show snmp user</b>  <b>Example:</b> switch(config) # show snmp user	1 人または複数の SNMP ユーザーに関する情報を表示します。
ステップ 4	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> switch(config) # 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。

**Example**

次に、SNMP ユーザーを構成する例を示します。

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

## ハッシュ化されたパスワードのオフラインでの生成

snmpv3 ベースのオープン ソース ハッシュ ジェネレータ ツールを使用して、ハッシュ化されたパスワードをオフラインで生成する手順は、次のとおりです。



(注) 例として挙げられている ID はサンプルの ID で、手順を説明するためだけのものです。

- スイッチから SNMP engineID を取得します。

```
switch# show snmp engineID
```

サンプル出力 :

```
Local SNMP engineID: [Hex] 8000000903D4C93CEA31CC
[Dec] 128:000:000:009:003:212:201:060:234:049:204
```

- SNMPv3 ベースのオープン ソース ハッシュ ジェネレータを使用して、ハッシュ化されたパスワードをオフラインで生成します。

```
Linux$ snmpv3-hashgen --auth Hello123 --engine 8000000903D4C93CEA31CC --user1 --mode
priv --hash md5
```

サンプル出力 :

```
User: user1
Auth: Hello123 / 84a716329158a97ac9f22780629bc26c
Priv: Hello123 / 84a716329158a97ac9f22780629bc26c
Engine: 8000000903D4C93CEA31CC
ESXi USM String:
u1/84a716329158a97ac9f22780629bc26c/84a716329158a97ac9f22780629bc26c/priv
```

- auth および priv の値を使用して、スイッチのパスワードを構成します。

```
snmp-server user user1 auth md5 0x84a716329158a97ac9f22780629bc26c priv des
0x84a716329158a97ac9f22780629bc26c localizedkey
```

## SNMP メッセージ暗号化の適用

着信要求に認証または暗号化が必要となるよう SNMP を設定できます。デフォルトでは、SNMP エージェントは認証および暗号化を行わないでも SNMPv3 メッセージを受け付けます。プライバシーを適用する場合、Cisco NX-OS は、**noAuthNoPriv** または **authNoPriv** のいずれかのセキュリティ レベル パラメータを使用するすべての SNMPv3 PDU 要求に対して、許可エラーで応答します。

SNMP メッセージの暗号化を特定のユーザーに強制するには、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)# <b>snmp-server user name enforcePriv</b>	このユーザーに対して 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 メッセージの暗号化をすべてのユーザーに強制するには、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)# <b>snmp-server globalEnforcePriv</b>	すべてのユーザーに対して 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 ユーザーを作成した後で、そのユーザーに複数のロールを割り当てることができます。



**Note** 他のユーザーにロールを割り当てる能够るのは、network-admin ロールに属するユーザーだけです。

コマンド	目的
switch(config)# <b>snmp-server user name group</b>	この SNMP ユーザーと設定されたユーザー 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)# <b>snmp-server community name group {ro   rw}</b>	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。

ACL を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
<pre>switch(config)# snmp-server community <i>community name</i> <b>use-acl</b> <i>acl-name</i></pre> <p><b>Example:</b></p> <pre>switch(config)# snmp-server community public use-acl my_acl_for_public</pre>	SNMP 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 レシーバに対して SNMP 通知を生成するよう Cisco NX-OS を構成できます。

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

コマンド	目的
<pre>switch(config)# snmp-server host <i>ip-address</i> <b>traps</b> <b>version 1</b> <i>community</i> [<b>udp_port</b> <i>number</i>]</pre>	SNMPv1 トランプのホスト レシーバを設定します。 <i>ip-address</i> は、 IPv4 アドレスまたは IPv6 アドレスである場合があります。 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 トラン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
<pre>switch(config)# snmp-server host <i>ip-address</i> {traps   informs} <b>version 2c</b> <i>community</i> [<b>udp_port</b> <i>number</i>]</pre>	SNMPv2c トランプまたはインフォームのホスト レシーバを設定します。 <i>ip-address</i> は、 IPv4 アドレスまたは IPv6 アドレスである場合があります。 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。

## ■ VRF を使用する SNMP 通知レシーバの設定

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
<code>switch(config)# snmp-server host ip-address {traps   informs} version 3 {auth   noauth   priv} username [udp_port number]</code>	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。 <code>ip-address</code> は、 IPv4 アドレスまたは IPv6 アドレスである場合があります。 ユーザー名は、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。



**Note** SNMP マネージャは SNMPv3 メッセージを認証して解読するために、Cisco Nexus デバイスの SNMP engineID に基づいてユーザー クレデンシャル (authKey/PrivKey) を調べる必要があります。

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。

### 手順の概要

1. `switch# configure terminal`
2. `switch# snmp-server host ip-address use-vrf vrf_name [udp_port number]`
3. (任意) `switch(config)# copy running-config startup-config`

## 手順の詳細

## 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	グローバル コ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# <b>snmp-server host ip-address use-vrf vrf_name [udp_port number]</b>	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	(任意) switch(config)# <b>copy running-config startup-config</b>	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。

## 例

次に、IP アドレス 192.0.2.1 の SNMP サーバー 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。

## 手順の概要

1. switch# **configure terminal**
2. switch(config)# **snmp-server host ip-address filter-vrf vrf\_name [udp\_port number]**
3. (任意) switch(config)# **copy running-config startup-config**

## ■ インバンドアクセスのための SNMP の設定

## 手順の詳細

## 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	グローバルコ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)# <b>snmp-server host ip-address filter-vrf vrf_name [udp_port number]</b>	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	(任意) switch(config)# <b>copy running-config startup-config</b>	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。

## 例

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
```

## 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。

## 手順の概要

1. switch# **configuration terminal**
2. switch(config)# **snmp-server context context-name vrf vrf-name**

3. switch(config)# **snmp-server community** *community-name* **group** *group-name*
4. switch(config)# **snmp-server mib community-map** *community-name* **context** *context-name*

## 手順の詳細

### 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configuration terminal</b>	グローバルコ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)# <b>snmp-server context</b> <i>context-name</i> <b>vrf</b> <i>vrf-name</i>	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。
ステップ 3	switch(config)# <b>snmp-server community</b> <i>community-name</i> <b>group</b> <i>group-name</i>	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)# <b>snmp-server mib community-map</b> <i>community-name</i> <b>context</b> <i>context-name</i>	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。

### 例

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ユーザーネーム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。



**Note** 値は、**snmp-server enable traps** CLI コマンドを使用すると、構成通知ホスト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 の通知を有効にする CLI コマンドを示します。

**Table 19: SNMP 通知のイネーブル化**

MIB	関連コマンド
すべての通知	<b>snmp-server enable traps</b>
CISCO-ERR-DISABLE-MIB	<b>snmp-server enable traps show interface status</b>
Q-BRIDGE-MIB	<b>snmp-server enable traps show mac address-table</b>
CISCO-SWITCH-QOS-MIB	<b>snmp-server enable traps show hardware internal buffer info pkt-stats</b>
BRIDGE-MIB	<b>snmp-server enable traps bridge newroot</b> <b>snmp-server enable traps bridge topologychange</b>
CISCO-AAA-SERVER-MIB	<b>snmp-server enable traps aaa</b>
ENTITY-MIB、 CISCO-ENTITY-FRU-CONTROL-MIB、 CISCO-ENTITY-SENSOR-MIB	<b>snmp-server enable traps entity</b> <b>snmp-server enable traps entity fru</b>
CISCO-LICENSE-MGR-MIB	<b>snmp-server enable traps license</b>
IF-MIB	<b>snmp-server enable traps link</b>
CISCO-PSM-MIB	<b>snmp-server enable traps port-security</b>
SNMPv2-MIB	<b>snmp-server enable traps snmp</b> <b>snmp-server enable traps snmp authentication</b>
CISCO-FCC-MIB	<b>snmp-server enable traps fcc</b>
CISCO-DM-MIB	<b>snmp-server enable traps fdomain</b>
CISCO-NS-MIB	<b>snmp-server enable traps fcns</b>
CISCO-FCS-MIB	<b>snmp-server enable traps fcs discovery-complete</b> <b>snmp-server enable traps fcs request-reject</b>

MIB	関連コマンド
CISCO-FDMI-MIB	<b>snmp-server enable traps ffdmi</b>
CISCO-FSPF-MIB	<b>snmp-server enable traps fspf</b>
CISCO-PSM-MIB	<b>snmp-server enable traps port-security</b>
CISCO-RSCN-MIB	<b>snmp-server enable traps rscn</b> <b>snmp-server enable traps rscn els</b> <b>snmp-server enable traps rscn ils</b>
CISCO-ZS-MIB	<b>snmp-server enable traps zone</b> <b>snmp-server enable traps zone default-zone-behavior-change</b> <b>snmp-server enable traps zone enhanced-zone-db-change</b> <b>snmp-server enable traps zone merge-failure</b> <b>snmp-server enable traps zone merge-success</b> <b>snmp-server enable traps zone request-reject</b> <b>snmp-server enable traps zone unsupp-mem</b>
CISCO-CONFIG-MAN-MIB  <b>Note</b> ccmCLIRunningConfigChanged 通知を除き、MIB オブジェクトをサポートしていません。	<b>snmp-server enable traps config</b>



**Note** 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)# <b>snmp-server enable traps</b>	すべての SNMP 通知をイネーブルにします。
switch(config)# <b>snmp-server enable traps aaa</b> [server-state-change]	AAA SNMP 通知をイネーブルにします。
switch(config)# <b>snmp-server enable traps entity</b> [fru]	ENTITY-MIB SNMP 通知をイネーブルにします。
switch(config)# <b>snmp-server enable traps license</b>	ライセンス SNMP 通知をイネーブルにします。

## リンクの通知の設定

コマンド	目的
switch(config)# <b>snmp-server enable traps port-security</b>	ポートセキュリティ SNMP 通知をイネーブルにします。
switch(config)# <b>snmp-server enable traps snmp [authentication]</b>	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 モニター 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。

## 手順の概要

1. **configure terminal**
2. **snmp-server enable traps link [cieLinkDown | cieLinkUp | cisco-xcvr-mon-status-chg | delayed-link-state-change] | extended-linkUp | extended-linkDown | linkDown | linkUp]**

## 手順の詳細

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 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	<pre>snmp-server enable traps link [cieLinkDown   cieLinkUp   cisco-xcvr-mon-status-chg   delayed-link-state-change]   extended-linkUp   extended-linkDown   linkDown   linkUp]</pre> <p>例 :</p> <pre>switch(config)# snmp-server enable traps link cieLinkDown</pre>	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。

### 手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface type slot/port**
3. switch(config -if)# **no snmp trap link-status**

### 手順の詳細

#### 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	グローバル コ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)# <b>interface type slot/port</b>	変更するインターフェイスを指定します。
ステップ 3	switch(config -if)# <b>no snmp trap link-status</b>	インターフェイスの SNMP リンクステート トラブル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)# <b>snmp-server tcp-session [auth]</b>	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

## 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することができます。

### SUMMARY STEPS

1. switch# **configuration terminal**
2. switch(config)# **snmp-server contact** *name*
3. switch(config)# **snmp-server location** *name*
4. (Optional) switch# **show snmp**
5. (Optional) switch# **copy running-config startup-config**

### DETAILED STEPS

#### Procedure

	<b>Command or Action</b>	<b>Purpose</b>
ステップ 1	switch# <b>configuration terminal</b>	グローバルコ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)# <b>snmp-server contact</b> <i>name</i>	sysContact (SNMP 担当者名) を設定します。
ステップ 3	switch(config)# <b>snmp-server location</b> <i>name</i>	sysLocation (SNMP ロケーション) を設定します。
ステップ 4	(Optional) switch# <b>show snmp</b>	1 つまたは複数の宛先プロファイルに関する情報を表示します。
ステップ 5	(Optional) switch# <b>copy running-config startup-config</b>	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。

### SUMMARY STEPS

1. switch# **configuration terminal**
2. switch(config)# **snmp-server context** *context-name* [**instance** *instance-name*] [**vrf** *vrf-name*] [**topology** *topology-name*]
3. switch(config)# **snmp-server mib community-map** *community-name* **context** *context-name*
4. (Optional) switch(config)# **no snmp-server context** *context-name* [**instance** *instance-name*] [**vrf** *vrf-name*] [**topology** *topology-name*]

## DETAILED STEPS

## Procedure

	Command or Action	Purpose
ステップ 1	switch# <b>configuration terminal</b>	グローバル コ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)# <b>snmp-server context context-name [instance instance-name] [vrf vrf-name] [topology topology-name]</b>	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)# <b>snmp-server mib community-map community-name context context-name</b>	SNMPv2c コミュニティを SNMP コンテキストにマッピングします。名前には最大 32 の英数字を使用できます。
ステップ 4	(Optional) switch(config)# <b>no snmp-server context context-name [instance instance-name] [vrf vrf-name] [topology topology-name]</b>	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。  <b>Note</b> 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。 <b>instance</b> 、 <b>vrf</b> 、または <b>topology</b> 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。

## SNMP ローカル エンジン ID の設定

Cisco NX-OS リリース 7.0 (3) F3 (1) 以降では、ローカル デバイスにエンジン ID を構成できます。

## SUMMARY STEPS

1. **configure terminal**
2. **snmp-server engineID local engineid-string**
3. **show snmp engineID**
4. **[no] snmp-server engineID local engineid-string**
5. **copy running-config startup-config**

## ■ SNMP の無効化

## DETAILED STEPS

## Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b>  <b>Example:</b> <pre>switch# configure terminal switch(config) #</pre>	グローバルコンフィギュレーションモードを開始します。
ステップ 2	<b>snmp-server engineID local engineid-string</b>  <b>Example:</b> <pre>switch(config) # snmp-server engineID local AA:BB:CC:1A:2C:10</pre>	ローカルデバイスの SNMP engineID を変更します。ローカルエンジン ID は、コロンで指定された 16 進数オクテットのリストとして設定する必要があります。ここでは 10 ~ 64 の範囲の偶数 16 進数文字が使用され、2 つの 16 進数文字ごとにコロンで区切れます。たとえば、i80:00:02:b8:04:61:62:63 です。
ステップ 3	<b>show snmp engineID</b>  <b>Example:</b> <pre>switch(config) # show snmp engineID</pre>	設定されている SNMP エンジンの ID を表示します。
ステップ 4	<b>[no] snmp-server engineID local engineid-string</b>  <b>Example:</b> <pre>switch(config) # no snmp-server engineID local AA:BB:CC:1A:2C:10</pre>	ローカルエンジン ID を無効にし、自動生成されたデフォルトのエンジン ID を設定します。
ステップ 5	Required: <b>copy running-config startup-config</b>  <b>Example:</b> <pre>switch(config) # copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

## SNMP の無効化

## 手順の概要

1. **configure terminal**
2. **switch(config) # no snmp-server protocol enable**

## 手順の詳細

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b>  例： <pre>switch# configure terminal switch(config) #</pre>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config) # <b>no snmp-server protocol enable</b>  例： <pre>no snmp-server protocol enable</pre>	SNMP を無効にします。 SNMP は、デフォルトで無効になっています。

## 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
<b>show snmp</b>	SNMP ステータスを表示します。
<b>show snmp community</b>	SNMP コミュニティ ストリングを表示します。
<b>show interface snmp-ifindex</b>	すべてのインターフェイスについて (IF-MIB から) SNMP の ifIndex 値を表示します。
<b>show running-config snmp [all]</b>	SNMP の実行コンフィギュレーションを表示します。
<b>show snmp engineID</b>	SNMP engineID を表示します。
<b>show snmp group</b>	SNMP ロールを表示します。
<b>show snmp sessions</b>	SNMP セッションを表示します。
<b>show snmp context</b>	SNMP コンテキスト マッピングを表示します。
<b>show snmp host</b>	設定した SNMP ホストの情報を表示します。
<b>show snmp source-interface</b>	設定した発信元インターフェイスの情報を表示します。
<b>show snmp trap</b>	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。
<b>show snmp user</b>	SNMPv3 ユーザを表示します。

## ■ SNMP 設定の確認



## 第 12 章

# PCAP SNMP パーサーの使用

この章は、次の項で構成されています。

- [PCAP SNMP パーサーの使用 \(181 ページ\)](#)

## PCAP SNMP パーサーの使用

PCAP SNMP パーサーは、.pcap 形式でキャプチャされた SNMP パケットを分析するツールです。スイッチ上で動作し、スイッチに送信されるすべての SNMP get、getnext、getbulk、set、trap、および response 要求の統計情報レポートを生成します。

PCAP SNMP パーサーを使用するには、次のいずれかのコマンドを使用します。

- **debug packet-analysis snmp [mgmt0 | inband] duration seconds [output-file] [keep-pcap]**—Tshark を使用して指定の秒数間のパケットをキャプチャし、一時 .pcap ファイルに保存します。次に、その .pcap ファイルに基づいてパケットを分析します。

結果は出力ファイルに保存されます。出力ファイルが指定されていない場合は、コンソールに出力されます。次のオプションを使用する場合を除き、一時 .pcap ファイルはデフォルトで削除されます。 **keep-pcap** オプションを使用します。パケット キャプチャは、デフォルトの管理インターフェイス (mgmt0)、または帯域内インターフェイスで実行できます。

例：

```
switch# debug packet-analysis snmp duration 100
switch# debug packet-analysis snmp duration 100 bootflash:snmp_stats.log
switch# debug packet-analysis snmp duration 100 bootflash:snmp_stats.log keep-pcap
switch# debug packet-analysis snmp inband duration 100
switch# debug packet-analysis snmp inband duration 100 bootflash:snmp_stats.log
switch# debug packet-analysis snmp inband duration 100 bootflash:snmp_stats.log
keep-pcap
```

## ■ PCAP SNMP パーサーの使用

- **debug packet-analysis snmp** *input-pcap-file* [*output-file*] : 既存の .pcap ファイルにあるキャプチャしたパケットを分析します。

例 :

```
switch# debug packet-analysis snmp bootflash:snmp.pcap
switch# debug packet-analysis snmp bootflash:snmp.pcap bootflash:snmp_stats.log
```

次に、**debug packet-analysis snmp [mgmt0 | inband] duration** command の統計情報レポートの例を示します :

```
switch# debug packet-analysis snmp duration 10
Capturing on eth0
36
wireshark-cisco-mtc-dissector: ethertype=0xde09, devicetype=0x0
wireshark-broadcom-rcpu-dissector: ethertype=0xde08, devicetype=0x0

Started analyzing. It may take several minutes, please wait!

Statistics Report
-----
SNMP Packet Capture Duration: 0 seconds
Total Hosts: 1
Total Requests: 18
Total Responses: 18
Total GET: 0
Total GETNEXT: 0
Total WALK: 1 (NEXT: 18)
Total GETBULK: 0
Total BULKWALK: 0 (BULK: 0)
Total SET: 0
Total TRAP: 0
Total INFORM: 0

Hosts      GET  GETNEXT  WALK(NEXT)  GETBULK  BULKWALK(BULK)  SET  TRAP  INFORM  RESPONSE
-----
10.22.27.244  0      0          1(18)      0          0(0)        0      0      0        18

Sessions
-----
1

MIB Objects  GET  GETNEXT  WALK(NEXT)  GETBULK(Non_rep/Max_rep)  BULKWALK(BULK,
Non_rep/Max_rep)
-----
ifName      0      0          1(18)      0          0

SET      Hosts
-----
0      10.22.27.244
```



## 第 13 章

# RMON の設定

この章は、次の項で構成されています。

- [RMONについて, on page 183](#)
- [RMONの設定時の注意事項および制約事項 \(185 ページ\)](#)
- [RMON 設定の確認, on page 185](#)
- [デフォルトの RMON 設定, on page 185](#)
- [RMON アラームの設定, on page 185](#)
- [RMON イベントの設定, on page 187](#)

## 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では、Cisco Nexusデバイスをモニターするための、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構成されていません。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、1.3.6.1.2.1.2.1.17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

## RMON イベント

- 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トリガーする、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



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

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



**Note** 下限しきい値には、上限しきい値よりも小さな値を指定してください。

## RMON イベント

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

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

下限アラームおよび上限アラームに異なるイベントを指定できます。

# 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 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
<b>show rmon alarms</b>	RMON アラームに関する情報を表示します。
<b>show rmon events</b>	RMON イベントに関する情報を表示します。
<b>show rmon hcalarms</b>	RMON 高容量アラームに関する情報を表示します。
<b>show rmon logs</b>	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。

*Table 20: デフォルトの RMON パラメータ*

パラメータ	デフォルト
アラーム	未設定
イベント	未設定

## 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

## RMON アラームの設定

- アラームのオーナー

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

### Before you begin

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

### SUMMARY STEPS

- switch# **configure terminal**
- switch(config)# **rmon alarm index mib-object sample-interval {absolute | delta} rising-threshold value [event-index] falling-threshold value [event-index] [owner name]**
- 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]**
- (Optional) switch# **show rmon {alarms | hcalarms}**
- (Optional) switch# **copy running-config startup-config**

### DETAILED STEPS

#### Procedure

	<b>Command or Action</b>	<b>Purpose</b>
ステップ 1	switch# <b>configure terminal</b>	グローバル コ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)# <b>rmon alarm index mib-object sample-interval {absolute   delta} rising-threshold value [event-index] falling-threshold value [event-index] [owner name]</b>	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)# <b>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]</b>	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。
ステップ 4	(Optional) switch# <b>show rmon {alarms   hcalarms}</b>	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	(Optional) switch# <b>copy running-config startup-config</b>	この設定変更を保存します。

#### Example

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。

### Before you begin

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

### SUMMARY STEPS

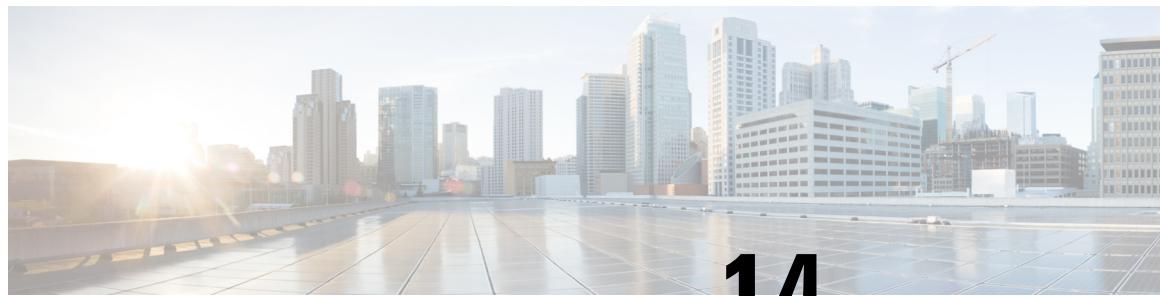
1. switch# **configure terminal**
2. switch(config)# **rmon event index [description string] [log] [trap] [owner name]**
3. (Optional) switch(config)# **show rmon {alarms | halarms}**
4. (Optional) switch# **copy running-config startup-config**

### DETAILED STEPS

#### Procedure

	<b>Command or Action</b>	<b>Purpose</b>
ステップ 1	switch# <b>configure terminal</b>	グローバル コ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)# <b>rmon event index [description string] [log] [trap] [owner name]</b>	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。
ステップ 3	(Optional) switch(config)# <b>show rmon {alarms   halarms}</b>	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	(Optional) switch# <b>copy running-config startup-config</b>	この設定変更を保存します。

## RMON イベントの設定



# 第 14 章

## オンライン診断の設定

この章は、次の項で構成されています。

- オンライン診断について, [on page 189](#)
- オンライン診断の注意事項と制約事項 ([191 ページ](#))
- オンライン診断の設定, [on page 191](#)
- オンライン診断設定の確認, [on page 192](#)
- オンライン診断のデフォルト設定, [on page 192](#)

### 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 3600 プラットフォームスイッチは、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。

**Table 21:** 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。
NVRAM	NVRAM (不揮発性 RAM) の整合性を確認します。

## ■ ヘルス モニタリング診断

診断	説明
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に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 デバイスを構成することも、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 トライフィックを処理するスイッチの状態を確認します。

## 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、起動時診断と共に実行されます。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。

**Table 22:** 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。

**Table 23:** 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。

## オンライン診断の注意事項と制約事項

オンライン診断には、次の注意事項と制限事項があります。

- 中断を伴うオンライン診断テストをオンデマンド方式で実行することはできません。
- BootupPortLoopback テストはサポートされていません。
- インターフェイス Rx および Tx パケット カウンタは、シャットダウン状態のポートで増えます（およそ 15 分ごとに 4 パケット）。
- 管理ダウンポートでは、ユニキャストパケット Rx および Tx のカウンタが、GOLD ループバック パケットに対して追加されます。PortLoopback テストは、オンデマンドです。したがって、テストを管理ダウンポートで実行する場合にのみ、パケットカウンタが追加されます。

## 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。



**Note** ブートアップオンライン診断レベルを `complete` に設定することを推奨します。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。

### SUMMARY STEPS

1. `switch# configure terminal`
2. `switch(config)# diagnostic bootup level [complete | bypass]`
3. (Optional) `switch# show diagnostic bootup level`

## オンライン診断設定の確認

### DETAILED STEPS

#### Procedure

	Command or Action	Purpose
ステップ1	switch# <b>configure terminal</b>	グローバルコ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)# <b>diagnostic bootup level [complete   bypass]</b>	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。 <ul style="list-style-type: none"> <li>• <b>complete</b> : すべてのブートアップ診断を実行します。これはデフォルト値です。</li> <li>• <b>bypass</b> : ブートアップ診断を実行しません。</li> </ul>
ステップ3	(Optional) switch# <b>show diagnostic bootup level</b>	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。

#### Example

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
<b>show diagnostic bootup level</b>	起動時診断レベルを表示します。
<b>show diagnostic result module slot</b>	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。

**Table 24:** デフォルトのオンライン診断パラメータ

パラメータ	デフォルト
起動時診断レベル	complete

## オンライン診断のデフォルト設定



# 第 15 章

## Embedded Event Manager の設定

この章は、次の項で構成されています。

- [組み込みイベント マネージャについて \(195 ページ\)](#)
- [Embedded Event Manager の設定 \(200 ページ\)](#)
- [Embedded Event Manager の設定確認 \(231 ページ\)](#)
- [Embedded Event Manager の設定例 \(232 ページ\)](#)
- [その他の参考資料 \(233 ページ\)](#)

### 組み込みイベント マネージャについて

Cisco NX-OS システム内のクリティカルイベントを検出して処理する機能は、ハイ アベイラビリティにとって重要です。Embedded Event Manager (EEM) は、デバイス上で発生するイベントをモニターし、設定に基づいてこれらのイベントを回復またはトラブルシューティングするためのアクションを実行することによってシステム内のイベントを検出して処理する、中央のポリシー駆動型のフレームワークを提供します。

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

何らかのアクション、回避策、または通知が必要になる可能性のある、別の Cisco NX-OS コンポーネントからモニターするイベント。

#### アクション文

電子メールの送信やインターフェイスのディセーブル化などの、イベントから回復するために EEM が実行できるアクション。

#### ポリシー

イベントのトラブルシューティングまたはイベントからの回復を目的とした 1 つまたは複数のアクションとペアになったイベント。

EEM を使用しない場合は、個々のコンポーネントが独自のイベントの検出および処理を行います。たとえば、ポートでフラップが頻繁に発生する場合は、「errDisable ステートにする」のポリシーが ETHPM に組み込まれます。

## Embedded Event Manager 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。

たとえば、いつカードがデバイスから取り外されたかを識別し、カードの取り外しに関する詳細を記録する EEM ポリシーを設定できます。カードの取り外しのインスタンスすべてを探すようにシステムに指示するイベント文および詳細を記録するようにシステムに指示するアクション文を設定します。

コマンドラインインターフェイス (CLI) または VSH スクリプトを使用して EEM ポリシーを設定できます。

EEM からデバイス全体のポリシー管理ビューが得られます。EEM ポリシーが構成されると、対応するアクションがトリガーされます。トリガーされたイベントのすべてのアクション（システムまたはユーザー設定）がシステムによって追跡され、管理されます。

### 事前設定済みのシステム ポリシー

Cisco NX-OS には、事前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。

一部のシステム ポリシーは上書きできます。このような場合、イベントまたはアクションに対する上書きを設定できます。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。



(注) 上書きポリシーにはイベント文を含める必要があります。イベント文が含まれていない上書きポリシーは、システム ポリシーで想定されるすべてのイベントを上書きします。

事前設定済みのシステム ポリシーを表示し、上書きできるポリシーを決定するには、**show event manager system-policy** コマンドを使用します。

### ユーザー作成ポリシー

ユーザー作成ポリシーを使用すると、ネットワークの EEM ポリシーをカスタマイズできます。ユーザー ポリシーがイベントに対して作成されると、ポリシーのアクションは、EEM が同じイベントに関連するシステム ポリシー アクションをトリガーした後にのみトリガーされます。

### ログ ファイル

EEM ポリシーの一貫に関連するデータが格納されたログ ファイルは、/log/event\_archive\_1 ディレクトリにある event\_archive\_1 ログ ファイルで維持されます。

## イベント文

対応策、通知など、一部のアクションが実行されるデバイスアクティビティは、EEMによってイベントと見なされます。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。

イベント文は、どのイベントがポリシー実行のトリガーになるかを指定します。



**ヒント** ポリシー内に複数の EEM イベントを作成し、区別してから、カスタムアクションをトリガーするためのイベントの組み合わせを定義することで、イベントの組み合わせに基づいた EEM ポリシーをトリガーするように EEM を設定できます。

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。

一部のコマンドまたは内部イベントが他のコマンドを内部的にトリガーします。これらのコマンドは表示されませんが、引き続きアクションをトリガーするイベント指定と一致します。これらのコマンドがアクションをトリガーするのを防ぐことはできませんが、どのイベントがアクションを引き起こしたかを確認できます。

### サポートされるイベント

EEM はイベント文で次のイベントをサポートします。

- カウンタイベント
- ファン欠損イベント
- ファン不良イベント
- メモリしきい値イベント
- 上書きされたシステム ポリシーで使用されるイベント
- SNMP 通知イベント
- syslog イベント
- システム マネージャイベント
- 温度イベント
- 追跡イベント

## アクション文

アクション文は、イベントが発生したときに、ポリシーによってトリガーされるアクションを説明します。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。

## VSH スクリプト ポリシー

トリガーされたイベントがデフォルト アクションを処理するために、デフォルト 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、一致文で CLI コマンドを照合する場合、EEM ポリシーに `event-default` アクション文を追加する必要があります。この文がないと、EEM ではコマンドを実行できません。



(注) ユーザー ポリシーまたは上書き ポリシー内のアクション文を設定する場合、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るようなことがないよう確認することが重要です。

### サポートされるアクション

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
- 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

## VSH スクリプト ポリシー

テキストエディタを使用して、VSH スクリプトでポリシーを作成できます。VSH スクリプトを使用して作成されたポリシーには、他のポリシーと同様にイベント文とアクション文が含まれます。また、これらのポリシーはシステム ポリシーを拡張するか、または無効にすることができます。

VSH スクリプト ポリシーを定義したら、それをデバイスにコピーしてアクティブにします。

## Embedded Event Manager 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。Cisco NX-OS のライセンス スキームの詳細は、『Cisco NX-OS ライセンス ガイド』を参照してください。

## Embedded Event Manager の前提条件

EEM を設定するには、network-admin の権限が必要です。

## Embedded Event Manager の注意事項および制約事項

EEM の設定を計画するときは、次の点を考慮します。

- 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ることがあります。このようにする必要があります。
- 発生したイベントでデフォルトのアクションを処理できるようにするには、デフォルトのアクションを許可する EEM ポリシーを設定する必要があります。たとえば、一致文で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 ではコマンドを実行できません。
- イベントログの自動収集とバックアップには、次の注意事項があります。
  - デフォルトでは、スイッチのログ収集を有効にすると、サイズ、規模、コンポーネントのアクティビティに応じて、15 分から数時間のイベントログが利用できるようになります。
  - 長期間にわたる関連ログを収集できるようにするには、必要な特定のサービス/機能に対してのみイベントログの保持を有効にします。「単一サービスの拡張ログファイル保持の有効化」を参照してください。内部イベントログをエクスポートすることもできます。「外部ログファイルストレージ」を参照してください。
  - トラブルシューティングを行うときは、内部イベントログのスナップショットを手動によりリアルタイムで収集することをお勧めします。「最近のログファイルのローカルコピーの生成」を参照してください。
- 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、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。

## ■ Embedded Event Manager のデフォルト設定

- イベント指定が CLI のパターンと一致する場合、SSH 形式のワイルドカード文字を使用できます。  
たとえば、すべての **show** コマンドを照合する場合は、**show\*** コマンドを入力します。このようなスイッチ（バンドル PID）に、**show.\*** コマンドは機能しませんでした。
- イベント指定が一致する syslog メッセージの正規表現の場合、適切な正規表現を使用できます。  
たとえば、syslog が生成されているポート上で ADMIN\_DOWN イベントを検出するには、**.ADMIN\_DOWN.** を使用します。このようなスイッチ（バンドル PID）に、**ADMIN\_DOWN** コマンドは機能しませんでした。
- syslog のイベント指定では、**regex** は、EEM ポリシーのアクションとして生成される syslog メッセージと一致しません。
- EEM イベントが CLI の **show** コマンドと一致していて、**show** コマンドの出力を画面に表示したい（および EEM ポリシーによってブロックされないように）場合は、**event-default** コマンドを EEM ポリシーの最初のアクションに使用する必要があります。

## Embedded Event Manager のデフォルト設定

表 25: デフォルトの EEM パラメータ

パラメータ	デフォルト
システム ポリシー	アクティブ

## Embedded Event Manager の設定

### 環境変数の定義

環境変数の定義はオプションの手順ですが、複数のポリシーで繰り返し使用する共通の値を設定する場合に役立ちます。

#### 手順の概要

- configure terminal**
- event manager environment variable-name variable-value**
- (任意) **show event manager environment {variable-name | all}**
- (任意) **copy running-config startup-config**

## 手順の詳細

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b>  例： <pre>switch# configure terminal switch(config) #</pre>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>event manager environment variable-name variable-value</b>  例： <pre>switch(config) # event manager environment emailto "admin@anyplace.com"</pre>	EEM 用の環境変数を作成します。 <i>variable-name</i> です。 <i>variable-value</i> では大文字と小文字が区別され、引用符で囲んだ最大 39 文字の英数字を使用できます。
ステップ 3	(任意) <b>show event manager environment {variable-name   all}</b>  例： <pre>switch(config) # show event manager environment all</pre>	設定した環境変数に関する情報を表示します。
ステップ 4	(任意) <b>copy running-config startup-config</b>  例： <pre>switch(config) # copy running-config startup-config</pre>	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。

## CLI によるユーザー ポリシーの定義

## 手順の概要

1. **configure terminal**
2. **event manager applet applet-name**
3. (任意) **description policy-description**
4. **event event-statement**
5. (任意) **tag tag {and | andnot | or} tag [and | andnot | or {tag}] {happens occurs in seconds}**
6. **action number[.number2] action-statement**
7. (任意) **show event manager policy-state name [module module-id]**
8. (任意) **copy running-config startup-config**

## CLI によるユーザー ポリシーの定義

## 手順の詳細

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b>  例： <pre>switch# configure terminal switch(config) #</pre>	グローバルコンフィギュレーション モードを開始します。
ステップ 2	<b>event manager applet applet-name</b>  例： <pre>switch(config) # event manager applet monitorShutdown switch(config-applet) #</pre>	EEM にアプレットを登録し、アプレット コンフィギュレーション モードを開始します。  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	(任意) <b>description policy-description</b>  例： <pre>switch(config-applet) # description "Monitors interface shutdown."</pre>	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	<b>event event-statement</b>  例： <pre>switch(config-applet) # event cli match "shutdown"</pre>	ポリシーのイベント文を設定します。
ステップ 5	(任意) <b>tag tag {and   andnot   or} tag [and   andnot   or {tag}] {happens occurs in seconds}</b>  例： <pre>switch(config-applet) # tag one or two happens 1 in 10000</pre>	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	<b>action number[number2] action-statement</b>  例： <pre>switch(config-applet) # action 1.0 cli show interface e 3/1</pre>	ポリシーのアクション文を設定します。アクション文が複数ある場合、このステップを繰り返します。
ステップ 7	(任意) <b>show event manager policy-state name [module module-id]</b>  例： <pre>switch(config-applet) # show event manager policy-state monitorShutdown</pre>	設定したポリシーの状態に関する情報を表示します。
ステップ 8	(任意) <b>copy running-config startup-config</b>  例： <pre>switch(config) # copy running-config startup-config</pre>	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。

## 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 (config-applet) で次のいずれかのコマンドを使用します。

### 始める前に

ユーザー ポリシーを定義します。

### 手順の概要

1. **event cli [tag tag] match expression [count repeats | time seconds]**
2. **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}}**
3. **event fanabsent [fan number] time seconds**
4. **event fanbad [fan number] time seconds**
5. **event memory {critical | minor | severe}**
6. **event policy-default count repeats [time seconds]**
7. **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**
8. **event sysmgr memory [module module-num] major major-percent minor minor-percent clear clear-percent**
9. **event temperature [module slot] [sensor number] threshold {any | down | up}**
10. **event track [tag tag] object-number state {any | down | up}**

### 手順の詳細

#### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>event cli [tag tag] match expression [count repeats   time seconds]</b>  <b>例 :</b> <pre>switch(config-applet) # event cli match "shutdown"</pre>	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。  <b>tag tag</b> 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。  繰り返し範囲は 1 ~ 65000 です。  <b>time</b> の範囲は 0 ~ 4294967295 です。0 は無制限を示します。
ステップ 2	<b>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}}</b>  <b>例 :</b>	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

## ■ イベント文の設定

	コマンドまたはアクション	目的
	switch(config-applet) # event counter name mycounter entry-val 20 gt	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。  <b>tag tag</b> 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。  <i>counter</i> の名前では、大文字と小文字を区別し、最大 28 の英数字を使用できます。  <i>entry</i> および <i>exit</i> 値の範囲は 0 ~ 2147483647 です。
ステップ 3	<b>event fanabsent [fan number] time seconds</b>  例： switch(config-applet) # event fanabsent time 300	秒数で設定された時間を超えて、ファンがデバイスから取り外されている場合に、イベントを発生させます。  <i>number</i> の範囲は 1 対 1 で、モジュールに依存します。  <i>seconds</i> の範囲は 10 ~ 64000 です。
ステップ 4	<b>event fanbad [fan number] time seconds</b>  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。  <i>number</i> の範囲はモジュールに依存します。  <i>seconds</i> の範囲は 10 ~ 64000 です。
ステップ 5	<b>event memory {critical   minor   severe}</b>  例： switch(config-applet) # event memory critical	メモリのしきい値を超えた場合にイベントを発生させます。
ステップ 6	<b>event policy-default count repeats [time seconds]</b>  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。  繰り返し範囲は 1 ~ 65000 です。  <i>seconds</i> の範囲は 0 ~ 4294967295 です。0 は無制限を示します。
ステップ 7	<b>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-time time polling-interval interval</b>  例： switch(config-applet) # event snmp oid 1.3.6.1.2.1.31.1.1.1.6 get-type next	SNMP OID が、開始演算子に基づいて開始のしきい値を超えた場合にイベントを発生させます。イベントはただちにリセットされます。または任意で、カウンタが終了のしきい値を超えたあとでリセットされるように、イベントを設定できます。OID はドット付き 10 進表記です。

	コマンドまたはアクション	目的
	entry-op lt 300 entry-val 0 exit-op eq 400 exit-time 30 polling-interval 300	<b>tag tag</b> 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。  <i>entry</i> および <i>exit</i> の値の範囲は 0 ~ 18446744073709551615 です。  <i>time</i> の範囲は 0 ~ 2147483647 秒です。  <i>interval</i> の範囲は 0 ~ 2147483647 秒です。
ステップ 8	<b>event sysmgr memory [module module-num] major major-percent minor minor-percent clear-clear-percent</b>  例： <pre>switch(config-applet) # event sysmgr memory minor 80</pre>	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。  <i>percent</i> の範囲は 1 ~ 99 です。
ステップ 9	<b>event temperature [module slot] [sensor number] threshold {any   down   up}</b>  例： <pre>switch(config-applet) # event temperature module 2 threshold any</pre>	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。  センサーの範囲は 1 ~ 18 です。
ステップ 10	<b>event track [tag tag] object-number state {any   down   up}</b>  例： <pre>switch(config-applet) # event track 1 state down</pre>	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。  <b>tag tag</b> 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。  <i>object-number</i> の範囲は 1 ~ 500 です。

### 次のタスク

アクション文を構成します。

すでにアクション文を設定した場合、または設定しないことを選択した場合は、次のオプション作業のいずれかを実行します。

- VSH スクリプトを使用してポリシーを定義します。その後、VSH スクリプト ポリシーを登録し、アクティブにします。
- メモリのしきい値を設定します。
- EEM パブリッシャとして syslog を設定します。
- EEM 設定を確認します。

## アクション文の設定

## アクション文の設定

EEM のコンフィギュレーション モード (config-applet) で次のいずれかのコマンドを使用して、アクションを設定できます。



(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、一致文で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 ではコマンドを実行できません。次の表で、**terminal event-manager bypass** コマンドを使用すると、一致するすべての EEM ポリシーでコマンドを実行できます。

## 始める前に

ユーザー ポリシーを定義します。

## 手順の概要

1. **action number[.number2] cli command1[command2.] [local]**
2. **action number[.number2] counter name counter value val op {dec | inc | nop | set}**
3. **action number[.number2] event-default**
4. **action number[.number2] policy-default**
5. **action number[.number2] reload [module slot [- slot]]**
6. **action number[.number2] snmp-trap [intdata1 integer-data1] [intdata2 integer-data2] [strdata string-data]**
7. **action number[.number2] syslog [priority prio-val] msg error-message**

## 手順の詳細

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>action number[.number2] cli command1[command2.] [local]</b> 例： <pre>switch(config-applet) # action 1.0 cli "show interface e 3/1"</pre>	設定済み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 には 1 ~ 16 行の任意の番号を指定できます。 number2 の範囲は 0 ~ 9 です。

	コマンドまたはアクション	目的
ステップ 2	<b>action</b> <i>number</i> [. <i>number2</i> ] <b>counter</b> <i>name</i> <b>counter</b> <i>value</i> <i>val</i> <b>op</b> { <b>dec</b>   <b>inc</b>   <b>nop</b>   <b>set</b> }	<p>設定された値および操作でカウンタを変更します。</p> <p>アクションラベルのフォーマットは<i>number1.number2</i>です。</p> <p><i>number</i> には 1 ~ 16 行の任意の番号を指定できます。</p> <p><i>number2</i> の範囲はは 0 ~ 9 です。</p> <p><i>counter</i> は、28 文字以内の英数字のストリング（大文字と小文字を区別）で指定します。</p> <p><i>val</i> には 0 ~ 2147483647 の整数または置換パラメータを指定できます。</p>
ステップ 3	<b>action</b> <i>number</i> [. <i>number2</i> ] <b>event-default</b> <b>例 :</b> <pre>switch(config-applet) # action 1.0 event-default</pre>	<p>関連付けられたイベントのデフォルトアクションを実行します。</p> <p>アクションラベルのフォーマットは<i>number1.number2</i>です。</p> <p><i>number</i> には 1 ~ 16 行の任意の番号を指定できます。</p> <p><i>number2</i> の範囲はは 0 ~ 9 です。</p>
ステップ 4	<b>action</b> <i>number</i> [. <i>number2</i> ] <b>policy-default</b> <b>例 :</b> <pre>switch(config-applet) # action 1.0 policy-default</pre>	<p>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。</p> <p>アクションラベルのフォーマットは<i>number1.number2</i>です。</p> <p><i>number</i> には 1 ~ 16 行の任意の番号を指定できます。</p> <p><i>number2</i> の範囲はは 0 ~ 9 です。</p>
ステップ 5	<b>action</b> <i>number</i> [. <i>number2</i> ] <b>reload</b> [ <b>module</b> <i>slot</i> [- <i>slot</i> ]] <b>例 :</b> <pre>switch(config-applet) # action 1.0 reload module 3-5</pre>	<p>システム全体に 1 つ以上のモジュールをリロードします。</p> <p>アクションラベルのフォーマットは<i>number1.number2</i>です。</p> <p><i>number</i> には 1 ~ 16 行の任意の番号を指定できます。</p> <p><i>number2</i> の範囲はは 0 ~ 9 です。</p>

## VSH スクリプトによるポリシーの定義

	コマンドまたはアクション	目的
ステップ 6	<b>action number[.number2] snmp-trap [intdata1 integer-data1] [intdata2 integer-data2] [strdata string-data]</b> 例： <pre>switch(config-applet) # action 1.0 snmp-trap strdata "temperature problem"</pre>	設定されたデータを使用して SNMP トランプルを送信します。アクション ラベルのフォーマットは <i>number1.number2</i> です。 <i>number</i> には 1 ~ 16 行の任意の番号を指定できます。 <i>number2</i> の範囲は 0 ~ 9 です。 <i>data</i> 要素には 80 行までの任意の数を指定できます。 <i>文字列</i> には最大 80 文字の英数字を使用できます。
ステップ 7	<b>action number[.number2] syslog [priority prio-val] msg error-message</b> 例： <pre>switch(config-applet) # action 1.0 syslog priority notifications msg "cpu high"</pre>	設定されたプライオリティで、カスタマイズした syslog メッセージを送信します。 アクション ラベルのフォーマットは <i>number1.number2</i> です。 <i>number</i> には 1 ~ 16 行の任意の番号を指定できます。 <i>number2</i> の範囲は 0 ~ 9 です。 <i>error-message</i> には最大 80 文字の英数字を引用符で囲んで使用できます。

## 次のタスク

イベント文を設定します。

すでにイベント文を設定した場合、または設定しないことを選択した場合は、次のオプション作業のいずれかを実行します。

- VSH スクリプトを使用してポリシーを定義します。その後、VSH スクリプト ポリシーを登録し、アクティブにします。
- メモリのしきい値を設定します。
- EEM パブリッシャとして syslog を設定します。
- EEM 設定を確認します。

## VSH スクリプトによるポリシーの定義

これはオプションのタスクです。VSH スクリプトを使用して EEM ポリシーを記述する場合は、次の手順を実行します。

## 手順の概要

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。
2. テキストファイルに名前をつけて保存します。
3. 次のシステムディレクトリにファイルをコピーします。bootflash://eem/user\_script\_policies

## 手順の詳細

### 手順

**ステップ1** テキストエディタで、ポリシーを定義するコマンドリストを指定します。

**ステップ2** テキストファイルに名前をつけて保存します。

**ステップ3** 次のシステムディレクトリにファイルをコピーします。bootflash://eem/user\_script\_policies

### 次のタスク

VSH スクリプト ポリシーを登録してアクティブにします。

## VSH スクリプト ポリシーの登録およびアクティブ化

これはオプションのタスクです。VSH スクリプトを使用して EEM ポリシーを記述する場合は、次の手順を実行します。

### 始める前に

ポリシーを VSH スクリプトを使用して定義し、システムディレクトリにファイルをコピーします。

## 手順の概要

1. **configure terminal**
2. **event manager policy *policy-script***
3. (任意) **event manager policy internal *name***
4. (任意) **copy running-config startup-config**

## 手順の詳細

### 手順

	コマンドまたはアクション	目的
<b>ステップ1</b>	<b>configure terminal</b> 例 :	グローバルコンフィギュレーションモードを開始します。

## ■ システム ポリシーの上書き

	コマンドまたはアクション	目的
	switch# configure terminal switch(config) #	
ステップ 2	<b>event manager policy</b> <i>policy-script</i>  例： switch(config) # event manager policy moduleScript	EEM スクリプト ポリシーを登録してアクティブにします。  値は、 <i>policy-script</i> は、29 文字以内の英数字のストリング（大文字と小文字を区別）で指定します。
ステップ 3	(任意) <b>event manager policy internal</b> <i>name</i>  例： switch(config) # event manager policy internal moduleScript	EEM スクリプト ポリシーを登録してアクティブにします。  値は、 <i>policy-script</i> は、29 文字以内の英数字のストリング（大文字と小文字を区別）で指定します。
ステップ 4	(任意) <b>copy running-config startup-config</b>  例： switch(config) # 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。

## 次のタスク

システム要件に応じて、次のいずれかを実行します。

- メモリのしきい値を設定します。
- EEM パブリッシャとして syslog を設定します。
- EEM 設定を確認します。

## システム ポリシーの上書き

### 手順の概要

1. **configure terminal**
2. (任意) **show event manager policy-state** *system-policy*
3. **event manager applet** *applet-name* **override** *system-policy*
4. **description** *policy-description*
5. **event** *event-statement*
6. **section** *number* *action-statement*
7. (任意) **show event manager policy-state** *name*
8. (任意) **copy running-config startup-config**

## 手順の詳細

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b>  例： <pre>switch# configure terminal switch(config) #</pre>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	(任意) <b>show event manager policy-state system-policy</b>  例： <pre>switch(config-applet)# show event manager policy-state __ethpm_link_flap Policy __ethpm_link_flap   Cfg count : 5   Cfg time interval : 10.000000 (seconds)   Hash default, Count 0</pre>	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。 <b>show event manager system-policy</b> コマンドを使用して、システム ポリシーの名前を探します。
ステップ 3	<b>event manager applet applet-name override system-policy</b>  例： <pre>switch(config-applet)# event manager applet ethport override __ethpm_link_flap switch(config-applet) #</pre>	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。 値は、 <i>applet-name</i> は、80 文字以内の英数字のストリング（大文字と小文字を区別）で指定します。 値は、 <i>system-policy</i> は、システム ポリシーの 1 つである必要があります。
ステップ 4	<b>description policy-description</b>  例： <pre>switch(config-applet)# description "Overrides link flap policy"</pre>	ポリシーの説明になるストリングを設定します。 値は、 <i>policy-description</i> は大文字と小文字を区別し、最大 80 文字の英数字を使用できますが、引用符で囲む必要があります。
ステップ 5	<b>event event-statement</b>  例： <pre>switch(config-applet)# event policy-default count 2 time 1000</pre>	ポリシーのイベント文を設定します。
ステップ 6	<b>section number action-statement</b>  例： <pre>switch(config-applet)# action 1.0 syslog priority warnings msg "Link is flapping."</pre>	ポリシーのアクション文を設定します。複数のアクション文では、この手順を繰り返します。
ステップ 7	(任意) <b>show event manager policy-state name</b>  例：	設定したポリシーに関する情報を表示します。

## ■ EEM パブリッシャとしての syslog の設定

	コマンドまたはアクション	目的
	switch(config-applet)# show event manager policy-state ethport	
ステップ 8	(任意) <b>copy running-config startup-config</b> 例： switch(config)# 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。

## EEM パブリッシャとしての syslog の設定

EEM パブリッシャとして syslog を設定すると、スイッチから syslog メッセージをモニターできます。



(注) syslog メッセージをモニターする検索文字列の最大数は 10 です。

### 始める前に

- EEM が syslog による登録で利用できることを確認します。
- syslog デーモンが設定され、実行されていることを確認します。

### 手順の概要

1. **configure terminal**
2. **event manager applet *applet-name***
3. **event syslog [tag *tag*] {occurs *number* | period *seconds* | pattern *msg-text* | priority *priority*}**
4. (任意) **copy running-config startup-config**

### 手順の詳細

#### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 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	<b>event manager applet <i>applet-name</i></b> 例： switch(config)# event manager applet abc switch (config-applet) #	EEM にアプレットを登録し、アプレットコンフィギュレーションモードを開始します。

	コマンドまたはアクション	目的
ステップ 3	<b>event syslog [tag tag] {occurs number   period seconds   pattern msg-text   priority priority}</b>  例： <pre>switch(config-applet)# event syslog occurs 10</pre>	EEM にアプレットを登録し、アプレット コンフィギュレーション モードを開始します。
ステップ 4	(任意) <b>copy running-config startup-config</b>  例： <pre>switch(config)# copy running-config startup-config</pre>	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。

#### 次のタスク

EEM 設定を確認します。

## Embedded Event Manager の設定確認

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
<b>show event manager environment [variable-name   all]</b>	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。
<b>show event manager event-types [event   all   module slot]</b>	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。
<b>show event manager history events [detail] [maximum num-events] [severity {catastrophic   minor   moderate   severe}]</b>	すべてのポリシーについて、イベント履歴を表示します。
<b>show event manager policy-state policy-name</b>	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。
<b>show event manager script system [policy-name   all]</b>	スクリプト ポリシーに関する情報を表示します。
<b>show event manager system-policy [all]</b>	定義済みシステム ポリシーに関する情報を表示します。
<b>show running-config eem</b>	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。
<b>show startup-config eem</b>	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。

## ■ イベント ログの自動収集とバックアップ

# イベント ログの自動収集とバックアップ

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

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

- 拡張ログ ファイルの保持
- トリガーベースのイベント ログの自動収集

## 拡張ログ ファイルの保持

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

### すべてのサービスの拡張ログ ファイル保持のイネーブル化

拡張ログ ファイル保持は、スイッチで実行されているすべてのサービスに対してデフォルトで有効になっています。スイッチがログ ファイル保持機能が有効になっていない場合 (**no bloggerd log-dump** が構成済み) 、次の手順を使用して有効にします。

#### 手順の概要

1. **configure terminal**
2. **bloggerd log-dump all**

#### 手順の詳細

##### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b>  例： <pre>switch# configure terminal switch(config) #</pre>	グローバル コンフィギュレーション モードを開始します
ステップ 2	<b>bloggerd log-dump all</b>  例： <pre>switch(config) # bloggerd log-dump all switch(config) #</pre>	すべてのサービスのログ ファイル保持機能をイネーブルにします。

**例**

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

```

**すべてのサービスの拡張ログ ファイル保持の無効化**

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

**手順の概要**

1. **configure terminal**
2. **no bloggerd log-dump all**

**手順の詳細****手順**

	コマンドまたはアクション	目的
<b>ステップ 1</b>	<b>configure terminal</b>  例： <pre>switch# configure terminal switch(config)# </pre>	グローバル コンフィギュレーション モードを開始します
<b>ステップ 2</b>	<b>no bloggerd log-dump all</b>  例： <pre>switch(config)# no bloggerd log-dump all switch(config)# </pre>	スイッチ上のすべてのサービスのログファイル保持機能を無効にします。

**例**

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

```

**単一サービスの拡張ログファイル保持の有効化**

拡張ログファイル保持は、スイッチで実行されているすべてのサービスに対してデフォルトで有効になっています。スイッチがログファイル保持機能が有効になっていない場合 (**no bloggerd log-dump** 構成済み)、次の手順を使用して単一のサービスに対して有効にします。

## ■ 単一サービスの拡張ログファイル保持の有効化

## 手順の概要

1. **show system internal sysmgr service name *service-type***
2. **configure terminal**
3. **bloggerd log-dump sap *number***
4. **show system internal bloggerd info log-dump-info**

## 手順の詳細

## 手順

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

## 例

```

switch# show system internal sysmgr service name aclmgr
Service "aclmgr" ("aclmgr", 80):
    UUID = 0x182, PID = 653, SAP = 351
    State: SRV_STATE_HANDSHAKED (entered at time Mon Nov 4 11:10:41 2019).
    Restart count: 1
    Time of last restart: Mon Nov 4 11:10:39 2019.
    The service never crashed since the last reboot.
    Tag = N/A
    Plugin ID: 0
switch(config)# configure terminal
switch(config)# bloggerd log-dump sap 351
Sending Enable Request to Bloggerd
Bloggerd Log Dump Successfully enabled
switch(config)# show system internal bloggerd info log-dump-info
-----
Log Dump config is READY

```

```

Log Dump is DISABLED for ALL application services in the switch
Exceptions to the above rule (if any) are as follows:
-----
Module      | VDC          | SAP          | Enabled?
-----
1          | 1            | 351 (MTS_SAP_ACLMGR) | Enabled
-----
Log Dump Throttle Switch-Wide Config:
-----
Log Dump Throttle                      : ENABLED
Minimum buffer rollover count (before throttling) : 5
Maximum allowed rollover count per minute      : 1
-----
switch(config)#

```

## 拡張ログ ファイルの表示

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

### 手順の概要

#### 1. **dir debug:log-dump/**

### 手順の詳細

#### 手順

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

#### 例

```

switch# dir debug:log-dump/
3676160 Dec 05 02:43:01 2019 20191205023755_evtlog_archive.tar
3553280 Dec 05 06:05:06 2019 20191205060005_evtlog_archive.tar

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

```

### 単一サービスに対する拡張ログファイル保持の無効化

拡張ログファイル保持は、スイッチ上のすべてのサービスに対してデフォルトで有効になっています。スイッチで单一またはすべてのサービス (Cisco NX-OS リリース9.3(5) ではデフォル

## ■ 単一サービスに対する拡張ログファイル保持の無効化

ト) に対してログファイル保持機能が有効になっている場合に、特定のサービスを無効にするには、次の手順を実行します。

### 手順の概要

1. **show system internal sysmgr service name *service-type***
2. **configure terminal**
3. **no bloggerd log-dump sap *number***
4. **show system internal bloggerd info log-dump-info**

### 手順の詳細

#### 手順

	コマンドまたはアクション	目的
ステップ1	<b>show system internal sysmgr service name <i>service-type</i></b> 例： switch# show system internal sysmgr service name aclmgr	サービス SAP番号を含む ACL Manager に関する情報を表示します。
ステップ2	<b>configure terminal</b> 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	<b>no bloggerd log-dump sap <i>number</i></b> 例： switch(config)# no bloggerd log-dump sap 351	ACL Managerサービスのログファイル保持機能を無効にします。
ステップ4	<b>show system internal bloggerd info log-dump-info</b> 例： switch(config)# show system internal bloggerd info log-dump-info	スイッチ上のログファイル保持機能に関する情報を表示します。

#### 例

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

```
switch# show system internal sysmgr service name aclmgr
Service "aclmgr" ("aclmgr", 80):
    UUID = 0x182, PID = 653, SAP = 351
    State: SRV_STATE_HANDSHAKED (entered at time Mon Nov 4 11:10:41 2019).
    Restart count: 1
    Time of last restart: Mon Nov 4 11:10:39 2019.
    The service never crashed since the last reboot.
    Tag = N/A
```

```

Plugin ID: 0
switch(config)# configure terminal
switch(config)# no bloggerd log-dump sap 351
Sending Disable Request to Bloggerd
Bloggerd Log Dump Successfully disabled
switch(config)# show system internal bloggerd info log-dump-info
-----
Log Dump config is READY
Log Dump is DISABLED for ALL application services in the switch
Exceptions to the above rule (if any) are as follows:
-----
Module      | VDC      | SAP      | Enabled?
-----
1          | 1        | 351 (MTS_SAP_ACLMGR) | Disabled
-----
Log Dump Throttle Switch-Wide Config:
-----
Log Dump Throttle : ENABLED
Minimum buffer rollover count (before throttling) : 5
Maximum allowed rollover count per minute : 1
-----
switch(config)#

```

## トリガーベースのイベントログの自動収集

トリガーベースのログ収集機能：

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

### トリガーベースのログファイルの自動収集の有効化

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

ログファイルの自動収集を有効にするカスタム YAML ファイルの作成の詳細については、[自動収集 YAML ファイルの設定 \(220 ページ\)](#) を参照してください。

## ■ 自動収集 YAML ファイル

### 自動収集 YAML ファイル

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

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

例：

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

### 自動収集 YAML ファイルの設定

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

スイッチの次のディレクトリで YAML ファイルを見つけます。

```
/bootflash/scripts
```

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

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

上記の例では、「test\_1」はアプレットの名前で、「test.yaml」が /bootflash/scripts ディレクトリにあるユーザー設定の YAML ファイルの名前です。

### YAML ファイルの例

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



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

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

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

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

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

## ■ コンポーネントあたりの自動収集の量の制限

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

上記の YAML エントリの syslog 出力の例 :

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

複数の値を指定するには、次の例を使用します。

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



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

Cisco リリース 10.1 (1) 以降、test.yaml は、複数の YAML ファイルが存在するフォルダに置き換えることができます。フォルダ内のすべての YAML ファイルは、ComponentName.yaml 命名ルールに従う必要があります。

次の例で、test.yaml は、次に置き換えられます。test\_folder:

```
test.yaml:
event manager applet logging2 override __syslog_trigger_default
  action 1.0 collect test.yaml rate-lmt 30 $__syslog_msg

test_folder:
event manager applet logging2 override __syslog_trigger_default
  action 1.0 collect test_folder rate-lmt 30 $__syslog_msg
```

次の例は、test\_folder:

```
ls /bootflash/scripts/test_folder
bgp.yaml ppm.yaml
```

## ■ コンポーネントあたりの自動収集の量の制限

自動収集の場合、コンポーネントイベントあたりのバンドル数の制限はデフォルトで3に設定されています。1つのコンポーネントで3つ以上のイベントが発生すると、イベントはドロップされます。

され、ステータスマッセージ **EVENTLOGLIMITREACHED** が表示されます。イベントログがロールオーバーすると、コンポーネントイベントの自動収集が再開されます。

例：

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

## 自動収集ログ ファイル

### 自動収集ログ ファイルについて

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

自動収集ログ ファイルは、次のディレクトリに保存されます。

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

### ログ ファイルへのアクセス

コマンド キーワード 「debug」 を使用してログを検索します：

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

次の表に、ログの場所と保存されるログの種類を示します。

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

## ■ 自動収集ログ ファイル

場所	説明
log-snapshot-user	このフォルダには、 <code>bloggerd log-snapshot &lt;&gt;</code> の実行時に収集されたログが保存されます。

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

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

### ログ tar ファイルの解析

tar ファイル内のログを解析するには、次の例を参考にしてください。

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

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

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

キーワード	説明
<b>to-datetime</b>	yy [mm [dd [HH [MM [SS]]]]] 形式で指定した、特定の日時までのログをデコードします。

### 別の場所へログをコピーする

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

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

### 自動収集ログファイルの消去

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

#### EventHistory ログの消去ロジック

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

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

#### EventBundle ログの消去ロジック

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

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

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

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

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

## ■ 自動収集ログ ファイル

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

**action** コマンド：**1.0** は、アクションが実行される順序の番号の例です。**collect** YAML ファイルを使用してデータが収集されることを示します。*test.yaml* は、YAML ファイルの名前の例です。**\$\_syslog\_msg** は、コンポーネントの名前を示しています。



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

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

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

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

**action** コマンド：**1.0** は、アクションが実行される順序の番号の例です。**collect** YAML ファイルを使用してデータが収集されることを示します。*test.yaml* は、YAML ファイルの名前の例です。**\$\_syslog\_msg** は、コンポーネントの名前を示しています。

リリース 10.1(1) 以降では、トリガーの最大数オプションを使用して収集レートを調整することもできます。これは、この数のトリガーだけを保つものです。**max-triggers** の値に達すると、**syslog** が発生しても、これ以上バンドルは収集されなくなります。

```
event manager applet test_1 override __syslog_trigger_default
  action 1.0 collect test.yaml rate-limt 30 max-triggers 5 $_syslog_msg
```



**(注)** `debug:log-snapshot-auto/` から自動収集されたバンドルを削除した後、次のイベントが発生したとき **max-triggers** 構成済みの数字に基づいてコレクションが再起動します。

## 自動収集の統計情報と履歴

トリガーベースの収集統計情報の例を次に示します。

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

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

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

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

## トリガーベースのログ収集の確認

トリガーベースのログ収集機能が有効になっていることを確認するには、この例では、**show event manager system-policy | i trigger** コマンドを入力します：

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

## トリガーベースのログ ファイル生成の確認

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

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

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

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

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

## ローカル ログ ファイルのストレージ

ローカル ログ ファイルのストレージ機能：

- ローカルデータストレージ時間の量は、導入の規模とタイプによって異なります。モジュラスイッチと非モジュラスイッチの両方で、ストレージ時間は 15 分から数時間のデータです。長期間にわたる関連ログを収集するには、次の手順を実行します。
- 必要な特定のサービス/機能に対してのみイベント ログの保持を有効にします。詳細は、[単一サービスの拡張ログファイル保持の有効化（215 ページ）](#)。

## ■ 最近のログ ファイルのローカル コピーの生成

- スイッチから内部イベント ログをエクスポートします。詳細は、[外部ログ ファイルのストレージ \(230 ページ\)](#)。
- 圧縮されたログは RAM に保存されます。
- 250MB のメモリは、ログ ファイルストレージ用に予約されています。
- ログ ファイルは tar 形式で最適化されます (5 分ごとに 1 ファイルまたは 10 MB のいずれか早い方)。
- スナップショット収集を許可します。

### 最近のログ ファイルのローカル コピーの生成

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

#### 手順の概要

- bloggerd log-snapshot [file-name] [ bootflash:file-path | logflash:file-path | usb1: ] [ sizefile-size ] [ time minutes ]**

#### 手順の詳細

##### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>bloggerd log-snapshot [file-name] [ bootflash:file-path   logflash:file-path   usb1: ] [ sizefile-size ] [ time minutes ]</b> <b>例 :</b> <pre>switch# bloggerd log-snapshot snapshot1</pre>	<p>スイッチに保存されている最新の 10 個のイベント ログのスナップショット バンドル ファイルを作成します。この操作のデフォルトのストレージは、<b>logflash</b>です。</p> <p><i>file-name</i> : 生成されたスナップショット ログ ファイル バンドル のファイル名。次には最大 64 文字を使用します。 <i>file-name</i> です。</p> <p>(注)  この変数はオプションです。設定されていない場合、システムはタイムスタンプと「_snapshot_bundle.tar」をファイル名として適用します。例：  20200605161704_snapshot_bundle.tar</p> <p><b>bootflash:file-path</b> : スナップショット ログ ファイル バンドル がブート フラッシュ に保存されているファイル パス。次の初期パスのいずれかを選択します。</p>

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

### 例

```

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

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

```

次の例のコマンドを使用して、同じファイルを表示します。

```

switch# dir debug:log-snapshot-user/
159098880 Dec 05 06:40:24 2019 snapshot1_snapshot_bundle.tar
159354880 Dec 05 06:40:40 2019 snapshot2_snapshot_bundle.tar

```

## 外部ログ ファイルのストレージ

```
Usage for debug://sup-local
929792 bytes used
4313088 bytes free
5242880 bytes total
```



(注) ファイル名は、例の最後に示されています。個々のログファイルは、生成された日時によっても識別されます。

リリース 10.1(1) 以降、LC コアファイルには、`log-snapshot` バンドルが含まれています。値は、`log-snapshot` バンドルファイル名は、`tac_snapshot_bundle.tar.gz`です。次に例を示します。

```
bash-4.2$ tar -tvf 1610003655_0x102_aclqos_log.17194.tar.gz
drwxrwxrwx root/root 0 2021-01-07 12:44 pss/
-rw-rw-rw- root/root 107 2021-01-07 12:44 pss/dev_shm_aclqos_runtime_info_lc.gz
-rw-rw-rw- root/root 107 2021-01-07 12:44 pss/dev_shm_aclqos_runtime_cfg_lc.gz
-rw-rw-rw- root/root 107 2021-01-07 12:44 pss/dev_shm_aclqos_debug.gz
-rw-rw-rw- root/root 129583 2021-01-07 12:44 pss/clqosdb_ver1_0_user.gz
-rw-rw-rw- root/root 20291 2021-01-07 12:44 pss/clqosdb_ver1_0_node.gz
-rw-rw-rw- root/root 444 2021-01-07 12:44 pss/clqosdb_ver1_0_ctrl.gz
drwxrwxrwx root/root 0 2021-01-07 12:44 proc/
-rw-rw-rw- root/root 15159 2021-01-07 12:44 0x102_aclqos_compress.17194.log.25162
-rw-rw-rw- root/root 9172392 2021-01-07 12:43 0x102_aclqos_core.17194.gz
-rw-rw-rw- root/root 43878 2021-01-07 12:44 0x102_aclqos_df_dmesg.17194.log.gz
-rw-rw-rw- root/root 93 2021-01-07 12:44 0x102_aclqos_log.17194
-rw-rw-rw- root/root 158 2021-01-07 12:44 0x102_aclqos_mcrc.17194.log.gz
drwxrwxrwx root/root 0 2021-01-07 12:44 usd17194/
-rw-rw-rw- root/root 11374171 2021-01-07 12:44 tac_snapshot_bundle.tar.gz
```

## 外部ログ ファイルのストレージ

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

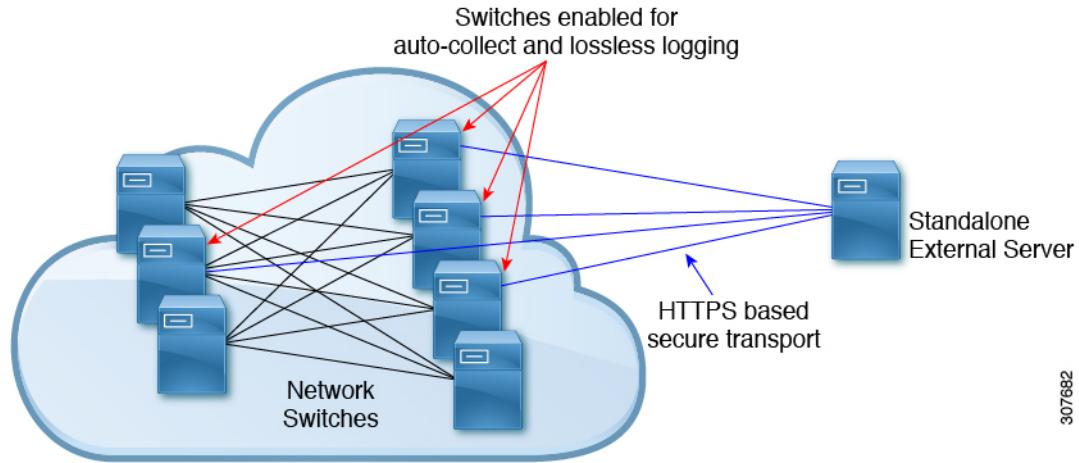


(注) 外部ストレージ機能を作成するため、Cisco Technical Assistance Center (TAC) に連絡して、外部サーバソリューションの展開をサポートを求めてください。

次に、外部ログ ファイルの保存機能を示します。

- オンデマンドで有効
- HTTPS ベースの転送
- ストレージ要件：
  - 非モジュラスイッチ : 300 MB
  - モジュラスイッチ : 12 GB (1 日あたり、スイッチあたり)

- 通常、外部サーバには 10 台のスイッチのログが保存されます。ただし、外部サーバでサポートされるスイッチの数に厳密な制限はありません。



307682

外部サーバソリューションには、次の特性があります。

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



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

## Embedded Event Manager の設定確認

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
<b>show event manager environment [variable-name   all]</b>	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。
<b>show event manager event-types [event   all   module slot]</b>	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。

## ■ Embedded Event Manager の設定例

コマンド	目的
<b>show event manager history events [detail] [maximum num-events] [severity {catastrophic   minor   moderate   severe}]</b>	すべてのポリシーについて、イベント履歴を表示します。
<b>show event manager policy-state policy-name</b>	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。
<b>show event manager script system [policy-name   all]</b>	スクリプト ポリシーに関する情報を表示します。
<b>show event manager system-policy [all]</b>	定義済みシステム ポリシーに関する情報を表示します。
<b>show running-config eem</b>	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。
<b>show startup-config eem</b>	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。

## Embedded Event Manager の設定例

次に、モジュール3の中断のないアップグレードの障害のしきい値だけを変更することによって、`_lcm_module_failure`システムポリシーを上書きする例を示します。また、`syslog`メッセージも送信します。その他のすべての場合、システムポリシー `_lcm_module_failure` の設定値が適用されます。

```
event manager applet example2 override _lcm_module_failure
  event module-failure type hitless-upgrade-failure module 3 count 2
    action 1 syslog priority errors msg module 3 "upgrade is not a hitless upgrade!"
    action 2 policy-default
```

次に、`_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例を示します。

```
event manager applet ethport override _ethpm_link_flap
  event policy-default count 2 time 1000
  action 1 cli conf t
  action 2 cli int et1/1
  action 3 cli no shut
```

次に、ユーザー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、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。

```
event manager applet TEST
  event cli match "conf t"
  action 1.0 snmp-trap strdata "Configuration change"
  action 2.0 event-default
```



(注) EEM ポリシーに **event-default** アクション文を追加する必要があります。この文がないと、EEM ではコマンドを実行できません。

次に、EEM ポリシーの複数イベントを関連付け、イベント トリガーの組み合わせに基づいて ポリシーを実行する例を示します。この例では、EEM ポリシーは、指定された syslog パターンのいずれかが 120 秒以内に発生したときにトリガーされます。

```
event manager applet eem-correlate
  event syslog tag one pattern "copy bootflash:.* running-config.*"
  event syslog tag two pattern "copy run start"
  event syslog tag three pattern "hello"
  tag one or two or three happens 1 in 120
  action 1.0 reload module 1
```

## 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
EEM コマンド	『Cisco Nexus 3600 NX-OS Command Reference』

### 標準

この機能では、新規の標準がサポートされることも、一部変更された標準がサポートされることもありません。また、既存の標準に対するサポートが変更されることもありません。

## ■ その他の参考資料



# 第 16 章

## オンボード障害ロギングの設定

この章は、次の項で構成されています。

- OBFL の概要 (235 ページ)
- OBFL の前提条件 (236 ページ)
- OBFL の注意事項と制約事項 (236 ページ)
- OBFL のデフォルト設定 (236 ページ)
- OBFL の設定 (237 ページ)
- OBFL 設定の確認 (239 ページ)
- OBFL のコンフィギュレーション例 (240 ページ)
- その他の参考資料 (241 ページ)

## OBFL の概要

Cisco NX-OS には永続ストレージに障害データを記録する機能があるので、あとから記録されたデータを取得して表示し、分析できます。このオンボード障害ロギング (OBFL) 機能は、障害および環境情報をモジュールの不揮発性メモリに保管します。この情報は、障害モジュールの分析に役立ちます。

OBFL は次のタイプのデータを保存します。

- 最初の電源投入時刻
- モジュールのシャーシスロット番号
- モジュールの初期温度
- ファームウェア、BIOS、FPGA、および ASIC のバージョン
- モジュールのシリアル番号
- クラッシュのスタックトレース
- CPU hog 情報
- メモリリーク情報

## OBFL の前提条件

- ・ソフトウェア エラーメッセージ
- ・ハードウェア例外ログ
- ・環境履歴
- ・OBFL 固有の履歴情報
- ・ASIC 割り込みおよびエラー統計の履歴
- ・ASIC レジスタ ダンプ

## OBFL の前提条件

network-admin ユーザ権限が必要です。

## OBFL の注意事項と制約事項

OBFL に関する注意事項および制約事項は、次のとおりです。

- ・OBFL はデフォルトでイネーブルになっています。
- ・OBFL フラッシュがサポートする書き込みおよび消去の回数には制限があります。イネーブルにするロギング数が多いほど、この書き込みおよび消去回数に早く達してしまいます。
- ・値は、**show system reset-reason module module num** コマンドでは、モジュール障害の場合にリセット理由が表示されません。モジュール **reset-reason** の永続的なストレージがないため、このコマンドはリブート後は有効ではありません。例外ログは永続ストレージで利用できるため、再起動後、**show logging onboard exception-log** コマンドを使用してリセット理由を表示できます。



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

## OBFL のデフォルト設定

次の表に、VACL パラメータのデフォルト設定を示します。

パラメータ	デフォルト
OBFL	すべての機能がイネーブル

# OBFL の設定

Cisco NX-OS デバイス上で OBFL 機能を設定できます。

## 始める前に

グローバル コンフィギュレーション モードになっていることを確認します。

## 手順の概要

1. **configure terminal**
2. **hw-module logging onboard**
3. **hw-module logging onboard counter-stats**
4. **hw-module logging onboard cphog**
5. **hw-module logging onboard environmental-history**
6. **hw-module logging onboard error-stats**
7. **hw-module logging onboard interrupt-stats**
8. **hw-module logging onboard module slot**
9. **hw-module logging onboard obfl-logs**
10. (任意) **show logging onboard**
11. (任意) **copy running-config startup-config**

## 手順の詳細

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b>  <b>例 :</b> <pre>switch# configure terminal switch(config)#</pre>	グローバル コンフィギュレーション モードを開始します
ステップ 2	<b>hw-module logging onboard</b>  <b>例 :</b> <pre>switch(config)# hw-module logging onboard Module: 7 Enabling ... was successful. Module: 10 Enabling ... was successful. Module: 12 Enabling ... was successful.</pre>	すべての OBFL 機能をイネーブルにします。
ステップ 3	<b>hw-module logging onboard counter-stats</b>  <b>例 :</b> <pre>switch(config)# hw-module logging onboard counter-stats Module: 7 Enabling counter-stats ... was successful. Module: 10 Enabling counter-stats ... was</pre>	OBFL カウンタ統計情報を有効にします。

## OBFL の設定

	コマンドまたはアクション	目的
	successful. Module: 12 Enabling counter-stats ... was successful.	
ステップ 4	<b>hw-module logging onboard cphog</b>  例：  switch(config)# hw-module logging onboard cphog Module: 7 Enabling cpu-hog ... was successful. Module: 10 Enabling cpu-hog ... was successful. Module: 12 Enabling cpu-hog ... was successful.	OBFL CPU hog イベントを有効にします。
ステップ 5	<b>hw-module logging onboard environmental-history</b>  例：  switch(config)# hw-module logging onboard environmental-history Module: 7 Enabling environmental-history ... was successful. Module: 10 Enabling environmental-history ... was successful. Module: 12 Enabling environmental-history ... was successful.	OBFL 環境履歴をイネーブルにします。
ステップ 6	<b>hw-module logging onboard error-stats</b>  例：  switch(config)# hw-module logging onboard error-stats Module: 7 Enabling error-stats ... was successful. Module: 10 Enabling error-stats ... was successful. Module: 12 Enabling error-stats ... was successful.	OBFL エラー統計をイネーブルにします。
ステップ 7	<b>hw-module logging onboard interrupt-stats</b>  例：  switch(config)# hw-module logging onboard interrupt-stats Module: 7 Enabling interrupt-stats ... was successful. Module: 10 Enabling interrupt-stats ... was successful. Module: 12 Enabling interrupt-stats ... was successful.	OBFL 割り込み統計をイネーブルにします。
ステップ 8	<b>hw-module logging onboard module slot</b>  例：  switch(config)# hw-module logging onboard module 7 Module: 7 Enabling ... was successful.	モジュールの OBFL 情報をイネーブルにします。
ステップ 9	<b>hw-module logging onboard obfl-logs</b>  例：	ブート動作時間、デバイス バージョン、および OBFL 履歴をイネーブルにします。

	コマンドまたはアクション	目的
	<pre>switch(config)# hw-module logging onboard obfl-logs Module: 7 Enabling obfl-log ... was successful. Module: 10 Enabling obfl-log ... was successful. Module: 12 Enabling obfl-log ... was successful.</pre>	
ステップ 10	<p>(任意) <b>show logging onboard</b></p> <p>例 :</p> <pre>switch(config)# show logging onboard</pre>	OBFL に関する情報を表示します。
ステップ 11	<p>(任意) <b>copy running-config startup-config</b></p> <p>例 :</p> <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

## OBFL 設定の確認

モジュールのフラッシュに保存されている OBFL 情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
<b>show logging onboard boot-uptime</b>	ブートおよび動作時間の情報を表示します。
<b>show logging onboard counter-stats</b>	すべての ASIC カウンタについて、統計情報を表示します。
<b>show logging onboard credit-loss</b>	OBFL クレジット損失のログを表示します。
<b>show logging onboard device-version</b>	デバイス バージョン情報を表示します。
<b>show logging onboard endtime</b>	指定した終了時刻までの OBFL ログを表示します。
<b>show logging onboard environmental-history</b>	環境履歴を表示します。
<b>show logging onboard error-stats</b>	エラー統計情報を表示します。
<b>show logging onboard exception-log</b>	例外ログ情報を表示します。
<b>show logging onboard interrupt-stats</b>	割り込み統計情報を表示します。
<b>show logging onboard module slot</b>	指定したモジュールの OBFL 情報を表示します。
<b>show logging onboard obfl-history</b>	履歴情報を表示します。
<b>show logging onboard obfl-logs</b>	ログ情報を表示します。

## ■ OBFL のコンフィギュレーション例

コマンド	目的
<b>show logging onboard stack-trace</b>	カーネル スタック トレース情報を表示します。
<b>show logging onboard starttime</b>	指定した開始時刻からの OBFL ログを表示します。
<b>show logging onboard status</b>	OBFL ステータス情報を表示します。

OBFL の構成ステータスを表示するには、**show logging onboard status** コマンドを使用します。

```
switch# show logging onboard status
-----
OBFL Status
-----
Switch OBFL Log: Enabled

Module: 4 OBFL Log: Enabled
cpu-hog Enabled
credit-loss Enabled
environmental-history Enabled
error-stats Enabled
exception-log Enabled
interrupt-stats Enabled
mem-leak Enabled
miscellaneous-error Enabled
obfl-log (boot-uptime/device-version/obfl-history) Enabled
register-log Enabled
request-timeout Enabled
stack-trace Enabled
system-health Enabled
timeout-drops Enabled
stack-trace Enabled

Module: 22 OBFL Log: Enabled
cpu-hog Enabled
credit-loss Enabled
environmental-history Enabled
error-stats Enabled
exception-log Enabled
interrupt-stats Enabled
mem-leak Enabled
miscellaneous-error Enabled
obfl-log (boot-uptime/device-version/obfl-history) Enabled
register-log Enabled
request-timeout Enabled
stack-trace Enabled
system-health Enabled
timeout-drops Enabled
stack-trace Enabled
```

OBFL の構成ステータスを表示するには、**clear logging onboard** コマンドを使用して、一覧に表示されている **show** コマンド オプションの各ホストの OBFL 情報をクリアします。

## OBFL のコンフィギュレーション例

モジュール 2 で環境情報について OBFL を有効にする例を示します。

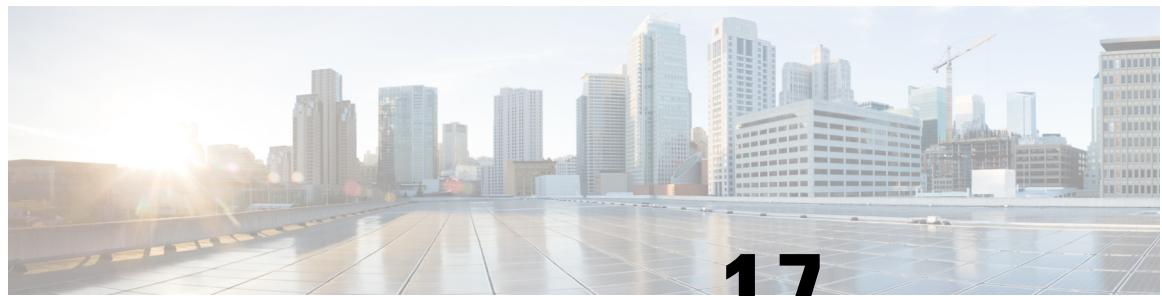
```
switch# configure terminal
switch(config)# hw-module logging onboard module 2 environmental-history
```

## その他の参考資料

### 関連資料

関連項目	マニュアルタイトル
コンフィギュレーションファイル	<i>Cisco Nexus 3600 NX-OS 基礎構成ガイド</i>

## ■ 関連資料



# 第 17 章

## SPAN の設定

この章は、次の項で構成されています。

- [SPANについて, on page 243](#)
- [SPAN送信元, on page 244](#)
- [送信元ポートの特性, on page 244](#)
- [SPAN宛先, on page 245](#)
- [接続先ポートの特性, on page 245](#)
- [SPANの注意事項および制約事項, on page 245](#)
- [SPANセッションの作成または削除, on page 247](#)
- [イーサネット宛先ポートの設定, on page 247](#)
- [送信元ポートの設定, on page 249](#)
- [SPANトラフィックのレート制限の設定 \(250 ページ\)](#)
- [送信元ポートチャネルのまたは VLAN を構成します。, on page 251](#)
- [SPANセッションの説明の設定, on page 252](#)
- [SPANセッションのアクティブ化, on page 253](#)
- [SPANセッションの一時停止, on page 253](#)
- [SPAN情報の表示, on page 254](#)
- [SPANのコンフィギュレーション例 \(255 ページ\)](#)

## SPANについて

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、ファイバチャネルアナライザ、またはその他のリモートモニタリング (RMON) プローブです。

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 送信元

SPAN 送信元とは、トライ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 デバイスはイーサネット、ポートチャネル、および SPAN 送信元として VLAN をサポートします。VLAN で、指定された VLAN でサポートされているすべてのインターフェイスは SPAN 送信元として含まれています。イーサネット、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 トライ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イフィックは、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イフィックは、SPAN 宛先ポートにコピーされます。

## 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、ネットワークトライ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）と任意の数のソース VLAN 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、または VLAN ポートタイプにできます。
- VLAN の SPAN 送信元は、6 VLANs を超えることはできません。
- ACL フィルタが設定されていない場合、方向または SPAN 宛先のいずれかが異なっていれば、複数のセッションに対して同じ送信元を設定することができます。ただし、各 SPAN RX の送信元は、ACL フィルタを使用して、1 つの SPAN セッションにのみ設定する必要があります。
- 宛先ポートには設定できません。
- モニターする方向（入力、出力、または両方）を設定できます。VLAN 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。VLAN SPAN セッションでは RX/TX オプションは使用できません。
- ACL を使用して入力トライ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。
- 同じ VLAN 内または異なる VLAN 内に存在できます。

## 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 3600 プラットフォームスイッチは、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。

## 接続先ポートの特性

各ローカル SPAN セッションには、送信元ポートからトラフィックのコピーを受信する接続先ポート（モニタリング ポートとも呼ばれる）が必要です。または VLAN。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、FCoE、およびファイバ チャネル ポートは宛先ポートにできません。
- 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。
- 送信元ポートにはなれません。
- ポート チャネルにはできません。
- 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 セッションの送信元 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。
- 同じ宛先インターフェイスを、複数の SPAN セッションに使用することはできません。ただし、インターフェイスは SPAN および ERSPAN セッションの宛先として機能できます。

## SPAN の注意事項および制約事項



### Note

スケール情報については、リリース固有の『Cisco Nexus 3600 NX-OS 確認済み拡張ガイド』を参照してください。

SPAN には、次の注意事項と制限事項があります。

- 同じ送信元（イーサネットまたはポートチャネル）は、複数のセッションの一部にすることができます。宛先が異なる2つのモニターセッションを設定することはできますが、同じ送信元 VLAN はサポートされていません。
- 複数の ACL フィルタは、同じ送信元でサポートされます。

## ■ SPAN の注意事項および制約事項

- Cisco Nexus 3600 プラットフォーム スイッチインターフェイスのアクセス ポートの出力 SPAN コピーには、常に dot1q ヘッダーがあります。
- 同じ送信元インターフェイスで 2 つの SPAN または ERSPAN セッションを 1 つのフィルタだけで設定することはできません。同じ送信元が複数の SPAN または ERSPAN セッションで使用されている場合は、すべてのセッションに異なるフィルタを設定するか、セッションにフィルタを設定しないでください。
- ACL フィルタリングは、Rx SPAN に対してのみサポートされます。Tx SPAN は、送信元インターフェイスで出力されるすべてのトラフィックをミラーリングします。
- TCAM カービングは、Cisco Nexus 3600 プラットフォーム スイッチの SPAN/ERSPAN には必要ありません。
- ACL フィルタリングは、TCAM (Ternary Content Addressable Memory) 幅の制限により、IPv6 および MAC ACL ではサポートされていません。
- SPAN TCAM サイズは、ASIC に応じて 128 または 256 です。1 つのエントリがデフォルトでインストールされ、4 つは ERSPAN 用に予約されます。
- 同じ送信元が複数の SPAN セッションで設定されていて、各セッションに ACL フィルタが設定されている場合、送信元インターフェイスは、最初のアクティブ SPAN セッションに対してのみプログラムされます。その他のセッションの ACE にプログラムされているハードウェア エントリは、この送信元インターフェイスには含まれません。
- 許可と拒否の両方のアクセス コントロール エントリ (ACE) は、同様に処理されます。ACE と一致するパケットは、ACL の許可エントリまたは拒否エントリを含んでいるかどうかに関係なく、ミラーリングされます。

**Note**

拒否 ACE により、パケットがドロップされることはありません。SPAN セッションに設定されている ACL によってのみ、パケットをミラーリングするかどうかが決まります。

- パフォーマンス向上のため、SPAN には RX タイプの送信元トラフィックのみを使用することをお勧めします。RX トラフィックがカットスルーであるのに対し、TX はストアアンドフォワードであるためです。したがって、両方向 (RX および TX) をモニターする場合、パフォーマンスは RX のみをモニターするときほど良好になりません。両方向のトラフィックをモニターする必要がある場合は、より多くの物理ポートで RX をモニターすると、トラフィックの両側をキャプチャすることができます。
- Cisco NX-OS リリース 10.2 (3) F 以降、ACL フィルタは次のプラットフォーム スイッチでサポートされています。
  - N3K-C36180YC-R
  - N3K-C3636C-R

# SPAN セッションの作成または削除

SPAN セッションを作成するためにはセッション番号を割り当てるには、**monitor session** コマンドを使用します。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。

## SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **monitor session session-number**

## DETAILED STEPS

### Procedure

	Command or Action	Purpose
ステップ 1	switch# <b>configure terminal</b>	グローバル コ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)# <b>monitor session session-number</b>	モニター 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。

### Example

次に、SPAN モニター 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。



**Note** 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。

## SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface ethernet slot/port**
3. switch(config-if)# **switchport monitor**

## ■ イーサネット宛先ポートの設定

4. switch(config-if)# **exit**
5. switch(config)# **monitor session session-number**
6. switch(config-monitor)# **destination interface ethernet slot/port**

## DETAILED STEPS

## Procedure

	<b>Command or Action</b>	<b>Purpose</b>
ステップ 1	switch# <b>configure terminal</b>	グローバルコ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)# <b>interface ethernet slot/port</b>	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。 <b>Note</b> この <b>switchport monitor</b> コマンドを仮想イーサネットポートで有効にするには、 <b>interface vethernet slot/port</b> コマンドを使用できます。
ステップ 3	switch(config-if)# <b>switchport monitor</b>	指定されたイーサネットインターフェイスのモニター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)# <b>exit</b>	グローバルコンフィギュレーションモードに戻ります。
ステップ 5	switch(config)# <b>monitor session session-number</b>	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)# <b>destination interface ethernet slot/port</b>	イーサネットSPAN宛先ポートを設定します。 <b>Note</b> モニター 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、 <b>destination interface vethernet slot/port</b> コマンドを使用できます。

## Example

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) #
```

## 送信元ポートの設定

送信元ポートは、イーサネットポートのみに設定できます。

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config) # **monitor session session-number**
3. switch(config-monitor) # **source interface type slot/port [rx | tx | both]**

### DETAILED STEPS

#### Procedure

	<b>Command or Action</b>	<b>Purpose</b>
ステップ1	switch# <b>configure terminal</b>	グローバル コ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) # <b>monitor session session-number</b>	指定したモニタリング セッションのモニター コンフィギュレーション モードを開始します。
ステップ3	switch(config-monitor) # <b>source interface type slot/port [rx   tx   both]</b>	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、またはリモート対応ファイバチャネルの範囲を入力できます。リスト。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。

#### Example

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
```

## ■ SPAN トラフィックのレート制限の設定

```
switch(config-monitor)# source interface ethernet 1/16
switch(config-monitor)#

```

次に、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 fc 2/1
switch(config-monitor)#

```

# SPAN トラフィックのレート制限の設定

モニター セッション全体で SPAN トラフィックのレート制限を 1Gbps に設定することで、モニターされた実稼働 トラフィックへの影響を回避できます。

- 1 Gbps を超える トラフィックを 1 Gb の SPAN 宛先インターフェイスに分散させる場合、SPAN 送信元 トラフィックはドロップされません。
- 6 Gbps を超える（ただし 10 Gbps 未満）の トラフィックを 10 Gb の SPAN 宛先インターフェイスに分散させる場合、SPAN トラフィックは、宛先またはスニファで 10 Gbps が可能な場合でも、1 Gbps に制限されます。
- SPAN は 8 ポート（1 ASIC）ごとに 5 Gbps にレート制限されます。
- RX-SPAN は、ポートの RX トラフィックが 5 Gbps を超える場合は、ポートごとに 0.71 Gbps にレート制限されます。

## 手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface ethernet slot/port**
3. switch(config-if)# **switchport monitor rate-limit 1G**
4. switch(config-if)# **exit**

## 手順の詳細

### 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	グローバル コ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)# <b>interface ethernet slot/port</b>	スロット値およびポート値による選択で指定されたイーサネット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 モードを開始します。 (注)

	コマンドまたはアクション	目的
		これが QSFP+ GEM の場合、 <i>slot/port</i> のシンタックスは、 <i>slot/QSFP-module/port</i> になります。
ステップ 3	switch(config-if)# <b>switchport monitor rate-limit 1G</b>	レート制限が 1 Gbps であることを指定します。 (注) このコマンドは、 Cisco Nexus N3K-C36180YC-R プラットフォーム スイッチではサポートされていません。
ステップ 4	switch(config-if)# <b>exit</b>	グローバル コンフィギュレーション モードに戻ります。

#### 例

次に、イーサネットインターフェイス 1/2 の帯域幅を 1 Gbps に制限する例を示します。

```
switch(config)# interface ethernet 1/2
switch(config-if)# switchport monitor rate-limit 1G
switch(config-if)#

```

## 送信元ポート チャネルの または **VLAN** を構成します。

SPAN セッションに送信元チャネルを設定できます。これらのポート および VLAN は、ポートチャネルにすることができます。モニタリング方向は入力、出力、または両方に設定でき、グループ内のすべての物理ポートに適用されます。

#### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config) # **monitor session session-number**
3. switch(config-monitor) # **source {interface {port-channel} channel-number [rx | tx | both] | vlan vlan-range}**

#### DETAILED STEPS

##### Procedure

	Command or Action	Purpose
ステップ 1	switch# <b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。

## ■ SPAN セッションの説明の設定

	Command or Action	Purpose
ステップ 2	switch(config) # <b>monitor session session-number</b>	指定した SPAN セッションのモニタ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 3	switch(config-monitor) # <b>source {interface {port-channel} channel-number [rx   tx   both]   vlan vlan-range}</b>	ポートチャネルまたは VLAN 送信元を設定します。VLAN 送信元の場合、モニタリング方向は暗黙的です。

**Example**

次に、ポートチャネル SPAN 送信元を設定する例を示します。

```
switch# configure terminal
switch(config) # monitor session 2
switch(config-monitor) # source interface port-channel 1 rx
switch(config-monitor) # source interface port-channel 3 tx
switch(config-monitor) # source interface port-channel 5 both
switch(config-monitor) #
```

次に、VLAN SPAN 送信元を設定する例を示します。

```
switch# configure terminal
switch(config) # monitor session 2
switch(config-monitor) # source vlan 1
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。

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config) # **monitor session session-number**
3. switch(config-monitor) # **description description**

### DETAILED STEPS

**Procedure**

	Command or Action	Purpose
ステップ 1	switch# <b>configure terminal</b>	グローバルコ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) # <b>monitor session session-number</b>	指定した SPAN セッションのモニタ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 3	switch(config-monitor) # <b>description description</b>	SPAN セッションのわかりやすい名前を作成します。

**Example**

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 セッションのアクティブ化

デフォルトでは、セッションステートは **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。

**SUMMARY STEPS**

1. switch# **configure terminal**
2. switch(config) # **no monitor session {all | session-number} shut**

**DETAILED STEPS****Procedure**

	<b>Command or Action</b>	<b>Purpose</b>
ステップ 1	switch# <b>configure terminal</b>	グローバル コ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) # <b>no monitor session {all   session-number} shut</b>	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。

**Example**

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 セッションの一時停止

デフォルトでは、セッション状態は **shut** です。

**SUMMARY STEPS**

1. switch# **configure terminal**
2. switch(config) # **monitor session {all | session-number} shut**

## ■ SPAN 情報の表示

## DETAILED STEPS

## Procedure

	Command or Action	Purpose
ステップ 1	switch# <b>configure terminal</b>	グローバル コ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) # <b>monitor session {all   session-number}</b> <b>shut</b>	指定された SPAN セッションまたはすべてのセッションを一時停止します。

## Example

次に、SPAN セッションを一時停止する例を示します。

```
switch# configure terminal
switch(config) # monitor session 3 shut
switch(config) #
```

## SPAN 情報の表示

## SUMMARY STEPS

1. switch# **show monitor [session {all | session-number | range session-range} [brief]]**

## DETAILED STEPS

## Procedure

	Command or Action	Purpose
ステップ 1	switch# <b>show monitor [session {all   session-number   range session-range} [brief]]</b>	SPAN 設定を表示します。

## Example

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          : 100
    tx          :
    both        :
  destination ports : Eth3/1
```

## SPAN のコンフィギュレーション例

### SPAN セッションのコンフィギュレーション例

SPAN セッションを設定する手順は、次のとおりです。

#### 手順の概要

1. アクセス モードで宛先ポートを設定し、SPAN モニタリングをイネーブルにします。
2. SPAN セッションを設定します。

#### 手順の詳細

##### 手順

**ステップ1** アクセス モードで宛先ポートを設定し、SPAN モニタリングをイネーブルにします。

例：

```
switch# configure terminal
switch(config)# interface ethernet 2/5
switch(config-if)# switchport
switch(config-if)# switchport monitor
switch(config-if)# no shut
switch(config-if)# exit
switch(config)#
```

**ステップ2** SPAN セッションを設定します。

例：

```
switch(config)# no monitor session 3
switch(config)# monitor session 3
switch(config-monitor)# source interface ethernet 2/1-3, ethernet 3/1 rx
switch(config-monitor)# source interface port-channel 2
switch(config-monitor)# source interface sup-eth 0 both
switch(config-monitor)# source vlan 3, 6-8 rx
switch(config-monitor)# source interface ethernet 101/1/1-3
```

## ■ 単一方向 SPAN セッションの設定例

```
switch(config-monitor)# destination interface ethernet 2/5
switch(config-monitor)# no shut
switch(config-monitor)# exit
switch(config)# show monitor session 3
switch(config)# copy running-config startup-config
```

---

## 単一方向 SPAN セッションの設定例

単一方向 SPAN セッションを設定するには、次の手順を実行します。

### 手順の概要

1. アクセス モードで宛先ポートを設定し、SPAN モニタリングをイネーブルにします。
2. SPAN セッションを設定します。

### 手順の詳細

#### 手順

---

**ステップ1** アクセス モードで宛先ポートを設定し、SPAN モニタリングをイネーブルにします。

例：

```
switch# configure terminal
switch(config)# interface ethernet 2/5
switch(config-if)# switchport
switch(config-if)# switchport monitor
switch(config-if)# no shut
switch(config-if)# exit
switch(config)#
```

**ステップ2** SPAN セッションを設定します。

例：

```
switch(config)# no monitor session 3
switch(config)# monitor session 3 rx
switch(config-monitor)# source interface ethernet 2/1-3, ethernet 3/1 rx
switch(config-monitor)# filter vlan 3-5, 7
switch(config-monitor)# destination interface ethernet 2/5
switch(config-monitor)# no shut
switch(config-monitor)# exit
switch(config)# show monitor session 3
switch(config)# copy running-config startup-config
```

## SPAN ACL の設定例

次に、SPAN ACL を設定する例を示します。

```
switch# configure terminal
switch(config)# ip access-list match_11_pkts
switch(config-acl)# permit ip 11.0.0.0 0.255.255.255 any
switch(config-acl)# exit
switch(config)# ip access-list match_12_pkts
switch(config-acl)# permit ip 12.0.0.0 0.255.255.255 any
switch(config-acl)# exit
switch(config)# vlan access-map span_filter 5
switch(config-access-map)# match ip address match_11_pkts
switch(config-access-map)# action forward
switch(config-access-map)# exit
switch(config)# vlan access-map span_filter 10
switch(config-access-map)# match ip address match_12_pkts
switch(config-access-map)# action forward
switch(config-access-map)# exit
switch(config)# monitor session 1
switch(config-erspan-src)# filter access-group span_filter
```

## UDF ベース SPAN の設定例

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

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

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

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

- 外部送信元 IP アドレス : 10.0.0.2
- 内部 TCP フラグ : 緊急 TCP フラグを設定

## UDF ベース SPAN の設定例

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

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



# 第 18 章

## ERSPAN の設定

この章は、次の内容で構成されています。

- [ERSPANについて \(259 ページ\)](#)
- [ERSPANの前提条件 \(260 ページ\)](#)
- [ERSPANの注意事項および制約事項 \(260 ページ\)](#)
- [ERSPANのデフォルト設定 \(264 ページ\)](#)
- [ERSPANの設定 \(264 ページ\)](#)
- [ERSPANの設定例 \(279 ページ\)](#)
- [その他の参考資料 \(281 ページ\)](#)

## ERSPANについて

ERSPANは、ERSPAN送信元セッション、ルーティング可能なERSPAN Generic Routing Encapsulation (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。ACLを使用し、入力トラフィックをフィルタ処理するようにERSPAN送信元セッションを設定することもできます。

## ERSPAN送信元

トラフィックをモニタできるモニタ元インターフェイスのことをERSPAN送信元と呼びます。送信元では、監視するトラフィックを指定し、さらに入力、出力、または両方向のトラフィックをコピーするかどうかを指定します。ERSPAN送信元には次のものが含まれます。

- イーサネットポート、ポートチャネル、およびサブインターフェイス。
- 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。

## マルチ ERSPAN セッション

- 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ーしません。
- 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。

## マルチ ERSPAN セッション

最大 18 個の ERSPAN セッションを定義できますが、同時に作動できるのは最大 4 個の ERSPAN または SPAN セッションのみです。受信ソースと送信ソースの両方が同じセッションに設定されている場合、同時に作動できるのは 2 つの ERSPAN または SPAN セッションのみです。未使用の ERSPAN セッションはシャットダウンもできます。

ERSPAN セッションのシャットダウンについては、[ERSPAN セッションのシャットダウンまたはアクティブ化 \(276 ページ\)](#) を参照してください。

## 高可用性

SPAN 機能はステートレスおよびステートフルリスタートをサポートします。リブートまたはスーパーバイザスイッチオーバー後に、実行コンフィギュレーションを適用します。

## ERSPAN の前提条件

ERSPAN の前提条件は、次のとおりです。

特定の ERSPAN 構成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構成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



(注)

スケール情報については、リリース固有の『Cisco Nexus 3600 NX-OS 確認済み拡張ガイド』を参照してください。

ERSPAN 設定時の注意事項と制限事項は次のとおりです。

- 同じ送信元は、複数のセッションの一部にすることができます。
- 複数の ACL フィルタは、同じ送信元でサポートされます。
- ERSPAN は次をサポートしています。
  - 4 ~ 6 個のトンネル

- トンネルなしパケット
- IPinIP トンネル
- IPv4 トンネル（制限あり）
- ERSPAN 送信元セッションタイプ（パケットは、汎用ルーティングカプセル化（GRE）トンネルパケットとしてカプセル化され、IP ネットワークで送信されます。ただし、他のシスコデバイスとは異なり、ERSPAN ヘッダーはパケットに追加されません。）。
- ERSPAN パケットは、カプセル化されたミラー パケットがレイヤ 2 MTU のチェックに失敗した場合、ドロップされます。
- 出力カプセルでは 112 バイトの制限があります。この制限を超えるパケットはドロップされます。このシナリオは、トンネルとミラーリングが混在する場合に発生することがあります。
- ERSPAN セッションは複数のローカル セッションで共有されます。最大 18 セッションが設定できます。ただし、同時に動作できるのは最大 4 セッションのみです。受信ソースと送信ソースの両方が同じセッションで設定されている場合、2 セッションのみが動作できます。
- ERSPAN および ERSPAN ACL は、スーパー バイザが生成したパケットではサポートされません。
- ERSPAN および ERSPAN（ACL フィルタリングあり）は、スーパー バイザが生成したパケットではサポートされません。
- ACL フィルタリングは、Rx ERSPAN に対してのみサポートされます。Tx ERSPAN は、送信元インターフェイスで出力されるすべてのトラフィックをミラーリングします。
- ACL フィルタリングは、TCAM 幅の制限があるため、IPv6 および MAC ACL ではサポートされません。
- 同じ送信元が複数の ERSPAN セッションで構成されていて、各セッションに ACL フィルタが構成されている場合、送信元インターフェイスは、最初のアクティブ ERSPAN セッションに対してのみプログラムされます。その他のセッションに属する ACE には、この送信元インターフェイスはプログラムされません。
- 同じ送信元を使用するように ERSPAN セッションおよびローカル SPAN セッション（filter access-group および allow-sharing オプションを使用）を設定する場合は、設定を保存してスイッチをリロードすると、ローカル SPAN セッションがダウンします。
- モニター セッションの filter access-group を使用する VLAN アクセスマップ設定では、ドロップアクションはサポートされていません。モニター セッションでドロップアクションのある VLAN アクセスマップに filter access-group が設定されている場合、モニター セッションはエラー状態になります。
- 許可 ACE と拒否 ACE は、どちらも同様に処理されます。ACE と一致するパケットは、ACL の許可エントリまたは拒否エントリを含んでいるかどうかに関係なく、ミラーリングされます。

## ERSPAN の注意事項および制約事項

- ERSPAN は、管理ポートではサポートされません。
- 宛先ポートは、一度に 1 つの ERSPAN セッションだけで設定できます。
- ポートを送信元ポートと宛先ポートの両方として設定することはできません。
- 1 つの ERSPAN セッションに、次の送信元を組み合わせて使用できます。
  - イーサネット ポートまたはポート チャネル（サブインターフェイスを除く）。
  - ポート チャネルサブインターフェイスに割り当てるこことできる VLAN またはポート チャネル。
  - コントロール プレーン CPU へのポート チャネル。



(注)

ERSPAN は送信元に関係なく、スーパーバイザによって生成されるパケットをモニターしません。

- 宛先ポートはスパンニングツリーインスタンスまたはレイヤ3プロトコルに参加しません。
- ERSPAN セッションに、送信方向または送受信方向でモニターされている送信元ポートが含まれている場合、パケットが実際にはその送信元ポートで送信されなくても、これらのポートを受け取るパケットが ERSPAN の宛先ポートに複製される可能性があります。送信元 ポート上でのこの動作の例を、次に示します。
  - フラッディングから発生するトラフィック
  - ブロードキャストおよびマルチキャスト トラフィック
- 入力と出力の両方が設定されている VLAN ERSPAN セッションでは、パケットが同じ VLAN 上でスイッチングされる場合に、宛先ポートから 2 つのパケット（入力側から 1 つ、出力側から 1 つ）が転送されます。
- VLAN ERSPAN がモニタするのは、VLAN のレイヤ2ポートを出入りするトラフィックだけです。
- Cisco Nexus 3600 プラットフォーム スイッチが ERSPAN 宛先の場合、GRE ヘッダーは、終端ポイントからミラーパケットが送信される前には削除されません。パケットは、GRE パケットである GRE ヘッダー、および GRE ペイロードである元のパケットとともに送信されます。
- ERSPAN 送信元セッションの出力インターフェイスは、**show monitor session <session-number>** CLI コマンドの出力に表示されるようになりました。出力インターフェイスには、物理ポートまたは port-channel を指定できます。ECMP の場合、ECMP メンバー内の 1 つのインターフェイスが出力に表示されます。この特定のインターフェイスがトラフィックの出力に使用されます。
- TCAM カービングは、Cisco Nexus 3600 プラットフォーム スイッチの SPAN/ERSPAN には必要ありません。

- SPAN/ERSPAN ACL 統計情報は、**show monitor filter-list** コマンドと同様です。このコマンドの出力には、SPAN TCAM の統計情報とともにすべてのエントリが表示されます。ACL 名は表示されず、エントリのみ出力に表示されます。**clear monitor filter-list statistics** コマンドと同様です。出力は、**show ip access-list** コマンドと同様です。Cisco Nexus 3600 プラットフォーム スイッチは、ACL レベルごとの統計情報をサポートしていません。この機能強化は、ローカル SPAN および ERSPAN の両方でサポートされています。
- CPU とやりとりされるトラフィックはスパニングされます。その他のインターフェイス SPAN に似ています。この機能強化は、ローカル SPAN でのみサポートされています。ACL 送信元ではサポートされていません。Cisco Nexus 3600 プラットフォーム スイッチは、CPU から送信される (RCPU.dest\_port != 0) ヘッダー付きのパケットはスパニングしません。
- SPAN 転送ドロップ トラフィックの場合、フォワーディング プレーンにおけるさまざまな原因でドロップされるパケットのみ SPAN されます。この機能強化は、ERSPAN 送信元セッションでのみサポートされています。SPAN ACL、送信元 VLAN、および送信元インターフェイスとともににはサポートされません。SPAN のドロップ トラフィックには、3 つの ACL エントリがインストールされます。ドロップ エントリに優先度を設定して、その他のモニターセッションの SPAN ACL エントリや VLAN SPAN エントリよりも高いまたは低い優先度にすることができます。デフォルトでは、ドロップ エントリの優先度の方が高くなります。
- SPAN UDF (ユーザー定義フィールド) ベースの ACL サポート
  - パケットの最初の 128 バイトのパケットヘッダーまたはペイロード (一定の長さ制限あり) を照合できます。
  - 照合のために、特定のオフセットと長さを指定して UDF を定義できます。
  - 1 バイトまたは 2 バイトの長さのみ照合できます。
  - 最大 8 個の UDF がサポートされます。
  - 追加の UDF 一致基準が ACL に追加されます。
  - UDF 一致基準は、SPAN ACL に対してのみ設定できます。この機能強化は、他の ACL 機能 (RACL、PACL、および VACL) ではサポートされていません。
  - ACE ごとに最大 8 個の UDF 一致基準を指定できます。
  - UDF および HTTP リダイレクト構成を、同じ ACL に共存させることはできません。
  - UDF 名は、SPAN TCAM に適合している必要があります。
  - UDF は、SPAN TCAM によって認定されている場合のみ有効です。
  - UDF 定義の構成および SPAN TCAM での UDF 名の認定では、**copy rs** コマンドを使用して、リロードする必要があります。
  - UDF の照合は、ローカル SPAN と ERSPAN 送信元セッションの両方でサポートされています。

## ERSPAN のデフォルト設定

- UDF 名の長さは最大 16 文字です。
- UDF のオフセットは 0 (ゼロ) から始まります。オフセットが奇数で指定されている場合、ソフトウェアの 1 つの UDF 定義に対して、ハードウェアで 2 つの UDF が使用されます。ハードウェアで使用している UDF の数が 8 を超えると、その設定は拒否されます。
- UDF の照合では、SPAN TCAM リージョンが倍幅になる必要があります。そのため、他の TCAM リージョンのサイズを減らして、SPAN の領域を確保する必要があります。
- SPAN UDF は、タップ アグリゲーション モードではサポートされていません。
- erspan-src セッションに sup-eth 送信元インターフェイスが設定されている場合、acl-span を送信元としてそのセッションに追加することはできません (その逆も同様)。
- ERSPAN サポートでの IPv6 ユーザー定義フィールド (UDF)
- ERSPAN 送信元および ERSPAN 宛先セッションでは、専用のループバックインターフェイスを使用する必要があります。そのようなループバックインターフェイスには、どのようなコントロールプレーンプロトコルも使用しません。

## 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 26: デフォルトの **ERSPAN** パラメータ

パラメータ	デフォルト
ERSPAN セッション	シャット ステートで作成されます。

## ERSPAN の設定

### ERSPAN 送信元セッションの設定

ERSPAN セッションを設定できるのはローカルデバイス上だけです。デフォルトでは、ERSPAN セッションはシャット ステートで作成されます。

送信元には、イーサネットポート、ポートチャネル、および VLAN を指定できます。単一の ERSPAN セッションには、イーサネットポートまたは VLAN を組み合わせた送信元を使用できます。



(注) ERSPAN は送信元に関係なく、スーパーバイザによって生成されるパケットをモニタしません。

## 手順の概要

1. **configure terminal**
2. **monitor erspan origin ip-address *ip-address* global**
3. **no monitor session {*session-number* | all}**
4. **monitor session {*session-number* | all} type erspan-source**
5. **description *description***
6. **filter access-group *acl-name***
7. **source {interface type [rx | tx | both] | vlan {*number* | range} [rx]}**
8. (任意) ステップ 6 を繰り返して、すべての ERSPAN 送信元を設定します。
9. (任意) **filter access-group *acl-filter***
10. **destination ip *ip-address***
11. (任意) **ip ttl *ttl-number***
12. (任意) **ip dscp *dscp-number***
13. **no shut**
14. (任意) **show monitor session {all | *session-number* | range *session-range*}**
15. (任意) **show running-config monitor**
16. (任意) **show startup-config monitor**
17. (任意) **copy running-config startup-config**

## 手順の詳細

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 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	<b>monitor erspan origin ip-address <i>ip-address</i> global</b> 例： switch(config)# monitor erspan origin ip-address 10.0.0.1 global	ERSPAN のグローバルな送信元 IP アドレスを設定します。
ステップ 3	<b>no monitor session {<i>session-number</i>   all}</b> 例： switch(config)# no monitor session 3	指定した ERSPAN セッションの設定を消去します。新しいセッション コンフィギュレーションは、既存のセッション コンフィギュレーションに追加されます。

## ERSPAN 送信元セッションの設定

	コマンドまたはアクション	目的
ステップ 4	<b>monitor session {session-number   all} type erspan-source</b>  例： <pre>switch(config)# monitor session 3 type erspan-source switch(config-erspan-src) #</pre>	ERSPAN 送信元セッションを設定します。
ステップ 5	<b>description description</b>  例： <pre>switch(config-erspan-src) # description erspan_src_session_3</pre>	セッションの説明を設定します。デフォルトでは、説明は定義されません。説明には最大 32 の英数字を使用できます。
ステップ 6	<b>filter access-group acl-name</b>  例： <pre>switch(config-erspan-src) # filter access-group acl1</pre>	ACL リストに基づいて、送信元ポートで入力トラフィックをフィルタリングします。アクセスリストに一致するパケットのみがスパニングされます。値は、 <i>acl-name</i> は、IP アクセスリストを指定できますが、アクセスマップは指定できません。
ステップ 7	<b>source {interface type [rx   tx   both]   vlan {number   range} [rx]}</b>  例： <pre>switch(config-erspan-src) # source interface ethernet 2/1-3, ethernet 3/1 rx</pre> 例： <pre>switch(config-erspan-src) # source interface port-channel 2</pre> 例： <pre>switch(config-erspan-src) # source interface sup-eth 0 both</pre> 例： <pre>switch(config-monitor) # source interface ethernet 101/1/1-3</pre>	
ステップ 8	(任意) ステップ 6 を繰り返して、すべての ERSPAN 送信元を設定します。	—
ステップ 9	(任意) <b>filter access-group acl-filter</b>  例： <pre>switch(config-erspan-src) # filter access-group ACL1</pre>	ACL を ERSPAN セッションにアソシエートします。  (注) 標準の ACL 構成プロセスを使用して ACL を作成できます。詳細については、プラットフォームの Cisco Nexus 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。

	コマンドまたはアクション	目的
ステップ 10	<b>destination ip ip-address</b>  例： switch(config-erspan-src)# destination ip 10.1.1.1	ERSPAN セッションの宛先 IP アドレスを設定します。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	(任意) <b>ip ttl ttl-number</b>  例： switch(config-erspan-src)# ip ttl 25	ERSPAN トラフィックの IP 存続可能時間 (TTL) 値を設定します。範囲は 1 ~ 255 です。
ステップ 12	(任意) <b>ip dscp dscp-number</b>  例： switch(config-erspan-src)# ip dscp 42	ERSPAN トラフィックのパケットの DiffServ コードポイント (DSCP) 値を設定します。範囲は 0 ~ 63 です。
ステップ 13	<b>no shut</b>  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) 同時に実行できる ERSPAN 送信元セッションは 2 つだけです。
ステップ 14	(任意) <b>show monitor session {all   session-number   range session-range}</b>  例： switch(config-erspan-src)# show monitor session 3	ERSPAN セッション設定を表示します。
ステップ 15	(任意) <b>show running-config monitor</b>  例： switch(config-erspan-src)# show running-config monitor	ERSPAN の実行コンフィギュレーションを表示します。
ステップ 16	(任意) <b>show startup-config monitor</b>  例： switch(config-erspan-src)# show startup-config monitor	ERSPAN のスタートアップ コンフィギュレーションを表示します。
ステップ 17	(任意) <b>copy running-config startup-config</b>  例： switch(config-erspan-src)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

## ■ ERSPAN 送信元セッションの SPAN 転送 ドロップ トラフィックの設定

# ERSPAN 送信元セッションの SPAN 転送 ドロップ トラフィックの設定

## 手順の概要

1. **configure terminal**
2. **monitor session {session-number | all} type erspan-source**
3. **vrf vrf-name**
4. **destination ip ip-address**
5. **source forward-drops rx [priority-low]**
6. **no shut**
7. (任意) **show monitor session {all | session-number | range session-range}**

## 手順の詳細

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b>  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	<b>monitor session {session-number   all} type erspan-source</b>  例：  switch(config)# monitor session 1 type erspan-source switch(config-erspan-src)#	ERSPAN 送信元セッションを設定します。
ステップ 3	<b>vrf vrf-name</b>  例：  switch(config-erspan-src)# vrf default	ERSPAN 送信元セッションがトラフィックの転送に使用する VRF を設定します。
ステップ 4	<b>destination ip ip-address</b>  例：  switch(config-erspan-src)# destination ip 10.1.1.1	ERSPAN セッションの宛先 IP アドレスを設定します。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 5	<b>source forward-drops rx [priority-low]</b>  例：  switch(config-erspan-src)# source forward-drops rx [priority-low]	ERSPAN 送信元セッションの SPAN 転送 ドロップ トラフィックを設定します。低い優先度に設定されている場合、この SPAN ACE の一致ドロップ条件は、ACL SPAN または VLAN ACL SPAN インターフェイスによって設定されているその他の SPAN ACE よりも優先度が低くなります。priority-low キーワードを指定しない場合、これらのドロップ ACE は、標準インターフェイスや VLAN SPAN ACL よりも優先度

	コマンドまたはアクション	目的
		が高くなります。優先度は、パケットの一致ドロップ ACE およびインターフェイス/VLAN SPAN ACL が設定されている場合のみ問題になります。
ステップ 6	<b>no shut</b>  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) 同時に実行できる ERSPAN 送信元セッションは 2 つだけです。
ステップ 7	(任意) <b>show monitor session {all   session-number   range session-range}</b>  例：  switch(config-erspan-src)# show monitor session 3	ERSPAN セッション設定を表示します。

### 例

```
switch# config t
switch(config)# monitor session 1 type erspan-source
switch(config-erspan-src)# vrf default
switch(config-erspan-src)# destination ip 40.1.1.1
switch(config-erspan-src)# source forward-drops rx
switch(config-erspan-src)# no shut
switch(config-erspan-src)# show monitor session 1

switch# config t
switch(config)# monitor session 1 type erspan-source
switch(config-erspan-src)# vrf default
switch(config-erspan-src)# destination ip 40.1.1.1
switch(config-erspan-src)# source forward-drops rx priority-low
switch(config-erspan-src)# no shut
switch(config-erspan-src)# show monitor session 1
```

## ERSPAN ACL の設定

デバイスに IPv4 ERSPAN ACL を作成して、ルールを追加できます。

### 始める前に

DSCP 値または GRE プロトコルを変更するには、新しい宛先モニタセッションを割り当てる必要があります。最大 4 つの宛先モニタセッションがサポートされます。

### 手順の概要

#### 1. **configure terminal**

## ■ ERSPAN ACL の設定

2. **ip access-list *acl-name***
3. **[sequence-number] {permit | deny} protocol source destination [set-erspan-dscp *dscp-value*] [set-erspan-gre-proto *protocol-value*]**
4. (任意) **show ip access-lists *name***
5. (任意) **show monitor session {all | session-number | range *session-range*} [brief]**
6. (任意) **copy running-config startup-config**

## 手順の詳細

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 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	<b>ip access-list <i>acl-name</i></b> 例： switch(config)# ip access-list erspan-acl switch(config-acl)#	ERSPAN ACLを作成して、IP ACLコンフィギュレーションモードを開始します。 <i>acl-name</i> 引数は64文字以内で指定できます。
ステップ 3	<b>[sequence-number] {permit   deny} protocol source destination [set-erspan-dscp <i>dscp-value</i>] [set-erspan-gre-proto <i>protocol-value</i>]</b> 例： switch(config-acl)# permit ip 192.168.2.0/24 any set-erspan-dscp 40 set-erspan-gre-proto 5555	ERSPAN ACL内にルールを作成します。多数のルールを作成できます。 <i>sequence-number</i> 引数には、1～4294967295の整数を指定します。 <b>permit</b> と <b>deny</b> コマンドには、トラフィックを識別するための多くの方法が用意されています。 <b>set-erspan-dscp</b> アクションのアクセスコントロールエントリ(ACE)は、ERSPAN外部IPヘッダーにDSCP値を設定します。DSCP値の範囲は0～63です。ERSPAN ACLに設定されたDSCP値でモニターセッションに設定されている値が上書きされます。ERSPAN ACLにこのオプションを含めない場合、0またはモニターセッションで設定されているDSCP値が設定されます。 <b>set-erspan-gre-proto</b> オプションは、ERSPAN GREヘッダーにプロトコル値を設定します。プロトコル値の範囲は0～65535です。ERSPAN ACLにこのオプションを含めない場合、ERSPANカプセル化パケットのGREヘッダーのプロトコルとしてデフォルト値の0x88beが設定されます。 <b>set-erspan-gre-proto</b> または <b>set-erspan-dscp</b> アクションのアクセスコントロールエントリ(ACE)は、

	コマンドまたはアクション	目的
		<p>1 つの接続先モニター セッションを消費します。ERSPAN ACL ごとに、これらのアクションのいずれかが設定されている最大 3 つの ACE がサポートされます。たとえば、次のいずれかを設定できます。</p> <ul style="list-style-type: none"> <li>次のアクションで設定された最大 3 つの ACE を持つ ACL が設定されている、1 つの ERSPAN セッション。 <b>set-erspan-gre-proto</b> または <b>set-erspan-dscp</b> アクションのアクセス コントロールエントリ (ACE) アクション</li> <li>次のアクションで設定された 2 つの ACE を持つ ACL が設定されている、1 つの ERSPAN セッション。 <b>set-erspan-gre-proto</b> または <b>set-erspan-dscp</b> アクションおよび 1 つの追加のローカルセッションまたは ERSPAN セッション</li> <li>次のアクションが設定された 1 つの ACE を持つ ACL が設定されている、2 つの ERSPAN セッションのうち大きなもの <b>set-erspan-gre-proto</b> または <b>set-erspan-dscp</b> アクションのアクセス コントロールエントリ (ACE) アクション</li> </ul>
ステップ 4	<p>(任意) <b>show ip access-lists name</b></p> <p>例 :</p> <pre>switch(config-acl)# show ip access-lists erspan-acl</pre>	ERSPAN ACL の構成を表示します。
ステップ 5	<p>(任意) <b>show monitor session {all   session-number   range session-range} [brief]</b></p> <p>例 :</p> <pre>switch(config-acl)# show monitor session 1</pre>	ERSPAN セッション設定を表示します。
ステップ 6	<p>(任意) <b>copy running-config startup-config</b></p> <p>例 :</p> <pre>switch(config-acl)# copy running-config startup-config</pre>	実行中の構成を、スタートアップ構成にコピーします。

## ユーザー定義フィールド (UDF) ベースの ACL サポートの設定

Cisco Nexus 3600 プラットフォームスイッチにユーザー定義フィールド (UDF) ベースの ACL のサポートを構成できます。次の手順を参照して、UDF に基づく ERSPAN を設定します。詳細については、「ERSPAN の注意事項および制約事項」を参照してください。

## ■ ユーザー定義フィールド (UDF) ベースの ACL サポートの設定

## 手順の概要

1. switch# **configure terminal**
2. switch(config)# **udf < udf -name> <packet start> <offset> <length>**
3. switch(config)# **udf < udf -name> header <Layer3/Layer4> <offset> <length>**
4. switch(config)# **hardware profile tcam region span qualify udf <name1>..... <name8>**
5. switch(config)# **permit ..... <regular ACE match criteria> udf <name1> < val > <mask> ..... <name8> < val > <mask>**
6. switch(config)# **show monitor session <session-number>**

## 手順の詳細

## 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	グローバルコ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)# <b>udf &lt; udf -name&gt; &lt;packet start&gt; &lt;offset&gt; &lt;length&gt;</b>  例： <pre>(config) # udf udf1 packet-start 10 2 (config) # udf udf2 packet-start 50 2</pre>	UDF を定義します。  (注) 複数の UDF を定義できますが、必要な UDF のみ設定することを推奨します。UDF は、TCAM カービング時 (ブートアップ時) にリージョンの修飾子セットに追加されるため、この設定は、UDF を TCAM リージョンにアタッチして、ボックスを再起動した後でのみ有効になります。
ステップ 3	switch(config)# <b>udf &lt; udf -name&gt; header &lt;Layer3/Layer4&gt; &lt;offset&gt; &lt;length&gt;</b>  例： <pre>(config) # udf udf3 header outer 14 0 1 (config) # udf udf3 header outer 14 10 2 (config) # udf udf3 header outer 14 50 1</pre>	UDF を定義します。
ステップ 4	switch(config)# <b>hardware profile tcam region span qualify udf &lt;name1&gt;..... &lt;name8&gt;</b>  例： <pre>(config) # hardware profile tcam region span qualify udf udf1 udf2 udf3 udf4 udf5 [SUCCESS] Changes to UDF qualifier set will be applicable only after reboot. You need to 'copy run start' and 'reload' config) #</pre>	SPAN TCAM に UDF 認定を設定します。TCAM カービング時 (ブートアップ時) に UDF を TCAM リージョンの修飾子セットに追加します。この設定では、SPAN リージョンにアタッチできる最大 4 つの UDF を許可できます。UDF はすべて、リージョンの單一コマンドでリストされます。リージョンの新しい設定により、既存の設定が置き換わりますが、設定を有効にするには再起動する必要があります。  UDF 修飾子が SPAN TCAM に追加されると、TCAM リージョンはシングル幅から倍幅に拡大します。拡大に使用できる十分な空き領域 (128 以上のシング

	コマンドまたはアクション	目的
		ル幅エントリ) があることを確認します。十分な領域がない場合、コマンドは拒否されます。未使用リージョンの TCAM 領域を削減して領域を確保したら、コマンドを再入力します。次のコマンドを使用して UDF が SPAN/ TCAM リージョンから切り離されると、 <b>no hardware profile team region span qualify udf &lt;name1&gt; ..&lt;name8&gt;</b> SPAN TCAM リージョンは単一の幅のエントリと見なされます。
<b>ステップ 5</b>	<pre>switch(config)# permit ..... &lt;regular ACE match criteria&gt; udf &lt;name1&gt; &lt;val&gt; &lt;mask&gt; .....&lt;name8&gt; &lt;val&gt; &lt;mask&gt;</pre> <p>例 :</p> <pre>(config)# ip access-list test 10 permit ip any any udf udf1 0x1234 0xffff udf3 0x56 0xff 30 permit ip any any dscp af11 udf udf5 0x22 0x22 config) #</pre>	UDF と一致する ACL を設定します。
<b>ステップ 6</b>	<pre>switch(config)# show monitor session &lt;session-number&gt;</pre> <p>例 :</p> <pre>(config)# show monitor session 1 session 1 ----- type          : erspan-source state         : up vrf-name      : default destination-ip: 40.1.1.1 ip-ttl        : 255 ip-dscp       : 0 acl-name      : test origin-ip     : 100.1.1.10 (global) source intf   :   rx          : Eth1/20   tx          : Eth1/20   both        : Eth1/20 source VLANs  :   rx          : source fwd drops: egress-intf   : Eth1/23 switch# config) #</pre>	<b>show monitor session &lt;session-number&gt;</b> コマンドを使用して ACL を表示します。BCM SHELL コマンドを使用して、SPAN TCAM リージョンがカービングされているかどうかを確認できます。

## ERSPAN での IPv6 ユーザー定義フィールド (UDF) の設定

Cisco Nexus 3600 プラットフォーム スイッチでは ERSPAN で IPv6 ユーザー定義フィールド (UDF) を構成できます。次の手順を参照して、IPv6 UDF に基づく ERSPAN を設定します。詳細については、「ERSPAN の注意事項および制約事項」を参照してください。

## ■ ERSPAN での IPv6 ユーザー定義フィールド (UDF) の設定

## 手順の概要

1. switch# **configure terminal**
2. switch(config)# **udf <udf-name> <packet start> <offset> <length>**
3. switch(config)# **udf <udf-name> header <Layer3/Layer4> <offset> <length>**
4. switch(config)# **hardware profile tcam region ipv6-span-l2 512**
5. switch(config)# **hardware profile tcam region ipv6-span 512**
6. switch(config)# **hardware profile tcam region span spanv6 qualify udf <name1>..... <name8>**
7. switch(config)# **hardware profile tcam region span spanv6-12 qualify udf <name1>..... <name8>**
8. switch (config-erspan-src)# **filter ..... ipv6 access-group....<aclname>.... <allow-sharing>**
9. switch(config)# **permit ..... <regular ACE match criteria> udf <name1> <val> <mask> ..... <name8> <val> <mask>**
10. switch(config)# **show monitor session <session-number>**

## 手順の詳細

## 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	グローバル コ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)# <b>udf &lt;udf-name&gt; &lt;packet start&gt; &lt;offset&gt; &lt;length&gt;</b>  例：  (config)# udf udf1 packet-start 10 2 (config)# udf udf2 packet-start 50 2	UDF を定義します。  (注) 複数の UDF を定義できますが、必要な UDF のみ設定することを推奨します。UDF は、TCAM カービング時 (ブートアップ時) にリージョンの修飾子セットに追加されるため、この設定は、UDF を TCAM リージョンにアタッチして、ボックスを再起動した後でのみ有効になります。
ステップ 3	switch(config)# <b>udf &lt;udf-name&gt; header &lt;Layer3/Layer4&gt; &lt;offset&gt; &lt;length&gt;</b>  例：  (config)# udf udf3 header outer 14 0 1 (config)# udf udf3 header outer 14 10 2 (config)# udf udf3 header outer 14 50 1	UDF を定義します。
ステップ 4	switch(config)# <b>hardware profile tcam region ipv6-span-l2 512</b>  例：  (config)# <b>hardware profile tcam region ipv6-span-12 512</b> Warning: Please save config and reload the system for the configuration to	レイヤ 2 ポートの UDF で IPv6 を設定します。リージョンの新しい設定により既存の設定が置き換わりますが、設定を有効にするにはスイッチを再起動する必要があります。

	コマンドまたはアクション	目的
	take effect. config) #	
ステップ 5	switch(config)# <b>hardware profile tcam region ipv6-span 512</b>  例： (config) # <b>hardware profile tcam region ipv6-span 512</b> Warning: Please save config and reload the system for the configuration to take effect. config) #	レイヤ3 ポートの UDF で IPv6 を設定します。リージョンの新しい設定により既存の設定が置き換わりますが、設定を有効にするにはスイッチを再起動する必要があります。
ステップ 6	switch(config)# <b>hardware profile tcam region span spanv6 qualify udf &lt;name1&gt;.....&lt;name8&gt;</b>  例： (config) # <b>hardware profile tcam region spanv6 qualify udf udf1</b> [SUCCESS] Changes to UDF qualifier set will be applicable only after reboot. You need to 'copy run start' and 'reload' config) #	レイヤ3 ポートの SPAN に UDF 認定を設定します。これにより、ipv6-span TCAM リージョンの UDF 照合が有効になります。TCAM カービング時 (ブートアップ時) に UDF を TCAM リージョンの修飾子セットに追加します。この設定では、SPAN リージョンにアタッチできる最大 2 つの IPv6 UDF を許可できます。UDF はすべて、リージョンの單一コマンドでリストされます。リージョンの新しい設定により、既存の設定が置き換わりますが、設定を有効にするには再起動する必要があります。
ステップ 7	switch(config)# <b>hardware profile tcam region span spanv6-12 qualify udf &lt;name1&gt;.....&lt;name8&gt;</b>  例： (config) # <b>hardware profile tcam region spanv6-12 qualify udf udf1</b> [SUCCESS] Changes to UDF qualifier set will be applicable only after reboot. You need to 'copy run start' and 'reload' config) #	レイヤ2 ポートの SPAN に UDF 認定を設定します。これにより、ipv6-span-12 TCAM リージョンの UDF 照合が有効になります。TCAM カービング時 (ブートアップ時) に UDF を TCAM リージョンの修飾子セットに追加します。この設定では、SPAN リージョンにアタッチできる最大 2 つの IPv6 UDF を許可できます。UDF はすべて、リージョンの單一コマンドでリストされます。リージョンの新しい設定により、既存の設定が置き換わりますが、設定を有効にするには再起動する必要があります。
ステップ 8	switch (config-erspan-src)# <b>filter ..... ipv6 access-group....&lt;aclname&gt;....&lt;allow-sharing&gt;</b>  例： (config-erspan-src) # <b>ipv6 filter access-group test</b> (config) #	SPAN および ERSPAN モードで IPv6 ACL を設定します。1 つのモニター セッションには「filter ip access-group」または「filter ipv6 access-group」のいずれか 1 つだけを設定できます。同じ送信元インターフェイスが IPv4 と IPv6 ERSPAN ACL モニター セッションの一部である場合は、モニター セッションの設定で「allow-sharing」に「filter [ipv6] access-group」を設定する必要があります。
ステップ 9	switch(config)# <b>permit ..... &lt;regular ACE match criteria&gt; udf &lt;name1&gt; &lt;val&gt; &lt;mask&gt; .....&lt;name8&gt; &lt;val&gt; &lt;mask&gt;</b>	UDF と一致する ACL を設定します。

## ■ ERSPAN セッションのシャットダウンまたはアクティブ化

	コマンドまたはアクション	目的
	例： (config-erspan-src)# <b>ipv6 access-list test</b> (config-ipv6-acl)# <b>permit ipv6 any any udf udf1 0x1 0x0</b>	
ステップ 10	switch(config)# <b>show monitor session &lt;session-number&gt;</b> 例： (config)# <b>show monitor session 1</b> session 1 ----- type : erspan-source state : up vrf-name : default destination-ip : 40.1.1.1 ip-ttl : 255 ip-dscp : 0 acl-name : test origin-ip : 100.1.1.10 (global) source intf : rx : Eth1/20 tx : Eth1/20 both : Eth1/20 source VLANs : filter VLANs : filter not specified rx : source fwd drops : egress-intf : Eth1/23 switch# config) #	次のコマンドを使用して ACL を表示します。 <b>show monitor session &lt;session-number&gt;</b> コマンドを使用します。

## 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。

### 手順の概要

1. **configuration terminal**
2. **monitor session {session-range | all} shut**
3. **no monitor session {session-range | all} shut**
4. **monitor session session-number type erspan-source**

5. **monitor session *session-number* type erspan-destination**
6. **shut**
7. **no shut**
8. (任意) **show monitor session all**
9. (任意) **show running-config monitor**
10. (任意) **show startup-config monitor**
11. (任意) **copy running-config startup-config**

### 手順の詳細

#### 手順

	コマンドまたはアクション	目的
ステップ1	<b>configuration terminal</b> <b>例 :</b> <pre>switch# configuration terminal switch(config)#</pre>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<b>monitor session {<i>session-range</i>   all} shut</b> <b>例 :</b> <pre>switch(config)# monitor session 3 shut</pre>	<p>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、1～18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。単方向の4つのセッション、または双方の2つのセッションを同時にアクティブにすることができます。</p> <p>(注)</p> <ul style="list-style-type: none"> <li>• 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。</li> <li>• 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。</li> </ul>
ステップ3	<b>no monitor session {<i>session-range</i>   all} shut</b> <b>例 :</b> <pre>switch(config)# no monitor session 3 shut</pre>	<p>指定の ERSPAN セッションを再開 (イネーブル) します。セッションの範囲は、1～18です。セッションの範囲は、1～18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。単方向の4つのセッション、または双方の2つのセッションを同時にアクティブにすることができます。</p> <p>(注)</p> <p>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、</p>

## ■ ERSPAN セッションのシャットダウンまたはアクティブ化

	コマンドまたはアクション	目的
		最初に <b>monitor session shut</b> コマンドを指定してから、 <b>no monitor session shut</b> コマンドを続ける必要があります。
ステップ 4	<b>monitor session session-number type erspan-source</b> 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	<b>monitor session session-number type erspan-destination</b> 例： switch(config-erspan-src) # monitor session 3 type erspan-destination	ERSPAN 宛先タイプのモニター コンフィギュレーションモードを開始します。
ステップ 6	<b>shut</b> 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	<b>no shut</b> 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	(任意) <b>show monitor session all</b> 例： switch(config-erspan-src) # show monitor session all	ERSPAN セッションのステータスを表示します。
ステップ 9	(任意) <b>show running-config monitor</b> 例： switch(config-erspan-src) # show running-config monitor	ERSPAN の実行コンフィギュレーションを表示します。
ステップ 10	(任意) <b>show startup-config monitor</b> 例： switch(config-erspan-src) # show startup-config monitor	ERSPAN のスタートアップ コンフィギュレーションを表示します。
ステップ 11	(任意) <b>copy running-config startup-config</b> 例： switch(config-erspan-src) # copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

## ERSPAN 設定の確認

ERSPAN 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
<b>show monitor session {all   session-number   range session-range}</b>	ERSPAN セッション設定を表示します。
<b>show running-config monitor</b>	ERSPAN の実行コンフィギュレーションを表示します。
<b>show startup-config monitor</b>	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# config t
switch(config)# interface e14/30
switch(config-if)# no shut
switch(config-if)# exit
switch(config)# monitor erspan origin ip-address 3.3.3.3 global
switch(config)# monitor session 1 type erspan-source
switch(config-erspan-src)# filter access-group acl1
switch(config-erspan-src)# source interface e14/30
switch(config-erspan-src)# ip ttl 16
switch(config-erspan-src)# ip dscp 5
switch(config-erspan-src)# vrf default
switch(config-erspan-src)# destination ip 9.1.1.2
switch(config-erspan-src)# no shut
switch(config-erspan-src)# exit
switch(config)# show monitor session 1
```

### ERSPAN ACL の設定例

次に、ERSPAN ACL を設定する例を示します。

```
switch# configure terminal
switch(config)# ip access-list match_11_pkts
switch(config-acl)# permit ip 11.0.0.0 0.255.255.255 any
switch(config-acl)# exit
switch(config)# ip access-list match_12_pkts
switch(config-acl)# permit ip 12.0.0.0 0.255.255.255 any
switch(config-acl)# exit
switch(config)# vlan access-map erspan_filter 5
switch(config-access-map)# match ip address match_11_pkts
switch(config-access-map)# action forward
switch(config-access-map)# exit
```

## UDF ベース ERSPAN の設定例

```

switch(config)# vlan access-map erspan_filter 10
switch(config-access-map)# match ip address match_12_pkts
switch(config-access-map)# action forward
switch(config-access-map)# exit
switch(config)# monitor session 1 type erspan-source
switch(config-erspan-src)# filter access_group erspan_filter

```

## UDF ベース ERSPAN の設定例

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

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

```

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

```

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

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

```

udf udf_pktsig_msb header outer 13 26 2
udf udf_pktsig_lsb header outer 13 28 2
hardware access-list tcam region racl qualify udf udf_pktsig_msb udf_pktsig_lsb
copy running-config startup-config
reload
ip access-list acl-udf-pktsig

```

```
permit udf udf_pktsig_msb 0xDEAD 0xFFFF udf udf_pktsig_lsb 0xBEEF 0xFFFF
monitor session 1 type erspan-source
  source interface Ethernet 1/1
  filter access-group acl-udf-pktsig
```

## 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	<i>Cisco Nexus NX-OS System Management Command Reference</i> お使いのプラットフォーム用。

## ■ 関連資料



## 第 19 章

# DNS の設定

この章は、次の内容で構成されています。

- [DNS クライアントについて \(283 ページ\)](#)
- [DNS クライアントの前提条件 \(284 ページ\)](#)
- [DNS クライアントのデフォルト設定 \(284 ページ\)](#)
- [DNS 送信元インターフェイスの設定 \(285 ページ\)](#)
- [DNS クライアントの設定 \(286 ページ\)](#)

## DNS クライアントについて

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ー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、Cisco 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 サーバーを指定して、DNS サービスをイネーブルにする必要があります。

## DNS の動作

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 サーバー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）。

## 高可用性

Cisco Nexus 3600 プラットフォーム スイッチは、DNS クライアントのステートレス リスト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	有効 (Enabled)

# DNS 送信元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に DNS を設定できます。

## 手順の概要

1. switch# **configure terminal**
2. switch(config)# **ip dns source-interface type slot/port**
3. switch(config)# **show ip dns source-interface**

## 手順の詳細

### 手順

	コマンドまたはアクション	目的
ステップ1	switch# <b>configure terminal</b>	グローバル コ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)# <b>ip dns source-interface type slot/port</b>	すべての DNS パケットの送信元インターフェイスを設定します。次のリストに、 <i>interface</i> の有効な値を含みます。 <ul style="list-style-type: none"> <li>• ethernet</li> <li>• loopback</li> <li>• mgmt</li> <li>• port-channel</li> <li>• vlan</li> </ul> (注) DNS の送信元インターフェイスを設定する場合、サーバーから開始される SCP コピー操作は失敗します。サーバーからの SCP コピー操作を実行するには、DNS 送信元インターフェイスの設定を削除します。
ステップ3	switch(config)# <b>show ip dns source-interface</b>	設定済みの DNS 送信元インターフェイスを表示します。

### 例

次に、DNS 送信元インターフェイスを設定する例を示します。

## DNS クライアントの設定

```

switch(config)# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ip dns source-interface ethernet 1/8
switch(config)# show ip dns source-interface
VRF Name                               Interface
default                                Ethernet1/8

```

# 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。

### 始める前に

- 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。

### 手順の概要

- switch# **configuration terminal**
- switch(config)# vrf context management
- switch(config)# {ip | ipv6} host name *ipv/ipv6 address1 [ip/ipv6 address2... ip/ipv6 address6]*
- (任意) switch(config)# **ip domain name** *name [use-vrf vrf-name]*
- (任意) switch(config)# **ip domain-list** *name [use-vrf vrf-name]*
- (任意) switch(config)# **ip name-server** *ip/ipv6 server-address1 [ip/ipv6 server-address2... ip/ipv6 server-address6] [use-vrf vrf-name]*
- (任意) switch(config)# **ip domain-lookup**
- (任意) switch(config)# **show hosts**
- switch(config)# **exit**
- (任意) switch# **copy running-config startup-config**

### 手順の詳細

#### 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configuration terminal</b>	グローバル コ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 management	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   ipv6} host name <i>ipv/ipv6 address1 [ip/ipv6 address2... ip/ipv6 address6]</i>	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	コマンドまたはアクション	目的
4	(任意) switch(config)# <b>ip domain name name [use-vrf vrf-name]</b>	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ーを定義します。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ー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ー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。
5	(任意) switch(config)# <b>ip domain-list name [use-vrf vrf-name]</b>	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ーを定義します。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ー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ー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。
6	(任意) switch(config)# <b>ip name-server ip/ipv6 server-address1 [ip/ipv6 server-address2... ip/ipv6 server-address6] [use-vrf vrf-name]</b>	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。
7	(任意) switch(config)# <b>ip domain-lookup</b>	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。
8	(任意) switch(config)# <b>show hosts</b>	DNS に関する情報を表示します。
9	switch(config)# <b>exit</b>	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。
10	(任意) switch# <b>copy running-config startup-config</b>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

## 例

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 20 章

## sFlow の設定

この章は、次の項で構成されています。

- [sFlowについて \(289 ページ\)](#)
- [前提条件 \(290 ページ\)](#)
- [sFlowの注意事項および制約事項 \(290 ページ\)](#)
- [sFlowのデフォルト設定 \(291 ページ\)](#)
- [サンプリングの最小要件 \(291 ページ\)](#)
- [sFlowの設定 \(291 ページ\)](#)
- [sFlow設定の確認 \(301 ページ\)](#)
- [sFlowの設定例 \(301 ページ\)](#)
- [sFlowに関する追加情報 \(301 ページ\)](#)

### sFlowについて

sFlowを使用すると、スイッチやルータを含むデータネットワーク内のリアルタイムトラフィックをモニターできます。sFlowでは、トラフィックをモニターするためにスイッチやルータ上のsFlowエージェントソフトウェアでサンプリングメカニズムを使用して、入力および出力ポート上のサンプルデータを中央のデータコレクタ(sFlowアナライザとも呼ばれる)に転送します。

sFlowの詳細については、RFC 3176を参照してください。

### sFlowエージェント

Cisco NX-OSソフトウェアに組み込まれているsFlowエージェントは、サンプリングされるパケットのデータソースに関連付けられたインターフェイスカウンタを定期的にサンプリングまたはポーリングします。このデータ送信元は、イーサネットインターフェイス、EtherChannelインターフェイス、または、その両方の範囲のいずれかです。イーサネットまたはポートチャネルのサブインターフェイスはサポートされていません。sFlowエージェントは、イーサネットポートマネージャにクエリーを送信して対応するEtherChannelメンバーシップ情報を確認するほか、イーサネットポートマネージャからもメンバーシップの変更の通知を受信します。

## ■ 前提条件

Cisco NX-OS ソフトウェアで sFlow サンプリングをイネーブルにすると、サンプリングレートとハードウェア内部の乱数に基づいて、入力パケットと出力パケットが sFlow でサンプリングされたパケットとして CPU に送信されます。sFlow エージェントはサンプリングされたパケットを処理し、sFlow アナライザに sFlow データグラムを送信します。sFlow データグラムには、元のサンプリングされたパケットに加えて、入力ポート、出力ポート、および元のパケット長に関する情報が含まれます。sFlow データグラムには、複数の sFlow サンプルを含めることができます。

## 前提条件

sFlow を構成するには、**feature sflow** コマンドを使用して sFlow 機能を有効にする必要があります。

## sFlow の注意事項および制約事項

sFlow 設定時の注意事項および制約事項は次のとおりです。

- ・インターフェイスの sFlow をイネーブルにすると、入力と出力の両方に対してイネーブルになります。入力だけまたは出力だけの sFlow をイネーブルにできません。
- ・マルチキャスト、ブロードキャスト、または未知のユニキャストパケットの sFlow の出力のサンプリングはサポートされません。
- ・システムの sFlow の設定およびトラフィックに基づいてサンプリングレートを設定する必要があります。
- ・Cisco Nexus 3600 プラットフォーム スイッチは、1 つの sFlow コレクタだけをサポートします。
- ・イーサネットまたはポートチャネルのサブインターフェイスは、sFlow データ送信元ポートとしてサポートされません。
- ・個々のポートチャネル メンバー ポートを sFlow データソースとして設定することはできません。ポートチャネルバンドルインターフェイスは、sFlow データソースインターフェイス po1 などの sFlow 対応のデータソース ポートにすることができます。
- ・Cisco Nexus N3K-C36180YC-R、N3K-C3636C-R、N9K-X9636C-RX、および N9K-X96136YC-R プラットフォーム スイッチの場合、出力サンプル トラフィックには、常に、リスト内の最初のデータ送信元インターフェイスが sflow レコードの送信元 ID インデックスとして示されています。

# sFlow のデフォルト設定

表 27: デフォルトの sFlow パラメータ

パラメータ	デフォルト
sFlow sampling-rate	4096
sFlow sampling-size	128
sFlow max datagram-size	1400
sFlow collector-port	6343
sFlow counter-poll-interval	20

## サンプリングの最小要件

これらが構成されていないと、パケットはサンプリングされません。 sFlow 機能を有効にした後、デバイスでパケットサンプリングを有効にするには、次の構成要素を明示的に構成する必要があります。

- Sflow Agent-IP
- Sflow Collector-IP
- Sflow Data-source interface

構成要素を構成しない場合、パケットはサンプリングされません。

sFlow のデフォルト設定として指定されているデフォルト構成要素はオプションです。

# sFlow の設定

## sFlow 機能のイネーブル化

スイッチの sFlow を設定する前に sFlow 機能をイネーブルにする必要があります。

### 手順の概要

1. switch# **configure terminal**
2. [no] **feature sflow**
3. (任意) **show feature**
4. (任意) switch(config)# **copy running-config startup-config**

## サンプリング レートの設定

### 手順の詳細

#### 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	グローバルコ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] <b>feature sflow</b>	sFlow 機能をイネーブルにします。
ステップ 3	(任意) <b>show feature</b>	イネーブルおよびディセーブルにされた機能を表示します。
ステップ 4	(任意) switch(config)# <b>copy running-config startup-config</b>	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。

#### 例

次に、sFlow 機能をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# feature sflow
switch(config)# copy running-config startup-config
```

## サンプリング レートの設定

#### 始める前に

sFlow 機能がイネーブルになっていることを確認します。

### 手順の概要

1. switch# **configure terminal**
2. [no] **sflow sampling-rate** *sampling-rate*
3. (任意) **show sflow**
4. (任意) switch(config)# **copy running-config startup-config**

## 手順の詳細

## 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	グローバル コ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] <b>sflow sampling-rate</b> <i>sampling-rate</i>	パケットの sFlow のサンプリング レートを設定します。 値は、 <i>sampling-rate</i> には 4096 ~ 1000000000 の整数を指定できます。デフォルト値は 4096 です。
ステップ 3	(任意) <b>show sflow</b>	sFlow 情報を表示します。
ステップ 4	(任意) switch(config)# <b>copy running-config startup-config</b>	リブートおよびリスト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。

## 例

次に、サンプリング レートを 50,000 に設定する例を示します。

```
switch# configure terminal
switch(config)# sflow sampling-rate 50000
switch(config)# copy running-config startup-config
```

上記の設定では、約 50,000 パケットごとに 1 パケットがサンプリングされ、sFlow コレクタに送信されます。わずかな差異がある可能性がありますので注意してください。

## 最大サンプリング サイズの設定

サンプリングされたパケットからコピーする最大バイト数を設定できます。

## 始める前に

sFlow 機能がイネーブルになっていることを確認します。

## 手順の概要

1. switch# **configure terminal**
2. [no] **sflow max-sampled-size** *sampling-size*
3. (任意) **show sflow**
4. (任意) switch(config)# **copy running-config startup-config**

## カウンタのポーリング間隔の設定

### 手順の詳細

#### 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	グローバルコ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] <b>sflow max-sampled-size</b> <i>sampling-size</i>	sFlow の最大サンプリングサイズパケットを設定します。 <i>sampling-size</i> の範囲は 64 ～ 256 バイトです。デフォルト値は 128 です。
ステップ 3	(任意) <b>show sflow</b>	構成された sFlow 値を表示します。
ステップ 4	(任意) switch(config)# <b>copy running-config startup-config</b>	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。

#### 例

次に、sFlow エージェントの最大サンプリングサイズを設定する例を示します。

```
switch# configure terminal
switch(config)# sflow max-sampled-size 200
switch(config)# copy running-config startup-config
```

## カウンタのポーリング間隔の設定

データソースに関するカウンタの継続的なサンプル間の最大秒数を設定できます。サンプリング間隔 0 は、カウンタのサンプリングをディセーブルにします。

#### 始める前に

sFlow 機能がイネーブルになっていることを確認します。

### 手順の概要

1. switch# **configure terminal**
2. [no] **sflow counter-poll-interval** *poll-interval*
3. (任意) **show sflow**
4. (任意) switch(config)# **copy running-config startup-config**

## 手順の詳細

## 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	グローバル コ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] <b>sflow counter-poll-interval</b> <i>poll-interval</i>	インターフェイスの sFlow のポーリング間隔を設定します。 <i>poll-interval</i> の範囲は 0 ~ 2147483647 秒です。デフォルト値は 20 です。0 を構成すると、カウンタのポーリングが無効になります。
ステップ 3	(任意) <b>show sflow</b>	sFlow 情報を表示します。
ステップ 4	(任意) switch(config)# <b>copy running-config startup-config</b>	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。

## 例

次に、インターフェイスの sFlow のポーリング間隔を設定する例を示します。

```
switch# configure terminal
switch(config)# sflow counter-poll-interval 100
switch(config)# copy running-config startup-config
```

## 最大データグラム サイズの設定

1 つのサンプル データグラムで送信できるデータの最大バイト数を設定できます。

## 始める前に

sFlow 機能がイネーブルになっていることを確認します。

## 手順の概要

1. switch# **configure terminal**
2. [no] **sflow max-datatype-size** *datatype-size*
3. (任意) **show sflow**
4. (任意) switch(config)# **copy running-config startup-config**

## ■ sFlow アナライザのアドレスの設定

## 手順の詳細

## 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	グローバルコ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] <b>sflow max-datatype-size datagram-size</b>	sFlow の最大データグラム サイズを設定します。 <i>[datagram-size]</i> の範囲は 200 ~ 9000 バイトです。デフォルト値は 1400 です。
ステップ 3	(任意) <b>show sflow</b>	構成済み sFlow 値が表示されます。
ステップ 4	(任意) switch(config)# <b>copy running-config startup-config</b>	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。

## 例

次に、sFlow の最大データグラム サイズを設定する例を示します。

```
switch# configure terminal
switch(config)# sflow max-datatype-size 2000
switch(config)# copy running-config startup-config
[#####] 100%
```

## sFlow アナライザのアドレスの設定

## 始める前に

sFlow 機能がイネーブルになっていることを確認します。

## 手順の概要

1. switch# **configure terminal**
2. [no] **sflow collector-ip vrf *IP-address vrf-instance***
3. (任意) **show sflow**
4. (任意) switch(config)# **copy running-config startup-config**

## 手順の詳細

## 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	グローバル コ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] <b>sflow collector-ip vrf IP-address vrf-instance</b>	sFlow アナライザの IPv4 アドレスを設定します。 <i>vrf-instance</i> は、次のいずれかです： <ul style="list-style-type: none"> <li>ユーザー定義の VRF 名：最大 32 文字の英数字を指定できます。</li> <li><b>vrf management</b>：sFlow データ コレクタが管理ポートに接続されたネットワークに存在する場合は、このオプションを使用する必要があります。</li> <li><b>vrf default</b>：デフォルト vrf に常駐する任意のフロント パネル ポートを通して sFlow データ コレクタが到達可能なネットワークに接続されている場合、このオプションを使用する必要があります。</li> </ul>
ステップ 3	(任意) <b>show sflow</b>	目的は、「構成された sFlow 値を表示します。
ステップ 4	(任意) switch(config)# <b>copy running-config startup-config</b>	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。

## 例

次に、管理ポートに接続されている sFlow データ コレクタの IPv4 アドレスを設定する例を示します。

```
switch# configure terminal
switch(config)# sflow collector-ip 192.0.2.5 vrf management
switch(config)# copy running-config startup-config
```

## sFlow アナライザ ポートの設定

sFlow データ グラムの宛先ポートを設定できます。

## sFlow エージェント アドレスの設定

### 始める前に

sFlow 機能がイネーブルになっていることを確認します。

### 手順の概要

1. switch# **configure terminal**
2. [no] **sflow collector-port** *collector-port*
3. (任意) **show sflow**
4. (任意) switch(config)# **copy running-config startup-config**

### 手順の詳細

#### 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	グローバル コ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] <b>sflow collector-port</b> <i>collector-port</i>	sFlow アナライザの UDP ポートを設定します。 <i>collector-port</i> の範囲は 0 ~ 65535 です。デフォルト値は 6343 です。
ステップ 3	(任意) <b>show sflow</b>	構成済み sFlow 値が表示されます。
ステップ 4	(任意) switch(config)# <b>copy running-config startup-config</b>	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。

#### 例

次に、sFlow データグラムの宛先ポートを設定する例を示します。

```
switch# configure terminal
switch(config)# sflow collector-port 7000
switch(config)# copy running-config startup-config
[#####] 100%
switch(config)#

```

## sFlow エージェント アドレスの設定

### 始める前に

sFlow 機能がイネーブルになっていることを確認します。

## 手順の概要

1. switch# **configure terminal**
2. [no] **sflow agent-ip ip-address**
3. (任意) **show sflow**
4. (任意) switch(config)# **copy running-config startup-config**

## 手順の詳細

## 手順

	コマンドまたはアクション	目的
ステップ1	switch# <b>configure terminal</b>	グローバル コ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] <b>sflow agent-ip ip-address</b>	sFlow エージェントの IPv4 アドレスを設定します。 デフォルトの <i>ip-address</i> は、0.0.0.0 です。つまり、すべてのサンプリングがスイッチで無効であることを示します。sFlow 機能をイネーブルにするには、有効な IP アドレスを指定する必要があります。構成される値には、ローカル システム上にある IP アドレス、またはトラッキング目的で必要なその他の任意の IP 値を指定できます。
ステップ3	(任意) <b>show sflow</b>	sFlow 情報を表示します。
ステップ4	(任意) switch(config)# <b>copy running-config startup-config</b>	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。

## 例

次に、sFlow エージェントの IPv4 アドレスを設定する例を示します。

```
switch# configure terminal
switch(config)# sflow agent-ip 192.0.2.3
switch(config)# copy running-config startup-config
```

## sFlow サンプリング データ ソースの設定

sFlow のサンプリングデータソースには、イーサネットポート、イーサネットポートの範囲、またはポート チャネルを指定できます。

## sFlow サンプリング データ ソースの設定

### 始める前に

- sFlow 機能がイネーブルになっていることを確認します。
- データ ソースとしてポート チャネルを使用する場合は、すでにポート チャネルを設定して、ポート チャネル番号がわかっていることを確認してください。

### 手順の概要

1. **switch# configure terminal**
2. **switch(config)# [no] sflow data-source interface [ethernet slot/port[-port] |port-channel channel-number]**
3. (任意) **switch(config)# show sflow**
4. (任意) **switch(config)# copy running-config startup-config**

### 手順の詳細

#### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>switch# configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>switch(config)# [no] sflow data-source interface [ethernet slot/port[-port]  port-channel channel-number]</b>	sFlow のサンプリング データ ソースを設定します。イーサネットのデータ ソースの場合、 <i>slot</i> はスロット番号で、 <i>port</i> は、単一のポート番号または <i>port-port</i> として指定されたポートの範囲のいずれかです。
ステップ 3	(任意) <b>switch(config)# show sflow</b>	構成済み sFlow 値が表示されます。
ステップ 4	(任意) <b>switch(config)# copy running-config startup-config</b>	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。

#### 例

次に、sFlow のサンプラーのイーサネット ポート 5~12 を設定する例を示します。

```
switch# configure terminal
switch(config)# sflow data-source interface ethernet 1/5-12
switch(config)# copy running-config startup-config
[#####] 100%
switch(config)#

```

次に、sFlow のサンプラーのポート チャネル 100 を設定する例を示します。

```
switch# configure terminal
switch(config)# sflow data-source interface port-channel 100
```

```
switch(config)# copy running-config startup-config
[#####
switch(config)#

```

## sFlow 設定の確認

sFlow 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
<b>show sflow</b>	sFlow のグローバル コンフィギュレーションを表示します。
<b>show sflow statistics</b>	sFlow の統計情報を表示します。
<b>clear sflow statistics</b>	sFlow 統計情報をクリアします。
<b>show running-config sflow [all]</b>	現在実行中の sFlow コンフィギュレーションを表示します。

## sFlow の設定例

次に sFlow を設定する例を示します。

```
feature sflow
sflow sampling-rate 5000
sflow max-sampled-size 200
sflow counter-poll-interval 100
sflow max-datatype-size 2000
sflow collector-ip 192.0.2.5 vrf management
sflow collector-port 7000
sflow agent-ip 192.0.2.3
sflow data-source interface ethernet 1/5
```

## sFlow に関する追加情報

表 28 : sFlow の関連資料

関連項目	マニュアルタイトル
sFlow CLI コマンド	『Cisco Nexus 3600 NX-OS コマンド参考資料』
RFC 3176	sFlow のパケット形式と SNMP MIB を定義します。 <a href="http://www.sflow.org/rfc3176.txt">http://www.sflow.org/rfc3176.txt</a>

## ■ sFlow に関する追加情報



## 第 21 章

# グレースフル挿入と削除の設定

この章は、次の内容で構成されています。

- グレースフル挿入と削除について (303 ページ)
- GIR ワークフロー (305 ページ)
- メンテナンス モードプロファイルの設定 (306 ページ)
- 通常モードプロファイルの設定 (307 ページ)
- スナップショットの作成 (308 ページ)
- スナップショットへの show コマンドの追加 (310 ページ)
- グレースフル削除のトリガー (312 ページ)
- グレースフル挿入のトリガー (315 ページ)
- メンテナンス モードの強化 (316 ページ)
- GIR 設定の確認 (318 ページ)

## グレースフル挿入と削除について

グレースフル挿入と削除を使用してスイッチを正常に取り出し、そのスイッチをネットワークから分離して、デバッグ操作やアップグレード操作を実行することができます。スイッチは、最小限のトラフィックの中止だけで、通常の転送パスから取り外されます。デバッグ操作やアップグレード操作の実行が終了したら、グレースフル挿入を使用して、そのスイッチを完全な運用（通常）モードに戻すことができます。

グレースフル削除では、すべてのプロトコルと vPC ドメインが正常に停止し、スイッチはネットワークから分離されます。グレースフル挿入では、すべてのプロトコルと vPC ドメインが復元されます。

次のプロトコルは、IPv4 と IPv6 両方のアドレス ファミリでサポートされます。

- Border Gateway Protocol (BGP)
- Enhanced Interior Gateway Routing Protocol (EIGRP)
- Intermediate System-to-Intermediate System (ISIS)
- Open Shortest Path First (OSPF)

## ■ プロファイル

- Protocol Independent Multicast (PIM)
- Routing Information Protocol (RIP)



(注) グレースフル挿入と削除の場合、PIM プロトコルは vPC 環境にのみ適用できます。グレースフル削除の間、vPC 転送ロールがマルチキャスト トラフィックのすべてのノースバウンド送信元に対する vPC ピアに転送されます。

## プロファイル

デフォルトでは、すべての有効なプロトコルは、グレースフル削除中に分離され、グレースフル挿入時に復元されます。プロトコルは、定義済みの順序で分離および復元されます。

プロトコルを個別に分離、シャットダウン、または復元する（あるいは追加の設定を実施する）場合は、グレースフル削除またはグレースフル挿入時に適用できる設定コマンドを使用して、プロファイルを作成できます。ただし、プロトコルの順序が正しいことを確認し、すべての依存関係を考慮する必要があります。

スイッチは、次のプロファイルをサポートしています。

- メンテナンス モード プロファイル：スイッチがメンテナンス モードになったときに、グレースフル削除中に実行されるすべてのコマンドが含まれます。
- 通常モード プロファイル：スイッチが通常モードに戻ったときに、グレースフル挿入中に実行されるすべてのコマンドが含まれます。

プロファイルでは、次のコマンド（および任意の設定コマンド）がサポートされています。

コマンド	説明
<b>isolate</b>	プロトコルをスイッチから分離し、プロトコルをメンテナンス モードにします。
<b>no isolate</b>	プロトコルを復元し、プロトコルを通常モードにします。
<b>shutdown</b>	プロトコルまたは vPC ドメインをシャットダウンします。
<b>no shutdown</b>	プロトコルまたは vPC ドメインを起動します。
<b>system interface shutdown [exclude fex-fabric]</b>	システム インターフェイスをシャットダウンします（管理インターフェイスを除く）。

コマンド	説明
<b>no system interface shutdown [exclude fex-fabric]</b>	システムインターフェイスを起動します。
<b>sleep instance instance-number seconds</b>	指定の秒数だけコマンドの実行を遅延させます。コマンドの複数のインスタンスを遅延できます。 collector-port <i>instance-number</i> および <i>seconds</i> 引数の範囲は 0 ~ 2177483647 です。
<b>python instance instance-number uri [python-arguments]</b> 例 : <b>python instance 1 bootflash://script1.py</b>	Python スクリプトの呼び出しをプロファイルに設定します。コマンドの複数の呼び出しをプロファイルに追加できます。 Python 引数には最大 32 文字の英数字を入力できます。

## スナップショット

Cisco NX-OS では、スナップショットは選択した機能の実行状態をキャプチャし、永続ストレージメディアに保存するプロセスです。

スナップショットは、グレースフル削除前とグレースフル挿入後のスイッチの状態を比較する場合に役立ちます。スナップショットプロセスは、次の 3 つの部分で構成されます。

- 事前に選択したスイッチの一部機能の状態のスナップショットを作成し、永続ストレージメディアに保存する
- さまざまな時間間隔で取得したスナップショットを一覧にして、管理する
- スナップショットを比較して、機能間の相違を表示する

## GIR ワークフロー

グレースフル挿入と削除 (GIR) のワークフローを完了する手順は、次のとおりです。

- (任意) メンテナンスモードプロファイルを作成します ([メンテナンスモードプロファイルの設定 \(306 ページ\)](#) を参照)
- (任意) 通常モードプロファイルを作成します ([通常モードプロファイルの設定 \(307 ページ\)](#) を参照)
- グレースフル削除をトリガーする前のスナップショットを取得します ([スナップショットの作成 \(308 ページ\)](#) を参照)

## メンテナンス モード プロファイルの設定

4. グレースフル削除をトリガーして、スイッチをメンテナンス モードにします（[グレースフル削除のトリガー（312 ページ）](#) を参照）
5. グレースフル挿入をトリガーして、スイッチを通常モードに戻します（[グレースフル挿入のトリガー（315 ページ）](#) を参照）
6. グレースフル挿入をトリガーした後のスナップショットを取得します（[スナップショットの作成（308 ページ）](#) を参照）
7. **show snapshots compare** コマンドを使用して、グレースフル削除と挿入の前後のスイッチの運用データを比較して、すべてが想定どおりに動作していることを確認します（[GIR 設定の確認（318 ページ）](#) を参照）

## メンテナンス モード プロファイルの設定

グレースフル削除またはグレースフル挿入時に適用できる設定コマンドを使用して、メンテナンス モード プロファイルを作成できます。

### 手順の概要

1. **configure maintenance profile maintenance-mode**
2. **end**
3. **show maintenance profile maintenance-mode**

### 手順の詳細

#### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure maintenance profile maintenance-mode</b> <b>例 :</b> <pre>switch# configure maintenance profile maintenance-mode Enter configuration commands, one per line. End with CNTL/Z. switch(config-mm-profile) #</pre>	メンテナンス モード プロファイルのコンフィギュレーション セッションを開始します。 設定しているプロトコルに応じて、プロトコルを停止する適切なコマンドを入力する必要があります。サポートされるコマンドの一覧については、 <a href="#">プロファイル（304 ページ）</a> を参照してください。
ステップ 2	<b>end</b> <b>例 :</b> <pre>switch(config-mm-profile) # end switch#</pre>	メンテナンス モード プロファイルを終了します。
ステップ 3	<b>show maintenance profile maintenance-mode</b> <b>例 :</b> <pre>switch# show maintenance profile maintenance-mode</pre>	メンテナンス モード プロファイルの詳細を表示します。

**例**

次に、メンテナンス モード プロファイルを作成する例を示します。

```
switch# configure maintenance profile maintenance-mode
Enter configuration commands, one per line. End with CNTL/Z.
switch(config-mm-profile)# ip pim isolate
switch(config-mm-profile)# vpc domain 10
switch(config-mm-profile-config-vpc-domain)# shutdown
switch(config-mm-profile)# router bgp 100
switch(config-mm-profile-router)# shutdown
switch(config-mm-profile-router)# router eigrp 10
switch(config-mm-profile-router)# shutdown
switch(config-mm-profile-router)# address-family ipv6 unicast
switch(config-mm-profile-router-af)# shutdown
switch(config-mm-profile)# system interface shutdown
switch(config-mm-profile)# end
Exit maintenance profile mode.
switch# show maintenance profile maintenance-mode
[Maintenance Mode]
ip pim isolate
vpc domain 10
    shutdown
router bgp 100
    shutdown
router eigrp 10
    shutdown
    address-family ipv6 unicast
        shutdown
    system interface shutdown
```

## 通常モード プロファイルの設定

グレースフル削除またはグレースフル挿入時に適用できる設定コマンドを使用して、通常モード プロファイルを作成できます。

### 手順の概要

1. **configure maintenance profile normal-mode**
2. **end**
3. **show maintenance profile normal-mode**

### 手順の詳細

#### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure maintenance profile normal-mode</b> 例： <b>例：</b>	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。

## スナップショットの作成

	コマンドまたはアクション	目的
	<pre>switch# configure maintenance profile normal-mode Enter configuration commands, one per line. End with CNTL/Z. switch(config-mm-profile) #</pre>	設定しているプロトコルに応じて、プロトコルを起動する適切なコマンドを入力する必要があります。サポートされるコマンドの一覧については、 <a href="#">プロファイル (304 ページ)</a> を参照してください。
ステップ 2	<b>end</b> 例： <pre>switch(config-mm-profile) # end switch#</pre>	通常モードプロファイルを終了します。
ステップ 3	<b>show maintenance profile normal-mode</b> 例： <pre>switch# show maintenance profile normal-mode</pre>	通常モードプロファイルの詳細を表示します。

## 例

次に、メンテナンスモードプロファイルを作成する例を示します。

```
switch# configure maintenance profile normal-mode
switch(config-mm-profile) # no system interface shutdown
switch(config-mm-profile) # router eigrp 10
switch(config-mm-profile-router) # no shutdown
switch(config-mm-profile-router) # address-family ipv6 unicast
switch(config-mm-profile-router-af) # no shutdown
switch(config-mm-profile) # router bgp 100
switch(config-mm-profile-router) # no shutdown
switch(config-mm-profile) # vpc domain 10
switch(config-mm-profile-config-vpc-domain) # no shutdown
switch(config-mm-profile) # no ip pim isolate
switch(config-mm-profile) # end
Exit maintenance profile mode.
switch# show maintenance profile normal-mode
[Normal Mode]
no system interface shutdown
router eigrp 10
  no shutdown
  address-family ipv6 unicast
    no shutdown
  router bgp 100
    no shutdown
  vpc domain 10
    no shutdown
  no ip pim isolate
```

## スナップショットの作成

選択した機能の実行状態のスナップショットを作成できます。スナップショットを作成すると、**show** コマンドの定義済みのセットが実行され、出力が保存されます。

## 手順の概要

1. **snapshot create snapshot-name description**
2. **show snapshots**
3. **show snapshots compare snapshot-name-1 snapshot-name-2 [summary | ipv4routes | ipv6routes]**

## 手順の詳細

## 手順

	コマンドまたはアクション	目的				
ステップ1	<b>snapshot create snapshot-name description</b> <b>例 :</b> <pre>switch# snapshot create snap_before_maintenance Taken before maintenance Executing 'show interface'... Done Executing 'show ip route summary vrf all'... Done Executing 'show ipv6 route summary vrf all'... Done Executing 'show bgp sessions vrf all'... Done Executing 'show ip eigrp topology summary'... Done Executing 'show ipv6 eigrp topology summary'... Done Feature 'vpc' not enabled, skipping... Executing 'show ip ospf vrf all'... Done Feature 'ospfv3' not enabled, skipping... Feature 'isis' not enabled, skipping... Feature 'rip' not enabled, skipping... Snapshot 'snap_before_maintenance' created</pre>	選択した機能の実行状態または運用データをキャプチャし、データを永続ストレージメディアに保存します。 最大 64 文字の英数字のスナップショット名と最大 254 文字の英数字の説明を入力できます。 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、 <b>snapshot delete {all   snapshot-name}</b> コマンドを使用します。				
ステップ2	<b>show snapshots</b> <b>例 :</b> <pre>switch# show snapshots Snapshot Name          Time Description </pre> <table border="1"> <tr> <td>snap_before_maintenance</td> <td>Wed Aug 19 13:53:28 2015</td> </tr> <tr> <td colspan="2">Taken before maintenance</td> </tr> </table>	snap_before_maintenance	Wed Aug 19 13:53:28 2015	Taken before maintenance		スイッチ上に存在するスナップショットを表示します。
snap_before_maintenance	Wed Aug 19 13:53:28 2015					
Taken before maintenance						
ステップ3	<b>show snapshots compare snapshot-name-1 snapshot-name-2 [summary   ipv4routes   ipv6routes]</b> <b>例 :</b> <pre>switch# show snapshots compare snap_before_maintenance snap_after_maintenance</pre>	2 つのスナップショットの比較を表示します。 値は、 <b>summary</b> 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。 値は、 <b>ipv4routes</b> および <b>ipv6routes</b> 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。				

## スナップショットへの **show** コマンドの追加

### 例

次に、2つのスナップショット間の変更の概要の例を示します。

```
switch# show snapshots compare snapshot1 snapshot2 summary
feature                                snapshot1      snapshot2      changed
basic summary
  # of interfaces                      16           12           *
  # of vlans                          10           4            *
  # of ipv4 routes                    33           3            *
  .....
interfaces
  # of eth interfaces                  3            0           *
  # of eth interfaces up              2            0           *
  # of eth interfaces down            1            0           *
  # of eth interfaces other           0            0           *
  .....
  # of vlan interfaces                 3            1           *
  # of vlan interfaces up              3            1           *
  # of vlan interfaces down            0            0           *
  # of vlan interfaces other           0            1           *
  .....
```

次に、2つのスナップショット間の IPv4 ルートの変更の例を示します。

```
switch# show snapshots compare snapshot1 snapshot2 ipv4routes
metric                                snapshot1      snapshot2      changed
# of routes                           33           3            *
# of adjacencies                      10           4            *
Prefix      Changed Attribute
-----
23.0.0.0/8    not in snapshot2
10.10.10.1/32  not in snapshot2
21.1.2.3/8    adjacency index has changed from 29 (snapshot1) to 38 (snapshot2)
.....
There were 28 attribute changes detected
```

## スナップショットへの **show** コマンドの追加

スナップショットでキャプチャされる追加の **show** コマンドを指定できます。それらの **show** コマンドは、ユーザー指定のスナップショットセクションで定義されます。

### 手順の概要

1. **snapshot section add section "show-command" row-id element-key1 [element-key2]**
2. **show snapshots sections**
3. **show snapshots compare snapshot-name-1 snapshot-name-2 [summary | ipv4routes | ipv6routes]**

## 手順の詳細

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>snapshot section add section "show-command" row-id element-key1 [element-key2]</b> <b>例 :</b> <pre>switch# snapshot section add myshow "show ip interface brief" ROW_intf intf-name</pre>	<p>ユーザ指定のセクションをスナップショットに追加します。セクションは、<b>show</b> コマンドの出力を名付けするために使用されます。任意の単語を使用して、セクションに名前を付けることができます。</p> <p><b>show</b> コマンドは、引用符で囲む必要があります。非<b>show</b> コマンドは、拒否されます。</p> <p><i>row-id</i>引数は、<b>show</b> コマンドの XML 出力の各行エントリのタグを指定します。<i>element-key1</i> および <i>element-key2</i>引数では、行エントリ間を区別するために使用されるタグを指定します。ほとんどの場合、<i>element-key1</i>引数のみ、行エントリ間を区別するために指定する必要があります。</p> <p>(注) スナップショットからユーザー指定のセクションを削除するには、<b>snapshot section delete section</b> コマンドを使用します。</p>
ステップ 2	<b>show snapshots sections</b> <b>例 :</b> <pre>switch# show snapshots sections</pre>	ユーザー指定のスナップショットセクションを表示します。
ステップ 3	<b>show snapshots compare snapshot-name-1 snapshot-name-2 [summary   ipv4routes   ipv6routes]</b> <b>例 :</b> <pre>switch# show snapshots compare snap1 snap2</pre>	<p>2つのスナップショットの比較を表示します。</p> <p><b>summary</b> オプションは、2つのスナップショット間の全体的な変更を確認するのに十分な情報のみ表示します。</p> <p><b>ipv4routes</b> および <b>ipv6routes</b> オプションは、2つのスナップショット間の IPv4 および IPv6 ルートの変更を表示します。</p>

## 例

次の例では、**show ip interface brief** コマンドを myshow スナップショットセクションに追加します。この例では、2つのスナップショット (snap1 および snap2) が比較され、両方のスナップショットにユーザ指定のセクションが表示されます。

```
switch# snapshot section add myshow "show ip interface brief" ROW_intf intf-name
switch# show snapshots sections
user-specified snapshot sections
```

## グレースフル削除のトリガー

```
-----
[myshow]
  cmd:  show ip interface brief
  row:  ROW_intf
  key1: intf-name
  key2: -

[sect2]
  cmd:  show ip ospf vrf all
  row:  ROW_ctx
  key1: instance_number
  key2: cname

switch# show snapshots compare snap1 snap2
=====
Feature           Tag           snap1           snap2
=====
[bgp]
-----
.....
[interface]
-----
[interface:mgmt0]
  vdc_lvl_in_pkts      692310          **692317**
  vdc_lvl_in_mcast     575281          **575287**
  vdc_lvl_in_bcast     77209           **77210**
  vdc_lvl_in_bytes     63293252        **63293714**
  vdc_lvl_out_pkts     41197            **41198**
  vdc_lvl_out_ucast    33966            **33967**
  vdc_lvl_out_bytes    6419714         **6419788**
.....
[ospf]
-----
.....
[myshow]
-----
[interface:Ethernet1/1]
  state            up          **down**
  admin_state      up          **down**
.....
```

## グレースフル削除のトリガー

デバッグ操作やアップグレード操作を実行するために、スイッチのグレースフル削除をトリガーして、スイッチを取り出し、ネットワークからそのスイッチを分離できます。

### 始める前に

作成したメンテナンスモードプロファイルを使用するシステムの場合は、[メンテナンスモードプロファイルの設定（306 ページ）](#)を参照してください。

## 手順の概要

1. **configure terminal**
2. **system mode maintenance [dont-generate-profile | timeout value | shutdown | on-reload reset-reason reason]**
3. (任意) **show system mode**
4. (任意) **copy running-config startup-config**

## 手順の詳細

## 手順

	コマンドまたはアクション	目的
ステップ1	<b>configure terminal</b> 例： <pre>switch# configure terminal switch(config)#</pre>	グローバル コンフィギュレーション モードを開始します。
ステップ2	<b>system mode maintenance [dont-generate-profile   timeout value   shutdown   on-reload reset-reason reason]</b> 例： <pre>switch(config)# system mode maintenance Following configuration will be applied:    ip pim isolate   router bgp 65502     isolate   router ospf p1     isolate   router ospfv3 p1     isolate  Do you want to continue (y/n)? [no] y Generating a snapshot before going into maintenance mode  Starting to apply commands...  Applying : ip pim isolate Applying : router bgp 65502 Applying :   isolate Applying : router ospf p1 Applying :   isolate Applying : router ospfv3 p1 Applying :   isolate  Maintenance mode operation successful.</pre>	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 ( <b>isolate</b> コマンドを使用します)。 次のオプションを使用できます。 <ul style="list-style-type: none"> <li>• <b>dont-generate-profile</b>—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 プロファイルに構成されているコマンドが実行されます。作成したメンテナンス モード プロファイルをシステムに使用させる場合は、このオプションを使用します。</li> <li>• <b>timeout value</b>—指定した分数の間、スイッチをメンテナンス モードのままにします。範囲は 5 ~ 65535 です。設定した時間が経過すると、スイッチは自動的に通常モードに戻ります。値は、<b>no system mode maintenance timeout</b> コマンドは、タイマーを無効にします。</li> <li>• <b>shutdown</b>—すべてのプロトコル、vPC ドメインおよび管理インターフェイスを除くインターフェイスをシャットダウンします ( <b>shutdown</b> コマンドを使用します)。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 ( <b>isolate</b> コマンドを使用します) の場合、中断は発生しません。</li> <li>• <b>on-reload reset-reason reason</b>—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</li> </ul>

## ■ グレースフル削除のトリガー

	コマンドまたはアクション	目的
		<p>を自動的にメンテナンスモードで起動します。値は、<b>no system mode maintenance on-reload reset-reason</b> コマンドを使用すると、システムクラッシュ時にスイッチがメンテナンスモードで起動するのを回避できます。</p> <p>メンテナンスモードのリセット理由は次のとおりです。</p> <ul style="list-style-type: none"> <li>• HW_ERROR : ハードウェア エラー</li> <li>• SVC_FAILURE : 重大なサービス障害</li> <li>• KERN_FAILURE : カーネルパニック</li> <li>• WDOG_TIMEOUT : ウオッチ ドッギング タイム アウト</li> <li>• FATAL_ERROR : 致命的なエラー</li> <li>• LC_FAILURE : ライン カード障害</li> <li>• MATCH_ANY : 上記のいずれかの理由</li> </ul> <p>続行を促すプロンプトが表示されます。Enter <b>y</b> を入力または、プロセスを終了するために <b>n</b> を入力します。</p>
ステップ3	(任意) <b>show system mode</b>  例： <pre>switch(config) # show system mode System Mode: Maintenance</pre>	現在のシステム モードを表示します。  スイッチはメンテナンスモードになっています。スイッチに対する目的のデバッグ操作やアップグレード操作を実行できます。
ステップ4	(任意) <b>copy running-config startup-config</b>  例： <pre>switch(config) # copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。このコマンドは、再起動後にメンテナンスモードを維持する場合に必要です。

## 例

次に、スイッチのすべてのプロトコル、vPC ドメイン、およびインターフェイスをシャットダウンする例を示します。

```
switch(config) # system mode maintenance shutdown
```

Following configuration will be applied:

```
vpc domain 10
shutdown
```

```
router bgp 65502
  shutdown
router ospf p1
  shutdown
router ospfv3 p1
  shutdown
system interface shutdown

Do you want to continue (y/n)? [no] y

Generating a snapshot before going into maintenance mode

Starting to apply commands...

Applying : vpc domain 10
Applying : shutdown
Applying : router bgp 65502
Applying : shutdown
Applying : router ospf p1
Applying : shutdown
Applying : router ospfv3 p1
Applying : shutdown

Maintenance mode operation successful.
```

次に、致命的なエラーが発生した場合に、スイッチを自動的にメンテナンスモードで起動する例を示します。

```
switch(config)# system mode maintenance on-reload reset-reason fatal_error
```

## グレースフル挿入のトリガー

デバッグ操作やアップグレード操作の実行が終了したら、グレースフル挿入をトリガーして、すべてのプロトコルを復元できます。

### 始める前に

作成する通常モードプロファイルをシステムに使用させる場合は、[メンテナンスモードプロファイルの設定（306 ページ）](#) を参照してください。

### 手順の概要

1. **configure terminal**
2. **no system mode maintenance [dont-generate-profile]**
3. (任意) **show system mode**

## メンテナンス モードの強化

## 手順の詳細

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b>  例： <pre>switch# configure terminal switch(config) #</pre>	グローバル設定モードを開始します。
ステップ 2	<b>no system mode maintenance [dont-generate-profile]</b>  例： <pre>switch(config) # no system mode maintenance dont-generate-profile Following configuration will be applied:    no ip pim isolate   router bgp 65502     no isolate   router ospf p1     no isolate   router ospfv3 p1     no isolate  Do you want to continue (y/n)? [no] y Starting to apply commands...  Applying : no ip pim isolate Applying : router bgp 65502 Applying :   no isolate Applying :   router ospf p1 Applying :   no isolate Applying :   router ospfv3 p1 Applying :   no isolate  Maintenance mode operation successful.  Generating Current Snapshot</pre>	すべての有効なプロトコルを通常モードにします（ <b>no isolate</b> コマンドを使用します）。 値は、 <b>dont-generate-profile</b> オプションを指定すると、有効なプロトコルの動的な検索が回避され、通常モードプロファイルに構成されているコマンドが実行されます。作成した通常モードプロファイルをシステムに使用させる場合は、このオプションを使用します。 続行を促すプロンプトが表示されます。 <b>y</b> を入力して続行するか、 <b>n</b> を入力してプロセスを終了します。
ステップ 3	(任意) <b>show system mode</b>  例： <pre>switch(config) # show system mode System Mode: Normal</pre>	現在のシステムモードを表示します。スイッチは通常モードになっていて、完全に機能しています。

## メンテナンス モードの強化

次のメンテナンス モードの機能拡張が Cisco Nexus 3600 プラットフォーム スイッチに追加されます。

- システム メンテナンス シャットダウン モードで次のメッセージが追加されます。

NOTE: The command `system interface shutdown` will shutdown all interfaces excluding `mgmt 0`.

- CLI コマンドを入力すると、**system mode maintenance** によって孤立ポートがチェックされ、アラートが送信されます。

- 隔離モードで vPC が設定されると、次のメッセージが追加されます。

NOTE: If you have vPC orphan interfaces, please ensure `vpc orphan-port suspend` is configured under them, before proceeding further.

- カスタムプロファイル構成: 新しい CLI コマンド、**system mode maintenance always-use-custom-profile** がカスタムプロファイル構成用に追加されました。新しい CLI コマンド **system mode maintenance non-interactive** は、Cisco Nexus 9000 シリーズスイッチのみに `#ifdef` の下に追加されました。

(メンテナンスまたは通常モードで) カスタムプロファイルを作成すると、次のメッセージが表示されます。

`Please use the command system mode maintenance always-use-custom-profile if you want to always use the custom profile.`

- `after_maintenance` スナップショットが撮られる前に遅延が追加されました。**no system mode maintenance** コマンドは、通常モードのすべての構成が適用され、モードが通常モードに変更され、`after_maintenance` スナップショットを取得するためのタイマーが開始されると終了します。タイマーの期限が切れると、`after_maintenance` スナップショットがバックグラウンドで取得され、スナップショットが完了すると新しい警告 Syslog、`MODE_SNAPSHOT_DONE` が送信されます。

CLI コマンドの最終出力 **no system mode maintenance** は、`after_maintenance` スナップショットがいつ生成されたかを示します:

`after_maintenance` スナップショットは、`<delay>` 秒で生成されます。その後は、`show snapshots compare before_maintenance after_maintenance` を使用してシステムの正常性を確認してください。`after_maintenance` スナップショットのタイマー遅延はデフォルトで 120 秒に設定されていますが、新しい構成コマンドで変更できます。

`after_maintenance snapshot` のタイマー遅延を変更するための新しい構成コマンドは、**system mode maintenance snapshot-delay <seconds>** です。この設定は、デフォルト設定の 120 秒を 0 ~ 65535 の任意の値に上書きします。これは ASCII 設定で表示されます。

新しい `show` コマンド **show maintenance snapshot-delay** は、`current snapshot-delay` の値を表示するために追加されています。この新しい `show` コマンドでは、XML 出力がサポートされています。

- システムがメンテナンス モードであるときに表示される CLI インジケータが追加されました。たとえば、`switch (m-mode) #` です。
- CLI リロードまたはシステムリセットによってデバイスがメンテナンス モードから通常モードおよびその逆に移行するときの SNMP トランプのサポートが追加されました。  
**snmp-server enable traps mmode cseMaintModeChangeNotify** トランプは、メンテナンス モードのトランプ通知の変更を有効にするために追加されました。**snmp-server enable**

**traps mmode cseNormalModeChangeNotify** は、通常モードへのトラップ通知の変更を有効にするために追加されました。デフォルトでは両方のトラップが無効になっています。

## GIR 設定の確認

GIR の設定を表示するには、次のいずれかの作業を行います。

コマンド	目的
<b>show interface brief</b>	インターフェイスの要約情報を表示します。
<b>show maintenance on-reload reset-reasons</b>	スイッチがメンテナンスモードで起動されることになる、リセット理由を表示します。メンテナンスモードのリセット理由の説明については、 <a href="#">グレースフル削除のトリガー (312 ページ)</a> を参照してください。
<b>show maintenance profile [maintenance-mode   normal-mode]</b>	メンテナンスモードまたは通常モードのプロファイルの詳細を表示します。
<b>show maintenance timeout</b>	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。
<b>show {running-config   startup-config} mmode [all]</b>	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。 <b>all</b> オプションには、デフォルト値が含まれます。
<b>show snapshots</b>	スイッチ上に存在するスナップショットを表示します。
<b>show snapshots compare snapshot-name-1 snapshot-name-2 [summary   ipv4routes   ipv6routes]</b>	2つのスナップショットの比較を表示します。 <b>summary</b> 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。 <b>ipv4routes</b> および <b>ipv6routes</b> 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。
<b>show snapshots dump snapshot-name</b>	スナップショットの取得時に生成された各ファイルの内容を表示します。

コマンド	目的
<b>show snapshots sections</b>	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。
<b>show system mode</b>	現在のシステムモードを表示します。





## 第 22 章

# コンフィギュレーションの置換の実行

この章は、次の項で構成されています。

- コンフィギュレーションの置換とコミットタイムアウトについて (321 ページ)
- 概要 (322 ページ)
- コンフィギュレーションの置換に関する注意事項と制限事項 (324 ページ)
- 構成の置換の推奨ワークフロー (327 ページ)
- コンフィギュレーションの置換の実行 (328 ページ)
- コンフィギュレーションの置換の確認 (331 ページ)
- 構成の置換の例 (331 ページ)

## コンフィギュレーションの置換とコミットタイムアウトについて

コンフィギュレーションの置換機能を使用すると、デバイスをリロードすることなく Cisco Nexus スイッチの実行コンフィギュレーションをユーザ指定のコンフィギュレーションに置換できます。コンフィギュレーション自体でリロードが必要な場合にのみ、デバイスのリロードが必要になることがあります。ユーザが提供する実行コンフィギュレーションファイルは、実行ファイルのコピーを使用して取得する必要があります。競合他社 **copy file: to running** と異なり、構成の置換機能はマージ操作ではありません。この機能では、実行コンフィギュレーション全体が、ユーザによって提供される新しいコンフィギュレーションに置換されます。コンフィギュレーションの置換に障害がある場合は、元のコンフィギュレーションがスイッチで復元されます。Cisco NX-OS リリース 9.3 (1) から、**best-effort** オプションが導入されました。このオプションを使用すると、コマンドでエラーが発生した場合でも、設定の置換によって完全なパッチが実行され、元の設定はスイッチに復元されません。

コミットタイムアウト機能を使用すると、コンフィギュレーションの置換操作の実行に成功した後に以前のコンフィギュレーションにロールバックすることができます。コミットタイマーの期限が切れると、ロールバック操作は自動的に開始されます。



(注)

- Cisco NX-OS デバイスで受信済みの有効な実行コンフィギュレーションを提供する必要があります。部分コンフィギュレーションにすることはできません。

## 概要

設定置換機能には、次の操作手順があります。

- コンフィギュレーションの置換では、Cisco Nexus スイッチの現在の実行コンフィギュレーションとユーザ指定のコンフィギュレーションとの間の違いをインテリジェントに計算し、2ファイルの差異のパッチファイルを生成します。コンフィギュレーションコマンドのセットが含まれているこのパッチファイルは表示できます。
- コンフィギュレーションの置換では、実行中のコマンドと同様にパッチファイルのコンフィギュレーションコマンドが適用されます。
- コンフィギュレーションは、次の状況下で以前の実行コンフィギュレーションにロールバックまたは復元されます。
  - パッチファイルが適用された後、コンフィギュレーションに不一致がある場合。
  - コミットタイムアウトを使用してコンフィギュレーション操作を実行し、コミットタイマーが期限切れになった場合。
- ベストエフォートオプションが使用されている場合、設定は以前の実行コンフィギュレーションにロールバックされず、復元もされません。このオプションを使用すると、コマンドでエラーが発生した場合でも、設定の置換によって完全なパッチが実行され、以前の設定にロールバックされません。
- show config-replace log exec** コマンドの交換ファイルとして、完全な Cisco NX-OS 構成ファイルを使用できます。
- スイッチを元のコンフィギュレーションに復元するときにエラーが発生しても復元操作は中断されません。復元操作は、残りのコンフィギュレーションを続行します。復元操作中に障害が発生したコマンドを一覧表示するには、**show config-replace log exec** コマンドを使用します。
- タイマーの期限が切れる前に **configure replace commit** コマンドを入力した場合、コミットタイマーは停止し、コンフィギュレーションの置換機能によって適用されているユーザ指定のコンフィギュレーションでスイッチが稼働します。
- コミットタイマーの期限が切れると、以前のコンフィギュレーションへのロールバックは自動的に開始されます。
- Cisco NX-OS リリース 9.3(1) では、セマンティック検証のサポートが設定の置換に追加されました。このセマンティック検証は、設定置換の事前チェックの一部として実行されます。パッチは、セマンティック検証が成功した場合にのみ適用されます。パッチファイル

を適用すると、コンフィギュレーションの置換によって検証プロセスがトリガーされます。コンフィギュレーションの置換は、検証プロセスで、実行コンフィギュレーションとユーザー構成ファイルを比較します。不一致がある場合、デバイスは元のコンフィギュレーションに復元されます。

コンフィギュレーションの置換と実行コンフィギュレーションへのファイルのコピーとの違いは、次のとおりです。

コンフィギュレーションの置換	ファイルのコピー
<b>configure replace &lt;target-url&gt;</b> コマンドは、現在の実行構成にのみ含まれ、置換ファイルには存在しないコマンドは削除します。また、現在の実行コンフィギュレーションに追加する必要があるコマンドも追加されます。	<b>copy &lt;source-url&gt; running-config</b> コマンドはマージ動作であり、ソース ファイルと現在の実行中の構成の両方のコマンドがすべて保持されます。このコマンドでは、現在の実行コンフィギュレーションにのみ含まれ、ソース ファイルには存在しないコマンドが削除されることはありません。
<b>configure replace &lt;target-url&gt;</b> コマンドの交換ファイルとして、完全な Cisco NX-OS 構成ファイルを使用できます。	<b>copy &lt;source-url&gt; running-config</b> コマンドのコピー元ファイルとして、構成ファイルの一部を使用できます。

## コンフィギュレーションの置換の利点

コンフィギュレーションの置換の利点は次のとおりです。

- スイッチをリロードしたり、CLIで実行コンフィギュレーションファイルに加えた変更を手動で元に戻したりすることなく、現在の実行コンフィギュレーションファイルをユーザ指定のコンフィギュレーションファイルと置換できます。その結果、システムのダウンタイムが減少します。
- 保存済みの Cisco NX-OS コンフィギュレーションの状態に戻すことができます。
- 追加や削除が必要なコマンドだけが影響を受ける場合、デバイスに完全なコンフィギュレーションファイルを適用することができるため、コンフィギュレーションの変更が簡素化されます。その他のサービスおよび変更されていないコンフィギュレーションには影響しません。
- コミットタイムアウト機能を設定すると、コンフィギュレーションの置換操作が成功したときでも以前のコンフィギュレーションにロールバックすることができます。

# コンフィギュレーションの置換に関する注意事項と制限事項

コンフィギュレーションの置換機能には、コンフィギュレーションに関する次のガイドラインと制限事項があります。

- 設定置換機能は、Cisco Nexus 3000 シリーズおよび Cisco Nexus 9000 シリーズスイッチでサポートされています。
- コンフィギュレーションの置換、チェックポイント、ロールバック操作、または実行コンフィギュレーションからスタートアップコンフィギュレーションへのコピーを同時に実行できるのは、1 ユーザだけです。複数の Telnet、SSH または NX-API セッション経由の操作などのパラレル操作はサポートされていません。複数のコンフィギュレーションの置換またはロールバック要求はシリアル化され、たとえば、最初の要求の完了後にのみ、2 番目の要求の処理が開始されます。
- コミットタイマーの実行中に別のコンフィギュレーションの置換操作を開始することはできません。タイマーを停止するために **configure replace commit** コマンドを使用する、またはコミットタイマーの期限が切れるまで待機してから別の構成の置換操作を開始する必要があります。
- **system default switchport shutdown** または **no system default switchport shutdown** が **configure replace bootflash:target\_config\_file** コマンドとともに使用する場合、ユーザーは、すべてのスイッチポートインターフェイスの **target\_config\_file** に目的のポートステート (shutdown または no shutdown) ステートメントが存在することを確認する必要があります。
- コンフィギュレーションの置換操作を正常に行うには、ターゲットコンフィギュレーションファイルの ACL のすべての ACE エントリにシーケンス番号が存在する必要があります。
- コミットタイムアウト機能は、コミットタイムアウトを使用してコンフィギュレーションの置換操作を実行する場合にのみ開始されます。タイマーの値の範囲は 30 ~ 3600 秒です。
- ユーザ指定のコンフィギュレーションファイルは、Cisco NX-OS デバイスから取得 (copy run file) された有効な **show running-configuration** の出力である必要があります。このコンフィギュレーションは部分コンフィギュレーションにすることはできず、user admin などの必須コマンドが含まれている必要があります。
- ソフトウェアバージョン違いで生成されたコンフィギュレーションファイルでコンフィギュレーションの置換操作を実行することは、操作が失敗する可能性があるため推奨されません。ソフトウェアバージョンの変更があるたびに新しいコンフィギュレーションファイルを再生成する必要があります。
- コンフィギュレーションの置換操作が進行中の場合、他のセッションからはコンフィギュレーションを変更しないことを推奨します。操作が失敗する可能性があります。

- コンフィギュレーションの置換機能については、次の点に注意してください。
  - コンフィギュレーションの置換機能は、リロードを必要とする機能をサポートしていません。このような機能の1例は、`system vlan reserve` です。
  - R ライン カード搭載の Cisco Nexus 9500 プラットフォームスイッチでは、コンフィギュレーションの置換機能はサポートされません。
  - 構成の置換機能は、実行中の構成に、**feature-set mpls** または **mpls static range** コマンドが含まれて、MPLS なしで構成に移動しようとしたか、ラベルの範囲を変更する場合、失敗する場合があります。
  - コンフィギュレーションの置換機能は、自動設定をサポートしていません。
- コンフィギュレーションの置換機能が適用されるラインカードがオフラインである場合、コンフィギュレーションの置換操作は失敗します。
- 構成置換機能を使用して ITD を変更する前に、ITD サービスをシャットダウンする必要があります (**shutdown**)。
- シーケンス番号は、CLI **ip community-list** および **ip as-path access-list** コマンドに必須です。シーケンス番号を指定しないと、構成の置換操作は失敗します。
- コンフィギュレーションを適用するために Cisco NX-OS デバイスをリロードする必要がある場合、これらのコンフィギュレーションをリロードしてからコンフィギュレーションの置換操作を行う必要があります。
- ユーザ指定のコンフィギュレーションファイルでのコマンドの順序は、Cisco Nexus スイッチの実行コンフィギュレーションでのこれらのコマンドと同じにする必要があります。
- CR を使用してスイッチの実行コンフィギュレーションを置き換える必要があるユーザコンフィギュレーションファイルは、新しいコマンドを設定した後、スイッチの実行コンフィギュレーションから生成する必要があります。ユーザコンフィギュレーションファイルは、CLI コマンドを使用して手動で編集しないでください。また、コンフィギュレーションコマンドのシーケンスを変更しないでください。
- セマンティック検証は、4 ギガビットメモリプラットフォームではサポートされていません。
- 異なるバージョンの機能が実行コンフィギュレーションとユーザコンフィギュレーションに存在する場合 (VRRPv2 と VRRPv3 など)、セマンティック検証オプションが期待どおりに機能しません。この問題は既知の制限です。
- Cisco NX-OS リリース 10.3(1)F 以降、構成の置換機能は機能アプリホスティングをサポートしません。
- Cisco NX-OS リリース 10.4(2)F 以降では、Cisco NX-OS デバイスの LDAP で構成の置換機能がサポートされています。

## ■ コンフィギュレーションの置換に関する注意事項と制限事項

- Cisco NX-OS リリース 10.4(2)F 以降では、大文字と小文字を区別しないコマンドで、実行構成ファイルと候補の構成ファイルのコマンド間に大文字と小文字の違いがある場合、**config replace show-patch** の出力には両方のコマンドが表示されます。
- Cisco NX-OS リリース 10.4(3)F 以降では、候補構成でポリモーフィック コマンドを使用して、構成の置換を実行することもできます。
- ユーザー データベースが SNMP と AAA (セキュリティ) の間で同期されるため、構成の置き換え用の **candidate-config** ファイルでは、クリア テキストのパスワードを使用できません。
- candidate-config** ファイルで、次のコマンドの必須シーケンス番号を必ず指定してください。シーケンス番号を指定しないと、構成の置換操作は失敗します。
  - ip prefix-list list-name seq seq {deny | permit} prefix**
  - ipv6 prefix-list list-name seq seq {deny | permit} prefix**
  - mac-list list-name seq seq {deny | permit} prefix**
  - ip community-list { standard | expanded} list-name seq seq {deny | permit} expression**
  - ip extcommunity-list {standard | expanded} list-name seq seq {deny | permit} expression**
  - ip large-community-list {standard | expanded} list-name seq seq {deny | permit} expression**
  - ip-as-path access-list list-name seq seq {deny | permit} expression**
- Cisco NX-OS リリース 10.5(1)F 以降では、次を同じ CR 候補ファイルの一部にすることはできません。
  - no hardware access-list update atomic**
  - 既存の実行構成 アトミック TCAM 構成の制限を超える ACL 構成
- Cisco NX-OS リリース 10.5(1)F 以降では、**vlan access-map** コマンドのシーケンス番号は必須です。シーケンス番号を指定しないと、構成の置換操作は失敗します。
- あるデバイスから生成された、別のデバイスに適用された構成のリプレイが実行され、CLI CR は成功しても、新しいデバイスでの SNMPv3 操作は失敗し、**認証の失敗** というメッセージが表示されます。

## PBR コマンドの構成の置換に関する注意事項と制限事項

このセクションの内容は、Cisco NX-OS リリース 10.4(3)F から適用されます。

PBR コマンドは、同じ親ルートマップの下に共存できません。相互に排他的な PBR コマンドが候補構成の同じルートマップで指定されている場合、**config-replace** パッチはルートマップの下の最後のコマンドバリエントに対してのみ生成され、CR 操作後に適用されます。

次の表に、いくつかの使用例を示します。

使用例	候補構成	変換後の候補構成
<p><b>ユース ケース 1:</b> 複数のコマンドバリアント: 最後のコマンドバリアントのみが保持されます。</p> <p>候補構成は、CRパッチが生成される前に、3番目の列に示すように自動的に変換されます。</p>	<pre>route-map rmap1 permit 10 set ip next-hop 1.1.1.1 2.2.2.2 set ipv6 next-hop 3::3 set ip next-hop verify-availability 4.4.4.4 set ip next-hop verify-availability 5.5.5.5 set ip vrf green next-hop 6.6.6.6 set ip vrf blue next-hop 7.7.7.7 8.8.8.8</pre>	<pre>route-map rmap1 permit 10 set ip vrf green next-hop 6.6.6.6 set ip vrf blue next-hop 7.7.7.7 8.8.8.8</pre>
<p><b>使用例 2:</b> トランク ID を構成するコマンド: ネクストホップが同じでトランク ID が異なる最後のコマンドバリアントのみが保持されます。</p> <p>verify-availability コマンドの場合、同じネクストホップのトランク ID を変更することはできません。候補構成は、CRパッチが生成される前に、3番目の列に示すように自動的に変換されます。</p>	<pre>route-map test permit 10 set ip next-hop verify-availability 1.1.1.1 track 1 set ip next-hop verify-availability 2.2.2.2 track 20 set ip next-hop verify-availability 2.2.2.2 track 30 set ip next-hop verify-availability 2.2.2.2 track 40 set ip next-hop verify-availability 3.3.3.3 track 3</pre>	<pre>route-map test permit 10 set ip next-hop verify-availability 1.1.1.1 track 1 set ip next-hop verify-availability 2.2.2.2 track 40 set ip next-hop verify-availability 3.3.3.3 track 3</pre>

## 構成の置換の推奨ワークフロー

構成の置換の推奨されるワークフローを次に示します。



(注)

- このワークフローは、候補構成でも同じである必要があります。
- 候補構成のデフォルト構成はサポートされていません。

- Cisco Nexus シリーズ デバイスで最初に構成を適用して構成ファイルを生成してから、構成ファイルとして **show running-configuration** 出力を使用します。このファイルを使用して、必要に応じて構成を変更します。次に、この生成または更新された構成ファイルを使用して、構成の置換を実行します。
- 次のコマンドを実行してパッチ ファイルを表示し、確認します。 **configure replace <file> show-patch** コマンドを使用します。この手順は任意です。
- commit-timeout <time>** 機能を使用またはスキップして構成置換ファイルを実行します。要件に基づいて、次の手順のいずれかを実行できます。

## ■ コンフィギュレーションの置換の実行

- **configure replace <file> verbose** を実行して、構成の置換で実行されるコマンドをコンソールに表示します。
  - 次のスーパーユーザー権限で、**configure replace [bootflash/scp/sftp] <user-configuration-file> verbose commit-timeout <time>** コマンドを使用してコミット時間を構成します。
4. 次のスーパーユーザー権限で、**configure replace commit** コマンドを実行し、コミットタイマーを停止します。この手順は、コミットタイムアウト機能で構成の置換操作を実行している場合に必要です。
  5. 構成のセマンティック検証を含むプレチェックを構成の置換で実行します。エラーがある場合、構成の置換操作は失敗します。不一致の構成を表示するには、**show config-replace log verify** コマンドを使用します。パッチファイルを適用すると、構成の置換によって検証プロセスがトリガーされます。構成の置換は、検証プロセスで、実行構成とユーザー構成ファイルを比較します。不一致がある場合、デバイスは元の構成に復元されます。不一致の構成を表示するには、**show config-replace log verify** コマンドを使用します。
  6. Cisco NX-OS リリース9.3 (1) では、次の構成の置換操作を実行できます。
    - セマンティック検証およびベストエフォート モードなしの構成の置換。
    - セマンティック検証なし、ベストエフォート モードありの構成の置換。
    - セマンティック検証あり、ベストエフォート モードなしの構成の置換。
    - セマンティック検証およびベストエフォート モードありの構成の置換。

## コンフィギュレーションの置換の実行

コンフィギュレーションの置換を実行するには、次の操作を行います。

### 始める前に

現在の構成ファイルと候補構成ファイルの IP アドレスに競合がないことを確認します。IP アドレスの競合の例は、現在の構成ファイルの eth インターフェイス 1/53 で 172.16.0.1/24 を構成し、候補構成ファイル内の eth 1/53 で 172.16.0.1/24 と 192.168.0.1/24 を使用してポートチャネル 30 を構成したとします。候補構成ファイルの構成置換を実行すると、IP アドレスの競合が発生します。

### 手順の概要

1. **configure replace {<uri\_local>|<uri\_remote>} [ verbose | show-patch ]**
2. **configure replace [ bootflash / scp / sftp ]<user-configuration-file> show-patch**
3. **configure replace [ bootflash / scp / sftp ]<user-configuration-file> verbose**
4. **configure replace <user-configuration-file> [best-effort]**
5. **configure replace <user-configuration-file> [verify-and-commit]**

6. **configure replace <user-configuration-file> [verify-only]**
7. (任意) **configure replace [ bootflash / scp / sftp ]<user-configuration-file> verbose**  
**commit-timeout <time>**
8. (任意) **configure replace [ commit ]**
9. (任意) **configure replace [ bootflash/scp/sftp] <user-configuration-file> non-interactive**

## 手順の詳細

## 手順

	コマンドまたはアクション	目的
ステップ1	<b>configure replace { &lt;uri_local&gt;   &lt;uri_remote&gt; } [ verbose   show-patch ]</b>	コンフィギュレーションの置換を実行します。コンフィギュレーションの置換の進行中にセッションを通じてコンフィギュレーションを変更すると、コンフィギュレーションの置換操作は失敗します。1つのコンフィギュレーション要求がすでに進行中であるときにコンフィギュレーションの置換要求を送信すると、要求はシリアル化されます。
ステップ2	<b>configure replace [ bootflash / scp / sftp ]&lt;user-configuration-file&gt; show-patch</b>	実行コンフィギュレーションとユーザ指定のコンフィギュレーションの違いを表示します。 (注) <ul style="list-style-type: none"> <li>• このコマンドでは、プレーンテキストパスワードは暗号化されません。</li> <li>• このコマンドは、CLI snmp-server traps コマンドの構成置換が成功した後でも、パッチを表示できます。</li> </ul>
ステップ3	<b>configure replace [ bootflash / scp / sftp ]&lt;user-configuration-file&gt; verbose</b>	スイッチのコンフィギュレーションを、ユーザが提供する新しいユーザコンフィギュレーションに置換します。コンフィギュレーションの置換は常にアトミックです。
ステップ4	<b>configure replace &lt;user-configuration-file&gt; [best-effort]</b>	スイッチの設定を新しいユーザ設定に置き換え、セマンティック検証による設定の置き換えを有効にします。 best-effort オプションを使用すると、コマンドでエラーが発生した場合でも設定の置換によって完全なパッチが実行され、以前の設定がロールバックされないようになります。 Cisco NX-OS リリース 10.5(1)F 以降、コンフィギュレーション置換機能は、Cisco Nexus

## コンフィギュレーションの置換の実行

	コマンドまたはアクション	目的
		9300-FX2/FX3/GX シリーズ スイッチのバッチ ACL コンフィギュレーションをサポートします。[システム名 (System Name) ] が空白の場合は、 <b>ベストエフォート</b> モードが有効になっている場合、バッチ構成内で障害が発生すると、その特定のバッチ内の構成セット全体がスキップされます。
ステップ 5	<b>configure replace &lt;user-configuration-file&gt; [verify-and-commit]</b>	<p>スイッチの設定を新しいユーザ設定に置き換え、セマンティック検証による設定の置き換えを有効にします。</p> <p>verify-and-commit オプションは、セマンティック検証を有効にするために使用されます。バッチは、完全なバッチのセマンティック検証に合格した場合にのみ実行されます。</p> <p>ベストエフォート オプション、verify-and-commit オプション、または両方のオプションを同時に使用できます。</p>
ステップ 6	<b>configure replace &lt;user-configuration-file&gt; [verify-only]</b>	バッチのみを表示し、バッチでセマンティック検証を実行し、結果を表示します。バッチはシステムに適用されません。
ステップ 7	(任意) <b>configure replace [ bootflash / scp / sftp ] &lt;user-configuration-file&gt; verbose commit-timeout &lt;time&gt;</b>	コミット時間を秒単位で設定します。タイマーは、コンフィギュレーションの置換操作が正常に完了した後に開始されます。
ステップ 8	(任意) <b>configure replace [ commit ]</b>	<p>コミットタイマーを停止し、コンフィギュレーションの置換設定を続行します。</p> <p>(注) この手順は、コミットタイムアウト機能を設定している場合にのみ適用されます。</p> <p>(注) 以前のコンフィギュレーションにロールバックするには、コミットタイマーの期限が切れるまで待機する必要があります。タイマーの期限が切れるると、スイッチは自動的に以前のコンフィギュレーションにロールバックされます。</p>
ステップ 9	(任意) <b>configure replace [ bootflash/scp/sftp] &lt;user-configuration-file&gt; non-interactive</b>	メンテナンス モードでは、ユーザプロンプトはありません。デフォルトでは、 <b>yes</b> のユーザー確認を受けてからロールバックが進行します。非インタラクティブ オプションは、メンテナンス モードでのみ使用できます。

# コンフィギュレーションの置換の確認

コンフィギュレーションの置換とそのステータスをチェックして確認するには、表に記載されているコマンドを使用します。

表 29:コンフィギュレーションの置換の確認

コマンド	目的
<b>configure replace</b> [bootflash/scp/sftp]<user-configuration-file> <b>show-patch</b>	実行コンフィギュレーションとユーザ指定のコンフィギュレーションの違いを表示します。
<b>show config-replace log exec</b>	実行したすべてのコンフィギュレーションと失敗したコンフィギュレーションのログを表示します。エラーの場合、そのコンフィギュレーションに対してエラー メッセージが表示されます。
<b>show config-replace log verify</b>	失敗したコンフィギュレーションをエラーメッセージとともに表示します。成功したコンフィギュレーションは表示されません。
<b>show config-replace status</b>	コンフィギュレーションの置換操作のステータス（進行中、成功、失敗など）を表示します。コミットタイムアウト機能を設定している場合、コミットとタイマーのステータスに加え、コミット タイムアウトの残り時間も表示されます。

## 構成の置換の例

以下の構成の置換の構成例を参照してください。

- **configure replace bootflash: <file> show-patch** CLI コマンドを使用して、実行中の構成とユーザー指定の構成の違いを表示します。

```
switch(config)# configure replace bootflash:<file> show-patch
Collecting Running-Config
Converting to checkpoint file
#Generating Rollback Patch
!!
no role name abc
```

- **configure replace bootflash: <file> verbose** CLI コマンドを使用して、スイッチの実行中の構成全体をユーザー構成コと置換します。

```
switch(config)# configure replace bootflash:<file> verbose
Collecting Running-Config
```

## 構成の置換の例

```

Generating Rollback patch for switch profile
Rollback Patch is Empty
Note: Applying config parallelly may fail Rollback verification
Collecting Running-Config
#Generating Rollback Patch
Executing Rollback Patch
=====
config t
no role name abc
=====
Generating Running-config for verification
Generating Patch for verification

Rollback completed successfully.

Sample Example with adding of BGP configurations.
switch(config)# sh run | section bgp
switch(config)# sh file bootflash:file | section bgp
feature bgp
router bgp 1
  address-family ipv4 unicast
    neighbor 1.1.1.1
switch(config)#
switch(config)# configure replace bootflash:file verbose
Collecting Running-Config
Generating Rollback patch for switch profile
Rollback Patch is Empty
Note: Applying config parallelly may fail Rollback verification
Collecting Running-Config
#Generating Rollback Patch
Executing Rollback Patch
=====
config t
feature bgp
router bgp 1
  address-family ipv4 unicast
  neighbor 1.1.1.1
=====
Generating Running-config for verification
Generating Patch for verification

Rollback completed successfully.

switch(config)# sh run | section bgp
feature bgp
router bgp 1
  address-family ipv4 unicast
  neighbor 1.1.1.1

Sample Example with ACL
switch(config)# configure replace bootflash:run_1.txt
Collecting Running-Config
Generating Rollback patch for switch profile
Rollback Patch is Empty
Note: Applying config parallelly may fail Rollback verification
Collecting Running-Config
#Generating Rollback Patch
Executing Rollback Patch
=====
config t
no ip access-list nexus-50-new-xyz
ip access-list nexus-50-new-xyz-jkl-abc
10 remark Newark
20 permit ip 17.31.5.0/28 any

```

```

30 permit ip 17.34.146.193/32 any
40 permit ip 17.128.199.0/27 any
50 permit ip 17.150.128.0/22 any
=====
Generating Running-config for verification
Generating Patch for verification

Rollback completed successfully.

switch(config)#

```

switch(config) # show run aclmgr | sec nexus-50-new-xyz-jkl-abc

```

ip access-list nexus-50-new-xyz-jkl-abc
  10 remark Newark
  20 permit ip 17.31.5.0/28 any
  30 permit ip 17.34.146.193/32 any
  40 permit ip 17.128.199.0/27 any
  50 permit ip 17.150.128.0/22 any

```

- **configure replace bootflash:user-config.cfg verify-only** CLI コマンドを使用して、パッチを意的生成および確認します。

```

switch(config) # configure replace bootflash:user-config.cfg verify-only

Version match between user file and running configuration.
Pre-check for User config PASSED
Collecting Running-Config
Converting to checkpoint file
Generating Rollback Patch
Validating Patch
=====
`config t `
`interface Ethernet1/1`
`shutdown`
`no switchport trunk allowed vlan`
`no switchport mode`
`no switchport`
`exit`
Skip non dme command for CR validation
`interface Vlan1`
`shutdown`
`interface Ethernet1/1`
`shutdown`
`no switchport`
`ip address 1.1.1.1/24`
`exit`
Skip non dme command for CR validation
=====
Patch validation completed successful
switch(config)#

```

- **configure replace bootflash:user-config.cfg best-effort verify-and-commit** パッチのセマンティック検証を実行した後、スイッチの実行構成を指定されたユーザー構成に置き換える CLI コマンド。

```

switch(config) # configure replace bootflash:user-config.cfg best-effort
verify-and-commit

Version match between user file and running configuration.
Pre-check for User config PASSED
ADVISORY: Config Replace operation started...
Modifying running configuration from another VSH terminal in parallel

```

## 構成の置換の例

```

is not recommended, as this may lead to Config Replace failure.

Collecting Running-Config
Generating Rollback patch for switch profile
Rollback Patch is Empty
Collecting Running-Config
Generating Rollback Patch

Validating Patch
Patch validation completed successful
Executing Rollback Patch
During CR operation, will retain L3 configuration
when vrf member change on interface
Generating Running-config for verification
Generating Rollback Patch

Configure replace completed successfully. Please run 'show config-replace log exec'
to see if there is any configuration that requires reload to take effect.

switch(config)#

```

- **show config-replace log exec** CLI コマンドを使用して、実行済みの構成と、存在する場合は障害をすべて確認します。

```

switch(config)# show config-replace log exec
Operation : Rollback to Checkpoint File
Checkpoint file name : .replace_tmp_28081
Scheme : tmp
Rollback done By : admin
Rollback mode : atomic
Verbose : enabled
Start Time : Wed, 06:39:34 25 Jan 2017
-----
time: Wed, 06:39:47 25 Jan 2017
Status: SUCCESS
End Time : Wed, 06:39:47 25 Jan 2017
Rollback Status : Success

Executing Patch:
-----
switch#config t
switch#no role name abc

```

- **show config-replace log verify** CLI コマンドを使用して、存在する場合は障害をすべて確認します。

```

switch(config)# show config-replace log verify
Operation : Rollback to Checkpoint File
Checkpoint file name : .replace_tmp_28081
Scheme : tmp
Rollback done By : admin
Rollback mode : atomic
Verbose : enabled
Start Time : Wed, 06:39:34 25 Jan 2017
End Time : Wed, 06:39:47 25 Jan 2017
Status : Success

Verification patch contains the following commands:
-----
!! !
! No changes
-----

```

```
time: Wed, 06:39:47 25 Jan 2017
Status: SUCCESS
```

- **show config-replace status** CLI コマンドを使用して、構成交換のステータスを確認します。

```
switch(config)# show config-replace status
Last operation : Rollback to file
Details:
  Rollback type: atomic replace tmp_28081
  Start Time: Wed Jan 25 06:39:28 2017
  End Time: Wed Jan 25 06:39:47 2017
  Operation Status: Success
switch(config)#
```

スイッチから生成された設定の代わりに手動で作成された設定を使用すると、[置換の設定 (Configure Replace) ] が失敗することがあります。失敗の原因として考えられるのは、show running configuration に示されていないデフォルト設定の潜在的な違いです。次の例を参照してください。

power redundancy コマンドがデフォルトのコマンドである場合、デフォルトの設定では表示されません。ただし、ユーザーが **show run all** コマンドを使用した場合に表示されます。次の例を参照してください。

```
switch# show run all

!Command: show running-config all
!Running configuration last done at: Tue Nov 12 11:07:44 2019
!Time: Tue Nov 12 11:16:09 2019

version 9.3(1) Bios:version 05.39
power redundancy-mode ps-redundant
no hardware module boot-order reverse
no license grace-period
<snip>
hostname n9k13
```

電源冗長コマンドは、show running configuration コマンド出力には表示されません。次の例を参照してください。

```
!Command: show running-config
!Running configuration last done at: Tue Nov 12 11:07:44 2019
!Time: Tue Nov 12 11:17:24 2019

version 9.3(1) Bios:version 05.39
hostname n9k13
```

構成置換のユーザー構成に **power redundancy-mode ps-redundant** コマンドが追加された場合、検証/コミットが失敗する可能性があります。次の例を参照してください。

```
switch# show file bootflash:test

!Command: show running-config
!Running configuration last done at: Tue Nov 12 10:56:49 2019
!Time: Tue Nov 12 11:04:57 2019

version 9.3(1) Bios:version 05.39
power redundancy-mode ps-redundant
hostname n9k13
```

**power redundancy-mode ps-redundant** コマンドは、構成置換の後の show running には表示されません。したがって、「欠落」と見なされ、CR は失敗します。次に例を示します。

## 構成の置換の例

```

switch# config replace bootflash:test verify-and-commit

Version match between user file and running configuration.
Pre-check for User config PASSED
ADVISORY: Config Replace operation started...
Modifying running configuration from another VSH terminal in parallel
is not recommended, as this may lead to Config Replace failure.

Collecting Running-Config
Generating Rollback patch for switch profile
Rollback Patch is Empty
Collecting Running-Config
. Generating Rollback Patch

Validating Patch
Patch validation completed successful
Executing Rollback Patch
During CR operation, will retain L3 configuration
when vrf member change on interface
Generating Running-config for verification
Generating Rollback Patch
Executing Rollback Patch
During CR operation, will retain L3 configuration
when vrf member change on interface
Generating Running-config for verification
Generating Patch for verification
Verification failed, Rolling back to previous configuration
Collecting Running-Config
Cleaning up switch-profile buffer
Generating Rollback patch for switch profile
Executing Rollback patch for switch profiles. WARNING - This will change the
configuration of switch profiles and will also affect any peers if configured
Collecting Running-Config
Generating Rollback Patch
Rollback Patch is Empty
Rolling back to previous configuration is successful

Configure replace failed. Use 'show config-replace log verify' or 'show config-replace
log exec' to see reasons for failure

n9k13# show config-replace log verify
Operation : Config-replace to user config
Checkpoint file name : .replace_tmp_31849
Scheme : tmp
Cfg-replace done By : agargula
Cfg-replace mode : atomic
Verbose : disabled
Start Time : Tue, 11:20:59 12 Nov 2019
Start Time UTC : Tue, 10:20:59 12 Nov 2019
-----
End Time : Tue, 11:21:28 12 Nov 2019
End Time UTC : Tue, 10:21:28 12 Nov 2019
Status : Failed

Verification patch contains the following commands:
-----
!!
Configuration To Be Added Missing in Running-config
=====
!
power redundancy-mode ps-redundant

Undo Log
-----

```

```
End Time : Tue, 11:21:32 12 Nov 2019
End Time UTC : Tue, 10:21:32 12 Nov 2019
Status : Success
n9k13#
```

上記の例では、CR は欠落しているデフォルトのコマンドを考慮します。

## 構成の置換の例



## 第 23 章

# ソフトウェアメンテナンスアップグレード (SMU) の実行

この章は、次の項で構成されています。

- SMU について (339 ページ)
- パッケージ管理 (340 ページ)
- SMU の前提条件 (341 ページ)
- SMU の注意事項と制約事項 (341 ページ)
- Cisco NX-OS のソフトウェアメンテナンスアップグレードの実行 (342 ページ)
- パッケージインストールの準備 (342 ページ)
- ローカルストレージデバイスまたはネットワーク サーバへのパッケージファイルのコピー (344 ページ)
- パッケージの追加とアクティブ化 (345 ページ)
- アクティブなパッケージセットのコミット (346 ページ)
- パッケージの非アクティブ化と削除 (347 ページ)
- インストール ログ情報の表示 (348 ページ)

## SMU について

ソフトウェアメンテナンスアップグレード (SMU) は、特定の障害の修正を含むパッケージファイルです。SMU は、直近の問題に対処するために作成され、新しい機能は含まれていません。通常、SMU がデバイスの動作に大きな影響を及ぼすことはありません。SMU のバージョンは、アップグレードするパッケージのメジャー、マイナー、およびメンテナンスバージョンに同期されます。

SMU の影響は次のタイプによって異なります。

- プロセスの再起動 SMU：アクティベーション時にプロセスまたはプロセスのグループの再起動を引き起こします。
- リロード SMU：スーパーバイザおよびラインカードのパラレル リロードを引き起こします。

SMU は、メンテナンスリリースの代わりになるものではありません。直近の問題に対する迅速な解決策を提供します。SMU で修正された障害は、メンテナンスリリースにすべて統合されます。

デバイスを新しい機能やメンテナンスリリースにアップグレードする詳細については、『Cisco Nexus 3500 シリーズ NX-OS ソフトウェアアップグレードおよびダウングレードガイド』を参照してください。



(注) SMU をアクティブにすると、以前の SMU、または SMU が適用されるパッケージが自動的に非アクティブ化されることはありません。

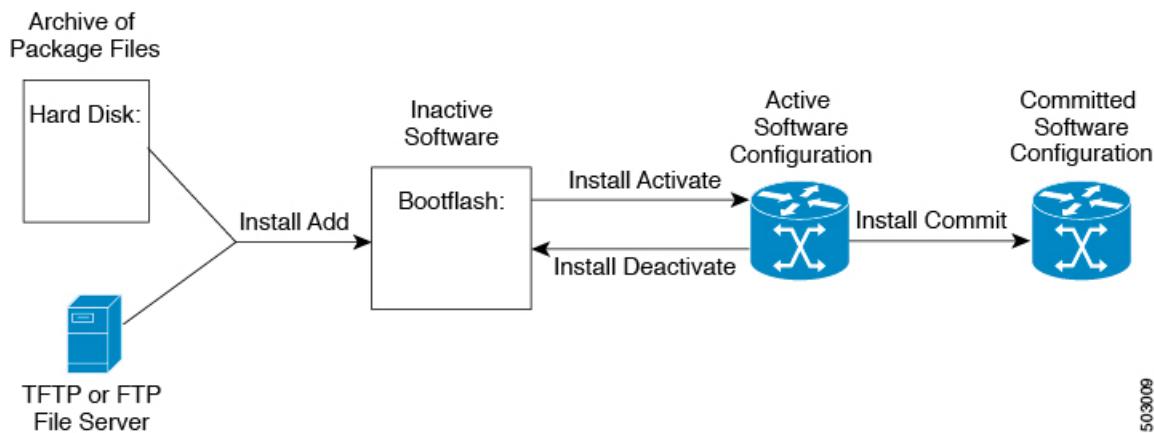
## パッケージ管理

デバイスでの SMU パッケージの追加およびアクティブ化の一般的な手順は次のとおりです。

1. パッケージファイルをローカルストレージデバイスまたはファイルサーバにコピーします。
2. **install add** コマンドを使用してデバイス上でパッケージを追加します。
3. **install activate** コマンドを使用してデバイス上でパッケージをアクティブ化します。
4. **install commit** コマンドを使用して、現在のパッケージのセットをコミットします。
5. (任意) 必要に応じて、パッケージを非アクティブ化して削除します。

次の図は、パッケージの管理プロセスの主要な手順について説明します。

図 2: SMU パッケージを追加、アクティブ化およびコミットするプロセス



503006

## SMU の前提条件

アクティブ化または非アクティブ化するパッケージでは、これらの前提条件が満たされている必要があります。

- 適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。ユーザ グループの割り当てが原因でコマンドを使用できないと考えられる場合、AAA 管理者に連絡してください。
- すべてのラインカードが取り付けられ、正常に動作していることを確認します。たとえば、ラインカードのブート中、ラインカードのアップグレード中または交換中、または自動スイッチオーバー アクティビティが予想される場合は、パッケージのアクティブ化や非アクティブ化はできません。

## SMU の注意事項と制約事項

SMU に関する注意事項および制約事項は次のとおりです。

- パッケージによっては、他のパッケージのアクティブ化または非アクティブ化が必要です。SMU に相互に依存関係がある場合は、前の SMU をまずアクティブにしないとそれらをアクティブ化できません。
- アクティブ化するパッケージは、現在のアクティブなソフトウェアのセットと互換性がある必要があります。
- 1 つのコマンドで複数の SMU をアクティブにできません。
- パッケージの互換性が確認できた場合に限り、アクティブ化が実行されます。競合がある場合は、エラー メッセージが表示されます。
- ソフトウェアパッケージをアクティブ化する間、その他の要求はすべての影響のあるノードで実行できません。これと同様のメッセージが表示されると、パッケージのアクティブ化は完了します。

Install operation 1 completed successfully at Thu Jan 9 01:19:24 2014

- 各 CLI インストール要求には要求 ID が割り当てられます。これは後でイベントを確認するのに使用できます。
- ソフトウェアメンテナンスアップグレードを実行後、デバイスを新しい Cisco Nexus 3500 ソフトウェア リリースにアップグレードする場合、新しいイメージで以前の Cisco Nexus 3500 リリースと SMU パッケージ ファイルの両方が上書きされます。
- Cisco NX-OS リリース 10.5(1)F 以降では、次のガイドラインが SMU に適用されます。
  - 有効でイメージと互換性のある SMU をアクティブ化する必要がある場合、アクティブ化が失敗すると、スイッチは自動的にリロードされます。ただし、4 回試行しても SMU がアクティブにならない場合は、SMU をアクティブにしないでください。一

方、スイッチの準備が整うと、SMUのアクティブ化が失敗したことを示すsyslogメッセージが表示されます。

- PID固有のSMUを、意図していないPIDにインストールしようとすると、次のメッセージが表示されます：[Install operation failed because SMU is not compatible for this switch model (SMUがこのスイッチモデルと互換ではないため、インストール操作は失敗しました)]。
- サポートされているSMUとサポートされていないSMUを含むSMU tarボールを使用してスイッチでISSUを実行すると、サポートされているSMUのみがISSUの後にインストールされます。

## Cisco NX-OS のソフトウェアメンテナンスアップグレードの実行

### パッケージインストールの準備

SMUパッケージのインストールの準備に関する情報を収集するには、複数の**show**コマンドを使用する必要があります。

#### 始める前に

ソフトウェアの変更が必要かどうかを確認します。

使用中のシステムで新しいパッケージがサポートされていることを確認する。ソフトウェアパッケージによっては、他のパッケージまたはパッケージバージョンをアクティブにする必要があり、特定のラインカードのみをサポートするパッケージもあります。

そのリリースに関する重要な情報についてリリースノートを確認し、そのパッケージとデバイス設定の互換性の有無を判断する。

システムの動作が安定していて、ソフトウェアの変更に対応できることを確認する。

#### 手順の概要

1. **show install active**
2. **show module**
3. **show clock**

## 手順の詳細

## 手順

	コマンドまたはアクション	目的
ステップ1	<b>show install active</b>  例： switch# show install active	デバイス上のアクティブなソフトウェアを表示します。デバイスに追加する必要があるソフトウェアを決定するため、またインストール操作完了後にアクティブなソフトウェアのレポートと比較するため、このコマンドを使用します。
ステップ2	<b>show module</b>  例： switch# show module	すべてのモジュールが安定状態であることを確認します。
ステップ3	<b>show clock</b>  例： switch# show clock	システムクロックが正しいことを確認します。ソフトウェア操作は、デバイスクロックの時刻に基づいて証明書を使用します。

## 例

次に、システム全体のアクティブなパッケージを表示する例を示します。この情報を使用して、ソフトウェアの変更が必要かどうかを判断します。

```
switch# show install active
Active Packages:
Active Packages on Module #3:
Active Packages on Module #6:
Active Packages on Module #7:
Active Packages on Module #22:
Active Packages on Module #30:
```

次に、現在のシステムクロックの設定を表示する例を示します。

```
switch# show clock
02:14:51.474 PST Wed Jan 04 2014
```

# ローカルストレージデバイスまたはネットワークサーバへのパッケージファイルのコピー

デバイスがアクセスできるローカルストレージデバイスまたはネットワークファイルサーバに SMU パッケージファイルをコピーする必要があります。この作業が完了したら、パッケージをデバイスに追加しアクティブにできます。

デバイスにパッケージファイルを保存する必要がある場合は、ハードディスクにファイルを保存することを推奨します。ブートデバイスは、パッケージを追加しアクティブにするローカルディスクです。デフォルトのブートデバイスは `bootflash:` です。



**ヒント** ローカルストレージデバイスにパッケージファイルをコピーする前に、`dir` コマンドを使用して、必要なパッケージファイルがすでにデバイス上に存在するかどうかを確認します。

SMU パッケージファイルがリモート TFTP、FTP、または SFTP サーバにある場合、ローカルストレージデバイスにファイルをコピーできます。ファイルがローカルストレージデバイスに置かれた後、パッケージをそのストレージデバイスからデバイスに追加しアクティブにできます。次のサーバプロトコルがサポートされます。

- **TFTP**：ネットワークを介して、あるコンピュータから別のコンピュータへファイルを転送できるようにします。通常は、クライアント認証（たとえば、ユーザ名およびパスワード）を使用しません。これは FTP の簡易版です。



**(注)** パッケージファイルによっては、大きさが 32 MB を超える場合もありますが、一部のベンダーにより提供される TFTP サービスではこの大きさのファイルがサポートされていない場合があります。32 MB を超えるファイルをサポートする TFTP サーバにアクセスできない場合は、FTP を使用してファイルをダウンロードします。

- **ファイル転送プロトコル**：FTP は TCP/IP プロトコルスタックの一部であり、ユーザ名とパスワードが必要です。
- **SSH ファイル転送プロトコル**：SFTP は、セキュリティパッケージの SSHv2 機能の一部で、セキュアなファイル転送を提供します。

SMU パッケージファイルをネットワークファイルサーバまたはローカルストレージデバイスに転送した後に、ファイルを追加しアクティブ化することができます。

# パッケージの追加とアクティブ化

ローカルストレージデバイスまたはリモートTFTP、FTP、SFTPサーバーに保存されているSMUパッケージファイルをデバイスに追加できます。



(注)

アクティブ化するSMUパッケージは、現在アクティブで動作可能なソフトウェアと互換性がなければなりません。アクティブ化が試行されると、システムは自動互換性チェックを実行し、パッケージがデバイス上でアクティブな他のソフトウェアと互換性があることを確認します。競合がある場合は、エラーメッセージが表示されます。アクティブ化が実行されるのは、すべての互換性が確認できた場合だけです。

## 手順の概要

1. **install add filename [activate]**
2. (任意) **show install inactive**
3. **install activate filename [test]**
4. すべてのパッケージがアクティブ化されるまで手順3を繰り返します。
5. (任意) **show install active**

## 手順の詳細

### 手順

	コマンドまたはアクション	目的
ステップ1	<b>install add filename [activate]</b> 例： switch# install add bootflash: n3500-uk9.6.0.2.U6.0.1.CSCab00001.bin	ローカルストレージデバイスまたはネットワークサーバからパッケージソフトウェアファイルを解凍してブートフラッシュおよびデバイスにインストールされているすべてのアクティブスーパーバイザおよびスタンバイスーパーバイザに追加します。 値は、 <i>filename</i> 引数は、次の形式をとることができます： <ul style="list-style-type: none"> <li>• <b>bootflash:filename</b></li> <li>• <b>tftp://hostname-or-ipaddress/directory-path/filename</b></li> <li>• <b>ftp://username:password@hostname-or-ipaddress/directory-path/filename</b></li> <li>• <b>sftp://hostname-or-ipaddress/directory-path/filename</b></li> </ul>
ステップ2	(任意) <b>show install inactive</b>  例： switch# show install inactive	デバイス上の非アクティブなパッケージを表示します。前述の手順で追加されたパッケージが表示に出ることを確認します。

## アクティブなパッケージセットのコミット

	コマンドまたはアクション	目的
ステップ3	<p>必須: <b>install activate filename [test]</b></p> <p>例 :</p> <pre>switch# install activate n3500-uk9.6.0.2.U6.0.1.CSCab00001.bin</pre> <p>例 :</p> <pre>switch# install activate n3500-uk9.6.0.2.U6.0.1.CSCab00001.bin Install operation 1 completed successfully at Thu Jan 9 01:27:56 2014</pre> <p>例 :</p> <pre>switch# install activate n3500-uk9.6.0.2.U6.0.1.CSCab00001.bin Install operation 2 !!WARNING!! This patch will get activated only after a reload of the switch. at Sun Mar 9 00:42:12 2014</pre>	<p>デバイスに追加されたパッケージをアクティブにします。SMUパッケージは、アクティブにされるまで無効のままであります。（<b>install add activate</b> コマンドを使用してパッケージが以前にアクティブ化されていた場合は、この手順を省略します）。</p> <p>（注）</p> <p>パッケージ名の一部を入力してから<b>?</b>を押すと、アクティベーション可能なすべての一一致が表示されます。一致するものが1つしかない場合は、<b>タブキー</b>を押して、パッケージ名の残りの部分を入力します。</p>
ステップ4	すべてのパッケージがアクティブ化されるまで手順3を繰り返します。	必要に応じて他のパッケージもアクティブ化します。
ステップ5	<p>（任意） <b>show install active</b></p> <p>例 :</p> <pre>switch# show install active</pre>	すべてのアクティブなパッケージを表示します。このコマンドを使用して、正しいパッケージがアクティブであるかどうかを判断します。

## アクティブなパッケージセットのコミット

SMUパッケージがデバイス上でアクティブになると、それは現在の実行コンフィギュレーションの一部になります。パッケージのアクティブ化をシステム全体のリロード間で持続させるには、デバイス上でパッケージをコミットする必要があります。

## 手順の概要

1. **install commit filename**
2. （任意） **show install committed**

## 手順の詳細

## 手順

	コマンドまたはアクション	目的
ステップ1	<b>install commit filename</b>  例：  switch# install commit n3500-uk9.6.0.2.U6.0.1.CSCab00001.bin	現在のパッケージのセットをコミットして、デバイスが再起動したときにこれらのパッケージが使用されるようにします。
ステップ2	(任意) <b>show install committed</b>  例：  switch# show install committed	コミットされたパッケージを表示します。

## パッケージの非アクティブ化と削除

パッケージを非アクティブ化すると、そのデバイスではアクティブではなくなりますが、パッケージファイルはブートディスクに残ります。パッケージファイルは、後で再アクティブ化できます。また、ディスクから削除もできます。

## 手順の概要

1. **install deactivate filename**
2. (任意) **show install inactive**
3. (任意) **install commit**
4. (任意) **install remove {filename | inactive}**

## 手順の詳細

## 手順

	コマンドまたはアクション	目的
ステップ1	<b>install deactivate filename</b>  例：  switch# install deactivate n3500-uk9.6.0.2.U6.0.1.CSCab00001.bin	デバイスに追加されたパッケージを非アクティブ化し、ラインカードのパッケージ機能をオフにします。  (注) パッケージ名を部分的に入力してから?を押すと、非アクティブ化に使用できるすべての候補が表示されます。一致するものが1つしかない場合は、タブキーを押して、パッケージ名の残りの部分を入力します。

## ■ インストールログ情報の表示

	コマンドまたはアクション	目的
ステップ2	(任意) <b>show install inactive</b>  例： <pre>switch# show install inactive</pre>	デバイス上の非アクティブなパッケージを表示します。
ステップ3	(任意) <b>install commit</b>  例： <pre>switch# install commit</pre>	現在のパッケージのセットをコミットして、デバイスが再起動したときにこれらのパッケージが使用されるようにします。  (注) パッケージを削除できるのは、非アクティブ化操作がコミットされた場合だけです。
ステップ4	(任意) <b>install remove {filename   inactive}</b>  例： <pre>switch# install remove n3500-uk9.6.0.2.U6.0.1.CSCab00001.bin Proceed with removing n3500-uk9.6.0.2.U6.0.1.CSCab00001.bin? (y/n)? [n] y</pre> 例： <pre>switch# install remove inactive Proceed with removing? (y/n)? [n] y</pre>	非アクティブなパッケージを削除します。 <ul style="list-style-type: none"><li>削除できるのは非アクティブなパッケージだけです。</li><li>パッケージは、デバイスのすべてのラインカードから非アクティブにされた場合にのみ削除できます。</li><li>パッケージの非アクティブ化はコミットする必要があります。</li><li>ストレージデバイスから特定の非アクティブなパッケージを削除するには、<b>install remove</b> コマンドと <i>filename</i> 引数を指定して使用します。</li><li>システムのすべてのノードから非アクティブなパッケージをすべて削除するには、<b>install remove</b> コマンドと <b>inactive</b> キーワードを使用します。</li></ul>

## インストールログ情報の表示

インストールログは、インストール動作の履歴についての情報を提供します。インストール動作が実行されるたびに、その動作に対して番号が割り当てられます。

- **show install log** コマンドを使用して、インストール動作の成功および失敗の両方について情報を表示します。
- **show install log** コマンドで引数を使用しない場合は、すべてのインストール動作のサマリーを表示します。*request-id*引数を指定して、ある動作に固有の情報を表示します。  
**detail** キーワードを使用して、ファイルの変更、リロードできなかったノード、その他プロセスに影響する操作など、特定の操作の詳細を表示します。

次に、すべてのインストール要求の情報を表示する例を示します。

```
switch# show install log
Thu Jan 9 01:26:09 2014
Install operation 1 by user 'admin' at Thu Jan 9 01:19:19 2018
Install add bootflash: n3500-uk9.6.0.2.U6.0.1.CSCab00001.bin
Install operation 1 completed successfully at Thu Jan 9 01:19:24 2014
-----
Install operation 2 by user 'admin' at Thu Jan 9 01:19:29 2018
Install activate n3500-uk9.6.0.2.U6.0.1.CSCab00001.bin
Install operation 2 completed successfully at Thu Jan 9 01:19:45 2018
-----
Install operation 3 by user 'admin' at Thu Jan 9 01:20:05 2018
Install commit n3500-uk9.6.0.2.U6.0.1.CSCab00001.bin
Install operation 3 completed successfully at Thu Jan 9 01:20:08 2018
-----
Install operation 4 by user 'admin' at Thu Jan 9 01:20:21 2018
Install deactivate n3500-uk9.6.0.2.U6.0.1.CSCab00001.bin
Install operation 4 completed successfully at Thu Jan 9 01:20:36 2018
-----
Install operation 5 by user 'admin' at Thu Jan 9 01:20:43 2018
Install commit n3500-uk9.6.0.2.U6.0.1.CSCab00001.bin
Install operation 5 completed successfully at Thu Jan 9 01:20:46 2014
-----
Install operation 6 by user 'admin' at Thu Jan 9 01:20:55 2018
Install remove n3500-uk9.6.0.2.U6.0.1.CSCab00001.bin
Install operation 6 completed successfully at Thu Jan 9 01:20:57 2018
```

## ■ インストールログ情報の表示



## 第 24 章

# ロールバックの設定

この章は、次の項で構成されています。

- ロールバックについて (351 ページ)
- ロールバックの注意事項と制約事項 (351 ページ)
- チェックポイントの作成 (352 ページ)
- ロールバックの実装 (353 ページ)
- ロールバック コンフィギュレーションの確認 (354 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ー 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とも、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と制約事項

ロールバックに関する設定時の注意事項および制約事項は、次のとおりです。

- 作成できるチェックポイント コピーの最大数は 10 です。
- 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。

## ■ チェックポイントの作成

- ・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。
- ・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** コマンドを入力した後、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。
- ・ポ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 **チェックポイント** *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スイッチオーバー時に存在します。
- ・ポートフラッシュ時のファイルへのロールバックは、**チェックポイント** *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。
- ・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。

### 手順の概要

1. switch# **checkpoint** { [cp-name] [description descr] |file file-name}
2. (任意) switch# **no checkpoint**cp-name
3. (任意) switch# **show checkpoint**cp-name

## 手順の詳細

## 手順

	コマンドまたはアクション	目的
ステップ1	<b>switch# checkpoint</b> { [cp-name] [description descr]  file file-name  例： switch# checkpoint stable	<p>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-&lt;number&gt; に設定します。ここで number は 1 ~ 10 の値です。</p> <p>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。</p>
ステップ2	(任意) <b>switch# no checkpoint</b> cp-name  例： switch# no checkpoint stable	<p>checkpoint コマンドの <b>no</b> 形式を使用して、チェックポイント名を削除します。</p> <p><b>delete</b> チェックポイントファイルを削除します。</p>
ステップ3	(任意) <b>switch# show checkpoint</b> cp-name  例： [ all] switch# show checkpoint stable	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。

## 手順の概要

- 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}
- rollback running-config** {checkpoint cp-name | file cp-file} atomic

## ■ ロールバック コンフィギュレーションの確認

## 手順の詳細

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>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}</b> 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	<b>rollback running-config {checkpoint cp-name   file cp-file} atomic</b> 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。

## 例

チェックポイントファイルを作成し、次に、ユーザー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
<b>show checkpoint name [ all]</b>	チェックポイント名の内容を表示します。
<b>show checkpoint all [user   system]</b>	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、ユーザー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。
<b>show checkpoint summary [user   system]</b>	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、ユーザー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。

コマンド	目的
<b>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}</b>	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。
<b>show rollback log [exec   verify]</b>	ロールバック ログの内容を表示します。



(注) **clear checkpoint database** コマンドを使用して、すべてのチェックポイントファイルを削除します。

## ■ ロールバック コンフィギュレーションの確認



# 第 25 章

## 候補構成の完全性チェック

本章では、候補構成の完全性チェックの方法について説明します。

この章は、次の項で構成されています。

- [候補構成について \(357 ページ\)](#)
- [候補構成の完全性チェックの注意事項と制限事項 \(357 ページ\)](#)
- [候補構成の完全性チェックの実行 \(363 ページ\)](#)
- [完全性チェックの例 \(364 ページ\)](#)

### 候補構成について

候補構成は、実行構成のサブセットです。実行構成は、追加、変更、または削除を行わずに、実行構成内に候補構成が存在するかどうかを確認します。

候補構成の完全性を確認するには、次のコマンドを使用します。

- `show diff running-config`
- `show diff startup-config`

CLI の詳細については、[候補構成の完全性チェックの実行 \(363 ページ\)](#) を参照してください。

### 候補構成の完全性チェックの注意事項と制限事項

候補構成の完全性チェックには、次の注意事項と制限事項があります。

- Cisco NX-OS リリース 10.2(3)F 以降、すべての Cisco Nexus スイッチに候補構成の完全性チェック オプションが導入されました。
- 完全な実行構成ファイルの完全性チェックを行うには、NX-OS システムが生成した実行構成を提供する必要があります。 **partial** キーワードは使用しないでください。次のキーワードは、入力候補を実行構成のサブセットとして扱います。 **partial** キーワードは、入力候補を実行構成のサブセットとして扱います。

## ■ 候補構成の完全性チェックの注意事項と制限事項

- 生成された実行構成に表示される行番号は、内部で生成されたものであるため、候補構成とは一致しません。
- 実行構成と候補構成に違いがある場合、インラインで出力表示されます。
- 候補ファイルの構成ブロック全体が新たに追加されたものである場合、生成される実行構成の最後に追加されます。
- 候補設定に SNMP または AAA ユーザー CLI とクリアテキスト パスワードがある場合、ユーザーがすでに設定されている場合でも、SNMP ユーザーは diff として表示されます。
- Cisco NX-OS リリース 10.4(3)F 以降では、候補構成でポリモーフィック コマンドを使用して、partial diff を実行することもできます。
- partial diff を実行する前に、EIGRP アドレス ファミリ IPv4 設定を、候補ファイルのルータ モード階層ではなく、EIGRP アドレス ファミリ 階層で設定しておくことをお勧めします。
- ターゲット/候補ファイルにデフォルトのコマンド（たとえば、`- log-neighbor-warnings` です）がサブモードではなくモードの下に直接構成されている場合、**router eigrp** つまり、**address-family ipv4 unicast** または **address-family ipv6 unicast** の場合、partial-diff は diff 内のデフォルト コマンドの出力に + が表示されます（たとえば、`+ log-neighbor-warnings` です）。
- 大文字と小文字が区別されないコマンドで、実行中の config ファイルと concurrent-config ファイル内のコマンドの間に大文字と小文字の相違がある場合、**partial diff** の出力には、大文字と小文字の違いにより両方のコマンドが表示されます。
- ユーザー データベースを SNMP と AAA（セキュリティ）の間で同期するため、候補 CONFIG\_FILE の partial diff を実行する場合は、クリアテキストのパスワードが許可されます。
- 設定プロファイル、メンテナンス プロファイル (mmode) 、およびスケジューラ モード の設定はサポートされていません。

マルチキャストコンポーネントのデフォルトコマンドの **partial diff** に関する注意事項と制約事項

このセクションの内容は、Cisco NX-OS リリース 10.4(3)F から適用されます。

マルチキャストコンポーネントのデフォルトコマンドが候補 CONFIG\_FILE に存在する場合、**show diff** では次のように表示されます。

マルチキャストコンポーネント	次の中のデフォルトコマンド <b>show diff</b>
PIM	<pre>ip access-list copp-system-p-acl-pim 10 permit pim any 224.0.0.0/24 20 permit udp any any eq pim-auto-rp ip access-list copp-system-p-acl-pim-mdt-join ip access-list copp-system-p-acl-pim-reg 10 permit pim any any</pre>

マルチキャストコンポーネント	次の中のデフォルトコマンド <b>show diff</b>
PIM6	ipv6 access-list copp-system-p-acl-pim6 10 permit pim any ff02::d/128 20 permit udp any any eq pim-auto-rp ipv6 access-list copp-system-p-acl-pim6-reg 10 permit pim any any
IGMP	ip access-list copp-system-p-acl-igmp 10 permit igmp any 224.0.0.0/3 class-map copp-system-p-class-normal-igmp
MLD	ipv6 access-list copp-system-p-acl-mld 10 permit icmp any any mld-query 20 permit icmp any any mld-report 30 permit icmp any any mld-reduction 40 permit icmp any any mldv2

#### の注意事項と制限事項 **show diff running-config file\_url [unified] [partial] [merged]** コマンド

- **unified**、**partial**、および **merged** オプションを使用して次の PBR コマンドの違いを確認すると、diff の出力は次のようにになります：

- **set ip next-hop**
- **set ip default next-hop**
- **set ip default vrf next-hop**
- **set ipv6 next-hop**
- **set ipv6 default next-hop**
- **set ipv6 default vrf next-hop**

1. 候補のネクストホップが実行中のネクストホップの（同じ順序とシーケンスの）サブセットであり、候補の追加フラグのが実行中のフラグのサブセットである場合、次の表に示すように、diff の出力は空になります。

候補構成	実行構成	部分的な統合マージ差分出力
route-map rmap1 permit 10 set ip next-hop 1.1.1.1 2.2.2.2 load-share	route-map rmap1 permit 10 set ip next-hop 1.1.1.1 2.2.2.2 3.3.3.3 load-share force-order	<no-diff>

2. 候補のネクストホップが実行中のネクストホップの（同じ順序とシーケンスの）サブセットであり、候補に実行構成には存在しない余分の追加フラグがある場合、diff の出力は、次の表に示すように、実行構成に候補構成に存在する追加のフラグを付加したものとなって、コマンドラインの場合と似た結果になります。

## 候補構成の完全性チェックの注意事項と制限事項

候補構成	実行構成	部分的な統合マージ差分出力
route-map rmap1 permit 10 set ip next-hop 1.1.1.1 2.2.2.2 load-share force-order	route-map rmap1 permit 10 set ip next-hop 1.1.1.1 2.2.2.2 3.3.3.3 load-share drop-on-fail	route-map rmap1 permit 10 - set ip next-hop 1.1.1.1 2.2.2.2 3.3.3.3 load-share drop-on-fail + set ip next-hop 1.1.1.1 2.2.2.2 3.3.3.3 load-share force-order drop-on-fail

3. 候補ネクストホップが実行中のネクストホップの（同じ順序とシーケンスの）サブセットではなく、候補と実行中のレコードに追加のフラグが存在し得る場合、diffの出力は、実行構成レコードを「-」で、候補構成レコードを「+」で示します。

この区別は、ネクストホップのシーケンスが重要となる、PBR コマンドで使用する場合、特に重要です。ネクストホップIP アドレスが同一であっても、その順序は機能に影響します。

たとえば、「1.1.1.1 2.2.2.2」は「2.2.2.2 1.1.1.1」とは異なります。



## 重要

候補構成とマージした後に保持する実行構成に追加のフラグがある場合は、そのフラグを候補構成に明示的に含める必要があります。これにより、必要なフラグが最終的なマージされた構成で保持されます。

候補構成	実行構成	部分的な統合マージ差分出力
route-map rmap1 permit 10 set ip next-hop 1.1.1.1 2.2.2.2 load-share drop-on-fail	route-map rmap1 permit 10 set ip next-hop 2.2.2.2 1.1.1.1 load-share force-order	route-map rmap1 permit 10 - set ip next-hop 2.2.2.2 1.1.1.1 load-share force-order + set ip next-hop 1.1.1.1 2.2.2.2 load-share drop-on-fail

- **Partial Unified** または **Partial Unified Merged** オプションが使用されている場合、すべての PBR コマンドは相互に排他的であり、同じ親ルートマップ内で共存できません。したがって、候補構成で单一のルートマップに複数の相互に排他的な PBR コマンドが指定されている場合、最後のコマンドバリエントのみが partial diff の出力に表示されます。

例1：この例では、候補構成で、单一のルートマップ **rmap1** の下に複数の PBR コマンドが含まれています：

```
route-map rmap1 permit 10
  set ip next-hop 1.1.1.1 2.2.2.2
  set ipv6 next-hop 3::3
  set ip next-hop verify-availability 4.4.4.4
  set ip next-hop verify-availability 5.5.5.5
  set ip vrf green next-hop 6.6.6.6
  set ip vrf blue next-hop 7.7.7.7 8.8.8.8
```

partial-diff 出力の生成前に、上記の候補構成は自動的に次のように変換されます。

```
route-map rmap1 permit 10
  set ip vrf green next-hop 6.6.6.6
  set ip vrf blue next-hop 7.7.7.7 8.8.8.8
```

例 2：この例では、候補構成に、ルートマップ **rmap2**のために異なるトラック ID が指定された、複数の「**set ip next-hop verify-availability**」コマンドが含まれています。同じネクストホップのトラック ID は変更できないため、次のコマンドは相互に排他的です。

```
route-map rmap2 permit 10
  set ip next-hop verify-availability 1.1.1.1 track 1
  set ip next-hop verify-availability 2.2.2.2 track 20
  set ip next-hop verify-availability 2.2.2.2 track 30
  set ip next-hop verify-availability 2.2.2.2 track 40
  set ip next-hop verify-availability 3.3.3.3 track 3
```

**partial-diff**の出力を生成する前、次に示すように、システムは各ネクストホップ IP アドレスの最後の **set ip next-hop verify-availability** コマンドのみを保持することで、これらのコマンドを自動的に統合します：

```
route-map rmap2 permit 10
  set ip next-hop verify-availability 1.1.1.1 track 1
  set ip next-hop verify-availability 2.2.2.2 track 40
  set ip next-hop verify-availability 3.3.3.3 track 3
```

- クライアントが **Partial Unified Merged** オプションを使用して、**verify-availability** の違いを確認するとき、特定のネクストホップのトラック ID は変更できません。

したがって、候補と実行構成に同じネクストホップが含まれていて、同じ親ルートマップの下に異なるトラック ID がある場合、コマンドラインの動作の場合のように、候補レコードを実行レコードと単純にマージすることはできません。したがって、同じネクストホップに異なるトラック ID を持つ候補レコードを適用するには、対応する実行構成レコードを最初に削除する必要があります (diffでは実行構成レコードは「-」で示されます)。その後、候補レコードをマージすると、それは同じ親ルートマップの下の最後のレコードの末尾に追加されます (候補構成レコードは「+」で示されます)。

次のテーブルは、サンプルの候補と様々なユース ケースの部分的な統合マージ 出力の実行構成を表示します：

- 候補と実行構成で同じネクストホップのトラック ID が異なる場合、diffの出力は次の表のようになります。

候補構成	実行構成	部分的な統合マージ差分出力
<pre>route-map rmap1 permit 10   set ip next-hop   verify-availability 1.1.1.1   track 1   set ip next-hop   verify-availability 2.2.2.2   track 20   set ip next-hop   verify-availability 3.3.3.3   track 3 load-share</pre>	<pre>route-map rmap1 permit 10   set ip next-hop   verify-availability 1.1.1.1   track 1   set ip next-hop   verify-availability 2.2.2.2   track 2   set ip next-hop   verify-availability 3.3.3.3   track 3 load-share</pre>	<pre>route-map test permit 10   set ip next-hop   verify-availability 1.1.1.1   track 1   - set ip next-hop   verify-availability 2.2.2.2   track 2   set ip next-hop   verify-availability 3.3.3.3   track 3   + set ip next-hop   verify-availability 2.2.2.2   track 20 load-share</pre>

## 候補構成の完全性チェックの注意事項と制限事項

2.  トラック ID が候補構成には存在せず、同じネクストホップの実行構成に存在する場合、diff の出力は、次の表に示すように空になります。

候補構成	実行構成	部分的な統合マージ差分出力
<pre>route-map rmap1 permit 10   set ip next-hop   verify-availability 1.1.1.1   track 1   set ip next-hop   verify-availability 2.2.2.2     set ip next-hop   verify-availability 3.3.3.3   track 3</pre>	<pre>route-map rmap1 permit 10   set ip next-hop   verify-availability 1.1.1.1   track 1   set ip next-hop   verify-availability 2.2.2.2   track 2   set ip next-hop   verify-availability 3.3.3.3   track 3</pre>	非比較

3.  トラック ID が実行構成には存在せず、同じネクストホップの候補構成にに存在する場合、diff の出力は次の表のようになります。

候補構成	実行構成	部分的な統合マージ差分出力
<pre>route-map rmap1 permit 10   set ip next-hop   verify-availability 1.1.1.1   track 1   set ip next-hop   verify-availability 2.2.2.2   track 20   set ip next-hop   verify-availability 3.3.3.3   track 3</pre>	<pre>route-map rmap1 permit 10   set ip next-hop   verify-availability 1.1.1.1   track 1   set ip next-hop   verify-availability 2.2.2.2     set ip next-hop   verify-availability 3.3.3.3   track 3</pre>	<pre>route-map rmap1 permit 10   set ip next-hop   verify-availability 1.1.1.1   track 1   - set ip next-hop   verify-availability 2.2.2.2     set ip next-hop   verify-availability 3.3.3.3   track 3   + set ip next-hop   verify-availability 2.2.2.2   track 20</pre>

RPM コマンドの **partial diff** に関する注意事項と制約事項

このセクションの内容は、Cisco NX-OS リリース 10.4(3)F から適用されます。

unified、partial、およびmerged オプションを使用して次の RPM コマンドの違いを確認すると、diff の出力は次のようになります。

- 候補構成では、diff の出力に反映されているように、RPM コマンドの構文検証が行われます。ただし、diff の出力では、意味上の検証は実行されません。候補構成のコマンドが意証的に正確であることを確認するのは、ユーザーの責任です。

候補構成内のコマンドが意証的に正しくなくても、diff はコマンドが実行可能であると誤って示すことがあります、実際には実行可能ではない場合があります。

- Candidate-config ファイルで、次のコマンドの必須シーケンス番号を必ず指定してください。

- **ip prefix-list list-name seq seq {deny | permit} prefix**
- **ipv6 prefix-list list-name seq seq {deny | permit} prefix**
- **mac-list list-name seq seq {deny | permit} prefix**

- **ip community-list {standard | expanded} list-name seq seq {deny | permit} expression**
- **ip extcommunity-list {standard | expanded} list-name seq seq {deny | permit} expression**
- **ip large-community-list {standard | expanded} list-name seq seq {deny | permit} expression**
- **ip-as-path access-list list-name seq seq {deny | permit} expression**

• 次のコマンドに、実行構成内の引用符で囲まれたスペースを含む式文字列が含まれている場合、diff 出力に違いは表示されません。

- **ip community-list expanded list-name seq seq {deny | permit} expression**
- **ip extcommunity-list expanded list-name seq seq {deny | permit} expression**
- **ip large-community-list expanded list-name seq seq {deny | permit} expression**
- **ip-as-path access-list list-name seq seq {deny | permit} expression**

候補構成	実行構成	部分的な統合（マージ）差分出力
ip community-list expanded list_abc seq 10 permit "1:1 "	ip community-list expanded list_abc seq 10 permit "1:1"	no-diff
ip extcommunity-list expanded list_abc seq 10 permit "1:1 "	ip extcommunity-list expanded list_abc seq 10 permit "1:1"	no-diff
ip large-community-list expanded list_abc seq 10 permit "1:1:1 "	ip large-community-list expanded list_abc seq 10 permit "1:1:1"	no-diff
ip as-path access-list list_abc seq 10 permit "1 "	ip as-path access-list list_abc seq 10 permit "1"	no-diff

## 候補構成の完全性チェックの実行

完全性チェックを実行するには、次のコマンドを実行します。

始める前に



(注) 完全性チェックを実行する前に、実行構成と候補構成が同じイメージバージョンに属していることを確認してください。

### 手順の概要

1. **show diff running-config file\_url [unified] [merged]**
2. **show diff startup-config file\_url [ unified ]**

## ■ 完全性チェックの例

## 手順の詳細

## 手順

	コマンドまたはアクション	目的
ステップ1	<b>show diff running-config</b> <i>file_url</i> [ <b>unified</b> ] [ <b>merged</b> ] 例： <pre>switch# show diff running-config bootflash:candidate.cfg partial unified</pre>	実行構成とユーザーが指定した候補構成の違いを表示します。 <ul style="list-style-type: none"> <li>• <i>file_url</i> : と比較するファイルのパス。</li> <li>• <b>unified</b> : 実行構成とユーザー構成の違いを統一された形式で表示します。</li> <li>• <b>merged</b> : <b>merged</b> サブコマンドを置き換えるのではなくマージする必要がある場合にのみ入力します。</li> </ul>
ステップ2	<b>show diff startup-config</b> <i>file_url</i> [ <b>unified</b> ] 例： <pre>switch# show diff startup-config bootflash:candidate.cfg unified</pre>	スタートアップ構成とユーザーが指定した候補構成の違いを表示します。 <ul style="list-style-type: none"> <li>• <i>file_url</i> : と比較するファイルのパス。</li> <li>• <b>unified</b> : スタートアップ構成とユーザー構成の違いを統一された形式で表示します。</li> </ul>

## 完全性チェックの例

## 実行構成と候補構成の間に相違点はない

```
switch# show diff running-config bootflash:base_running.cfg
switch#
```

## 実行構成と候補構成の間の相違点

```
switch# show diff running-config bootflash:modified-running.cfg unified
--- running-config
+++ User-config
@@ -32,11 +32,11 @@
 
 interface Ethernet1/1
     mtu 9100
     link debounce time 0
     beacon
-    ip address 2.2.2.2/24
+    ip address 1.1.1.1/24
     no shutdown
 
 interface Ethernet1/2
 
 interface Ethernet1/3
switch#
```

### 実行構成と部分候補構成の間の相違点

```

switch# show file bootflash:intf_vlan.cfg
interface Vlan101
  no shutdown
  no ip redirects
  ip address 1.1.2.1/24 secondary
  ip address 1.1.1.1/24
switch#
switch# show diff running-config bootflash:intf_vlan.cfg partial unified
--- running-config
+++ User-config
@@ -3897,10 +3883,14 @@
  mtu 9100
  ip access-group IPV4_EDGE in
  ip address 2.2.2.12/26 tag 54321

  interface Vlan101
+ no shutdown
+ no ip redirects
+ ip address 1.1.2.1/24 secondary
+ ip address 1.1.1.1/24

  interface Vlan102
    description Vlan102
    no shutdown
    mtu 9100
switch#

```

### 部分的な構成の差分がマージされた

```

switch# show file po.cfg
interface port-channel500
description po-123
switch#
switch# sh run int po500

!Command: show running-config interface port-channel1500
!Running configuration last done at: Fri Sep 29 12:27:28 2023
!Time: Fri Sep 29 12:30:24 2023

version 10.4(2) Bios:version 07.69

interface port-channel500
  ip address 192.0.2.0/24
  ipv6 address 2001:DB8:0:ABCD::1/48

switch#
switch# show diff running-config po.cfg partial merged unified
--- running-config
+++ User-config
@@ -124,10 +110,11 @@
interface port-channel100
  interface port-channel500
    ip address 192.0.2.0/24
    ipv6 address 2001:DB8:0:ABCD::1/48
+ description po-123
  interface port-channel4096
  interface Ethernet1/1
switch#

```

## ■ 完全性チェックの例



# 第 26 章

## ユーザ アカウントおよび RBAC の設定

この章は、次の項で構成されています。

- ユーザ アカウントと RBAC について, [on page 367](#)
- ユーザー アカウントの注意事項および制約事項, [on page 371](#)
- ユーザ アカウントの設定, [on page 371](#)
- RBAC の設定 (373 ページ)
- ユーザー アカウントと RBAC の設定の確認, [on page 378](#)
- ユーザー アカウントおよび RBAC のデフォルト設定, [on page 378](#)

### ユーザ アカウントと RBAC について

Cisco Nexus 3600 プラットフォームスイッチは、ロールベースアクセスコントロール (RBAC) を使用して、ユーザーがスイッチにログインするときに各ユーザー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ー ロールを定義し、各ユーザー ロールがどの管理操作を実行できるかを指定します。スイッチのユーザー アカウントを作成するとき、そのアカウントにユーザー ロールを関連付けます。これにより個々のユーザー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

ユーザー ロールには、そのロールを割り当てられたユーザーが実行できる操作を定義するルールが含まれています。各ユーザー ロールに複数のルールを含めることができます。各ユーザー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ーは、設定操作とデバッグ操作にアクセスできます。特定の VLAN やインターフェイスだけに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 ユーザー ロールが用意されています。

#### network-admin (スーパーユーザー)

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。

**network-operator**

スイッチに対する完全な読み取りアクセス権。

**Note**

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 ロール B 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。

## 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コマンドです。次の制御パラメータは機能です。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、機能グループです。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。

## ユーザー ロール ポリシー

ユーザー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と VLAN へのアクセスを制限するために、ユーザー 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ルールで制約されます。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構成しないと、ユーザー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）へのアクセスを許可した場合、ユーザーがそのユーザーに関連付けられたユーザー ロール ポリシーに含まれていなくても、ユーザーはこれらのリソースへのアクセスを許可されます。

## ユーザー アカウントの設定の制限事項

次の語は予約済みであり、ユーザー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
- shutdown
- sync
- sys
- uucp
- xfs

## ■ ユーザ パスワードの要件



## 注意

Cisco Nexus 3600 プラットフォーム スイッチでは、すべて数字のユーザー名が 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ー名はサポートされません。AAA サーバに数字だけのユーザー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 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。



## (注)

Cisco NX-OS Release 7.2(0)N1(1) 以降、Cisco Nexus デバイスのパスワードには、ドル記号 (\$) やパーセント記号 (%) などの特殊文字を使用できます。



## (注)

Cisco Nexus デバイスのパスワードには、ドル記号 (\$) やパーセント記号 (%) などの特殊文字を使用できます。

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。各ユーザー 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。

## ユーザー アカウントの注意事項および制約事項

ユーザー アカウントおよび RBAC を設定する場合、ユーザー 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。

- ユーザ ロールに設定された読み取り/書き込みルールに関係なく、一部のコマンドは、あらかじめ定義された network-admin ロールでのみ実行できます。
- 最大 256 個のルールをユーザー ロールに追加できます。
- 最大 64 個のユーザー ロールをユーザー アカウントに割り当てることができます。
- 1 つのユーザー ロールを複数のユーザー アカウントに割り当てることができます。
- network-admin および network-operator などの事前定義されたロールは編集不可です。



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

## ユーザー アカウントの設定



**Note** ユーザー アカウントの属性に加えられた変更は、そのユーザー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。

ユーザー名の最初の文字として、任意の英数字または \_ (アンダースコア) を使用できます。最初の文字にその他の特殊文字を使用することはできません。ユーザー名に許可されていない文字が含まれている場合、指定したユーザーはログインできません。

### SUMMARY STEPS

1. switch# **configure terminal**
2. (Optional) switch(config)# **show role**
3. switch(config) # **username user-id [password password] [expire date] [role role-name]**
4. switch(config) # **exit**
5. (Optional) switch# **show user-account**
6. (Optional) switch# **copy running-config startup-config**

## ユーザ アカウントの設定

## DETAILED STEPS

## Procedure

	Command or Action	Purpose
ステップ 1	switch# <b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	(Optional) switch(config)# <b>show role</b>	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) # <b>username user-id [password password] [expire date] [role role-name]</b>	<p>ユーザ アカウントを設定します。</p> <p>値は、<i>user-id</i> 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。</p> <p>デフォルトの パスワード は、未定義です。</p> <p><b>Note</b></p> <p>パスワードを指定しなかった場合、ユーザーはスイッチにログインできない場合があります。</p> <p><b>Note</b></p> <p>リリース 7.0 (3) F3 (1) 以降では、パスワード強度をチェックするための新しい内部関数が実装されています。</p> <p>値は、<b>expire date</b> オプションのフォーマットは YYYY-MM-DD です。デフォルトでは、失効日はありません。</p>
ステップ 4	switch(config) # <b>exit</b>	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	(Optional) switch# <b>show user-account</b>	ロール設定を表示します。
ステップ 6	(Optional) switch# <b>copy running-config startup-config</b>	実行 コンフィギュレーション 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。

## Example

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
```

次の例は、リリース 7.0 (3) F3 (1) 以降のパスワード強度チェックを有効にする基準を示しています。

```

switch(config)# username xyz password nbv12345
password is weak
Password should contain characters from at least three of the following classes: lower
case letters, upper case letters, digits and special characters.
switch(config)# username xyz password Nbv12345
password is weak
it is too simplistic/systematic
switch(config)#

```

## RBAC の設定

### ユーザ ロールおよびルールの作成

指定したルール番号は、ルールが適用される順番を決定します。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。

#### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config) # **role name role-name**
3. switch(config-role) # **rule number {deny | permit} command command-string**
4. switch(config-role) # **rule number {deny | permit} {read | read-write}**
5. switch(config-role) # **rule number {deny | permit} {read | read-write} feature feature-name**
6. switch(config-role) # **rule number {deny | permit} {read | read-write} feature-group group-name**
7. (Optional) switch(config-role) # **description text**
8. switch(config-role) # **end**
9. (Optional) switch# **show role**
10. (Optional) switch# **copy running-config startup-config**

#### DETAILED STEPS

##### Procedure

	<b>Command or Action</b>	<b>Purpose</b>
ステップ1	switch# <b>configure terminal</b>	グローバル コ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) # <b>role name role-name</b>	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。 値は、 <i>role-name</i> 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) # <b>rule number {deny   permit} command command-string</b>	コマンド ルールを設定します。

## ユーザ ロールおよびルールの作成

	Command or Action	Purpose
		値は、 <i>command-string</i> 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)# <b>rule number {deny   permit} {read   read-write}</b>	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)# <b>rule number {deny   permit} {read   read-write} feature feature-name</b>	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。 <b>show role feature</b> 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)# <b>rule number {deny   permit} {read   read-write} feature-group group-name</b>	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。 <b>show role feature-group</b> コマンドを使用して、機能グループのリストを表示します。 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	(Optional) switch(config-role)# <b>description text</b>	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)# <b>end</b>	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	(Optional) switch# <b>show role</b>	ユーザ ロールの設定を表示します。
ステップ 10	(Optional) switch# <b>copy running-config startup-config</b>	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。

## Example

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

## SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config) # **role feature-group** *group-name*
3. switch(config) # **exit**
4. (Optional) switch# **show role feature-group**
5. (Optional) switch# **copy running-config startup-config**

## DETAILED STEPS

### Procedure

	<b>Command or Action</b>	<b>Purpose</b>
ステップ 1	switch# <b>configure terminal</b>	グローバル コ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) # <b>role feature-group</b> <i>group-name</i>	ユーザー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。 [ <i>group-name</i> 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) # <b>exit</b>	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	(Optional) switch# <b>show role feature-group</b>	ロール機能グループ設定を表示します。
ステップ 5	(Optional) switch# <b>copy running-config startup-config</b>	リブートおよびリスト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。

### Example

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 ポリシーの変更

ユーザー ロール インターフェイス ポリシーを変更することで、ユーザー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。

## SUMMARY STEPS

1. **switch# configure terminal**
2. **switch(config) # role name *role-name***
3. **switch(config-role) # interface policy deny**
4. **switch(config-role-interface) # permit interface *interface-list***
5. **switch(config-role-interface) # exit**
6. (Optional) **switch(config-role) # show role**
7. (Optional) **switch(config-role) # copy running-config startup-config**

## DETAILED STEPS

### Procedure

	Command or Action	Purpose
ステップ 1	<b>switch# configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>switch(config) # role name <i>role-name</i></b>	ユーザー 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	<b>switch(config-role) # interface policy deny</b>	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	<b>switch(config-role-interface) # permit interface <i>interface-list</i></b>	<p>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。</p> <p>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。</p> <p>このコマンドでは、イーサネットインターフェイスを指定できます。</p>
ステップ 5	<b>switch(config-role-interface) # exit</b>	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	(Optional) <b>switch(config-role) # show role</b>	ロール 設定を表示します。
ステップ 7	(Optional) <b>switch(config-role) # copy running-config startup-config</b>	実行 コンフィギュレーション 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。

**Example**

次に、ユーザーがアクセスできるインターフェイスを制限するために、ユーザー 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 fc 3/1
switch(config-role-interface)# permit interface vfc 30/1
```

## ユーザ ロール VLAN ポリシーの変更

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

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config) # **role name role-name**
3. switch(config-role) # **vlan policy deny**
4. switch(config-role-vlan) # **permit vlan vlan-list**
5. switch(config-role-vlan) # **exit**
6. (Optional) switch# **show role**
7. (Optional) switch# **copy running-config startup-config**

### DETAILED STEPS

**Procedure**

	<b>Command or Action</b>	<b>Purpose</b>
ステップ 1	switch# <b>configure terminal</b>	グローバル コ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) # <b>role name role-name</b>	ユーザー 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) # <b>vlan policy deny</b>	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) # <b>permit vlan vlan-list</b>	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。

## ■ ユーザー アカウントと RBAC の設定の確認

	Command or Action	Purpose
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	(Optional) switch# <b>show role</b>	ロール設定を表示します。
ステップ 7	(Optional) switch# <b>copy running-config startup-config</b>	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。

## ユーザー 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。

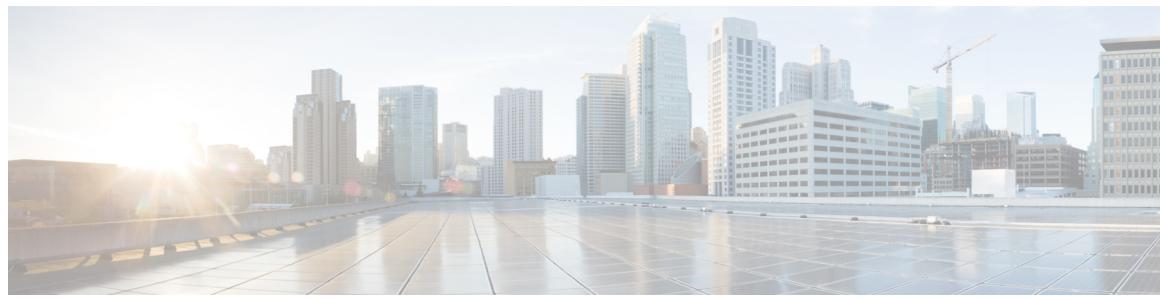
コマンド	目的
<b>show role [role-name]</b>	ユーザー ロールの設定を表示します。
<b>show role feature</b>	機能リストを表示します。
<b>show role feature-group</b>	機能グループの設定を表示します。
<b>show startup-config security</b>	スタートアップコンフィギュレーションのユーザ アカウント設定を表示します。
<b>show running-config security [all]</b>	実行コンフィギュレーションのユーザ アカウント設定を表示します。 <b>all</b> 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。
<b>show user-account</b>	ユーザ アカウント情報を表示します。

## ユーザー アカウントおよび RBAC のデフォルト設定

次の表に、ユーザー 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。

Table 30: デフォルトのユーザー アカウントおよび RBAC パラメータ

パラメータ	デフォルト
ユーザ アカウント パスワード	未定義。
ユーザー 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にアクセス可能。
VLAN ポリシー	すべての VLAN にアクセス可能。



## 索引

### C

Call Home の通知 **135**  
  syslog の XML 形式 **135**  
  syslog のフルテキスト形式 **135**  
clear logging logfile **101**  
clear logging nvram **101**  
clear logging onboard **240**  
configure maintenance profile maintenance-mode **306**  
configure maintenance profile normal-mode **307**

### E

EEE **199**  
  注意事項と制約事項 **199**  
EEM ポリシーの定義 **208**  
  VSH スクリプト **208**  
EEM **196–198, 200–201, 203, 206, 209–210, 212, 233**  
  syslog スクリプト **212**  
  VSH スクリプト ポリシー **198**  
  VSH スクリプト **209**  
    登録およびアクティブ化 **209**  
  アクション文 **197**  
  アクション文、設定 **206**  
  イベント文 **197**  
  イベント文、設定 **203**  
  システム ポリシー、上書き **210**  
  その他の参考資料 **233**  
  デフォルト設定 **200**  
  ポリシー **196**  
  ユーザー ポリシー、定義 **201**  
  ライセンス **198**  
  環境変数の定義 **200**  
  前提条件 **198**  
ERSPAN **259–260, 264, 279, 281**  
  セッション **260**  
    multiple **260**  
  デフォルト パラメータ **264**  
  概要 **259**  
  関連資料 **281**  
  高可用性 **260**  
  前提条件 **260**

### ERSPAN (続き)

  送信元 **259, 279**  
    設定例 **279**  
  送信元セッション **264**  
    ERSPAN の設定 **264**  
  送信元セッションの設定 **264**

### G

GOLD 診断 **189–190**  
  ヘルス モニタリング **190**  
  ランタイム **189**  
  拡張モジュール **190**  
  構成 **190**

### H

hw-module logging onboard counter-stats **237**  
hw-module logging onboard cpuhog **238**  
hw-module logging onboard environmental-history **238**  
hw-module logging onboard error-stats **238**  
hw-module logging onboard interrupt-stats **238**  
hw-module logging onboard module **238**  
hw-module logging onboard obfl-logs **239**  
hw-module logging onboard **237**

### I

ID **114**  
  シリアル ID **114**  
isolate **304**

### L

linkDown 通知 **174–175**  
linkUp 通知 **174–175**  
logging console **85**  
logging event {link-status | trunk-status} {enable | default} **89**  
logging level **90, 92**  
logging logfile **88**  
logging message interface type ethernet description **87**  
logging module **90**  
logging monitor **86**

logging origin-id 87  
 logging server 94, 96  
 logging source-interface Loopback 95  
 logging timestamp {microseconds | milliseconds | seconds} 92

**N**

no isolate 304  
 no shutdown 304  
 no system interface shutdown 305  
 no system mode maintenance dont-generate-profile 316  
 no system mode maintenance on-reload reset-reason 314  
 no system mode maintenance 316  
 NTP ブロードキャストサーバ、設定 70  
 NTP マルチキャストクライアント、設定 72  
 NTP マルチキャストサーバ、設定 71  
 ntp 57, 59  
 仮想化 59  
 情報 57

**P**

PTP 45–47, 49–50, 52  
 インターフェイス、設定 52  
 グローバル設定 50  
 デバイス タイプ 46  
 デフォルト設定 49  
 プロセス 47  
 概要 45  
 python instance 305

**R**

RBAC 367–369, 371, 373, 375–378  
 ルール 368  
 ユーザ ロール 367  
 ユーザ ロールおよびルール、設定 373  
 ユーザー アカウント、設定 371  
 ユーザー アカウントの制限事項 369  
 ユーザー ロール VLAN ポリシー、変更 377  
 ユーザー ロールインターフェイス ポリシー、変更 376  
 確認 378  
 機能グループ、作成 375

**S**

scheduler 141–146, 148–149, 151–152, 154  
 ジョブ、削除 148  
 タイムテーブル、定義 149  
 デフォルト設定 143  
 リモート ユーザー認証、設定 145–146  
 リモート ユーザ認証 142

scheduler (続き)  
 ログ ファイル サイズ、定義 144  
 ログ ファイル 142  
 ログ ファイル、消去 151  
 概要 141  
 規格 154  
 設定、確認 152  
 注意事項と制約事項 142  
 ディセーブル化 152  
 有効化 143  
 Session Manager 105, 107–108  
 ACL セッションの設定例 108  
 ガイドライン 105  
 セッションのコミット 107  
 セッションの確認 107  
 セッションの廃棄 108  
 セッションの保存 107  
 構成の確認 108  
 制限事項 105  
 説明 105  
 sFlow 289–292, 294–299, 301  
 show コマンド 301  
 アナライザ ポート 297  
 アナライザのアドレス 296  
 エージェント アドレス 298  
 ガイドライン 290  
 カウンタのポーリング間隔 294  
 サンプリング データ ソース 299  
 サンプリング レート 292  
 データ グラム サイズ 295  
 デフォルト設定 291  
 設定例 301  
 前提条件 290  
 show interface brief 318  
 show logging console 86, 102  
 show logging info 89, 102  
 show logging last 101–102  
 show logging level 91, 102  
 show logging logfile end-time 101–102  
 show logging logfile start-time 101–102  
 show logging logfile 101–102  
 show logging module 90, 102  
 show logging monitor 86, 102  
 show logging nvram last 101–102  
 show logging nvram 101–102  
 show logging onboard boot-uptime 239  
 show logging onboard counter-stats 239  
 show logging onboard credit-loss 239  
 show logging onboard device-version 239  
 show logging onboard endtime 239  
 show logging onboard environmental-history 239  
 show logging onboard error-stats 239

show logging onboard exception-log 239  
 show logging onboard interrupt-stats 239  
 show logging onboard module 239  
 show logging onboard obfl-history 239  
 show logging onboard obfl-logs 239  
 show logging onboard stack-trace 240  
 show logging onboard starttime 240  
 show logging onboard status 240  
 show logging onboard 239  
 show logging origin-id 88, 102  
 show logging server 95–96, 102  
 show logging timestamp 92, 102  
 show maintenance on-reload reset-reasons 318  
 show maintenance profile maintenance-mode 306, 318  
 show maintenance profile normal-mode 308, 318  
 show maintenance profile 318  
 show maintenance timeout 318  
 show running-config mmode 318  
 show snapshots compare 309, 318  
 show snapshots dump 318  
 show snapshots sections 319  
 show snapshots 309, 318  
 show startup-config mmode 318  
 show system mode 314, 316, 319  
 show コマンド 301  
 sFlow 301  
 show コマンドの追加、アラート グループ 127  
     smart call home 127  
 シヤットダウン 304  
 sleep instance 305  
 Smart Call Home のメッセージ 110, 113  
     フォーマット オプション 110  
     レベルの構成 113  
 smart call home 109–111, 119–121, 123–124, 126–127, 129–134  
     show コマンドの追加、アラート グループ 127  
         アラート グループ 111  
         アラート グループのアソシエート 126  
         デフォルト設定 120  
         メッセージ フォーマット オプション 110  
         宛先プロファイル 110  
         宛先プロファイル、作成 123  
         確認 134  
         重複メッセージ抑制、ディセーブル化 131–132  
         接続先プロファイル、変更 124  
         設定のテスト 133  
         説明 109  
         前提条件 119  
         担当者情報、設定 121  
         注意事項と制約事項 119  
         定期的なインベントリ通知 130  
         電子メールの詳細、設定 129  
         登録 120

SMU 339–342, 345–348  
     アクティブなパッケージ セットのコミット 346  
     ガイドライン 341  
     パッケージインストールの準備 342  
     パッケージのアクティブ化 345  
     パッケージの削除 347  
     パッケージの追加 345  
     パッケージの非アクティブ化 347  
     パッケージ管理 340  
     制限事項 341  
     説明 339  
     前提条件 341  
 snapshot create 309  
 snapshot delete 309  
 SNMP のデフォルト設定 161  
 SNMP 通知 169  
     VRF に基づくフィルタリング 169  
 SNMP 通知レシーバ 168  
     VRF による設定 168  
 SNMP 要求のフィルタリング 166  
 SNMP 155–156, 158–161, 163, 165–167, 170, 177–178  
     CLI を使用したユーザの同期 159  
     アクセス グループ 160  
     インバンドアクセス 170  
     グループベースのアクセス 160  
     セキュリティ モデル 158  
     デフォルト設定 161  
     トランプ通知 156  
     バージョン 3 のセキュリティ機能 156  
     メッセージの暗号化 165  
     ユーザベースのセキュリティ 158  
         SNMP 158  
         ユーザーの構成 163  
         ローカル engineID の設定 177  
         機能の概要 155  
         注意事項と制約事項 160  
         通知レシーバ 167  
         無効化 178  
         要求のフィルタリング 166  
 snmp-server name 163  
 SNMP (簡易ネットワーク管理プロトコル) 157  
     バージョン 157  
 SNMPv3 156, 166  
     セキュリティ機能 156  
     複数のロールの割り当て 166  
 SPAN 送信元 244  
     出力 244  
     入力 244  
 SPAN 243–245, 247, 249–255  
     VLAN、設定 251  
     イーサネット宛先ポート、設定 247

## SPAN (続き)

セッションのアクティブ化 **253**ソフトウェアのダウングレード時の設定の損失 **245**モニタリングの送信元 **243**レート制限、設定 **250**宛先 **245**作成、セッションの削除 **247**出力送信元 **244**情報の表示 **254**接続先ポート、特性 **245**設定例 **255**説明、設定 **252**送信元ポート チャネル、設定 **251**送信元ポート、設定 **249**注意事項と制約事項 **245**特性、送信元ポート **244**入力送信元 **244**syslog **212**組み込みイベントマネージャ (EEM) **212**system interface shutdown **304**system mode maintenance dont-generate-profile **313**system mode maintenance on-reload reset-reason **314**

## T

terminal monitor **85**

## V

VRF **168-169**SNMP 通知のフィルタリング **169**SNMP 通知レシーバの設定 **168**VSH スクリプト ポリシー **198, 209**EEM **198**登録およびアクティブ化 **209**VSH スクリプト **208**EEM ポリシーの定義 **208**

## あ

アクション文 **197**EEM **197**アクション文、設定 **206**組み込みイベントマネージャ (EEM) **206**アナライザポート **297**sFlow **297**アナライザのアドレス **296**sFlow **296**アラート グループ **111**smart call home **111**アラート グループのアソシエート **126**smart call home **126**

## い

イーサネット宛先ポート、設定 **247**SPAN **247**イベント文 **197**EEM **197**イベント文、設定 **203**組み込みイベントマネージャ (EEM) **203**インストール ログ情報の表示 **348**インターフェイス、設定 **52**PTP **52**インターフェイスでのNTP、イネーブル化およびディセーブル化 **61**

## え

エージェント アドレス **298**sFlow **298**

## か

ガイドライン **290**sFlow **290**カウンタのポーリング間隔 **294**sFlow **294**

## こ

コミット **75**NTP 設定変更 **75**

## さ

サーバー ID **114**説明 **114**サンプリング データ ソース **299**sFlow **299**サンプリング レート **292**sFlow **292**

## し

システム ポリシー、上書き **210**組み込みイベントマネージャ (EEM) **210**システムモードメンテナンスシャットダウン **313**システムモードメンテナンスタイムアウト **313**ジョブ スケジュール、表示 **153**例 **153**

ジョブ、削除 **148**  
 scheduler **148**  
 シリアル ID **114**  
 説明 **114**

## す

スイッチプロファイルバッファ、表示 **35, 43**  
 スイッチプロファイル **21, 35–36, 41–43**  
 バッファ、表示 **35, 43**  
 リブート後のコンフィギュレーションの同期 **36**  
 確認とコミット、表示 **42**  
 実行コンフィギュレーション、表示 **41**  
 注意事項と制約事項 **21**  
 例、ローカルとピアの同期 **41, 43**  
 スイッチドポートアナライザ **243**  
 スケジューラジョブ、スケジューリング **153**  
 例 **153**  
 スケジューラジョブ、結果の表示 **154**  
 例 **154**  
 スケジューラジョブ、作成 **153**  
 例 **153**

## せ

セッションのアクティブ化 **253**  
 SPAN **253**  
 セッションの実行 **107**

## そ

その他の参考資料 **233**  
 EEM **233**  
 ソフトウェア **245**  
 ダウングレード **245**  
 SPAN構成の損失 **245**  
 ソフトウェアのダウングレード **245**  
 SPAN構成の損失 **245**

## た

タイムテーブル、定義 **149**  
 scheduler **149**

## て

ディスカーディング **76**  
 NTP設定変更 **76**  
 無効化 **152**  
 スケジューラ **152**

データグラムサイズ **295**  
 sFlow **295**  
 デバイスID **114**  
 Call Homeの形式 **114**  
 デフォルトパラメータ **264**  
 ERSPAN **264**  
 デフォルト設定 **60, 108, 120, 143, 200, 291**  
 EEM **200**  
 scheduler **143**  
 sFlow **291**  
 smart call home **120**  
 ロールバック **108**

## と

トラップ通知 **156**

## は

パスワード要件 **370**

## へ

ヘルスモニタリング診断 **190**  
 情報 **190**

## ほ

ポリシー **196**  
 組み込みイベントマネージャ(EEM) **196**

## め

メッセージの暗号化 **165**  
 SNMP **165**

## ゆ

ユーザーロール **367**  
 RBAC **367**  
 ユーザーロールおよびルール、作成 **373**  
 RBAC **373**  
 ユーザーアカウントの制限事項 **369**  
 RBAC **369**  
 ユーザーポリシー、定義 **201**  
 組み込みイベントマネージャ(EEM) **201**  
 ユーザーロールVLANポリシー、変更 **377**  
 RBAC **377**  
 ユーザーロールインターフェイスポリシー、変更 **376**  
 RBAC **376**

ユーザー **367**  
 説明 **367**  
 ユーザーアカウント **370–371, 378**  
 パスワード **370**  
 確認 **378**  
 注意事項と制約事項 **371**

ら

ライセンス **198**  
 EEM **198**  
 ランタイム診断 **189**  
 情報 **189**

り

リブート後のコンフィギュレーションの同期 **36**  
 スイッチプロファイル **36**  
 リモートユーザー認証、設定 **145–146**  
 scheduler **145–146**  
 リモートユーザー認証 **142**  
 scheduler **142**

る

rules **368**  
 RBAC **368**

れ

レート制限、設定 **250**  
 SPAN **250**

ろ

ロール **367**  
 認証 **367**  
 ロールバック **105, 108**  
 ガイドライン **105**  
 チェック ポイントのコピー **105**  
 チェック ポイント コピーの作成 **105**  
 チェック ポイント ファイルの削除 **105**  
 チェック ポイント ファイルへの復帰 **105**  
 デフォルト設定 **108**  
 ロールバックの実装 **105**  
 構成の確認 **108**  
 高可用性 **105**  
 制限事項 **105**  
 設定例 **105**  
 説明 **105**  
 ログ ファイル サイズ、定義 **144**  
 scheduler **144**  
 ログ ファイル **142**  
 scheduler **142**  
 ログ ファイル、消去 **151**  
 scheduler **151**

## 翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。