



## **Cisco Nexus 3548 スイッチ NX-OS システム管理構成ガイド、リリース 10.6 (x)**

最終更新：2025 年 12 月 9 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、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 xvii

対象読者 xvii

表記法 xvii

Cisco Nexus 3500 シリーズ 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 xviii

通信、サービス、およびその他の情報 xviii

---

#### 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 6

サポートされるプラットフォーム 6

---

#### 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

**PTP の設定 17**

PTP に関する情報 17

PTP 時間分配保留 18

PTP デバイス タイプ 19

    クロック モード 20

PTP プロセス 20

PTP のハイ アベイラビリティ 21

PTP の注意事項および制約事項 21

PTP のデフォルト設定 23

PTP の設定 23

    PTP のグローバルな設定 23

    インターフェイスでの PTP の設定 26

    PTP 混合モード 28

    複数の PTP ドメインの設定 28

    PTP グランドマスター クロックの設定 31

    インターフェイスでの PTP コストの設定 33

    クロック ID の設定 34

    PTP インターフェイスがマスター ステートを維持する設定 35

    タイムスタンプ タギング 37

        タイムスタンプ タギングの構成 37

        TTAG マーカー パケットと時間間隔の構成 38

    PTP 設定の確認 41

---

第 5 章

**NTP の設定 43**

NTP の概要 43

時間サーバとしての NTP 44

CFS を使用した NTP の配信 44

クロック マネージャ 44

仮想化のサポート 45

NTP の注意事項と制約事項	45
デフォルト設定	46
NTP の設定	46
NTP サーバーおよびピアの構成	46
NTP 認証の設定	48
NTP アクセス制限の設定	50
NTP ソース IP アドレスの設定	52
NTP ソース インターフェイスの設定	52
NTP ログインの設定	53
NTP 用の CFS 配信のイネーブル化	54
NTP 構成変更のコミット	55
NTP 設定変更の廃棄	56
CFS セッション ロックの解放	57
NTP の設定確認	57
NTP の設定例	59
NTP の関連資料	60
NTP 機能の履歴	60

---

## 第 6 章

システムメッセージロギングの設定	61
システム メッセージ ロギングの概要	61
Syslogサーバ	62
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	62
システム メッセージ ロギングのデフォルト設定	63
システム メッセージ ロギングの設定	63
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	63
ファイルへのシステム メッセージ ロギングの設定	66
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	68
ロギング タイムスタンプの設定	70
RFC 5424 に準拠したロギング syslog の構成	71
syslog サーバの設定	72
UNIX または Linux システムでの syslog の設定	74

syslog サーバー設定の配布の設定	75
ログ ファイルの表示およびクリア	76
DOM ロギングの構成	78
DOM ロギングの有効化	78
DOM ロギングの無効化	78
DOM ロギング構成の確認	79
システム メッセージ ロギングの設定確認	79
繰り返されるシステム ロギング メッセージ	80

## 第 7 章

**Smart Call Home の設定 81**

Smart Call Home に関する情報	81
Smart Call Home の概要	82
Smart Call Home 宛先プロファイル	82
Smart Call Home アラート グループ	83
Smart Call Home のメッセージ レベル	85
Call Home のメッセージ形式	86
Smart Call Home の注意事項および制約事項	91
Smart Call Home の前提条件	91
Call Home のデフォルト設定	91
Smart Call Home の設定	92
Smart Call Home の登録	92
連絡先情報の設定	93
宛先プロファイルの作成	95
宛先プロファイルの変更	96
アラート グループと宛先プロファイルのアソシエート	98
アラート グループへの show コマンドの追加	99
電子メール サーバーの詳細の設定	100
定期的なインベントリ通知の設定	102
重複メッセージ抑制のディセーブル化	103
Smart Call Home のイネーブル化またはディセーブル化	104
Smart Call Home 設定のテスト	105

Smart Call Home 設定の確認	106
フルテキスト形式での syslog アラート通知の例	106
XML 形式での syslog アラート通知の例	107

---

**第 8 章**

<b>Session Manager の設定</b>	<b>111</b>
Session Manager の概要	111
Session Manager の注意事項および制約事項	111
Session Manager の設定	112
セッションの作成	112
セッションでの ACL の設定	112
セッションの確認	113
セッションのコミット	113
セッションの保存	114
セッションの廃棄	114
Session Manager のコンフィギュレーション例	114
Session Manager 設定の確認	114

---

**第 9 章**

<b>スケジューラの設定</b>	<b>117</b>
スケジューラの概要	117
リモート ユーザ認証	118
スケジューラ ログ ファイル	118
スケジューラの注意事項および制約事項	118
スケジューラのデフォルト設定	119
スケジューラの設定	119
スケジューラのイネーブル化	119
スケジューラ ログ ファイル サイズの定義	120
リモート ユーザ認証の設定	121
ジョブの定義	122
ジョブの削除	123
タイムテーブルの定義	124
スケジューラ ログ ファイルの消去	126

スケジューラのディセーブル化	127
スケジューラの設定確認	127
スケジューラの設定例	128
スケジューラ ジョブの作成	128
スケジューラ ジョブのスケジューリング	128
ジョブ スケジュールの表示	128
スケジューラ ジョブの実行結果の表示	129
スケジューラの標準	129

## 第 10 章

**SNMP の設定 131**

SNMP に関する情報	131
SNMP 機能の概要	131
SNMP 通知	132
SNMPv3	132
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	133
ユーザベースのセキュリティ モデル	134
CLI および SNMP ユーザの同期	135
グループベースの SNMP アクセス	136
SNMP の注意事項および制約事項	136
SNMP のデフォルト設定	137
SNMP の設定	137
SNMP ユーザの設定	137
SNMP メッセージ暗号化の適用	139
SNMPv3 ユーザに対する複数のロールの割り当て	139
SNMP コミュニティの作成	139
SNMP 要求のフィルタリング	140
SNMP 通知レシーバの設定	140
VRF を使用する SNMP 通知レシーバの設定	142
VRF に基づく SNMP 通知のフィルタリング	143
インバンド アクセスのための SNMP の設定	143
SNMP 通知のイネーブル化	145

リンクの通知の設定	147
インターフェイスでのリンク通知のディセーブル化	148
TCP での SNMP に対するワнтаイム認証のイネーブル化	149
SNMP スイッチの連絡先および場所の情報の割り当て	149
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	150
SNMP のディセーブル化	151
SNMP 設定の確認	151
その他の参考資料	152

---

## 第 11 章

### **RMON の設定** 153

RMON について	153
RMON アラーム	153
RMON イベント	154
RMON の設定時の注意事項および制約事項	155
RMON の設定	155
RMON アラームの設定	155
RMON イベントの設定	156
RMON 設定の確認	157
デフォルトの RMON 設定	157

---

## 第 12 章

### **オンライン診断の設定** 159

オンライン診断について	159
ブートアップ診断	159
ヘルス モニタリング診断	160
拡張モジュール診断	161
オンライン診断の注意事項と制約事項	162
オンライン診断の設定	162
オンライン診断設定の確認	163
オンライン診断のデフォルト設定	163

---

## 第 13 章

### **Embedded Event Manager の設定** 165

組み込みイベント マネージャについて	165
Embedded Event Manager ポリシー	166
イベント文	167
アクション文	168
VSH スクリプト ポリシー	168
Embedded Event Manager の前提条件	169
Embedded Event Manager の注意事項および制約事項	169
Embedded Event Manager のデフォルト設定	170
環境変数の定義	170
CLI によるユーザ ポリシーの定義	171
イベント文の設定	173
アクション文の設定	176
VSH スクリプトによるポリシーの定義	179
VSH スクリプト ポリシーの登録およびアクティブ化	179
システム ポリシーの上書き	180
EEM パブリッシャとしての syslog の設定	182
イベント ログの自動収集とバックアップ	183
拡張ログ ファイルの保持	183
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	183
すべてのサービスの拡張ログ ファイル保持の無効化	184
単一サービスの拡張ログファイル保持の有効化	185
拡張ログ ファイルの表示	187
単一サービスに対する拡張ログファイル保持の無効化	187
トリガーベースのイベント ログの自動収集	189
トリガーベースのログ ファイルの自動収集の有効化	189
自動収集 YAML ファイル	189
コンポーネントあたりの自動収集の量の制限	192
自動収集ログ ファイル	193
トリガーベースのログ収集の確認	196
トリガーベースのログ ファイル生成の確認	197
ローカル ログ ファイルのストレージ	197

最近のログ ファイルのローカル コピーの生成	197
外部ログ ファイルのストレージ	200

---

**第 14 章****SPAN の設定 203**

SPAN について	203
SPAN の注意事項および制約事項	204
SPAN 送信元	204
送信元ポートの特性	204
SPAN 宛先	205
宛先ポートの特性	205
SPAN および ERSPAN フィルタ処理	205
SPAN および ERSPAN フィルタ処理の注意事項および制限事項	206
SPAN および ERSPAN 制御パケットのフィルタ処理	207
SPAN および ERSPAN サンプリング	207
SPAN および ERSPAN サンプリングの注意事項および制限事項	207
SPAN および ERSPAN の切り捨て	208
SPAN および ERSPAN 切り捨ての注意事項および制限事項	208
SPAN セッションの作成または削除	208
イーサネット宛先ポートの設定	209
送信元ポートの設定	211
送信元ポート チャンネルまたは VLAN の設定	211
SPAN セッションの説明の設定	212
SPAN セッションのアクティブ化	213
SPAN セッションの一時停止	214
SPAN フィルタの構成	214
SPAN サンプリングの構成	216
SPAN 切り捨ての設定	217
SPAN 情報の表示	219

---

**第 15 章****ワープ SPAN の構成 221**

ワープ SPAN に関する情報	221
-----------------	-----

ワープ SPAN の注意事項および制限事項	222
ワープ SPAN の構成	223
ワープ SPAN モード構成の確認	224
ワープ SPAN 機能の履歴	226

---

**第 16 章****ERSPAN の設定 227**

ERSPAN に関する情報	227
ERSPAN タイプ	227
ERSPAN 送信元	228
ERSPAN 宛先	228
ERSPAN セッション	228
マルチ ERSPAN セッション	229
ERSPAN マーカー パケット	229
高可用性	229
ERSPAN の前提条件	229
ERSPAN の注意事項および制約事項	230
ERSPAN のデフォルト設定	232
ERSPAN の設定	232
ERSPAN 送信元セッションの設定	232
ERSPAN 宛先セッションの設定	235
ERSPAN セッションのシャットダウンまたはアクティブ化	238
ERSPAN フィルタリングの設定	241
ERSPAN サンプリングの設定	243
ERSPAN 切り捨ての設定	245
ERSPAN マーカー パケットの構成	247
ERSPAN 設定の確認	247
ERSPAN の設定例	248
ERSPAN 送信元セッションの設定例	248
ERSPAN 宛先セッションの設定例	248
その他の参考資料	249
関連資料	249

---

**第 17 章****DNS の設定 251**

DNS クライアントに関する情報 251

ネーム サーバ 251

DNS の動作 252

高可用性 252

DNS クライアントの前提条件 252

DNS クライアントのデフォルト設定 252

DNS クライアントの設定 252

---

**第 18 章****トラフィック転送モードの構成 255**

ワーブモードに関する情報 255

ワーブモードの注意事項および制限事項 255

ワーブモードの有効化と無効化 256

ワーブモードのステータスの確認 257

ワーブモードの機能履歴 257

---

**第 19 章****実行中バッファ監視の構成 259**

実行中バッファ監視の構成に付いての情報 259

アクティブ バッファ モニタリングの概要 259

バッファ ヒストグラム データのアクセスおよび収集 260

実行中バッファ監視の構成 260

バッファ ヒストグラム データの表示 262

---

**第 20 章****ソフトウェア メンテナンス アップグレード (SMU) の実行 267**

SMU について 267

パッケージ管理 268

SMU の前提条件 269

SMU の注意事項と制約事項 269

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 270

パッケージ インストールの準備 270

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	272
パッケージの追加とアクティブ化	273
アクティブなパッケージセットのコミット	274
パッケージの非アクティブ化と削除	275
インストール ログ情報の表示	276

---

第 21 章	<b>コンフィギュレーションの置換の実行</b>	279
	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	279
	概要	280
	コンフィギュレーションの置換の利点	281
	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	282
	コンフィギュレーションの置換の推奨ワークフロー	286
	コンフィギュレーションの置換の実行	287
	コンフィギュレーションの置換の確認	290
	コンフィギュレーションの置換の例	291

---

第 22 章	<b>ロールバックの設定</b>	297
	ロールバックについて	297
	ロールバックの注意事項と制約事項	297
	チェックポイントの作成	298
	ロールバックの実装	299
	ロールバック コンフィギュレーションの確認	300

---

第 23 章	<b>候補構成の完全性チェック</b>	303
	候補構成について	303
	候補構成の完全性チェックの注意事項と制限事項	303
	候補構成の完全性チェックの実行	309
	完全性チェックの例	310

---

第 24 章	<b>ユーザ アカウントおよび RBAC の設定</b>	313
--------	------------------------------	-----

ユーザーアカウントおよびRBACの概要	313
ユーザーロール	313
ルール	314
ユーザーロールポリシー	315
ユーザーアカウントの設定の制限事項	315
ユーザーパスワードの要件	316
ユーザーアカウントの注意事項および制約事項	317
ユーザーアカウントの設定	317
RBACの設定	319
ユーザーロールおよびルールの作成	319
機能グループの作成	320
ユーザーロールインターフェイスポリシーの変更	321
ユーザーロールVLANポリシーの変更	323
ユーザーアカウントとRBACの設定の確認	324
ユーザーアカウントおよびRBACのユーザーアカウントデフォルト設定	324

---

**第 25 章**

<b>安全な消去の設定</b>	<b>325</b>
安全に消去する (Secure Erase) 機能に関する情報	325
安全な消去を実行するための前提条件	326
安全な消去の注意事項と制約事項	326
安全な消去の設定	326



# 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

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。
[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。イタリック体を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。

表記法	説明
太字の <code>screen</code> フォント	ユーザが入力しなければならない情報は、太字のスクリーンフォントで示しています。
イタリック体の <code>screen</code> フォント	ユーザが値を指定する引数は、イタリック体の <code>screen</code> 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 3500 シリーズ スイッチの関連資料

Cisco Nexus 3500 シリーズ スイッチ全体のマニュアルセットは、次の URL にあります。

<https://www.cisco.com/c/en/us/support/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いいたします。

## 通信、サービス、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、[Cisco Profile Manager](#) でサインアップしてください。
- 重要な技術によ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](#) にアクセスしてください。
- 一般的なネットワーキング、トレーニング、認定関連の出版物を入手するには、[Cisco Press](#) にアクセスしてください。

- 特定の製品または製品ファミリの保証情報を探すには、[Cisco Warranty Finder](#) にアクセスしてください。

### **Cisco バグ検索ツール**

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





# 第 1 章

## 新機能および変更された機能に関する情報

- [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、Cisco Nexus 3548 スイッチ NX-OS システム管理構成ガイド、リリース 10.6 (x) に記載されている新機能および変更機能をまとめたものです。それぞれの説明が記載されている箇所も併記されています。

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	このリリースに追加された新機能はありません。	10.6(1)F	N/A





## CHAPTER 2

### 概要

この章は、次の内容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 (6 ページ)
- サポートされるプラットフォーム (6 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
実行中のバッファの監視	実行中のバッファの監視機能は、詳細なバッファ占有率のデータを提供し、ネットワーク輻輳の検出、ネットワーク輻輳がネットワーク運用にいつどのような影響を与えているかを理解するための過去のイベントの確認、過去の傾向の理解、アプリケーショントラフィックフローのパターンの識別に役立ちます。
ワープモード	ワープモードでは、転送テーブルを単一のテーブルに統合することによりアクセスパスが短縮されるため、フレームおよびパケットの処理がより高速になります。ワープモードでは、遅延が最大 20 パーセント削減されます。
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。

特長	説明
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。
オンライン診断	Cisco Generic Online Diagnostics (GOLD) では、複数のシスコプラットフォームにまたがる診断操作の共通フレームワークを定義しています。オンライン診断フレームワークでは、中央集中システムおよび分散システムに対応する、プラットフォームに依存しない障害検出アーキテクチャを規定しています。これには共通の診断 CLI とともに、起動時および実行時に診断するための、プラットフォームに依存しない障害検出手順が含まれます。  プラットフォーム固有の診断機能は、ハードウェア固有の障害検出テストを行い、診断テストの結果に応じて適切な対策を実行できます。
システム メッセージ ロギング	システムメッセージロギング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シビラティ（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 サーバーへのロギングを設定できます。  システム メッセージ ロギングは RFC 3164 に準拠しています。システムメッセージのフォーマットおよびデバイスが生成するメッセージの詳細については、『Cisco NX-OS System Messages Reference』を参照してください。
Smart Call Home	Call Home は重要なシステム ポリシーを電子メールで通知します。Cisco NX-OS では、ポケットベル サービス、標準的な電子メール、または XML ベースの自動化された解析アプリケーションとの最適な互換性のために、広範なメッセージ形式が提供されています。この機能を使用して、ネットワーク サポート エンジニアやネットワーク 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。

特長	説明
設定のロールバック	設定のロールバック機能を使用すると、Cisco NX-OS のコンフィギュレーションのスナップショットまたはユーザー 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ても、いつでもそのコンフィギュレーションをスイッチに再適用できます。権限のある管理者であれば、チェックポイントで設定されている機能について専門的な知識がなくても、ロールバック機能を使用して、そのチェックポイント コンフィギュレーションを適用できます。
SNMP	簡易ネットワーク管理プロトコル (SNMP) は、SNMP マネージャとエージェント間の通信メッセージフォーマットを提供する、アプリケーションレイヤプロトコルです。SNMP では、ネットワーク内のデバイスのモニタリングと管理に使用する標準フレームワークと共通言語が提供されます。
RMON	RMON は、各種のネットワーク エージェントおよびコンソールシステムがネットワーク モニタリング データを交換できるようにするための、Internet Engineering Task Force (IETF) 標準モニタリング仕様です。Cisco NX-OS では、Cisco NX-OS デバイスをモニターするための、RMON アラーム、イベント、およびログをサポートします。
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、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) プロブです。
GIR	グレースフル挿入および削除 (GIR) メンテナンス モードは、N3500 プラットフォームではサポートされていません。

## 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 Licensing Guide](#)』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。



## 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。

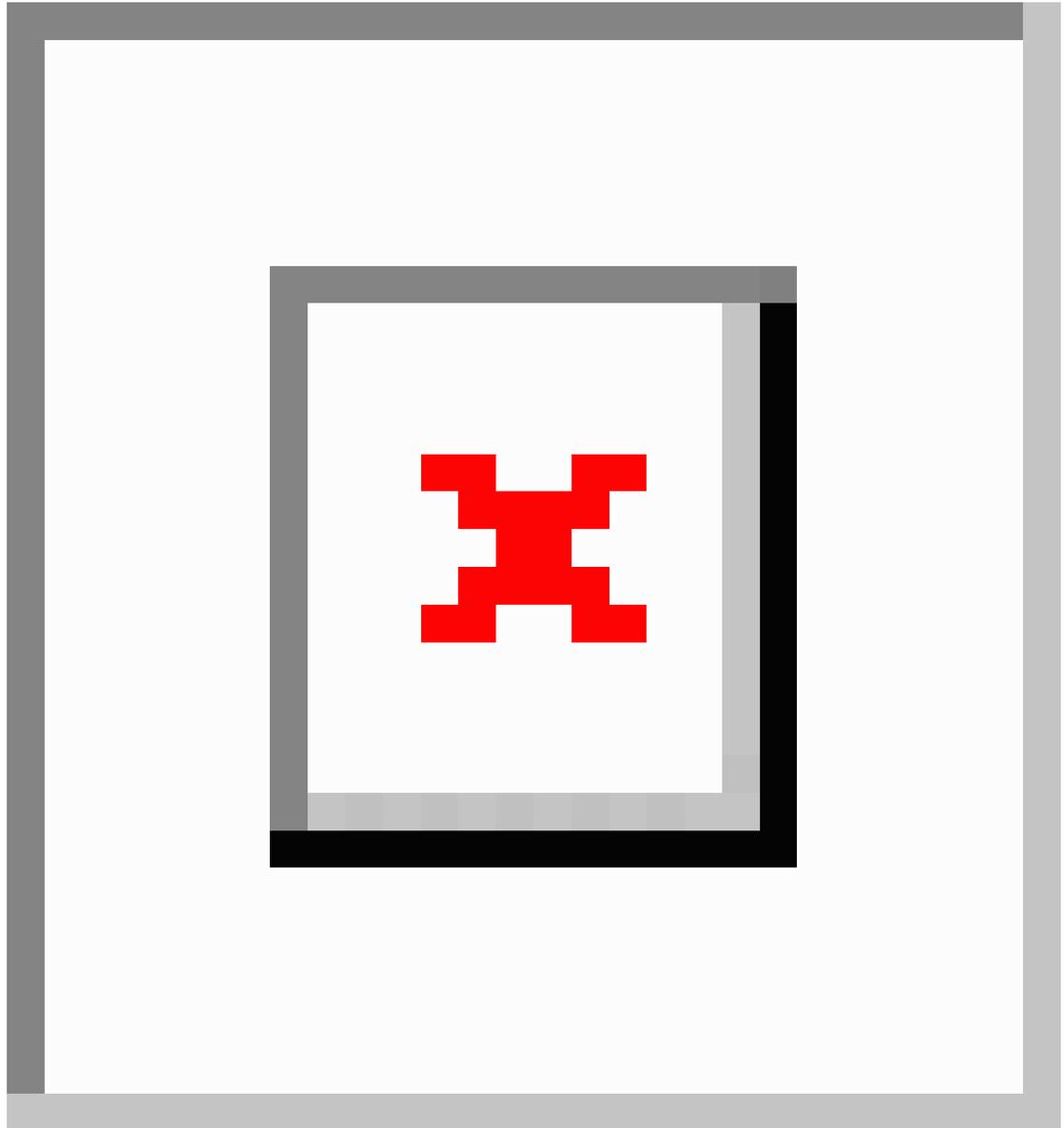
- [2 段階構成のコミットについて \(7 ページ\)](#)
- [注意事項と制約事項 \(8 ページ\)](#)
- [2 ステージ コンフィギュレーション コミット モードでの設定 \(9 ページ\)](#)
- [2 ステージコンフィギュレーションコミットモードの中止 \(13 ページ\)](#)
- [コミット ID の表示 \(14 ページ\)](#)
- [ロールバック機能 \(14 ページ\)](#)
- [現在のセッション設定の表示 \(14 ページ\)](#)

## 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** コマンドを実行するまで実行コンフィギュレーションに影響しません。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。**commit** コマンドを実行しないと、指定した時間が経過してもスイッチは以前の設定に戻ります。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。

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。
- 機能関連のコンフィギュレーション 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。
- 変更を確定する前に、**show configuration** コマンドを使用して設定を確認します。
- 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> 例 : <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 feature_name</b> 例 :	機能を有効にします。 (注)

	コマンドまたはアクション	目的
	<pre>switch(config-dual-stage)# feature bgp switch(config-dual-stage)#</pre>	<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ることはできません。</li> </ul>
ステップ 3	<p><b>commit [confirmedseconds]</b></p> <p>例 :</p> <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  switch(config-dual-stage)# switch(config-dual-stage)# commit Confirming commit for trial session. switch(config-dual-stage)#</pre> <p>例 :</p> <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>秒: グローバル コンフィギュレーション モードで、最低 30 秒間、最大 65535 秒間の試験稼働のためにコンフィギュレーションをコミットします。</li> </ul> <p>(注) トライアル期間を入力する場合は、<b>commit</b> コマンドを実行して設定を確認します。<b>commit</b> 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	<p>例 :</p> <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>	<p>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。</p>
ステップ 5	<p><b>show configuration</b></p> <p>例 :</p> <pre>switch(config-dual-stage-router)# show configuration</pre>	<p>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> <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	<p><b>commit [confirmed seconds]</b></p> <p>例 :</p> <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	<p>(任意) <b>show configuration commit [changes] commit-id</b></p> <p>例 :</p> <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> <p>例 :</p> <pre>switch(config-dual-stage)# show configuration commit 1000000003 feature bgp router bgp 64515.46   router-id 141.8.139.131 . . .</pre>	<p>コミット関連情報を表示します。</p> <p>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。</p> <p>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するには、<b>show configuration commit changes commit-id</b> コマンドを使用します。</p> <p>指定したコミットの完全な設定を表示するには、<b>show configuration commit commit-id</b> コマンドを使用します。</p>
ステップ 8	<p>(任意) <b>save configuration filename</b></p> <p>例 :</p> <pre>switch(config-dual-stage)# save configuration bootflash:test.cfg</pre>	<p>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。</p> <p>(注)</p> <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>

	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>保存したコンフィギュレーション ファイルを表示するには、<b>show configuration filename</b> コマンドを実行します。</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>
<b>ステップ 9</b>	<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> コマンドを使用します。</p> <p><b>save configuration filename</b> コマンドのみを使用して保存したターゲット コンフィギュレーションをロードできます。</p>
<b>ステップ 10</b>	<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>
<b>ステップ 11</b>	<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に指示されます。</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ず。

```
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。

最後の 50 のコミット ID に関する情報を表示するには、`show configuration commit list` コマンドを使用します。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

`show configuration` コマンドを使用して、現在のコンフィギュレーションセッションを表示できます。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-ipmcmis
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)#
```





## 第 4 章

# PTP の設定

この章は、次の内容で構成されています。

- [PTP に関する情報](#) (17 ページ)
- [PTP 時間分配保留](#) (18 ページ)
- [PTP デバイス タイプ](#) (19 ページ)
- [PTP プロセス](#) (20 ページ)
- [PTP のハイアベイラビリティ](#) (21 ページ)
- [PTP の注意事項および制約事項](#) (21 ページ)
- [PTP のデフォルト設定](#) (23 ページ)
- [PTP の設定](#) (23 ページ)

## PTP に関する情報

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

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

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

Cisco NXOS リリース 6.0(2)A8(3)以降、PTPは、複数のPTPクロッキングドメイン、PTPグランドマスター機能、スレーブおよびパッシブ選択のためのインターフェイスでのPTPコスト、およびクロックIDの設定をサポートします。

マルチドメイン環境のすべてのスイッチは、1つのドメインに属しています。境界クロックの一部であるスイッチでは、マルチドメイン機能が有効になっている必要があります。各ドメインには、ドメインの優先度、クロッククラスのしきい値、クロック精度のしきい値など、ユーザーが構成可能なパラメータがあります。各ドメインのクロックは、そのドメインのマスタークロックと同期したままです。ドメイン内の GPS に障害が発生した場合、ドメイン内のマスタークロックは、GPS がアクティブであるドメイン内のマスタークロックから送られたアナウンスメッセージに関連付けられているデータセットとの間で、時刻の同期を行います。最も優先度の高いドメインからのマスタークロックがクロック品質属性を満たさない場合、基準に一致する後続のドメインのクロックが選択されます。どのドメインでも、必要なクロック品質属性が満たされていない場合は、Best Master Clock Algorithm (BMCA) を使用してマスタークロックが選択されます。すべてのドメインの優先順位が等しく、しきい値がマスタークロック属性よりも小さい場合、またはしきい値がマスタークロック属性よりも大きい場合、BMCA を使用してマスタークロックが選択されます。

グランドマスター機能は、接続されている他のデバイスにクロックを伝達するスイッチの機能を制御します。スイッチは、インターフェイスでアナウンスメッセージを受信すると、クロッククラスのしきい値とクロック精度のしきい値をチェックします。これらのパラメータの値が事前定義された限界内にある場合、スイッチは IEEE 1588v2 で指定された PTP 標準に従って動作します。スイッチが外部ソースからアナウンスメッセージを受信していない場合、または受信したアナウンスメッセージのパラメータが事前定義された限界内にない場合、ポートの状態はリスニングモードに変更されます。スレーブポートのないスイッチでは、すべての PTP 対応ポートの状態がリスニングとしてレンダリングされます。1つのスレーブポートがあるスイッチでは、BMCA を使用してすべての PTP 対応ポートの状態が判断されます。コンバージェンス時間は、スイッチでグランドマスター機能が無効になっている場合に、PTP レベルでタイミングループが発生するのを防止するためのものです。スイッチでスレーブポートが選択されていない場合、スイッチのすべてのポートは、コンバージェンス時間で指定された最小間隔の間、リスニング状態になります。コンバージェンス時間の範囲は 3 ~ 2600 秒で、デフォルトは 30 秒です。

PTP が有効にされた各ポートでインターフェイスコストが適用されるのは、グランドマスタークロックへの複数のパスがスイッチにある場合です。最小のコスト値を持つポートがスレーブとして選択され、残りのポートはパッシブポートのままになります。

クロック識別子は、スイッチの MAC アドレスに基づいた文字配列の形式で表示される、一意の 8 オクテット配列です。クロック識別子は、IEEE1588v2-2008 仕様に従って MAC から決定されます。クロック ID は、IEEE1588v2 で定義されている VLAN MAC アドレスのバイトの組み合わせです。

## 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 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、同期する必要がある、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。

## クロック モード

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

### 1 ステップ モード :

1 ステップモードでは、クロック同期メッセージに、マスターポートがメッセージを送信した時刻が含まれます。ASIC は、同期メッセージがポートを出るときにタイムスタンプを追加します。1 ステップモードで動作するマスターポートは、Cisco Nexus 9508-FM-R および 9504-FM-R ファブリック モジュールおよび Cisco Nexus 9636C-R、9636Q-R、9624D-R2、および 9636C-RX ラインカードで使用できます。

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

### 2 ステップ モード :

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

## PTP プロセス

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

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

- 受信したすべての (マスターステートのポートによって発行された) アナウンスメッセージの内容を検査します
- 外部マスターのデータセット (アナウンスメッセージ内) とローカルクロックで、優先順位、クロッククラス、精度などを比較します

- 自身のステートがマスターまたはスレーブのいずれであるかを決定します

マスター/スレーブ階層が確立されると、クロックは次のように同期されます。

- マスターはスレーブに同期メッセージを送信し、送信された時刻を記録します。
- スレーブは同期メッセージを受信し、受信した時刻を記録します。すべての同期メッセージには、フォローアップメッセージがあります。同期メッセージの数は、フォローアップメッセージの数と同じである必要があります。
- スレーブはマスターに遅延要求メッセージを送信し、送信された時刻を記録します。
- マスターは遅延要求メッセージを受信し、受信した時刻を記録します。
- マスターはスレーブに遅延応答メッセージを送信します。遅延要求メッセージの数は、遅延応答メッセージの数と同じ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 3500 のみの環境では、PTP クロック修正は、1 ~ 99 ナノ秒の 1 ~ 2 桁の範囲であると予想されます。ただし、混合環境では、PTP クロック修正は最大 3 桁 (100 ~ 999 ナノ秒) になるものと予想されます。
- Cisco Nexus 3500 シリーズ スイッチでは、マスター PTP ポートで操作の非ネゴシエートモードの混合がサポートされます。つまり、スレーブクライアントがユニキャスト遅延要求 PTP パケットを送信すると、Cisco Nexus 3500 がユニキャスト遅延応答パケットで応答することを意味します。また、スレーブクライアントがマルチキャスト遅延要求 PTP パケットを送信すると、Cisco Nexus 3500 はマルチキャスト遅延応答パケットで応答します。混合非ネゴシエートモードが機能するには、BC デバイスの `ptp source <IP address>` 構成で使用される送信元 IP アドレスが、BC デバイスの物理または論理インターフェイスでも構成されている必要があります。推奨されるベストプラクティスは、デバイスのループバック インターフェイスを使用することです。
- Cisco Nexus 3500 シリーズ スイッチは、`ptp source` をサポートします。
- Cisco Nexus 3500 シリーズ スイッチは、40G インターフェイスでの PTP をサポートしていません。

- 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、クロック プロトコルが PTP に設定されている場合に動作します。PTP と NTP を同時に構成することはサポートされていません。
- 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 acl-redirect` が構成されている場合、PTP 管理パケットはソフトウェアで転送されます。管理パケットは 100 パケット/秒以内であることが期待されます。これは CoPP ドロップを回避するためです。
- PTP 対応ポートは、ポート上で PTP を有効にしない場合、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、パケットを処理のため CPU にリダイレクトしたりしません。これは、ポートで PTP が無効になっている場合、デバイスは、タイプに関係なく、マルチキャストステートが存在すると仮定して、任意のマルチキャスト PTP パケットをルーティングできることを意味します。このポートからのこれらのマルチキャスト PTP パケットは、処理のために CPU にリダイレクトされません。これは、それらを CPU にリダイレクトするために適用される例外が、それぞれのポートで PTP が有効かどうかに基づいて、ポートごとにプログラムされるためです。
- 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、-3 ~ 1 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。
- すべてのユニキャストおよびマルチキャスト PTP 管理メッセージは、転送ルールに従って転送されます。すべての PTP 管理メッセージは通常のマルチキャスト パケットとして扱われ、他の非 PTP マルチキャスト パケットが Cisco Nexus 3500 スイッチによって処理されるのと同じ方法で処理されます。
- PTP ユニキャスト パケットの転送を有効にするには、着信ポートを L3/SVI として構成する必要があります。
- Cisco Nexus 3500 スイッチは、ユニキャストマスターとクライアント間のユニキャストネゴシエーションに参加させないことを推奨します。
- ワンステップ PTP は、Cisco Nexus 3500 シリーズ プラットフォーム スイッチではサポートされません。
- 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、ターゲット補正值に落ち着くまで、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. PTP はデフォルトで無効になっています。
クロックをアドバタイズする場合、PTP プライオリティ 1 値	255
クロックをアドバタイズする場合、PTP プライオリティ 2 値	255
PTP アナウンス間隔	1 ログ秒
PTP 同期間隔	1 ログ秒
PTP アナウンス タイムアウト	3 アナウンス間隔
PTP 最小遅延要求間隔	1 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. **configure terminal**
2. **[no] feature ptp**
3. **[no] ptp source ip-address**
4. (任意) **[no] ptp domain number**
5. (任意) **[no] ptp priority1 value**

6. (任意) `[no] ptp priority2 value`
7. (任意) `[no] ptp acl-redirect`
8. (任意) `show ptp brief`
9. (任意) `show ptp clock`
10. (任意) `[no] ptp time distribution-hold [correction-threshold <corr_limit>] [delay-threshold <max_delay_time>]`
11. `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： <code>switch# configure terminal</code>	グローバル設定モードを開始します。
ステップ 2	<b>[no] feature ptp</b> 例： <code>switch(config) # feature ptp</code>	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	<b>[no] ptp source ip-address</b> 例： <code>switch(config) # ptp source 10.2.3.4</code>	すべての PTP パケットのソース IP アドレスを構成します。  <i>ip-address</i> : IPv4 形式。
ステップ 4	(任意) <b>[no] ptp domain number</b> 例： <code>switch(config) # ptp domain 24</code>	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つのネットワーク上で、複数の独立した PTP クロッキング サブドメインを使用できます。  <i>number</i> : 有効な範囲は 0 ~ 128 です。
ステップ 5	(任意) <b>[no] ptp priority1 value</b> 例： <code>switch(config) # ptp priority1 10</code>	このクロックをアドバタイズするときに使用する <i>priority1</i> 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> : 範囲は 0 ~ 255 です。
ステップ 6	(任意) <b>[no] ptp priority2 value</b> 例： <code>switch(config) # ptp priority2 20</code>	このクロックをアドバタイズするときに使用する <i>priority2</i> 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、

	コマンドまたはアクション	目的
		<p>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、<b>priority2</b> 値を使用して、特定のスイッチが他の同等のスイッチよりも優先されるようにすることができます。</p> <p><i>value</i> : 範囲は 0 ~ 255 です。</p>
ステップ 7	<p>(任意) <b>[no] ptp acl-redirect</b></p> <p>例 :</p> <pre>switch (config)# ptp acl-redirect</pre>	<p>ACL エントリを使用してハードウェアで PTP ユニキャスト パケットを転送するようにシステムを構成します。</p> <p>(注)</p> <p>TCAM SUP リージョン サイズが 48 より大きいことを確認してください。そうでない場合、コマンドの入力時に次のエラー メッセージが表示されます。</p> <pre>switch(config)# ptp acl-redirect ERROR: PTP acl-redirect supported only if TCAM sup size is greater than 48 2020 May 6 21:27:04 switch %ACLQOS-SLOT1-2-ACLQOS_OOTR: Tcam resource exhausted: Need to reconfigure SUP region</pre>
ステップ 8	<p>(任意) <b>show ptp brief</b></p> <p>例 :</p> <pre>switch(config) # show ptp brief</pre>	PTP のステータスを表示します。
ステップ 9	<p>(任意) <b>show ptp clock</b></p> <p>例 :</p> <pre>switch(config) # show ptp clock</pre>	ローカル クロックのプロパティを表示します。
ステップ 10	<p>(任意) <b>[no] ptp time distribution-hold</b> <b>[correction-threshold &lt;corr_limit&gt;] [delay-threshold &lt;max_delay_time&gt;]</b></p> <p>例 :</p> <pre>switch(config)# ptp time distribution-hold correction-threshold 9000ns delay threshold 4000s</pre>	<p>PTP 時間分配保留機能を有効にします。</p> <p><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。</p> <p><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。</p> <p>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。</p> <p>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。</p>

	コマンドまたはアクション	目的
ステップ 11	<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構成をスタートアップ構成にコピーして、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. (任意) switch(config-if) # [no] **ptp announce { interval log seconds | timeout count}**
4. (任意) switch(config-if) # [no] **ptp delay request minimum interval log seconds**
5. (任意) switch(config-if) # [no] **ptp sync interval log seconds**
6. (任意) switch(config-if) # [no] **ptp vlan vlan-id**
7. (任意) switch(config-if) # **show ptp brief**
8. (任意) switch(config-if) # **show ptp port interface interface slot/port**
9. (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 ethernet slot/port</b>	PTP をイネーブルにするインターフェイスを指定し、インターフェイス構成モードを開始します。
ステップ 3	(任意) switch(config-if) # [no] <b>ptp announce { interval log seconds   timeout count}</b>	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 4	(任意) switch(config-if) # [no] <b>ptp delay request minimum interval log seconds</b>	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 5	(任意) switch(config-if) # [no] <b>ptp sync interval log seconds</b>	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 -3 ログ秒 ~ 1 ログ秒です。
ステップ 6	(任意) switch(config-if) # [no] <b>ptp vlan vlan-id</b>	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 7	(任意) switch(config-if) # <b>show ptp brief</b>	PTP のステータスを表示します。
ステップ 8	(任意) switch(config-if) # <b>show ptp port interface interface slot/port</b>	PTP ポートのステータスを表示します。

	コマンドまたはアクション	目的
ステップ 9	(任意) <code>switch(config-if)# copy running-config startup-config</code>	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 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 1/1
PTP Port Dataset: Eth1/1
Port identity: clock identity: f4:4e:05:ff:fe:84:7e:7c
Port identity: port number: 0
PTP version: 2
Port state: Slave
VLAN info: 1
Delay request interval(log mean): 0
Announce receipt time out: 3
Peer mean path delay: 0
Announce interval(log mean): 1
Sync interval(log mean): 1
Delay Mechanism: End to End
Cost: 255
Domain: 5
switch(config-if)#
```

## PTP 混合モード

PTP は、接続されたクライアントから受信した `delay_req` メッセージのタイプに基づいて、Cisco Nexus デバイスによって自動的に検出される PTP メッセージを配信するための混合モードをサポートします。このモードでは、スレーブがユニキャストメッセージで `delay_req` を送信すると、マスターもユニキャスト `delay_resp` メッセージで応答します。

## 複数の PTP ドメインの設定

単一のネットワークに対して、複数の PTP クロッキングドメインを設定することができます。各ドメインには、特定の優先順位の値が関連付けられます。デフォルト値は 255 です。

## 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]**
4. switch(config) # [no] **ptp multi-domain**
5. switch(config) # [no] **ptp domain value priority value**
6. switch(config) # [no] **ptp domain value clock-class-threshold value**
7. switch(config) # [no] **ptp domain value clock-accuracy-threshold value**
8. switch(config) # [no] **ptp multi-domain transition-attributes priority1 value**
9. switch(config) # [no] **ptp multi-domain transition-attributes priority2 value**
10. switch(config-if) # [no] **ptp domain value**

## 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 アドレスを設定します。  <i>ip-address</i> には IPv4 形式を使用できます。
ステップ 4	switch(config) # [no] <b>ptp multi-domain</b>	スイッチでマルチ ドメイン機能をイネーブルにします。ここでは、優先順位、クロッククラスのしきい値、クロック精度のしきい値、移行の優先順位などの属性もスイッチに設定できます。
ステップ 5	switch(config) # [no] <b>ptp domain value priority value</b>	ドメインおよび優先度の値を指定します。  <i>domain</i> の <i>value</i> の範囲は 0 ~ 127 です。 <i>domain</i> のデフォルト値は 0 です。  <i>priority</i> の <i>value</i> の範囲は 0 ~ 255 です。 <i>priority</i> のデフォルト値は 255 です。
ステップ 6	switch(config) # [no] <b>ptp domain value clock-class-threshold value</b>	ドメインおよびクロック クラスのしきい値を指定します。デフォルト値は 248 です。

	コマンドまたはアクション	目的
		<p>domain の <i>value</i> の範囲は 0 ～ 127 です。</p> <p>clock-class-threshold の <i>value</i> の範囲は 0 ～ 255 です。</p> <p>(注)</p> <p>クロック クラスのしきい値で、いずれかのポート上のスレーブクロックを必ず選択する必要はありません。スイッチはこの値を使用して、送信元クロックがトレース可能かを判断します。ピアからのクロッククラス値がドメインのクロッククラスのしきい値に等しいかより高い場合、スイッチは BMCA を実行してドメインからスレーブポートを選択します。しきい値より低いクロッククラスがどのドメインにもない場合、スイッチは PTP がイネーブルなすべてのポートで BMCA を実行して最適なクロックを選択します。</p>
ステップ 7	switch(config) # [no] ptp domain <i>value</i> clock-accuracy-threshold <i>value</i>	<p>ドメインおよびクロックの精度のしきい値を指定します。デフォルト値は 254 です。</p> <p>domain の <i>value</i> の範囲は 0 ～ 127 です。</p> <p>clock-accuracy-threshold の <i>value</i> の範囲は 0 ～ 255 です。</p>
ステップ 8	switch(config) # [no] ptp multi-domain transition-attributes priority1 <i>value</i>	<p>当該ドメインからピア ドメインへのパケット送信時に使用する <i>domain transition-attributes priority1</i> 値を設定します。リモートポートからのアナウンスメッセージ内の <i>priority1</i> の値は、ドメイン内のピアにアナウンスメッセージを送信する必要があり、その値がスレーブ インターフェイスの値と異なる場合、<i>domain transition-attributes priority1</i> の値で置き換えられます。デフォルト値は 255 です。</p> <p>transition-attributes priority1 の <i>value</i> の範囲は 0 ～ 255 です。</p>
ステップ 9	switch(config) # [no] ptp multi-domain transition-attributes priority2 <i>value</i>	<p>当該ドメインからピア ドメインへのパケット送信時に使用する <i>domain transition-attributes priority2</i> 値を設定します。リモートポートからのアナウンスメッセージ内の <i>priority2</i> の値は、ドメイン内のピアにアナウンスメッセージを送信する必要があり、その値がスレーブ インターフェイスの値と異なる場合、<i>domain transition-attributes priority2</i> の値で置き換えられます。デフォルト値は 255 です。</p>

	コマンドまたはアクション	目的
		transition-attributes priority2 の value の範囲は 0 ~ 255 です。
ステップ 10	switch(config-if) # [no] <b>ptp domain value</b>	PTP がイネーブルにされたインターフェイスとドメインを関連付けます。インターフェイスへの明示的なドメイン指定を行わない場合は、デフォルト値 (0) が適用されます。  domain の value の範囲は 0 ~ 127 です。

### 例

次に、スイッチに設定されている PTP ドメインを表示する例を示します。

```
switch(config)# show ptp domain data
MULTI DOMAIN : ENABLED
GM CAPABILITY : ENABLED
PTP DEFAULT DOMAIN : 0
PTP TRANSITION PRIORITY1 : 20
PTP TRANSITION PRIORITY2 : 255
PTP DOMAIN PROPERTY
Domain-Number Domain-Priority Clock-Class Clock-Accuracy Ports
0          255          248          254          Eth1/1
1           1           1           254
```

```
switch(config)#
```

次に、PTP がイネーブルにされた各インターフェイスに関連付けられたドメインを表示する例を示します。

```
switch(config)# show ptp interface domain
PTP port interface domain
-----
Port          Domain
-----
Eth1/1        0
1             1          254
```

```
switch(config)#
```

## PTP グランドマスター クロックの設定

スイッチでグランドマスター機能が無効になっている場合に、PTP レベルでタイミングループが発生しないようにコンバージェンス時間を設定できます。デバイスでは、グランドマスター機能がデフォルトで有効になっています。

### 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]
4. switch(config) # no ptp grandmaster-capable [ convergence-time]
5. switch(config) # [no] ptp domain value clock-class-threshold value
6. switch(config) # [no] ptp domain value clock-accuracy-threshold value
7. switch(config) # ptp grandmaster-capable

## 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 アドレスを設定します。  <i>ip-address</i> には IPv4 形式を使用できます。
ステップ 4	switch(config) # <b>no ptp grandmaster-capable [ convergence-time]</b>	スイッチのグランドマスター機能を無効にします。どのドメインにも使用可能な外部グランドマスターがない場合、デバイスがグランドマスターとして機能しないようにします。デフォルトの時間は 30 秒です。
ステップ 5	switch(config) # [no] <b>ptp domain value clock-class-threshold value</b>	ドメインおよびクロッククラスのしきい値を指定します。クロッククラスしきい値は、デバイスがソースクロックをグランドマスタークロックと見なすことができるかどうかを判断するために使用するクロック クラスしきい値を定義します。  <i>domain</i> の <i>value</i> の範囲は 0 ~ 127 です。  <i>clock-class-threshold</i> の <i>value</i> の範囲は 0 ~ 255 です。  (注) スイッチはこの値を使用して、送信元クロックがトレース可能かを判断します。すべてのピアからのクロック クラス値がクロック クラスのしきい値より

	コマンドまたはアクション	目的
		も高い場合、BMCA はすべてのポートの状態をリスニングに変更する場合があります。
ステップ 6	<code>switch(config) # [no] ptp domain value</code> <code>clock-accuracy-threshold value</code>	ドメインおよびクロックの精度のしきい値を指定します。  domain の value の範囲は 0 ~ 127 です。  clock-accuracy-threshold の value の範囲は 0 ~ 255 です。
ステップ 7	<code>switch(config) # ptp grandmaster-capable</code>	スイッチでグランドマスター機能を有効にします。

### 例

次の例では、PTP クロック情報を表示します。

```
switch(config-if)# show ptp clock
PTP Device Type: Boundary clock
Clock Identity : f4:4e:05:ff:fe:84:7e:7c
Clock Domain: 5
Number of PTP ports: 2
Priority1 : 129
Priority2 : 255
Clock Quality:
Class : 248
Accuracy : 254
Offset (log variance) : 65535
Offset From Master : 0
Mean Path Delay : 391
Steps removed : 1
Local clock time:Wed Nov 9 10:31:21 2016
switch(config-if)#
```

## インターフェイスでの PTP コストの設定

Cisco Nexus 3500 スイッチで PTP がイネーブルにされた各ポートには、インターフェイスコストを設定できます。PTP がイネーブルにされた各ポートでコストが適用されるのは、グランドマスタークロックへの複数のパスがスイッチにある場合です。

### 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]`
4. `switch(config) # interface ethernet slot/port`
5. `switch(config-if) # [no] ptp cost value`

## 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 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) # <b>[no] ptp source ip-address [ vrf vrf]</b>	すべての PTP パケットのソース IP アドレスを設定します。  <i>ip-address</i> には IPv4 形式を使用できます。
ステップ 4	switch(config) # <b>interface ethernet slot/port</b>	PTP をイネーブルにするインターフェイスを指定し、インターフェイス構成モードを開始します。
ステップ 5	switch(config-if) # <b>[no] ptp cost value</b>	PTP がイネーブルにされたインターフェイスにコストを関連付けます。コストが最も低いインターフェイスが、スレーブ インターフェイスになります。  コストの範囲は 0 ~ 255 です。デフォルト値は 255 です。

## 例

次に、PTP がイネーブルにされた各インターフェイスに関連付けられたコストを表示する例を示します。

```
switch(config)# show ptp cost
PTP port costs
-----
Port          Cost
-----
Eth1/1        255
switch(config)#
```

## クロック ID の設定

Cisco Nexus 3500 スイッチにはクロック ID を設定できます。デフォルトのクロック ID は、スイッチの MAC アドレスをベースにした固有の 8 オクテット文字列です。

## 手順の概要

1. switch# **configure terminal**
2. switch(config) # **[no] feature ptp**
3. switch(config-if) # **ptp clock-identity** *MAC 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	switch(config) # <b>[no] 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-if) # <b>ptp clock-identity</b> <i>MAC Address</i>	PTP clock-identity として 6 バイトの MAC アドレスを割り当てます。デフォルトのクロック ID は、スイッチの MAC アドレスをベースにしています。クロック ID は IEEE 標準によって定義されます (MAC-48 Byte0   MAC-48 Byte1   MAC-48 Byte2   FF   FE   MAC-48 Bytes3-5)。

## PTP インターフェイスがマスター ステートを維持する設定

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

### 始める前に

- スイッチ上でグローバルに PTP をイネーブルにし、PTP 通信の送信元 IP アドレスを設定したことを確認します。
- PTP をグローバルにイネーブルにしても、デフォルトで、サポートされているすべてのインターフェイス上でイネーブルになりません。PTP インターフェイスは個別にイネーブルに設定する必要があります。

## 手順の概要

1. switch # **configure terminal**
2. switch(config) # **interface ethernet slot/port**
3. switch(config) # [no] **ptp**
4. switch(config-if) # **ptp transmission multicast**
5. switch(config-if) # **ptp role master**

## 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>	PTP をイネーブルにするインターフェイスを指定し、インターフェイス構成モードを開始します。
ステップ 3	switch(config) # [no] <b>ptp</b>	インターフェイスで PTP をイネーブルまたはディセーブルにします。
ステップ 4	switch(config-if) # <b>ptp transmission multicast</b>	インターフェイスで使用される PTP 伝送方式を設定します。
ステップ 5	switch(config-if) # <b>ptp role master</b>	インターフェイスの PTP ロールを設定します。  <b>master</b> : マスタークロックは、インターフェイスの PTP ロールとして割り当てられます。

## 例

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

```
switch(config)# show ptp brief

PTP port status
-----
Port                State
-----
Eth1/1              Slave
switch(config)# interface ethernet 1/1
switch(config-if)# ptp multicast master-only
2001 Jan  7 07:50:03 A3-MTC-CR-1 %$ VDC-1 %$ %PTP-2-PTP_GM_CHANGE: Grandmaster clock has changed
from 60:73:5c:ff:fe:62:a1:41 to 58:97:bd:ff:fe:0d:54:01 for the PTP protocol
2001 Jan  7 07:50:03 A3-MTC-CR-1 %$ VDC-1 %$ %PTP-2-PTP_STATE_CHANGE: Interface Eth1/1 change from
PTP_BMC_STATE_SLAVE to PTP_BMC_STATE_PRE_MASTER
2001 Jan  7 07:50:03 A3-MTC-CR-1 %$ VDC-1 %$ %PTP-2-PTP_TIMESYNC_LOST: Lost sync with master clock
2001 Jan  7 07:50:07 A3-MTC-CR-1 %$ VDC-1 %$ %PTP-2-PTP_STATE_CHANGE: Interface Eth1/1 change from
PTP_BMC_STATE_PRE_MASTER to PTP_BMC_STATE_MASTER
```

## タイムスタンプタギング

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

インターフェイスで **ttag** を構成すると、すべての着信トラフィックがタグ付けされます。インターフェイスで **ttag-strip** を構成すると、**ttag** を持つすべての発信トラフィックが削除されます。

### タイムスタンプタギングの構成



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



- (注)
- VXLANEVPN マルチサイト展開で **ttag** 機能を使用する場合は、クラウドに接続する BGW の DCI インターフェイスで **ttag** が削除されていることを確認します (**ttag-strip**)。詳細に説明すると、**ttag** が、**ether-type 0x8905** をサポートしない Nexus 9000 以外のデバイスに接続されている場合、**ttag** の除去が必要です。ストリッピングが行われない場合、Nexus 以外のデバイスはパケットをドロップします。
  - DCI の BGW バックツーバック モデルでは **ttag** の削除は必要ありません。
  - Cloudscale プラットフォームでは、パケットが TTAG ヘッダー (EtherType 0x8905) とともに受信された場合、**ttag-strip** が発信インターフェイスで設定されていない限り、それが保持されます。スイッチングまたはルーティングの後、スイッチから送信されるパケットにも TTAG ヘッダーが含まれます。これを行うには、スイッチに PTP または TTAG 関連の設定を行う必要はありません。ネクストホップが Catalyst switch などの非 Cloudscale プラットフォームの場合、イーサネットタイプ 0x8905 を認識しない可能性があり、パケットがドロップされる可能性があります。
  - Cisco Nexus 9800 スイッチは、**ether-type 0x8905** パケットのルーティングをサポートしていません。

#### 始める前に

PTP オフロードがグローバルに有効になっていることを確認します。

## 手順の概要

1. **configure terminal**
2. **interface type slot/port**
3. **[no] ttag**

## 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>interface type slot/port</b> 例： switch(config)# interface ethernet 2/2 switch(config-if)#	指定したインターフェイスに対してインターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<b>[no] ttag</b> 例： switch(config-if)# ttag	レイヤ 2 またはレイヤ 3 出力インターフェイスでタイムスタンプ タギングを設定します。これは、スイッチの出力時にタグ付けする必要があるトラフィックの入力ポートで必要です。これは、出力ポートでは必要ありません。

## TTAG マーカー パケットと時間間隔の構成

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

フィールド	位置 (バイト : ビット)	長さ	定義
Magic		16	デフォルトでは、このフィールドには A6A6 と表示されます。これにより、パケットストリーム上の ttag-marker パケットを識別できます。
バージョン		8	バージョン番号。デフォルトのバージョンは 1 です。

精度		16	このフィールドは、48ビットのタイムスタンプサイズの粒度を表します。デフォルトの値は04で、これは100ピコ秒つまり0.1ナノ秒を表します。
UTc_offset		8	ASIC と UTC クロック間の <code>utc_offset</code> 値です。デフォルト値は0です。
Timestamp_hi		32	48ビットのASICハードウェアタイムスタンプの上位16ビットです。  (注) 64ビットのASICハードウェアタイムスタンプを取得するために、[Timestamp_hi] および [Timestamp_lo] フィールドに [Correction_hi] および [Correction_lo] を追加します。
Timestamp_lo		32	48ビットのASICハードウェアタイムスタンプの下位32ビットです。  (注) 64ビットのASICハードウェアタイムスタンプを取得するために、[Timestamp_hi] および [Timestamp_lo] フィールドに [Correction_hi] および [Correction_lo] を追加します。
UTC sec		32	Cisco Nexus 9000 シリーズ スイッチの CPU クロックに基づく UTC タイムスタンプの秒の部分です。
UTC sec		32	Cisco Nexus 9000 シリーズ スイッチの CPU クロックに基づく UTC タイムスタンプのナノ秒の部分です。
予約済み		32	将来的な使用のために予約されています。

Correction_hi		32	<p>Cisco Nexus 9000 シリーズ スイッチの累積 PTP 補正の上位 32 ビット。</p> <p>(注) 64 ビットの ASIC ハードウェア タイムスタンプを取得するために、[Timestamp_hi] および [Timestamp_lo] フィールドに [Correction_hi] および [Correction_lo] を追加します。</p>
Correction_lo		32	<p>Cisco Nexus 9000 シリーズ スイッチの累積 PTP 補正の下位 32 ビット。</p> <p>(注) 64 ビットの ASIC ハードウェア タイムスタンプを取得するために、[Timestamp_hi] および [Timestamp_lo] フィールドに [Correction_hi] および [Correction_lo] を追加します。</p>
署名 (Signature)		32	<p>デフォルト値は 0xA5A5A5A5 です。これにより、マーカーパケットの前方検索が可能になり、UTC タイムスタンプへの参照が提供されるため、クライアント ソフトウェアはその参照 UTC を使用して、各パケット ヘッダーの 32 ビットのハードウェア タイムスタンプを回復できます。</p>
パッド		64	<p>これは、ttag-marker の位置を合わせを 4 バイト境界に変換するための位置合わせバイトです。</p>

### 始める前に

PTP オフロードがグローバルにイネーブル化されていることを確認します。

### 手順の概要

1. **configure terminal**
2. **ttag-marker-interval seconds**

3. `interface type slot/port`
4. `[no] ttag-marker enable`
5. `ttag-strip`

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

## PTP 設定の確認

次のいずれかのコマンドを使用して、設定を確認します。

表 3: PTP Show コマンド

コマンド	目的
<code>show ptp brief</code>	PTP のステータスを表示します。
<code>show ptp clock</code>	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 <i>slot/port</i></b>	スイッチの PTP ポートのステータスを表示します。
<b>show ptp domain data</b>	複数のドメインデータ、ドメインプライオリティ、クロックしきい値、およびグランドマスター機能に関する情報を表示します。
<b>show ptp interface domain</b>	インターフェイスとドメインの関連付けに関する情報を表示します。
<b>show ptp cost</b>	PTP ポートとコストアソシエーションを表示します。
<b>show ptp detail</b>	各 PTP ポートに接続されているすべてのピアのリストが表示され、ルールが静的か動的かが示されます。
<b>show ptp time-property</b>	PTP クロック プロパティを表示します。



## 第 5 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 \(43 ページ\)](#)
- [時間サーバとしての NTP \(44 ページ\)](#)
- [CFS を使用した NTP の配信 \(44 ページ\)](#)
- [クロック マネージャ \(44 ページ\)](#)
- [仮想化のサポート \(45 ページ\)](#)
- [NTP の注意事項と制約事項 \(45 ページ\)](#)
- [デフォルト設定 \(46 ページ\)](#)
- [NTP の設定 \(46 ページ\)](#)
- [NTP の関連資料 \(60 ページ\)](#)
- [NTP 機能の履歴 \(60 ページ\)](#)

## 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)。
- 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。

## 時間サーバとしての NTP

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

## 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。

クロック マネージャを使用して、システム内のさまざまなクロックを制御するプロトコルを指定できます。プロトコルを指定すると、システム クロック更新が開始します。

## 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 の注意事項と制約事項

NTP に関する設定時の注意事項および制約事項は、次のとおりです。

- NTP 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 は、クロック プロトコルが NTP に設定されている場合に動作します。PTP と NTP を同時に構成することはサポートされていません。
- 別のデバイスとの間にピアアソシエーションを設定できるのは、使用するクロックの信頼性が確実な場合（つまり、信頼できる NTP サーバのクライアントである場合）に限られます。
- 単独で設定したピアは、サーバの役割を担いますが、バックアップとして使用する必要があります。サーバが 2 台ある場合、いくつかのデバイスが一方のサーバに接続し、残りのデバイスが他方のサーバに接続するように設定できます。その後、2 台のサーバ間にピアアソシエーションを設定すると、信頼性の高い NTP 構成になります。
- サーバが 1 台だけの場合は、すべてのデバイスをそのサーバのクライアントとして設定する必要があります。
- 設定できる NTP エンティティ（サーバおよびピア）は、最大 64 です。
- NTP に対して CFS がディセーブルになっていると、その NTP からコンフィギュレーションは配信されず、ネットワーク内の他のデバイスからの配信も受け取られません。
- NTP に対して CFS 配信をイネーブルにしても、commit コマンドを入力するまで、NTP コンフィギュレーション コマンドのエントリは NTP コンフィギュレーションに対してネットワークをロックします。ロック中は、ネットワーク内の（ロックを保持しているデバイス以外の）すべてのデバイスは NTP コンフィギュレーションを変更できません。
- CFS を使用して NTP をディセーブルにする場合、ネットワーク内のすべてのデバイスは、NTP に対して使用するよう設定したのと同じ VRF を持っている必要があります。
- VRF で NTP を設定する場合は、NTP サーバおよびピアが、設定された VRF を介して相互にアクセスできることを確認します。
- ネットワーク全体の NTP サーバおよび Cisco NX-OS デバイスに、NTP 認証キーを手動で配信する必要があります。

## デフォルト設定

表 4: デフォルトの NTP パラメータ

パラメータ	デフォルト
NTP 認証	無効
NTP アクセス	有効
NTP ログイン	無効

## NTP の設定

### NTP サーバーおよびピアの構成

NTP サーバーおよびピアを設定できます。

#### 始める前に

NTP サーバとそのピアの IP アドレスまたは DNS 名がわかっていることを確認します。

CFS を使用して他のデバイスに NTP コンフィギュレーションを配信する場合は、次を完了している必要があります。

- CFS 配信の有効化。
- CFS for NTP の有効化。

#### 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)# [ <b>no</b> ] <b>ntp server</b> { <i>ip-address</i>   <i>ipv6-address</i>   <i>dns-name</i> } [ <b>key</b> <i>key-id</i> ] [ <b>maxpoll</b> <i>max-poll</i> ] [ <b>minpoll</b> <i>min-poll</i> ] [ <b>prefer</b> ] [ <b>use-vrf</b> <i>vrf-name</i> ]	<p>1 つのサーバと 1 つのサーバ アソシエーションを形成します。</p> <p>NTP サーバとの通信で使用するキーを設定するには、<b>key</b> キーワードを使用します。key-id 引数の範囲は 1 ~ 65535 です。</p> <p>サーバをポーリングする最大および最小の間隔を設定するには、<b>maxpoll</b> および <b>minpoll</b> キーワードを使用します。max-poll および min-poll 引数の範囲は 4~16 (2 の累乗として設定されます。つまり、実質的に 16~65536 秒) で、デフォルト値はそれぞれ 6 と 4 です (maxpoll デフォルト = 64 秒、minpoll デフォルト = 16 秒)。</p> <p>これをデバイスの優先 NTP サーバーにするには、<b>prefer</b> キーワードを使用します。</p> <p>指定された VRF を介して通信するように NTP サーバを設定するには、<b>use-vrf</b> キーワードを使用します。vrf-name 引数として、default、management、または 32 文字までの任意の英数字の文字列を使用できます (大文字と小文字は区別されます)。</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)# [ <b>no</b> ] <b>ntp peer</b> { <i>ip-address</i>   <i>ipv6-address</i>   <i>dns-name</i> } [ <b>key</b> <i>key-id</i> ] [ <b>maxpoll</b> <i>max-poll</i> ] [ <b>minpoll</b> <i>min-poll</i> ] [ <b>prefer</b> ] [ <b>use-vrf</b> <i>vrf-name</i> ]	<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せん。</p> <p>NTP ピアとの通信で使用するキーを設定するには、<b>key</b> キーワードを使用します。key-id 引数の範囲は 1 ~ 65535 です。</p> <p>サーバをポーリングする最大および最小の間隔を設定するには、<b>maxpoll</b> および <b>minpoll</b> キーワードを使用します。max-poll および min-poll 引数の範</p>

	コマンドまたはアクション	目的
		<p>圏は4～16（2の累乗として設定されます。つまり、実質的に16～131072秒）で、デフォルト値はそれぞれ6と4です（<i>maxpoll</i> デフォルト=64秒、<i>minpoll</i> デフォルト=16秒）。</p> <p>これをデバイスの優先 NTP サーバーにするには、<b>prefer</b> キーワードを使用します。</p> <p>指定された VRF を介して通信するように NTP サーバを設定するには、<b>use-vrf</b> キーワードを使用します。<b>vrf-name</b> 引数として、<b>default</b>、<b>management</b>、または32文字までの任意の英数字の文字列を使用できます（大文字と小文字は区別されます）。</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>	<p>リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ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。</p>

### 例

NTP サーバおよびピアを設定する例を示します。

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ntp server 192.0.2.10 key 10 use-vrf Red
switch(config)# ntp peer 2001:0db8::4101 prefer use-vrf Red
switch(config)# show ntp peers
-----
Peer IP Address Serv/Peer
-----
2001:0db8::4101 Peer (configured)
192.0.2.10 Server (configured)
switch(config)# copy running-config startup-config
[#####] 100%
switch(config)#
```

## 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** コマンドによって指定されたいずれかの認証キーを時刻ソースが保持している場合のみ、デバイスはその時刻ソースと同期します。デバイスは、認証チェック

に失敗したすべてのパケットをドロップし、それらのパケットでローカルクロックがアップデートされないようにします。NTP 認証はデフォルトでディセーブルになっています。

### 始める前に

この手順で指定する予定の認証キーによって、NTP サーバが設定されていることを確認します。

### 手順の概要

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)# <b>[no] ntp authentication-key number md5 md5-string</b>	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 number</b> 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)# <b>[no] ntp trusted-key number</b>	1 つ以上のキーを指定します。デバイスが時刻ソースと同期するために、時刻ソースはこのキーを NTP パケット内に提供する必要があります。trusted key の範囲は 1 ~ 65535 です。  このコマンドにより、デバイスが、信頼されていない時刻源と誤って同期する、ということが防止されます。
ステップ 5	(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。

	コマンドまたはアクション	目的
ステップ 6	switch(config)# <b>[no] 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# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ntp authentication-key 42 md5 aNiceKey
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 {peer | serve | serve-only | query-only} access-list-name**
3. (任意) 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)# <b>[no] ntp access-group {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>• <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>• <b>serve</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>• <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>• <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> </ul>
ステップ 3	(任意) switch(config)# <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。
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構成する例を示します。

```
switch# config t
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。

NTP ソース IP アドレスを設定するには、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。

### 手順の概要

1. switch(config)# [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(config)# [no] ntp source ip-address	すべての NTP パケットにソース IP アドレスを設定します。 <i>ip-address</i> には IPv4 または IPv6 形式を使用できます。

### 例

次に、NTP をソース IP アドレスに構成する例を示します。

```
switch(config)# ntp source 192.0.2.1
```

## 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。

NTP ソース インターフェイスを設定するには、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。

#### 手順の概要

1. switch(config)# **[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(config)# <b>[no] 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。サポートされているインターフェイスのリストを表示するには、? キーワードを使用します。

#### 例

次に、NTP を特定のインターフェイスに構成する例を示します。

```
switch(config)# ntp source-interface
ethernet 2/1
```

## NTP ロギングの設定

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

#### 手順の概要

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**

#### 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。

	コマンドまたはアクション	目的
ステップ 2	switch(config)# <b>[no] 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 ログをイネーブルにする例を示します。

```
switch# config t
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)# <b>[no] 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、NTP のための CFS 配信をイネーブルにする例を示します。

```
switch# config t
Enter configuration commands, one per
line. End with CNTL/Z.
switch(config)# ntp distribute
switch(config)# copy running-config
startup-config
```

## NTP 構成変更のコミット

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。
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。

## 例

次に、NTP 構成の変更をコミットする例を示します。

```
switch(config)# ntp commit
```

## 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。

NTP コンフィギュレーションの変更を破棄するには、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。

## 手順の概要

1. 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(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。

**例**

次の例は、NTP の構成変更を破棄する方法を示しています。

```
switch(config)# ntp abort
```

## 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。

任意のデバイスからセッションロックを解放し、保留データベースの変更を破棄するには、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。

**手順の概要**

1. `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	<code>switch(config)# clear ntp session</code>	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。

**例**

次の例は、CFS セッション ロックを解放する方法を示しています。

```
switch(config)# clear ntp session
```

## NTP の設定確認

NTP 設定を表示するには、次のタスクのうちのいずれかを実行します。

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

**clear ntp statistics** コマンドを使用して、NTP 統計情報をクリアします。

**手順の概要**

1. `show ntp access-groups`
2. `show ntp authentication-keys`
3. `show ntp authentication-status`

4. `show ntp logging-status`
5. `show ntp peer-status`
6. `show ntp peers`
7. `show ntp pending`
8. `show ntp pending-diff`
9. `show ntp rts-update`
10. `show ntp session status`
11. `show ntp source`
12. `show ntp source-interface`
13. `show ntp statistics {io | local | memory | peer {ipaddr {ipv4-addr | ipv6-addr} | name peer-name}}`
14. `show ntp status`
15. `show ntp trusted-keys`
16. `show running-config ntp`

## 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>show ntp access-groups</code>	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 2	<code>show ntp authentication-keys</code>	設定済みの NTP 認証キーを表示します。
ステップ 3	<code>show ntp authentication-status</code>	NTP 認証の状況を表示します。
ステップ 4	<code>show ntp logging-status</code>	NTP のロギング状況を表示します。
ステップ 5	<code>show ntp peer-status</code>	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。
ステップ 6	<code>show ntp peers</code>	すべての NTP ピアを表示します。
ステップ 7	<code>show ntp pending</code>	NTP 用の一時 CFS データベースを表示します。
ステップ 8	<code>show ntp pending-diff</code>	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。
ステップ 9	<code>show ntp rts-update</code>	RTS アップデートの状況を表示します。
ステップ 10	<code>show ntp session status</code>	NTP CFS 配信セッションの情報を表示します。
ステップ 11	<code>show ntp source</code>	設定済みの NTP ソース IP アドレスを表示します。
ステップ 12	<code>show ntp source-interface</code>	設定済みの NTP ソース インターフェイスを表示します。

	コマンドまたはアクション	目的
ステップ 13	<code>show ntp statistics {io   local   memory   peer {ipaddr {ipv4-addr   ipv6-addr}   name peer-name}}</code>	NTP 統計情報を表示します。
ステップ 14	<code>show ntp status</code>	NTP CFS の配信状況を表示します。
ステップ 15	<code>show ntp trusted-keys</code>	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 16	<code>show running-config ntp</code>	NTP 情報を表示します。

## NTP の設定例

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

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ntp server 192.0.2.105 key 42
switch(config)# ntp peer 2001:0db8::4101
switch(config)# show ntp peers
-----
Peer IP Address          Serv/Peer
-----
2001:db8::4101          Peer (configured)
192.0.2.105             Server (configured)
switch(config)# ntp authentication-key 42 md5 aNiceKey
switch(config)# show ntp authentication-keys
-----
Auth key      MD5 String
-----
42            aNicekey
switch(config)# ntp trusted-key 42
switch(config)# show ntp trusted-keys
Trusted Keys:
42
switch(config)# ntp authenticate
switch(config)# show ntp authentication-status
Authentication enabled.
switch(config)# ntp logging
switch(config)# show ntp logging
NTP logging enabled.
switch(config)# copy running-config startup-config
[#####] 100%
switch(config)#
```

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

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

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

```

switch# config 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 の関連資料

関連項目	マニュアル タイトル
NTP CLI コマンド	<i>Cisco Nexus 3548</i> スイッチ <i>NX-OS</i> システム管理コマンドリファレンス ガイド

## NTP 機能の履歴

この表には、機能の追加や変更によるリリースの更新内容のみが記載されています。

機能名	リリース	機能情報
NTP	5.0(3)A1(1)	この機能が導入されました。



## 第 6 章

# システムメッセージロギングの設定

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概要, on page 61
- 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 (62 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 63
- システムメッセージロギングの設定 (63 ページ)
- DOM ロギングの構成 (78 ページ)
- システムメッセージロギングの設定確認, on page 79
- 繰り返されるシステムロギングメッセージ (80 ページ)

## システムメッセージロギングの概要

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

システムメッセージのフォーマットおよびデバイスが生成するメッセージの詳細については、『[Cisco NX-OS System Messages Reference](#)』を参照してください。

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

デフォルトでは、スイッチはシステムメッセージをログファイルに記録します。

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

**Table 5:** システムメッセージの重大度

レベル	説明
0 : 緊急	システムが使用不可
1 : アラート	即時処理が必要
2 : クリティカル	クリティカル状態

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

重大度 0、1、または 2 の最新のメッセージを 100 個まで不揮発性 RAM (NVRAM) ログに記録します。NVRAM へのロギングは設定できません。

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

## Syslogサーバ

syslog サーバーは、syslog プロトコルに基づいてシステムメッセージを記録するよう設定されたリモートシステムで稼働します。最大 8 台の syslog サーバーにログを送信するように Cisco Nexus シリーズスイッチを構成できます。CFS が有効の場合は、最大 3 台の syslog サーバーを構成できます。

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



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

## システムメッセージロギングの注意事項および制約事項

システムメッセージロギング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。
- Cisco NX-OS リリース 10.3(4a)M 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] [STRUCTURED-DATA] フィールドに値が使用できない場合、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**

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**。

## 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 6:** 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 2 でイネーブル
ログファイルロギング	重大度 5 のメッセージロギングがイネーブル
モジュールロギング	重大度 5 でイネーブル
ファシリティロギング	イネーブル
タイムスタンプ単位	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

### ターミナルセッションへのシステムメッセージロギングの設定

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

デフォルトでは、ターミナルセッションでロギングはイネーブルです。

## SUMMARY STEPS

1. switch# **terminal monitor**
2. switch# **configure terminal**
3. switch(config)# **logging console** [*severity-level*]
4. (Optional) switch(config)# **no logging console** [*severity-level*]
5. switch(config)# **logging monitor** [*severity-level*]
6. (Optional) switch(config)# **no logging monitor** [*severity-level*]
7. (Optional) switch# **show logging console**
8. (Optional) switch# **show logging monitor**
9. (Optional) switch# **copy running-config startup-config**

## DETAILED STEPS

## Procedure

	Command or Action	Purpose
ステップ 1	switch# <b>terminal monitor</b>	コンソールから現在の端末セッションに syslog メッセージをコピーします。
ステップ 2	switch# <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 3	switch(config)# <b>logging console</b> [ <i>severity-level</i> ]	<p>指定されたシビラティ（重大度）（またはそれ以上）に基づくコンソールセッションへのメッセージの記録をイネーブルにします（数字が小さいほうがシビラティ（重大度）が高いことを示します）。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>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。</p>
ステップ 4	(Optional) switch(config)# <b>no logging console</b> [ <i>severity-level</i> ]	コンソールへのログギングメッセージをディセーブルにします。

	Command or Action	Purpose
ステップ 5	switch(config)# <b>logging monitor</b> [severity-level]	<p>指定されたシビラティ（重大度）（またはそれ以上）に基づくモニターへのメッセージの記録をイネーブルにします（数字が小さいほうがシビラティ（重大度）が高いことを示します）。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>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。</p> <p>設定は Telnet および SSH セッションに適用されます。</p>
ステップ 6	(Optional) switch(config)# <b>no logging monitor</b> [severity-level]	Telnet および SSH セッションへのメッセージロギングをディセーブルにします。
ステップ 7	(Optional) switch# <b>show logging console</b>	コンソール ロギング設定を表示します。
ステップ 8	(Optional) switch# <b>show logging monitor</b>	モニタ ロギング設定を表示します。
ステップ 9	(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、コンソールのロギング レベルを 3 に設定する例を示します。

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

次に、コンソールのロギングの設定を表示する例を示します。

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

次に、コンソールのロギングをディセーブルにする例を示します。

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

次に、ターミナルセッションのロギングレベルを4に設定する例を示します。

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

次に、ターミナルセッションのロギングの設定を表示する例を示します。

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

次に、ターミナルセッションのロギングをディセーブルにする例を示します。

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

## ファイルへのシステムメッセージロギングの設定

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

### SUMMARY STEPS

1. `switch# configure terminal`
2. `switch(config)# logging logfile logfile-name severity-level [ size bytes]`
3. (Optional) `switch(config)# no logging logfile [logfile-name severity-level [ size bytes]]`
4. (Optional) `switch# show logging info`
5. (Optional) `switch# copy running-config startup-config`

### DETAILED STEPS

#### Procedure

	Command or Action	Purpose
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)# logging logfile logfile-name severity-level [ size bytes]</code>	システムメッセージを保存するのに使用するログファイルの名前と、記録する最小シビラティ（重大度）を設定します。任意で最大ファイルサイズを指

	Command or Action	Purpose
		<p>定できます。デフォルトの重大度は5です。ファイルサイズは4194304です。</p> <p>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>ファイルサイズは4096～10485760バイトです。</p>
ステップ 3	(Optional) switch(config)# <b>no logging logfile</b> [ <i>logfile-name severity-level</i> [ <b>size bytes</b> ]]	ログファイルへのロギングをディセーブルにします。任意で最大ファイルサイズを指定できます。デフォルトの重大度は5です。ファイルサイズは4194304です。
ステップ 4	(Optional) switch# <b>show logging info</b>	ロギング設定を表示します。任意で最大ファイルサイズを指定できます。デフォルトの重大度は5です。ファイルサイズは4194304です。
ステップ 5	(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、システムメッセージをファイルに記録するようスイッチを設定する例を示します。

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

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

```
switch# show logging info
Logging console:           enabled (Severity: debugging)
Logging monitor:          enabled (Severity: debugging)
Logging timestamp:        Seconds
Logging server:           disabled
Logging logfile:          enabled
```

```

Name - my_log: Severity - informational Size - 4194304
Facility      Default Severity      Current Session Severity
-----
aaa           3                          3
afm           3                          3
altos        3                          3
auth         0                          0
authpriv     3                          3
bootvar      5                          5
callhome     2                          2
capability   2                          2
cdp          2                          2
cert_enroll  2                          2
...

```

## モジュールおよびファシリティメッセージのログの設定

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. switch# **configure terminal**
2. switch(config)# **logging module** [*severity-level*]
3. switch(config)# **logging level** *facility severity-level*
4. (Optional) switch(config)# **no logging module** [*severity-level*]
5. (Optional) switch(config)# **no logging level** [*facility severity-level*]
6. (Optional) switch# **show logging module**
7. (Optional) switch# **show logging level** [*facility*]
8. (Optional) switch# **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>logging module</b> [ <i>severity-level</i> ]	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> </ul>

	Command or Action	Purpose
		<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>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。</p>
ステップ 3	<code>switch(config)# logging level facility severity-level</code>	<p>指定された重大度またはそれ以上の重大度である指定のファシリティからのロギングメッセージをイネーブルにします。重大度は 0 ~ 7 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>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。デフォルト値については、<b>show logging level</b> コマンドを参照してください。</p> <p><b>Note</b> コンポーネントの現行セッションのシビラティ（重大度）がデフォルトのシビラティ（重大度）と同じ場合には、実行構成でそのコンポーネントのログレベルが表示されないことが予想されます。</p>
ステップ 4	(Optional) <code>switch(config)# no logging module [severity-level]</code>	モジュール ログ メッセージをディセーブルにします。
ステップ 5	(Optional) <code>switch(config)# no logging level [facility severity-level]</code>	指定されたファシリティのロギングシビラティ（重大度）をデフォルトレベルにリセットします。ファシリティおよびシビラティ（重大度）を指定しないと、スイッチはすべてのファシリティをデフォルトレベルにリセットします。

	Command or Action	Purpose
ステップ 6	(Optional) switch# <b>show logging module</b>	モジュール ロギング設定を表示します。
ステップ 7	(Optional) switch# <b>show logging level</b> [facility]	ファシリティごとに、ロギング レベル設定およびシステムのデフォルト レベルを表示します。ファシリティを指定しないと、スイッチはすべてのファシリティのレベルを表示します。
ステップ 8	(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、モジュールおよび特定のファシリティメッセージのシビラティ（重大度）を設定する例を示します。

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

## ロギング タイムスタンプの設定

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

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **logging timestamp** {microseconds | milliseconds | seconds}
3. (Optional) switch(config)# **no logging timestamp** {microseconds | milliseconds | seconds}
4. (Optional) switch# **show logging timestamp**
5. (Optional) switch# **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>logging timestamp</b> {microseconds   milliseconds   seconds}	ロギング タイムスタンプ単位を設定します。デフォルトでは、単位は秒です。

	Command or Action	Purpose
ステップ 3	(Optional) switch(config)# <b>no logging timestamp</b> {microseconds   milliseconds   seconds}	ロギングタイムスタンプ単位をデフォルトの秒にリセットします。
ステップ 4	(Optional) switch# <b>show logging timestamp</b>	設定されたロギングタイムスタンプ単位を表示します。
ステップ 5	(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、メッセージのタイムスタンプ単位を設定する例を示します。

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

## 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：

- **[no] logging rfc-strict 5424**
- **show logging rfc-strict 5424**

### 手順の概要

1. switch(config)#**[no] 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)# <b>[no] logging rfc-strict 5424</b>	(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がある RFC を設定します。
ステップ 3	switch(config)# <b>show logging rfc-strict 5424</b>	RFC 5424 に準拠する syslog を表示します

## syslog サーバの設定

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

### SUMMARY STEPS

1. **configure terminal**
2. **logging server** *host* [*severity-level* [ **use-vrf** *vrf-name* [ **facility** *facility*]]]
3. (Optional) **no logging server** *host*
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>logging server</b> <i>host</i> [ <i>severity-level</i> [ <b>use-vrf</b> <i>vrf-name</i> [ <b>facility</b> <i>facility</i> ]]]	ホストが syslog メッセージを受信するように設定します。 <ul style="list-style-type: none"> <li>• <i>host</i> 引数は、syslog サーバ ホストのホスト名または IPv4 または IPv6 アドレスを示します。</li> <li>• <i>severity-level</i> 引数は、指定したレベルに syslog サーバへのメッセージのロギングを制限します。シビラティ（重大度）は 0～7 の範囲です。Table 5: システムメッセージの重大度, on page 61 を参照してください。</li> <li>• <b>use vrf</b> <i>vrf-name</i> 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。特定の VRF が指定されない場合は、<b>management</b> がデフォルトです。</li> </ul> <p><b>show running</b> コマンドの出力には、次の構成シナリオに基づいて VRF が表示される場合と表示されない場合があります：</p> <ul style="list-style-type: none"> <li>• VRF が構成されていない場合、システムは管理 VRF をデフォルトとして使用します。この VRF は出力に表示されません。</li> </ul>

	Command or Action	Purpose
		<ul style="list-style-type: none"> <li>管理 VRF が構成済みである。その後、この VRF は、システムがデフォルトとして識別するため、 の出力には表示されません。</li> <li>その他の VRF が構成されています。それから、この VRF が出力に表示されます。</li> </ul> <p><b>Note</b> 現在の Cisco Fabric Services (CFS) 配信では VRF をサポートしていません。CFS 配信がイネーブルの場合、デフォルト VRF で構成されているロギングサーバーは管理 VRF として配布されます。</p> <ul style="list-style-type: none"> <li>facility 引数は syslog ファシリティタイプを指定します。デフォルトの発信ファシリティは local7 です。</li> </ul> <p>ファシリティは、使用している Cisco Nexus シリーズ ソフトウェアのコマンドリファレンスに記載されています。</p> <p><b>Note</b> デバッグは CLI ファシリティですが、デバッグの syslog はサーバーに送信されません。</p>
ステップ 3	(Optional) <b>no logging server host</b> <b>Example:</b> <pre>switch(config)# no logging server 172.28.254.254 5</pre>	指定されたホストのロギングサーバーを削除します。
ステップ 4	(Optional) <b>show logging server</b> <b>Example:</b> <pre>switch# show logging server</pre>	Syslog サーバー構成を表示します。
ステップ 5	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> <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。

### Example

次に、syslog サーバーを設定する例を示します。

```
switch# configure terminal
switch(config)# logging server 172.28.254.254 5
```

```
use-vrf default facility local3

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

## UNIX または Linux システムでの syslog の設定

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

```
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。

**Table 7: 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。  <b>Note</b> 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、前にアットマーク (@) が付いたホスト名、カンマで区切られたユーザー リストです。アスタリスク (*) を使用するとすべてのログインユーザーを指定します。

### SUMMARY STEPS

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。

## DETAILED STEPS

### Procedure

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

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

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

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

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

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

## syslog サーバー設定の配布の設定

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

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



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

### Before you begin

1 つまたは複数の syslog サーバーを設定しておく必要があります。

## SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **logging distribute**
3. switch(config)# **logging commit**
4. switch(config)# **logging abort**
5. (Optional) switch(config)# **no logging distribute**
6. (Optional) switch# **show logging pending**

7. (Optional) switch# **show logging pending-diff**
8. (Optional) switch# **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>logging distribute</b>	CFS インフラストラクチャを使用して、ネットワーク スイッチへの <b>syslog</b> サーバー設定の配布をイネーブルにします。デフォルトでは、配布はディセーブルです。
ステップ 3	switch(config)# <b>logging commit</b>	ファブリック内のスイッチへ配布するための Syslog サーバー設定に対する保留中の変更をコミットします。
ステップ 4	switch(config)# <b>logging abort</b>	Syslog サーバー設定に対する保留中の変更をキャンセルします。
ステップ 5	(Optional) switch(config)# <b>no logging distribute</b>	CFS インフラストラクチャを使用して、ネットワーク スイッチへの <b>syslog</b> サーバー設定の配布をディセーブルにします。設定変更が保留中の場合は、配布をディセーブルにできません。 <b>logging commit</b> および <b>logging abort</b> コマンドを参照してください。デフォルトでは、配布はディセーブルです。
ステップ 6	(Optional) switch# <b>show logging pending</b>	Syslog サーバー設定に対する保留中の変更を表示します。
ステップ 7	(Optional) switch# <b>show logging pending-diff</b>	syslog サーバー設定の保留中の変更に対して、現在の syslog サーバー設定との違いを表示します。
ステップ 8	(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。

## 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. switch# **show logging last number-lines**
2. switch# **show logging logfile** [ **start-time** yyyy mmm dd hh:mm:ss ] [ **end-time** yyyy mmm dd hh:mm:ss ]

3. switch# **show logging nvram** [ *last number-lines*]
4. switch# **clear logging logfile**
5. switch# **clear logging nvram**

## DETAILED STEPS

### Procedure

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

### Example

次に、ログファイルのメッセージを表示する例を示します。

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

次に、ログファイルのメッセージをクリアする例を示します。

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

# DOM ロギングの構成

## DOM ロギングの有効化

### 手順の概要

1. switch# **configure terminal**
2. switch(config)# **system ethernet dom polling**

### 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>system ethernet dom polling</b>	トランシーバのデジタル オプティカル モニタリングの定期的なポーリングを有効にします。

### 例

次に、DOM ロギングを有効にする例を示します。

```
switch# configure terminal
switch(config)# system ethernet dom polling
```

## DOM ロギングの無効化

### 手順の概要

1. switch# **configure terminal**
2. switch(config)# **no system ethernet dom polling**

### 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。

	コマンドまたはアクション	目的
ステップ 2	<code>switch(config)# no system ethernet dom polling</code>	トランシーバのデジタル オプティカル モニタリングの定期的なポーリングを無効にします。

### 例

次の例は、DOM ロギングを無効にする方法を示しています。

```
switch# configure terminal
switch(config)# no system ethernet dom polling
```

## DOM ロギング構成の確認

コマンド	目的
<code>show system ethernet dom polling status</code>	トランシーバのデジタルオプティカルモニタリングの定期的なポーリング ステータスを表示します。

## システム メッセージ ロギングの設定確認

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

コマンド	目的
<code>show logging console</code>	コンソール ロギング設定を表示します。
<code>show logging info</code>	ロギング設定を表示します。
<code>show logging ip access-list cache</code>	IP アクセス リスト キャッシュを表示します。
<code>show logging ip access-list cache detail</code>	IP アクセス リスト キャッシュに関する詳細情報を表示します。
<code>show logging ip access-list status</code>	IP アクセス リスト キャッシュのステータスを表示します。
<code>show logging last <i>number-lines</i></code>	ログ ファイルの末尾から指定行数を表示します。
<code>show logging level [<i>facility</i>]</code>	ファシリティ ロギングシビラティ（重大度）設定を表示します。
<code>show logging logfile [ <i>start-time</i> yyyy mmm dd hh:mm:ss ] [ <i>end-time</i> yyyy mmm dd hh:mm:ss ]</code>	ログ ファイルのメッセージを表示します。

コマンド	目的
<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 number-lines]</b>	NVRAM ログのメッセージを表示します。
<b>show logging pending</b>	Syslog サーバーの保留中の配布設定を表示します。
<b>show logging pending-diff</b>	Syslog サーバーの保留中の配布設定の違いを表示します。
<b>show logging server</b>	Syslog サーバー設定を表示します。
<b>show logging session</b>	ロギングセッションのステータスを表示します。
<b>show logging status</b>	ロギングステータスを表示します。
<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。

## 繰り返されるシステム ロギング メッセージ

システム プロセスはロギングメッセージを生成します。生成される重大度レベルを制御するために使用されるフィルタによっては、多数のメッセージが生成され、その多くが繰り返されます。

ロギングメッセージの量を管理するスクリプトの開発を容易にし、**show logging log** コマンドの出力の「フラッディング」から繰り返されるメッセージを排除するために、繰り返されるメッセージをロギングする次の方法が使用されます。

以前の方法では、同じメッセージが繰り返された場合、デフォルトでは、メッセージ内でメッセージが再発生した回数が表示されていました。

```
2019 Mar 11 13:42:44 Cisco-customer %PTP-2-PTP_INCORRECT_PACKET_ON_SLAVE:
Incorrect delay response packet received on slave interface Eth1/48 by
2c:5a:0f:ff:fe:51:e9:9f. Source Port Identity is 08:00:11:ff:fe:22:3e:4e. Requesting
Port
Identity is 00:1c:73:ff:ff:ee:f6:e5
2019 Mar 11 13:43:15 Cisco-customer last message repeated 242 times
```

新しいメソッドは、繰り返しメッセージの最後に繰り返し回数を追加するだけです。

```
2019 Mar 11 13:42:44 Cisco-customer %PTP-2-PTP_INCORRECT_PACKET_ON_SLAVE:
Incorrect delay response packet received on slave interface Eth1/48 by
2c:5a:0f:ff:fe:51:e9:9f. Source Port Identity is 08:00:11:ff:fe:22:3e:4e. Requesting
Port
Identity is 00:1c:73:ff:ff:ee:f6:e5

2019 Mar 11 13:43:15 Cisco-customer %PTP-2-PTP_INCORRECT_PACKET_ON_SLAVE:
Incorrect delay response packet received on slave interface Eth1/48 by
2c:5a:0f:ff:fe:51:e9:9f. Source Port Identity is 08:00:11:ff:fe:22:3e:4e. Requesting
Port
Identity is 00:1c:73:ff:ff:ee:f6:e5 (message repeated 242 times)
```



## 第 7 章

# Smart Call Home の設定

この章は、次の内容で構成されています。

- [Smart Call Home に関する情報, on page 81](#)
- [Smart Call Home の注意事項および制約事項 \(91 ページ\)](#)
- [Smart Call Home の前提条件, on page 91](#)
- [Call Home のデフォルト設定, on page 91](#)
- [Smart Call Home の設定 \(92 ページ\)](#)
- [Smart Call Home 設定の確認, on page 106](#)
- [フルテキスト形式での syslog アラート通知の例, on page 106](#)
- [XML 形式での syslog アラート通知の例, on page 107](#)

## Smart Call Home に関する情報

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。

- 継続的なデバイス ヘルス モニタリングとリアルタイムの診断アラート。
- ご使用のデバイスからの Smart Call Home メッセージの分析と、必要に応じた自動サービス リクエストの生成は、問題を迅速に解決するための詳細な診断情報とともに、適切な TAC チームにルーティングされます。

- セキュアなメッセージ転送が、ご使用のデバイスから直接、またはダウンロード可能な Transport Gateway (TG) 集約ポイントを経由して行われます。複数のデバイスでサポートを必要としている場合、またはセキュリティ要件の関係でご使用のデバイスをインターネットに直接接続できない場合は、TG 集約ポイントを使用できます。
- Smart Call Home メッセージと推奨事項、すべての Smart Call Home デバイスのインベントリおよび設定情報、および Field Notice、セキュリティ勧告、およびサポート終了日情報への Web ベースのアクセス。

## Smart Call Home の概要

Smart Call Home を使用すると、重要なイベントがデバイスで発生した場合に外部エンティティに通知できます。Smart Call Home では、ユーザ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 8:** 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 宛での、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>

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でないイベントであり、情報はステータスおよび使用権に使用されます。	<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。

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

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

## Smart Call Home のメッセージ レベル

Smart Call Home を使用すると、緊急度に基づいてメッセージをフィルタリングできます。各宛先プロファイル（定義済みおよびユーザー定義）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 9:** 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 10:** ショートテキストメッセージフォーマット

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

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

**Table 11:** 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、<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>• <i>@</i> は区切り文字です。</li> <li>• <i>Sid</i> は C で、シリアル ID をシャーマ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識別される番号です。</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

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、<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>• <i>@</i> は区切り文字です。</li> <li>• <i>Sid</i> は C で、シリアル ID をシャード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識別される番号です。</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
モデル名	デバイスのモデル名（製品ファミリー名に含まれる具体的なモデル）。	/aml/body/chassis/name

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 12:** 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
FRU スロット	イベントメッセージを生成する FRU のスロット番号。	/aml/body/fru/slot

データ項目（プレーンテキストおよび XML）	説明（プレーンテキストおよび XML）	XML タグ（XML のみ）
FRU ハードウェア バージョン	関連 FRU のハードウェアバージョン。	/aml/body/fru/hwVersion
FRU ソフトウェアのバージョン	関連 FRU で稼働しているソフトウェアバージョン。	/aml/body/fru/swVersion

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 13: 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 14: 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
プロセス状態	プロセスの状態（実行中、中止など）	/aml/body/process/processState

データ項目（プレーンテキストおよび XML）	説明（プレーンテキストおよび XML）	XML タグ（XML のみ）
プロセス例外	原因コードの例外	/aml/body/process/exception

## Smart Call Home の注意事項および制約事項

- IP 接続がない場合、またはプロファイル宛先への仮想ルーティングおよびフォワーディング（VRF）インスタンス内のインターフェイスがダウンしている場合、スイッチは Smart Call Home メッセージを送信できません。
- 任意の SMTP 電子メール サーバーで動作します。

## 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 15: 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

パラメータ	デフォルト
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

1. ブラウザで、次の Smart Call Home Web ページに移動します。
2. **[Getting Started]** 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]** 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。
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>	<p>スイッチの担当者の電子メールアドレスを設定します。</p> <p><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。</p> <p><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。</p>
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。

	Command or Action	Purpose
		<p><b>Note</b></p> <p>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。</p>
ステップ 6	switch(config-callhome)# <b>streetaddress</b> <i>address</i>	<p>スイッチの主担当者の住所を設定します。</p> <p><i>address</i> には、最大 255 の英数字を使用できます。スペースを使用できます。</p>
ステップ 7	(Optional) switch(config-callhome)# <b>contract-id</b> <i>contract-number</i>	<p>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。</p> <p><i>contract-number</i> には最大 255 の英数字を使用できます。</p>
ステップ 8	(Optional) switch(config-callhome)# <b>customer-id</b> <i>customer-number</i>	<p>サービス契約からこのスイッチの顧客番号を設定します。</p> <p><i>customer-number</i> には最大 255 の英数字を使用できます。</p>
ステップ 9	(Optional) switch(config-callhome)# <b>site-id</b> <i>site-number</i>	<p>このスイッチのサイト番号を設定します。</p> <p><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。</p>
ステップ 10	(Optional) switch(config-callhome)# <b>switch-priority</b> <i>number</i>	<p>このスイッチのスイッチプライオリティを設定します。</p> <p>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。</p> <p><b>Note</b></p> <p>スイッチのプライオリティは、運用要員または TAC サポート要員によって、最初に対処すべき Call Home メッセージを決定するために使用されます。各スイッチから送信されるシビラティ (重大度) が同じ Call Home アラートに優先順位を設定できます。</p>
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>	リポ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}} | **profilename** { **alert-group** group | **email-addr** address | **format** {XML | full-txt | short-txt} | **http** URL | **message-level** level | **message-size** size | **transport-method** {email | http}} | **full-txt-destination** { **alert-group** group | **email-addr** address | **http** URL | **message-level** level | **message-size** size | **transport-method** {email | http}} | **short-txt-destination** { **alert-group** group | **email-addr** address | **http** URL | **message-level** level | **message-size** size | **transport-method** {email | http}}}}
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</b> {ciscoTAC-1 { <b>alert-group</b> group   <b>email-addr</b> address   <b>http</b> URL   <b>transport-method</b> {email   http}}	新しい宛先プロファイルを作成し、そのプロファイルのメッセージフォーマットを設定します。プロ

	Command or Action	Purpose
	<code>profilename { alert-group group   email-addr address   format {XML   full-txt   short-txt}   http URL   message-level level   message-size size   transport-method {email   http} }   full-txt-destination { alert-group group   email-addr address   http URL   message-level level   message-size size   transport-method {email   http} }   short-txt-destination { alert-group group   email-addr address   http URL   message-level level   message-size size   transport-method {email   http} }</code>	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) <code>switch# show callhome destination-profile [ profile name]</code>	1 つまたは複数の宛先プロファイルに関する情報を表示します。
ステップ 5	(Optional) <code>switch(config)# copy running-config startup-config</code>	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
```

## 宛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。

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

	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</b> { <i>name</i>   <b>full-txt-destination</b>   <b>short-txt-destination</b> } <b>email-addr</b> <i>address</i>	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。宛先プロファイルには、最大 50 個の E メールアドレスを設定できます。
ステップ 4	<b>destination-profile</b> { <i>name</i>   <b>full-txt-destination</b>   <b>short-txt-destination</b> } <b>message-level</b> <i>number</i>	この宛先プロファイルの 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> に指定できる範囲は 0～9 です。9 は最大のシビラティ（重大度）を示します。
ステップ 5	switch(config-callhome)# <b>destination-profile</b> { <i>name</i>   <b>full-txt-destination</b>   <b>short-txt-destination</b> } <b>message-size</b> <i>number</i>	この宛先プロファイルの最大メッセージサイズを設定します。 <b>full-txt-destination</b> の値の範囲は 0～5000000 で、デフォルトは 2500000 です。 <b>short-txt-destination</b> の値の範囲は 0～100000 で、デフォルトは 4000 です。CiscoTAC-1 では、値は 5000000 で、これは変更不可能です。
ステップ 6	(Optional) switch# <b>show callhome destination-profile</b> [ <i>profile name</i> ]	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</b> <i>name</i> <b>alert-group</b> { <b>All</b>   <b>Cisco-TAC</b>   <b>Configuration</b>   <b>Diagnostic</b>   <b>Environmental</b>   <b>Inventory</b>   <b>License</b>   <b>Linecard-Hardware</b>   <b>Supervisor-Hardware</b>   <b>Syslog-group-port</b>   <b>System</b>   <b>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。キーワード <b>All</b> 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</b> [ <b>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。

	Command or Action	Purpose
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

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

## アラートグループへの show コマンドの追加

1つのアラートグループには、最大5個のユーザー定義 **show** コマンドを割り当てることができます。

### SUMMARY STEPS

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

	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。

	Command or Action	Purpose
ステップ 3	switch(config-callhome)# <b>alert-group</b> { <b>Configuration</b>   <b>Diagnostic</b>   <b>Environmental</b>   <b>Inventory</b>   <b>License</b>   <b>Linecard-Hardware</b>   <b>Supervisor-Hardware</b>   <b>Syslog-group-port</b>   <b>System</b>   <b>Test</b> } <b>user-def-cmd</b> <i>show-cmd</i>	<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> コマンドだけが受け入れられます。  <b>Note</b> CiscoTAC-1 宛先プロファイルには、ユーザー定義の <b>show</b> コマンドを追加できません。
ステップ 4	(Optional) switch# <b>show callhome user-def-cmds</b>	アラート グループに追加されたすべてのユーザー定義 <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

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

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

### 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	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>transport email smtp-server ip-address [ port number] [ use-vrf vrf-name]</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。  番号の範囲は 1 ~ 65535 です。デフォルトのポート番号は 25 です。  この SMTP サーバ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) switch(config-callhome)# <b>transport email from email-address</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) switch(config-callhome)# <b>transport email reply-to email-address</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) switch# <b>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) 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 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

	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>periodic-inventory notification</b> [ <b>interval days</b> ] [ <b>timeofday time</b> ]	定期的なインベントリ メッセージを設定します。 <b>interval days</b> の範囲は 1 ~ 30 日です。 デフォルトは 7 日です。 <b>timeofday time</b> は HH:MM の形式です。
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 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>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。
ステップ 3	switch(config-callhome) # <b>[no] enable</b>	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)# <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)# 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**

## 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。
<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:2018-02-08T11:10:44
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:2018 Feb  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, Feb 25, 2018 7:20 AM
To: User (user)
Subject: System Notification From Router - syslog - 2018-02-25 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>2018-02-25 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>2018-02-25 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>abcdefgl2345</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 0x20000
00:00:54: RP: Currently running ROMMON from F2 region
00:01:05: %SYS-5-CONFIG_I: Configured from memory by console
]]>

```

```
00:01:09: %SYS-5-RESTART: System restarted --Cisco IOS Software,
s72033_rp Software (s72033_rp-ADVENTERPRISEK9_DBG-VM), Experimental
Version 12.2(20070421:012711) Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Thu 26-Feb-18 15:54 by xxx
Firmware compiled 11-Apr-07 03:34 by integ Build [100]00:01:01: %PFREDUN-6-ACTIVE:
  Initializing as ACTIVE processor for this switch00:01:01: %SYS-3-LOGGER_FLUSHED:
System was paused for 00:00:00 to ensure console debugging output.00:03:00: SP: SP:
  Currently running ROMMON from F1 region00:03:07: %C6K_PLATFORM-SP-4-CONFREG_BREAK
_ENABLED: The default factory setting for config register is 0x2102.It is advisable
to retain 1 in 0x2102 as it prevents returning to ROMMON when break is issued.00:03:18:

%SYS-SP-5-RESTART: System restarted --Cisco IOS Software, s72033_sp Software
(s72033_sp-ADVENTERPRISEK9_DBG-VM), Experimental Version 12.2(20070421:012711)Copyright
(c) 1986-2007 by Cisco Systems, Inc.
Compiled Thu 26-Apr-07 18:00 by xxx
00:03:18: %SYS-SP-6-BOOTTIME: Time taken to reboot after reload = 339 seconds
00:03:18: %OIR-SP-6-INSPS: Power supply inserted in slot 1
00:03:18: %C6KPWR-SP-4-PSOK: power supply 1 turned on.
00:03:18: %OIR-SP-6-INSPS: Power supply inserted in slot00:01:09: %SSH-5-ENABLED:
  SSH 1.99 has been enabled
00:03:18: %C6KPWR-SP-4-PSOK: power supply 2 turned on.
00:03:18: %C6KPWR-SP-4-PSREDUNDANTMISMATCH: power supplies rated outputs do not match.
00:03:18: %C6KPWR-SP-4-PSREDUNDANTBOTHSUPPLY: in power-redundancy mode, system is
operating on both power supplies.
00:01:10: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
00:01:10: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
00:03:20: %C6KENV-SP-4-FANHIOUTPUT: Version 2 high-output fan-tray is in effect
00:03:22: %C6KPWR-SP-4-PSNOREDUNDANCY: Power supplies are not in full redundancy,
power usage exceeds lower capacity supply
00:03:26: %FABRIC-SP-5-FABRIC_MODULE_ACTIVE: The Switch Fabric Module in slot 6
became active.
00:03:28: %DIAG-SP-6-RUN_MINIMUM: Module 6: Running Minimal Diagnostics...
00:03:50: %DIAG-SP-6-DIAG_OK: Module 6: Passed Online Diagnostics
00:03:50: %OIR-SP-6-INSCARD: Card inserted in slot 6, interfaces are now online
00:03:51: %DIAG-SP-6-RUN_MINIMUM: Module 3: Running Minimal Diagnostics...
00:03:51: %DIAG-SP-6-RUN_MINIMUM: Module 7: Running Minimal Diagnostics...
00:03:51: %DIAG-SP-6-RUN_MINIMUM: Module 9: Running Minimal Diagnostics...
00:01:51: %MFIB_CONST_RP-6-REPLICATION_MODE_CHANGE: Replication Mode Change Detected.
  Current system replication mode is Ingress
00:04:01: %DIAG-SP-6-DIAG_OK: Module 3: Passed Online Diagnostics
00:04:01: %OIR-SP-6-DOWNGRADE: Fabric capable module 3 not at an appropriate hardware
revision level, and can only run in flowthrough mode
00:04:02: %OIR-SP-6-INSCARD: Card inserted in slot 3, interfaces are now online
00:04:11: %DIAG-SP-6-DIAG_OK: Module 7: Passed Online Diagnostics
00:04:14: %OIR-SP-6-INSCARD: Card inserted in slot 7, interfaces are now online
00:04:35: %DIAG-SP-6-DIAG_OK: Module 9: Passed Online Diagnostics
00:04:37: %OIR-SP-6-INSCARD: Card inserted in slot 9, interfaces are now online
00:00:09: DaughterBoard (Distributed Forwarding Card 3)
Firmware compiled 11-Apr-07 03:34 by integ Build [100]
00:00:22: %SYS-DFC4-5-RESTART: System restarted --
Cisco DCOS Software, c6lc2 Software (c6lc2-SPDBG-VM), Experimental Version 4.0
(20080421:012711)Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Thu 26-Feb-18 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-Feb-18 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-Feb-18 16:40 by username1
00:00:25: DFC1: Currently running ROMMON from F2 region
00:05:30: %DIAG-SP-6-DIAG_OK: Module 4: Passed Online Diagnostics
00:05:31: %SPAN-SP-6-SPAN_EGRESS_REPLICATION_MODE_CHANGE: Span Egress HW
Replication Mode Change Detected. Current replication mode for unused asic
session 0 is Centralized
00:05:31: %SPAN-SP-6-SPAN_EGRESS_REPLICATION_MODE_CHANGE: Span Egress HW
Replication Mode Change Detected. Current replication mode for unused asic
session 1 is Centralized
00:05:31: %OIR-SP-6-INSCARD: Card inserted in slot 4, interfaces are now online
00:06:02: %DIAG-SP-6-DIAG_OK: Module 1: Passed Online Diagnostics
00:06:03: %OIR-SP-6-INSCARD: Card inserted in slot 1, interfaces are now online
00:06:31: %DIAG-SP-6-DIAG_OK: Module 2: Passed Online Diagnostics
00:06:33: %OIR-SP-6-INSCARD: Card inserted in slot 2, interfaces are now online
00:04:30: %XDR-6-XDRIPCNOTIFY: Message not sent to slot 4/0 (4) because of IPC
error timeout. Disabling linecard. (Expected during linecard OIR)
00:06:59: %DIAG-SP-6-DIAG_OK: Module 8: Passed Online Diagnostics
00:06:59: %OIR-SP-6-DOWNGRADE_EARL: Module 8 DFC installed is not identical to
system PFC and will perform at current system operating mode.
00:07:06: %OIR-SP-6-INSCARD: Card inserted in slot 8, interfaces are now online
Router#]]>
</aml-block:Data>
</aml-block:Attachment>
</aml-block:Attachments>
</aml-block:Block>
</soap-env:Body>
</soap-env:Envelope>
```



## 第 8 章

# Session Manager の設定

この章は、次の内容で構成されています。

- [Session Manager の概要, on page 111](#)
- [Session Manager の注意事項および制約事項 \(111 ページ\)](#)
- [Session Manager の設定 \(112 ページ\)](#)
- [Session Manager 設定の確認, on page 114](#)

## Session Manager の概要

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

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

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

## Session Manager の注意事項および制約事項

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

- Session Manager は、アクセス コントロール リスト (ACL) 機能のみサポートします。
- 作成できるコンフィギュレーションセッションの最大数は 32 です。
- すべてのセッションで設定できるコマンドの最大数は 20,000 です。

## Session Manager の設定

### セッションの作成

作成できるコンフィギュレーションセッションの最大数は 32 です。

#### SUMMARY STEPS

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

#### DETAILED STEPS

##### Procedure

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

1. switch# **configure session** *name*
2. switch(config-s)# **ip access-list** *name*
3. (Optional) switch(config-s-acl)# **permit** *protocol source destination*
4. switch(config-s-acl)# **interface** *interface-type number*

5. 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</b> <i>name</i>	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</b> <i>name</i>	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</b> <i>name</i> <b>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</b> [ <i>name</i> ]	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</b> [ <b>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</b> [ <b>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。

コマンド	目的
switch(config-s)# <b>save location</b>	(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
<b>show configuration session [name]</b>	コンフィギュレーション ファイルの内容を表示します。

コマンド	目的
<b>show configuration session status</b> [ <i>name</i> ]	コンフィギュレーションセッションのステータスを表示します。
<b>show configuration session summary</b>	すべてのコンフィギュレーションセッションのサマリーを表示します。





## 第 9 章

# スケジューラの設定

この章は、次の内容で構成されています。

- [スケジューラの概要](#) (117 ページ)
- [スケジューラの注意事項および制約事項](#) (118 ページ)
- [スケジューラのデフォルト設定](#) (119 ページ)
- [スケジューラの設定](#) (119 ページ)
- [スケジューラの設定確認](#) (127 ページ)
- [スケジューラの設定例](#) (128 ページ)
- [スケジューラの標準](#) (129 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単一または複数のコマンドで構成されています。ジョブは、1 回だけ、または定期的な間隔でスケジューリングすることができます。

スケジューラでは、ジョブと、そのタイムテーブルを次のように定義できます。

### ジョブ

コマンドリストとして定義され、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することができます。

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。
- 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。
- ジョブは開始されると非インタラクティブ方式で実行されるため、ジョブの定義中、インタラクティブなreloadコマンドや中断を伴うコマンド（例：**copy bootflash: file ftp:URI**、

**write erase**、およびその他類似のコマンド) が指定されていないことを確認してください。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、スケジュール構成では使用しないでください。

## スケジュールのデフォルト設定

表 16: コマンドスケジュールのパラメータのデフォルト

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

## スケジュールの設定

### スケジュールのイネーブル化

#### 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`

#### 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) # feature scheduler</code>	スケジュールをイネーブルにします。
ステップ 3	(任意) <code>switch(config) # show scheduler config</code>	スケジュール設定を表示します。
ステップ 4	(任意) <code>switch(config) # copy running-config startup-config</code>	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

### 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

リモートユーザーは、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。

**show running-config** 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。コマンドの暗号化オプション (**7**) は、ASCII デバイス設定をサポートします。

### 手順の概要

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**
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。

## 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	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 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。 <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-job) # <b>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) switch(config-job) # <b>show scheduler job [name]</b>	ジョブ情報を表示します。 <i>name</i> は 31 文字までに制限されています。

	コマンドまたはアクション	目的
ステップ 5	(任意) <code>switch(config-job) # copy running-config startup-config</code>	リポ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ル ジョブを作成します。
- 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。
- 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

### 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	<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) # no scheduler job name name</code>	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。  <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) <code>switch(config-job) # show scheduler job [name]</code>	ジョブ情報を表示します。

	コマンドまたはアクション	目的
ステップ 4	(任意) <code>switch(config-job) # copy running-config startup-config</code>	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** コマンドで時刻を設定しない場合は、スケジューラは現在の時刻を使用します。たとえば、現在の時刻が 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。

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



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

### 手順の概要

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`

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) # scheduler schedule name name</code>	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。  <i>name</i> は 31 文字までに制限されています。
ステップ 3	<code>switch(config-schedule) # job name name</code>	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。  <i>name</i> は 31 文字までに制限されています。
ステップ 4	<code>switch(config-schedule) # time daily time</code>	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	<code>switch(config-schedule) # time weekly [[day-of-week:] HH:] MM</code>	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（たとえば、日曜日は <b>1</b> 、月曜日は <b>2</b> ）または略語（たとえば、 <b>sun</b> 、 <b>mon</b> ）で表します。  引数全体の最大長は 10 文字です。
ステップ 6	<code>switch(config-schedule) # time monthly [[day-of-month:] HH:] MM</code>	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	<code>switch(config-schedule) # time start { now repeat repeat-interval   delta-time [ repeat repeat-interval]}</code>	ジョブが定期的に開始することを意味します。  <i>start-time</i> の形式は [[[[yyyy:]mmm:]dd:]JHH]:MM です。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>• <b>delta-time</b> : スケジュールの設定後、ジョブの開始までの待機時間を指定します。</li> <li>• <b>now</b> : ジョブが今から 2 分後に開始することを指定します。</li> <li>• <b>repeat repeat-interval</b> : 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) <code>switch(config-schedule) # show scheduler config</code>	スケジューラの情報を表示します。
ステップ 9	(任意) <code>switch(config-schedule) # copy running-config startup-config</code>	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

### 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	<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) # clear scheduler logfile</code>	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

### 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>	スケジューラをディセーブルにします。
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 17: スケジューラの `show` コマンド

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

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ル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
```

```

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)#

```

## スケジュール ジョブの実行結果の表示

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

```

switch# show scheduler logfile
Job Name       : back-cfg                Job Status: Failed (1)
Schedule Name  : daily                  User Name : admin
Completion time: Fri Jan 1  1:00:01 2009
----- Job Output -----
`cli var name timestamp 2009-01-01-01.00.00`
`copy running-config bootflash:/${(HOSTNAME)}-cfg.${(timestamp)} `
`copy bootflash:/switch-cfg.2009-01-01-01.00.00 tftp://1.2.3.4/ vrf management `
copy: cannot access file '/bootflash/switch-cfg.2009-01-01-01.00.00'
=====
Job Name       : back-cfg                Job Status: Success (0)
Schedule Name  : daily                  User Name : admin
Completion time: Fri Jan 2  1:00:01 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.
[                               ] 0.50KBTrying to connect to tftp server.....
[#####                        ] 24.50KB
TFTP put operation was successful
=====
switch#

```

## スケジュールの標準

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 10 章

# SNMP の設定

この章は、次の内容で構成されています。

- [SNMP に関する情報, on page 131](#)
- [SNMP の注意事項および制約事項 \(136 ページ\)](#)
- [SNMP のデフォルト設定, on page 137](#)
- [SNMP の設定 \(137 ページ\)](#)
- [SNMP のディセーブル化 \(151 ページ\)](#)
- [SNMP 設定の確認, on page 151](#)
- [その他の参考資料 \(152 ページ\)](#)

## SNMP に関する情報

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

## SNMP 機能の概要

SNMP フレームワークは 3 つの部分で構成されます。

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



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

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

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

## SNMP 通知

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

Cisco NX-OS は、トラップまたはインフォームとして SNMP 通知を生成します。トラップは、エージェントからホスト レシーバテーブルで指定された SNMP マネージャに送信される、非同期の非確認応答メッセージです。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 Nexus デバイスが応答を受信しない場合、インフォーム要求を再び送信できます。

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

## SNMPv3

SNMPv3 は、ネットワーク経由のフレームの認証と暗号化を組み合わせることによって、デバイスへのセキュアアクセスを実現します。SNMPv3 が提供するセキュリティ機能は次のとおりです。

- メッセージの完全性：パケットが伝送中に改ざんされていないことを保証します。
- 認証：メッセージのソースが有効かどうかを判別します。
- 暗号化：許可されていないソースにより判読されないように、パケットの内容のスクランブルを行います。

SNMPv3 では、セキュリティ モデルとセキュリティ レベルの両方が提供されています。セキュリティ モデルは、ユーザおよびユーザが属するロールを設定する認証方式です。セキュリティ レベルとは、セキュリティ モデル内で許可されるセキュリティのレベルです。セキュリティ モデルとセキュリティ レベルの組み合わせにより、SNMP パケット処理中に採用されるセキュリティ メカニズムが決まります。

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

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

- noAuthNoPriv : 認証または暗号化を実行しないセキュリティ レベル。このレベルは、SNMPv3 ではサポートされていません。
- authNoPriv : 認証は実行するが、暗号化を実行しないセキュリティ レベル。
- authPriv : 認証と暗号化両方を実行するセキュリティ レベル。

SNMPv1、SNMPv2c、および SNMPv3 の 3 つのセキュリティ モデルを使用できます。セキュリティ モデルとセキュリティ レベルの組み合わせにより、SNMP メッセージの処理中に適用されるセキュリティ メカニズムが決まります。

**Table 18: 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。

モデル	レベル	認証	暗号化	結果
v3	authNoPriv	HMAC-MD5、 HMAC-SHA、ま たは SHA-256	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、 HMAC-SHA、ま たは SHA-256	DES	HMAC-MD5 アル ゴリズムまたは HMAC-SHA アル ゴリズムに基づい て認証します。 データ暗号規格 (DES) の 56 ビット暗号化、お よび暗号ブロック 連鎖 (CBC) DES (DES-56) 標準 に基づいて認証し ます。

## ユーザベースのセキュリティ モデル

SNMPv3 ユーザーベース 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
- SHA-256 認証プロトコル

Cisco NX-OS リリース 9.3(7) 以降では、SNMPv3 に HMAC-SHA-256 認証プロトコルが使用されます。



**Note** SHA-256 SNMP ユーザがスイッチで設定されている場合、ISSD は **install all** コマンドを使用することを推奨します。そうしないと、設定が失われます。

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管理により、Cisco NX-OS の SNMP エージェントは AAA サーバのユーザ認証サービスを利用できます。ユーザ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設定を同期化します。

- **snmp-server user** コマンドで指定された **auth** パスフレーズは、CLI ユーザ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、SNMP ユーザーの **auth** および **priv** パスフレーズになります。

- SNMP または CLI を使用してユーザ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。

## グループベースの SNMP アクセス



**Note** 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 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 NX-OS は、イーサネット MIB への読み取り専用アクセスをサポートします。サポートされる MIB の詳細については、次の URL を参照してください。  
<ftp://ftp.cisco.com/pub/mibs/supportlists/nexus3000/Nexus3000MIBSupportList.html>
- Cisco NX-OS は、SNMPv3 noAuthNoPriv セキュリティ レベルをサポートしていません。
- Cisco Nexus 3548 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 10.5 (2) 以降、ユーザーは、AES-256 を SNMPv3 のプライバシー プロトコルとして構成できます。

- 以前のリリースにダウングレードする前に、暗号化AES-256 を使用する既存のユーザーを AES-128 に再構成するか、暗号化化 AES-256 を使用するユーザーを削除します。
- この機能は、すべての N9K プラットフォームでサポートされています。

## SNMP のデフォルト設定

Table 19: 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 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 [auth {md5 | sha | sha-256} passphrase [auto] [priv [aes-256] passphrase] [engineID id] [localizedkey] [localizedV2key]]**
3. (Optional) switch# **show snmp user**
4. (Optional) **copy running-config startup-config**

#### DETAILED STEPS

##### Procedure

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

	Command or Action	Purpose
	switch# configure terminal switch(config)#	
ステップ 2	<b>snmp-server user</b> <i>name</i> [ <b>auth</b> { <b>md5</b>   <b>sha</b>   <b>sha-256</b> } <i>passphrase</i> [ <b>auto</b> ] [ <b>priv</b> [ <b>aes-256</b> ] <i>passphrase</i> ] [ <b>engineID</b> <i>id</i> ] [ <b>localizedkey</b> ] [ <b>localizedV2key</b> ]]  <b>Example:</b> switch(config)# snmp-server user Admin auth sha abcd1234 priv abcdefgh	<p>認証およびプライバシー パラメータのある SNMP ユーザを設定します。パスワードには最大 64 文字の英数字を使用できます。大文字と小文字が区別されます。 <b>localizedkey</b> キーワードを使用する場合は、パスワードに大文字と小文字を区別した英数字を 130 文字まで使用できます。</p> <p><b>localizedV2key</b> キーを使用する場合、パスワードは大文字と小文字を区別し、先頭に 0x/0X を付けずに最大 130 文字の英数字文字列にすることができます。これは暗号化されたデータであり、オフラインで生成できないため、「show run」から <b>localizedV2key</b> を収集することが常に推奨されます。</p> <p><b>engineID</b> 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>• 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 10.5 (2) 以降、ユーザーは、AES-256 を SNMPv3 のプライバシープロトコルとして構成できます。</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
```

## 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。

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ことができるのは、**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tring を作成します。

## SNMP 要求のフィルタリング

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

ACL は次のパラメータで作成します。

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

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



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

IPv4 または IPv6 を SNMPv3 コミュニティに割り当てて SNMP 要求のフィルタ処理を行うには、グローバル構成モードで次のコマンドを実行します。

コマンド	目的
<pre>switch(config)# snmp-server community name [use-ipv4acl ipv4acl-name] [use-ipv6acl ipv6acl-name]  switch(config)# snmp-server community public use-ipv4acl myacl</pre>	IPv4 ACL または IPv6 ACL を SNMPv3 コミュニティに割り当てて SNMP 要求のフィルタ処理を行います。

## SNMP 通知レシーバの設定

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

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

コマンド	目的
switch(config)# <b>snmp-server host</b> <i>ip-address</i> <b>traps version 1</b> <i>community</i> [ <b>udp_port number</b> ]	SNMPv1 トラップのホスト レシーバを設定します。 <i>ip-address</i> は IPv4 または IPv6 アドレスを使用できます。 コミュニティは、最大 255 文字の英数字で指定できます。 UDP ポート番号の範囲は 0 ~ 65535 です。

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

コマンド	目的
switch(config)# <b>snmp-server host</b> <i>ip-address</i> { <b>traps</b>   <b>informs</b> } <b>version 2c</b> <i>community</i> [ <b>udp_port number</b> ]	SNMPv2c トラップまたはインフォームのホストレシーバを設定します。 <i>ip-address</i> は IPv4 または IPv6 アドレスを使用できます。 コミュニティは、最大 255 文字の英数字で指定できます。 UDP ポート番号の範囲は 0 ~ 65535 です。

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

コマンド	目的
switch(config)# <b>snmp-server host</b> <i>ip-address</i> { <b>traps</b>   <b>informs</b> } <b>version 3</b> { <b>auth</b>   <b>noauth</b>   <b>priv</b> } <i>username</i> [ <b>udp_port number</b> ]	SNMPv2c トラップまたはインフォームのホストレシーバを設定します。 <i>ip-address</i> は IPv4 または IPv6 アドレスを使用できます。 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暗号解除するため、Cisco Nexus デバイスの SNMP engineID に基づくユーザー クレデンシャル (authKey/PrivKey) を認識していなければなりません。

次に、SNMPv1 トラップのホスト レシーバを設定する例を示します。

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

次に、SNMPv2 インフォームのホスト レシーバを設定する例を示します。

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

次に、SNMPv3 インフォームのホスト レシーバを設定する例を示します。

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

## VRF を使用する SNMP 通知レシーバの設定

設定された VRF をホスト レシーバに接続するように Cisco NX-OS を設定できます。SNMP 通知レシーバの VRF 到達可能性およびフィルタリング オプションを設定すると、SNMP によって CISCO-SNMP-TARGET-EXT-MIB の cExtSnmptargetVrfTable にエンタリが追加されます。



(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-MIB の ExtSnmptargetVrfTable にエンタリが追加されます。
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**

### 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	<code>switch# configuration 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)# snmp-server context context-name vrf vrf-name</code>	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。  (注) デフォルトでは、SNMP は管理 VRF を使用してトラップを送信します。管理 VRF を使用しない場合は、このコマンドを使用して対象の VRF を指定する必要があります。
ステップ 3	<code>switch(config)# snmp-server community community-name group group-name</code>	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	<code>switch(config)# snmp-server mib community-map community-name context context-name</code>	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 ユーザー名とパスワードを使用する方法を示しています。

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

## SNMP 通知のイネーブル化

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



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

次の表に、Cisco NX-OS MIB の通知をイネーブルにする CLI コマンドを示します。

**Table 20: SNMP 通知のイネーブル化**

MIB	関連コマンド
すべての通知	<code>snmp-server enable traps</code>
BRIDGE-MIB	<code>snmp-server enable traps bridge newroot</code> <code>snmp-server enable traps bridge topologychange</code>
CISCO-AAA-SERVER-MIB	<code>snmp-server enable traps aaa</code>

MIB	関連コマンド
ENITY-MIB、 CISCO-ENTITY-FRU-CONTROL-MIB、 CISCO-ENTITY-SENSOR-MIB	<code>snmp-server enable traps entity</code> <code>snmp-server enable traps entity fru</code>
CISCO-LICENSE-MGR-MIB	<code>snmp-server enable traps license</code>
IF-MIB	<code>snmp-server enable traps link</code>
CISCO-PSM-MIB	<code>snmp-server enable traps port-security</code>
SNMPv2-MIB	<code>snmp-server enable traps snmp</code> <code>snmp-server enable traps snmp authentication</code>
CISCO-FCC-MIB	<code>snmp-server enable traps fcc</code>
CISCO-DM-MIB	<code>snmp-server enable traps fcdomain</code>
CISCO-NS-MIB	<code>snmp-server enable traps fens</code>
CISCO-FCS-MIB	<code>snmp-server enable traps fcs discovery-complete</code> <code>snmp-server enable traps fcs request-reject</code>
CISCO-FDMI-MIB	<code>snmp-server enable traps fdmi</code>
CISCO-FSPF-MIB	<code>snmp-server enable traps fspf</code>
CISCO-PSM-MIB	<code>snmp-server enable traps port-security</code>
CISCO-RSCN-MIB	<code>snmp-server enable traps rscn</code> <code>snmp-server enable traps rscn els</code> <code>snmp-server enable traps rscn ils</code>
CISCO-ZS-MIB	<code>snmp-server enable traps zone</code> <code>snmp-server enable traps zone default-zone-behavior-change</code> <code>snmp-server enable traps zone enhanced-zone-db-change</code> <code>snmp-server enable traps zone merge-failure</code> <code>snmp-server enable traps zone merge-success</code> <code>snmp-server enable traps zone request-reject</code> <code>snmp-server enable traps zone unsupp-mem</code>
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。	<code>snmp-server enable traps config</code>



**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。
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</b> [authentication]	SNMP エージェント通知をイネーブルにします。

## リンクの通知の設定

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

- **cieLinkDown** : シスコ拡張リンク ステート ダウン通知をイネーブルにします。
- **cieLinkUp** : シスコ拡張リンク ステート アップ通知をイネーブルにします。
- **cisco-xcvr-mon-status-chg** : シスコ インターフェイス トランシーバ モニター 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。
ステップ 2	<b>snmp-server enable traps link [cieLinkDown   cieLinkUp   cisco-xcvr-mon-status-chg   delayed-link-state-change]   extended-linkUp   extended-linkDown   linkDown   linkUp]</b> 例： switch(config)# snmp-server enable traps link cieLinkDown	リンク SNMP 通知をイネーブルにします。

## インターフェイスでのリンク通知のディセーブル化

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

## 手順の概要

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。

	コマンドまたはアクション	目的
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 トラップをディセーブルにします。この機能は、デフォルトでイネーブルにされています。

## TCP での SNMP に対するワンタイム認証のイネーブル化

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

コマンド	目的
switch(config)# <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

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

### 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

	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 contact name</b>	sysContact (SNMP 担当者名) を設定します。
ステップ 3	switch(config)# <b>snmp-server location name</b>	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</b> <i>context-name</i> [ <b>instance</b> <i>instance-name</i> ] [ <b>vrf</b> <i>vrf-name</i> ] [ <b>topology</b> <i>topology-name</i> ]	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</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。
ステップ 4	(Optional) switch(config)# <b>no snmp-server context</b> <i>context-name</i> [ <b>instance</b> <i>instance-name</i> ] [ <b>vrf</b> <i>vrf-name</i> ] [ <b>topology</b> <i>topology-name</i> ]	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 のディセーブル化

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

# SNMP 設定の確認

SNMP 設定情報を表示するには、次の作業を行います。

コマンド	目的
<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 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 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。

## その他の参考資料

### MIB

MIB	MIB のリンク
SNMP に関連する MIB	サポートされている MIB を検索およびダウンロードするための URL にアクセスしてください。 <a href="https://cisco.github.io/cisco-mibs/supportlists/nexus3548/Nexus3548MIBSupportList.html">https://cisco.github.io/cisco-mibs/supportlists/nexus3548/Nexus3548MIBSupportList.html</a>



# 第 11 章

## RMON の設定

この章は、次の内容で構成されています。

- [RMON について, on page 153](#)
- [RMON の設定時の注意事項および制約事項 \(155 ページ\)](#)
- [RMON の設定 \(155 ページ\)](#)
- [RMON 設定の確認, on page 157](#)
- [デフォルトの RMON 設定, on page 157](#)

## RMON について

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

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

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

## RMON アラーム

SNMP INTEGER タイプの解決を行う任意の MIB オブジェクトにアラームを設定できます。指定されたオブジェクトは、標準のドット付き表記 (たとえば、1.3.6.1.2.1.2.2.1.17 は ifOutOctets.17 を表します) の既存の SNMP MIB オブジェクトでなければなりません。

アラームを作成する場合、次のパラメータを指定します。

- モニタリングする MIB オブジェクト

- サンプルング間隔：MIB オブジェクトのサンプル値を収集するのに Cisco Nexus デバイスを使用する間隔
- サンプルタイプ：絶対サンプルでは、MIB オブジェクト値の現在のスナップショットを使用します。デルタサンプルは連続した2つのサンプルを使用し、これらの差を計算します。
- 上限しきい値：Cisco Nexus デバイスが上限アラームを発生させる、または下限アラームをリセットするときの値
- 下限しきい値：Cisco Nexus デバイスが下限アラームを発生させる、または上限アラームをリセットするときの値
- イベント：アラーム（上限または下限）の発生時に Cisco Nexus デバイスが実行するアクション



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

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



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

## RMON イベント

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

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

下限アラームおよび上限アラームに異なるイベントを指定できます。

# RMON の設定時の注意事項および制約事項

RMON には、次の注意事項および制限事項があります。

- SNMP 通知イベントタイプを使用するには、SNMP ユーザおよび通知レシーバを設定する必要があります。
- 整数になる MIB オブジェクトに、RMON アラームのみを設定できます。

## RMON の設定

### RMON アラームの設定

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

次のパラメータを任意で指定することもできます。

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

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

#### 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 alarm index mib-object sample-interval {absolute | delta} rising-threshold value [event-index] falling-threshold value [event-index] [owner name]**
3. switch(config)# **rmon hcalarm index mib-object sample-interval {absolute | delta} rising-threshold-high value rising-threshold-low value [event-index] falling-threshold-high value falling-threshold-low value [event-index] [owner name] [storage type type]**
4. (Optional) switch# **show rmon {alarms | hcalarms}**
5. (Optional) switch# **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。

	Command or Action	Purpose
ステップ 2	switch(config)# <b>rmon alarm</b> <i>index mib-object sample-interval</i> {absolute   delta} <b>rising-threshold</b> <i>value</i> [ <i>event-index</i> ] <b>falling-threshold</b> <i>value</i> [ <i>event-index</i> ] [ <b>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</b> <i>index mib-object sample-interval</i> {absolute   delta} <b>rising-threshold-high</b> <i>value</i> <b>rising-threshold-low</b> <i>value</i> [ <i>event-index</i> ] <b>falling-threshold-high</b> <i>value</i> <b>falling-threshold-low</b> <i>value</i> [ <i>event-index</i> ] [ <b>owner name</b> ] [ <b>storage 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</b> {alarms   hcalarms}	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 | hcalarms}
4. (Optional) switch# **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>rmon event index</b> [ <b>description string</b> ] [log] [trap] [ <b>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</b> {alarms   hcalarms}	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 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 21: 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



## 第 12 章

# オンライン診断の設定

この章は、次の内容で構成されています。

- [オンライン診断について, on page 159](#)
- [オンライン診断の注意事項と制約事項 \(162 ページ\)](#)
- [オンライン診断の設定, on page 162](#)
- [オンライン診断設定の確認, on page 163](#)
- [オンライン診断のデフォルト設定, on page 163](#)

## オンライン診断について

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

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

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

## ブートアップ診断

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

**Table 22:** 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。

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通するテストセットも含まれます。

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

起動診断テストをバイパスするように Cisco Nexus デバイスを設定することも、またはすべての起動診断テストを実行するように設定することもできます。

## ヘルス モニタリング診断

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

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

次の表に、スイッチのヘルス モニタリング診断を示します。

**Table 23:** ヘルス モニタリング診断テスト

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

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

**Table 24:** ヘルス モニタリングおよび起動時診断テスト

診断	説明
SPROM	バックプレーンとスーパーバイザ SPROM の整合性を確認します。
ファブリックエンジン	スイッチファブリック ASIC をテストします。
ファブリックポート	スイッチファブリック ASIC 上のポートをテストします。

診断	説明
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。

## 拡張モジュール診断

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

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

**Table 25:** 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 26:** 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。

- Cisco NX-OS リリース 10.2 (4) 以降、バックプレーン テストは Nexus 3548 スイッチではサポートされていません。

## 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** 起動時オンライン診断レベルを **complete** に設定することを推奨します。起動時オンライン診断をバイパスすることは推奨しません。

### SUMMARY STEPS

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

### 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> : すべての起動時診断を実行します。これはデフォルト値です。</li> <li>• <b>bypass</b> : 起動時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 ( <b>bypass</b> または <b>complete</b> ) 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 27:** 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





## 第 13 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 \(165 ページ\)](#)
- [Embedded Event Manager ポリシー \(166 ページ\)](#)
- [Embedded Event Manager の前提条件 \(169 ページ\)](#)
- [Embedded Event Manager の注意事項および制約事項 \(169 ページ\)](#)
- [Embedded Event Manager のデフォルト設定 \(170 ページ\)](#)
- [環境変数の定義 \(170 ページ\)](#)
- [CLI によるユーザ ポリシーの定義 \(171 ページ\)](#)
- [イベント文の設定 \(173 ページ\)](#)
- [アクション文の設定 \(176 ページ\)](#)
- [VSH スクリプトによるポリシーの定義 \(179 ページ\)](#)
- [VSH スクリプト ポリシーの登録およびアクティブ化 \(179 ページ\)](#)
- [システム ポリシーの上書き \(180 ページ\)](#)
- [EEM パブリッシャとしての syslog の設定 \(182 ページ\)](#)
- [イベント ログの自動収集とバックアップ \(183 ページ\)](#)

## 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 ポリシーが設定されると、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。

### 設定済みのシステム ポリシー

Cisco NX-OS には、設定済みのさまざまなシステム ポリシーがあります。これらのシステムポリシーでは、デバイスに関連する多数の一般的なイベントおよびアクションが定義されています。システムポリシー名は、2個の下線記号 (\_\_) から始まります。

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。

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ポリシーの一致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。

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に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たりするようなことがないようにする必要があります。
- 発生したイベントでデフォルトのアクションを処理できるようにするには、デフォルトのアクションを許可する EEM ポリシーを設定する必要があります。たとえば、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 イベント関連はシステムのデフォルト ポリシーを上書きしません。
- 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。
- 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。**show .\*** コマンドを入力すると、機能しません。
- 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。**ADMIN\_DOWN** コマンドを入力すると、機能しません。
- 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、画面に表示するために（および EEM ポリシーによってブロックされないために）**show** コマンドの出力が必要な場合は、EEM ポリシーの最初のアクションに対して、**event-default** コマンドを指定する必要があります。
- Cisco Nexus 3500 シリーズ スイッチは、Cisco NX-OS リリース 7.0(3)I7(2) およびそれ以前のリリースの Embedded Event Manager をサポートしていません。

## Embedded Event Manager のデフォルト設定

表 28: 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

## 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

#### 1. configure terminal

2. **event manager environment** *variable-name variable-value*
3. (任意) **show event manager environment** {*variable-name* | **all**}
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>event manager environment</b> <i>variable-name variable-value</i> 例： <pre>switch(config) # event manager environment emailto "admin@anyplace.com"</pre>	EEM 用の環境変数を作成します。  <i>variable-name</i> は大文字と小文字を区別し、最大 29 文字の英数字を使用できます。  <i>variable-value</i> 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</b> { <i>variable-name</i>   <b>all</b> }	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。

### 次のタスク

ユーザー ポリシーを設定します。

## CLI によるユーザ 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**

## 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</b> <i>applet-name</i> 例： switch(config)# event manager applet monitorShutdown switch(config-applet)#	EEM にアプレットを登録し、アプレット コンフィギュレーション モードを開始します。  <i>applet-name</i> は大文字と小文字を区別し、最大 29 文字の英数字を使用できます。
ステップ 3	(任意) <b>description</b> <i>policy-description</i> 例： switch(config-applet)# description "Monitors interface shutdown."	ポリシーの説明になるストリングを設定します。  <i>string</i> には最大 80 文字の英数字を使用できます。ストリングは引用符で囲みます。
ステップ 4	<b>event</b> <i>event-statement</i> 例： switch(config-applet)# event cli match "shutdown"	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</b> <i>tag</i> { <b>and</b>   <b>andnot</b>   <b>or</b> } <i>tag</i> [ <b>and</b>   <b>andnot</b>   <b>or</b> { <i>tag</i> }] { <b>happens occurs in seconds</b> }	ポリシー内の複数のイベントを相互に関連付けます。  <i>occurs</i> 引数の範囲は 1 ~ 4294967295 です。 <i>seconds</i> 引数の範囲は 0 ~ 4294967295 秒です。
ステップ 6	<b>action</b> <i>number</i> [. <i>number2</i> ] <i>action-statement</i> 例： switch(config-applet)# action 1.0 cli show interface e 3/1	ポリシーのアクション文を設定します。アクション文が複数ある場合、このステップを繰り返します。
ステップ 7	(任意) <b>show event manager policy-state</b> <i>name</i> [ <b>module</b> <i>module-id</i> ] 例： switch(config-applet)# show event manager policy-state monitorShutdown	設定したポリシーの状態に関する情報を表示します。

	コマンドまたはアクション	目的
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。

### 次のタスク

イベント文およびアクション文を設定します。

## 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> 例： <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。 <b>repeats</b> の範囲は 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> 例： <pre>switch(config-applet) # event counter name mycounter entry-val 20 gt</pre>	カウンタが、開始演算子に基づいて開始のしきい値を超えた場合にイベントを発生させます。イベントはただちにリセットされます。任意で、カウンタが終了のしきい値を超えたあとでリセットされるように、イベントを設定できます。 <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。 <b>counter name</b> 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。 <b>entry</b> および <b>exit</b> の値の範囲は 0 ~ 2147483647 です。
ステップ 3	<b>event fanabsent [ fan number] time seconds</b> 例： <pre>switch(config-applet) # event fanabsent time 300</pre>	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。 <b>number</b> の範囲はモジュールに依存します。 <b>seconds</b> の範囲は 10 ~ 64000 です。
ステップ 4	<b>event fanbad [ fan number] time seconds</b> 例： <pre>switch(config-applet) # event fanbad time 3000</pre>	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。 <b>number</b> の範囲はモジュールに依存します。 <b>seconds</b> の範囲は 10 ~ 64000 です。
ステップ 5	<b>event memory {critical   minor   severe}</b> 例： <pre>switch(config-applet) # event memory critical</pre>	メモリのしきい値を超えた場合にイベントを発生させます。

	コマンドまたはアクション	目的
ステップ 6	<b>event policy-default count repeats [ time seconds]</b> 例 : <pre>switch(config-applet) # event policy-default count 3</pre>	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。 <i>repeats</i> の範囲は 1 ~ 65000 です。 <i>seconds</i> の範囲は 0 ~ 4294967295 秒です。0 は無制限を示します。
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 exit-time time polling-interval interval</b> 例 : <pre>switch(config-applet) # event snmp oid 1.3.6.1.2.1.31.1.1.1.6 get-type next entry-op lt 300 entry-val 0 exit-op eq 400 exit-time 30 polling-interval 300</pre>	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。 <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。 <i>sensor</i> 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。 指定できる <i>object-number</i> の範囲は 1 ~ 500 です。

## 次のタスク

アクション文を設定します。

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

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。 **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</b> <i>number</i> [. <i>number2</i> ] <b>cli</b> <i>command1</i> [ <i>command2</i> . ] <b>[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 <i>number1.number2</i> です。 <i>number</i> には 1～16 桁の任意の番号を指定できます。 <i>number2</i> の範囲は 0～9 です。
ステップ 2	<b>action</b> <i>number</i> [. <i>number2</i> ] <b>counter</b> <i>name</i> <i>counter</i> <b>value</b> <i>val</i> <b>op</b> { <b>dec</b>   <b>inc</b>   <b>nop</b>   <b>set</b> } 例： <pre>switch(config-applet) # action 2.0 counter name mycounter value 20 op inc</pre>	設定された値および操作でカウンタを変更します。 アクションラベルのフォーマットは <i>number1.number2</i> です。 <i>number</i> には 1～16 桁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>counter</i> は大文字と小文字を区別し、最大 28 文字の英数字を使用できます。 <i>val</i> には 0～2147483647 の整数または置換パラメータを指定できます。
ステップ 3	<b>action</b> <i>number</i> [. <i>number2</i> ] <b>event-default</b> 例： <pre>switch(config-applet) # action 1.0 event-default</pre>	関連付けられたイベントのデフォルトアクションを実行します。 アクションラベルのフォーマットは <i>number1.number2</i> です。 <i>number</i> には 1～16 桁の任意の番号を指定できます。 <i>number2</i> の範囲は 0～9 です。
ステップ 4	<b>action</b> <i>number</i> [. <i>number2</i> ] <b>policy-default</b> 例： <pre>switch(config-applet) # action 1.0 policy-default</pre>	上書きしているポリシーのデフォルトアクションを実行します。 アクションラベルのフォーマットは <i>number1.number2</i> です。 <i>number</i> には 1～16 桁の任意の番号を指定できます。 <i>number2</i> の範囲は 0～9 です。
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> ] ] 例：	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。

	コマンドまたはアクション	目的
	switch(config-applet) # action 1.0 reload module 3-5	アクションラベルのフォーマットは <code>number1.number2</code> です。  <i>number</i> には 1～16 桁の任意の番号を指定できます。 <i>number2</i> の範囲は 0～9 です。
ステップ 6	<b>action <i>number</i>[<i>number2</i>] snmp-trap [ <i>intdata1 integer-data1</i>] [ <i>intdata2 integer-data2</i>] [ <i>strdata string-data</i>]</b>  例： switch(config-applet) # action 1.0 snmp-trap strdata "temperature problem"	設定されたデータを使用して SNMP トラップを送信します。アクションラベルのフォーマットは <code>number1.number2</code> です。  <i>number</i> には 1～16 桁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 桁までの任意の数を指定できます。 <i>string</i> には最大 80 文字の英数字を使用できます。
ステップ 7	<b>action <i>number</i>[<i>number2</i>] syslog [ <i>priority prio-val</i>] msg <i>error-message</i></b>  例： switch(config-applet) # action 1.0 syslog priority notifications msg "cpu high"	設定されたプライオリティで、カスタマイズした syslog メッセージを送信します。  アクションラベルのフォーマットは <code>number1.number2</code> です。  <i>number</i> には 1～16 桁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
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 policy <i>policy-script</i></b> 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。 <i>policy-script</i> は大文字と小文字を区別し、最大 29 文字の英数字を使用できます。
ステップ 3	(任意) <b>event manager policy internal <i>name</i></b> 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。 <i>policy-script</i> は大文字と小文字を区別し、最大 29 の英数字を使用できます。
ステップ 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。  <i>applet-name</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。  <i>system-policy</i> は、システム ポリシーの 1 つにする必要があります。
ステップ 4	<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。  <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。

	コマンドまたはアクション	目的
ステップ 7	(任意) <b>show event manager policy-state name</b> 例： switch(config-applet)# show event manager policy-state ethport	設定したポリシーに関する情報を表示します。
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。

	コマンドまたはアクション	目的
ステップ 2	<b>event manager applet</b> <i>applet-name</i> 例 : <pre>switch(config)# event manager applet abc switch (config-applet)#</pre>	EEM にアプレットを登録し、アプレット コンフィギュレーション モードを開始します。
ステップ 3	<b>event syslog</b> [ <i>tag tag</i> ] { <i>occurs number</i>   <i>period seconds</i>   <i>pattern msg-text</i>   <i>priority priority</i> } 例 : <pre>switch(config-applet)# event syslog occurs 10</pre>	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。

## イベント ログの自動収集とバックアップ

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

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

- 拡張ログ ファイルの保持
- トリガーベースのイベント ログの自動収集

### 拡張ログ ファイルの保持

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

### すべてのサービスの拡張ログ ファイル保持のイネーブル化

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

## すべてのサービスの拡張ログ ファイル保持の無効化

### 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
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 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。スイッチで (**no bloggerd log-dump** が設定されていて) ログファイル保持機能が有効になっていない場合、次の手順を使用して単一のサービスに対して有効にします。

## 手順の概要

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 :	サービス SA P番号を含む ACL Manager に関する情報を表示します。

	コマンドまたはアクション	目的
	switch# show system internal sysmgr service name aclmgr	
ステップ 2	<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 number</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><code>dir debug:log-dump/</code></b>  例 : <code>switch# dir debug:log-dump/</code>	スイッチに現在保存されているイベント ログ ファイルを表示します。

#### 例

```
switch# dir debug:log-dump/

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

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

## 単一サービスに対する拡張ログファイル保持の無効化

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

### 手順の概要

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 SA P 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せん。
  - イメージのアップグレード時は新しいトリガーを自動的に更新します。
- ログをスイッチにローカルに保存するか、外部サーバにリモートで保存します。
- 重大度 0、1、および 2 の syslog をサポートします：
- アドホック イベントのカスタム syslog (syslog と接続する自動収集コマンド)

## トリガーベースのログ ファイルの自動収集の有効化

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

ログ ファイルの自動収集を有効にするカスタム YAML ファイルの作成の詳細については、[自動収集 YAML ファイルの設定 \(190 ページ\)](#) を参照してください。

## 自動収集 YAML ファイル

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

ンファイル `/bootflash/scripts` とともに `bootflash/scripts/test.yaml` ディレクトリにある場合、`platform.yaml` ファイルで定義された命令がデフォルトの `test.yaml` ファイルに存在するプラットフォーム コンポーネントの手順よりも優先します。

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

例：

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

## 自動収集 YAML ファイルの設定

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

スイッチの次のディレクトリで YAML ファイルを見つけます。

```
/bootflash/scripts
```

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

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

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

## YAML ファイルの例

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



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

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

```
tech-sup: port
commands: show module
```

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

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

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

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

上記の YAML エントリの syslog 出力の例 :

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

複数の値を指定するには、次の例を使用します。

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



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

リリース 10.1(1) 以降では、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 命名規則に従う必要があります。

次の例では、test.yaml が test\_folder に置き換えられます。

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

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

次の例は、test\_folder のパスとコンポーネントを示しています。

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

例：

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

```
2020-Jun-27 07:02:56 40101277 ACLMGR-0-TEST_SYSLOG PROCESSED:3:10542045
2020-Jun-27 07:02:52 40101277 ACLMGR-0-TEST_SYSLOG PROCESSING
```

## 自動収集ログ ファイル

### 自動収集ログ ファイルについて

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

自動収集ログ ファイルは、次のディレクトリに保存されます。

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

### ログ ファイルへのアクセス

コマンドキーワード「debug」を使用してログを検索します。

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

次の表に、ログの場所と保存されるログの種類を示します。

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

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

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

### ログ tar ファイルの解析

tar ファイル内のログを解析するには、次の例を参考にしてください。

```

switch# show system internal event-logs parse
debug:log-dump/20191022104656_evtlog_archive.tar
-----LOGS:/tmp/BLOGGERD0.991453012199/tmp/1-191022104658-191022110741-device_test-M27-V1-I1:0-P884.gz-----
2019 Oct 22 11:07:41.597864 E_DEBUG Oct 22 11:07:41 2019(diag_test_start):Data Space
Limits(bytes): Soft: -1  Hard: -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）。
<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けるのに十分なメモリが使用可能になるまで、最も古いファイルから消去されます。

### EventBundle ログの消去ロジック

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

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

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

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

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

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

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



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

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

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

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

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

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-limit 30 max-triggers 5 $_syslog_msg
```



(注) 自動収集されたバンドルを `debug:log-snapshot-auto/` により手動で削除すれば、次のイベントが発生したとき、**max-triggers** の設定数に基づいて収集が再開されます。

### 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

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

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

## トリガーベースのログ ファイル生成の確認

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

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

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

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

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

## ローカル ログ ファイルのストレージ

ローカル ログ ファイルのストレージ機能：

- ローカルデータストレージ時間の量は、導入の規模とタイプによって異なります。モジュラスイッチと非モジュラスイッチの両方で、ストレージ時間は15分から数時間のデータです。長期間にわたる関連ログを収集するには、次の手順を実行します。
  - 必要な特定のサービス/機能に対してのみイベント ログの保持を有効にします。「[単一サービスの拡張ログファイル保持の有効化 \(185 ページ\)](#)」を参照してください。
  - スイッチから内部イベント ログをエクスポートします。「[外部ログ ファイルのストレージ \(200 ページ\)](#)」を参照してください。
- 圧縮されたログは RAM に保存されます。
- 250MB のメモリは、ログ ファイル ストレージ用に予約されています。
- ログ ファイルは tar 形式で最適化されます (5 分ごとに 1 ファイルまたは 10 MB のいずれか早い方)。
- スナップショット収集を許可します。

## 最近のログ ファイルのローカル コピーの生成

拡張ログファイル保持は、スイッチで実行されているすべてのサービスに対してデフォルトで有効になっています。ロ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

1. **bloggerd log-snapshot** [*file-name*] [**bootflash:** *file-path* | **logflash:** *file-path* | **usb1:** ] [**size** *file-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	<p><b>bloggerd log-snapshot</b> [<i>file-name</i>] [<b>bootflash:</b> <i>file-path</i>   <b>logflash:</b> <i>file-path</i>   <b>usb1:</b> ] [<b>size</b> <i>file-size</i>] [<b>time</b> <i>minutes</i>]</p> <p>例 :</p> <pre>switch# bloggerd log-snapshot snapshot1</pre>	<p>スイッチに保存されている最新の 10 個のイベント ログのスナップショットバンドル ファイルを作成します。この操作のデフォルトのストレージは <b>logflash</b> です。</p> <p><b>file-name</b> : 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。 <b>file-name</b> には最大 64 文字を使用します。</p> <p>(注)</p> <p>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 :</p> <pre>20200605161704_snapshot_bundle.tar</pre> <p><b>bootflash:</b> <i>file-path</i> : スナップショット ログファイルバンドルがブートフラッシュに保存されているファイルパス。次の初期パスのいずれかを選択します。</p> <ul style="list-style-type: none"> <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:</b> <i>file-path</i> : 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> </ul>

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <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# bloggerd log-snapshot snapshot1
Snapshot generated at logflash:evt_log_snapshot/snapshot1_snapshot_bundle.tar Please
cleanup once done.
switch#
switch# dir logflash:evt_log_snapshot
159098880 Dec 05 06:40:24 2019 snapshot1_snapshot_bundle.tar
159354880 Dec 05 06:40:40 2019 snapshot2_snapshot_bundle.tar

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

次の例のコマンドを使用して、同じファイルを表示します。

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

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



- (注) 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せん。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_mcore.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

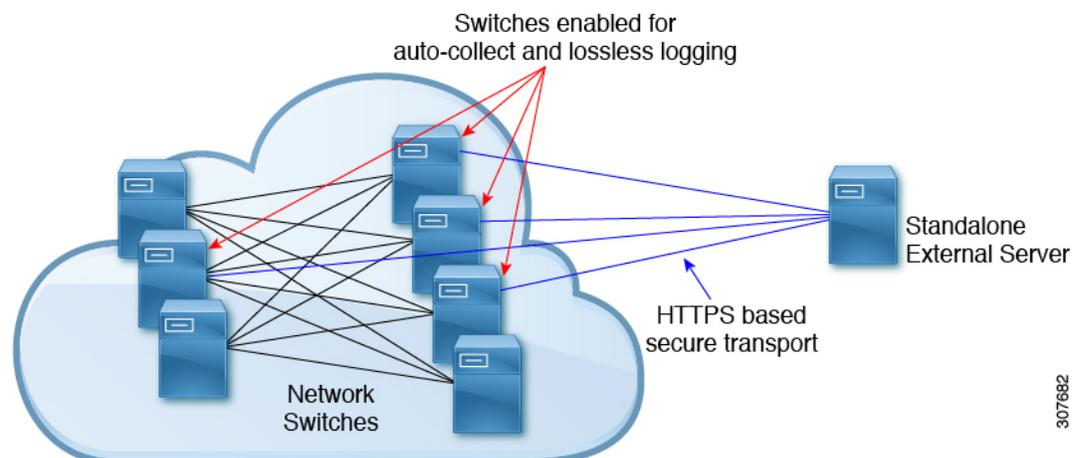
外部サーバソリューションは、ログを安全な方法でオフスイッチに保存する機能を提供します。



(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、シスコサーバへのログの展開とアップロード。
  - 限定的なオンプレミス処理



---

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

---





## 第 14 章

# SPAN の設定

この章は、次の内容で構成されています。

- [SPAN について, on page 203](#)
- [SPAN の注意事項および制約事項 \(204 ページ\)](#)
- [SPAN 送信元, on page 204](#)
- [送信元ポートの特性, on page 204](#)
- [SPAN 宛先, on page 205](#)
- [宛先ポートの特性, on page 205](#)
- [SPAN および ERSPAN フィルタ処理 \(205 ページ\)](#)
- [SPAN および ERSPAN サンプリング \(207 ページ\)](#)
- [SPAN および ERSPAN の切り捨て \(208 ページ\)](#)
- [SPAN セッションの作成または削除, on page 208](#)
- [イーサネット宛先ポートの設定, on page 209](#)
- [送信元ポートの設定, on page 211](#)
- [送信元ポート チャンネルまたは VLAN の設定, on page 211](#)
- [SPAN セッションの説明の設定, on page 212](#)
- [SPAN セッションのアクティブ化, on page 213](#)
- [SPAN セッションの一時停止, on page 214](#)
- [SPAN フィルタの構成 \(214 ページ\)](#)
- [SPAN サンプリングの構成 \(216 ページ\)](#)
- [SPAN 切り捨ての設定 \(217 ページ\)](#)
- [SPAN 情報の表示, on page 219](#)

## 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 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 の注意事項および制約事項

SPAN には、次の注意事項と制約事項があります。

- 複数のローカル SPAN セッションで同じ送信元インターフェイス（物理ポートまたはポートチャネル）を監視できます。
- Cisco Nexus 3500 シリーズスイッチは、SPAN セッションの `access-group` コマンドをサポートしていません。

## SPAN 送信元

SPAN 送信元とは、トラフィックをモニタリングできるインターフェイスを表します。Cisco Nexus デバイスは、SPAN 送信元として、イーサネット、ポートチャネル、および VLAN をサポートしています。VLAN では、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が SPAN 送信元として含まれます。イーサネットインターフェイスで、入力方向、出力方向、または両方向の SPAN トラフィックを選択できます。

- 入力送信元 (Rx) : この送信元ポートを介してデバイスに入るトラフィックは、SPAN 宛先ポートにコピーされます。
- 出力送信元 (Tx) : この送信元ポートを介してデバイスから出るトラフィックは、SPAN 宛先ポートにコピーされます。

## 送信元ポートの特性

送信元ポート（モニタリング対象ポートとも呼ばれる）は、ネットワークトラフィック分析のためにモニタリングするスイッチドインターフェイスです。スイッチは、任意の数の入力送信元ポート（スイッチで使用できる最大数のポート）と任意の数のソース 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。
- 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。
- 同じ VLAN 内または異なる VLAN 内に存在できます。

**Note**

- SPAN セッションあたりの送信元ポートの最大数は 128 ポートです。

## SPAN 宛先

SPAN 宛先とは、送信元ポートをモニタリングするインターフェイスを表します。Cisco Nexus シリーズデバイスは、SPAN 宛先として、イーサネットインターフェイスをサポートします。

## 宛先ポートの特性

各ローカル SPAN セッションには、送信元ポートまたは VLAN からトラフィックのコピーを受信する宛先ポート（モニタリングポートとも呼ばれる）が必要です。宛先ポートの特性は、次のとおりです。

- すべての物理ポートが可能です。送信元イーサネットおよび FCoE ポートは、宛先ポートにできません。
- 送信元ポートにはなれません。
- ポート チャネルには設定できません。
- 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 および ERSPAN フィルタ処理

SPAN または ERSPAN セッションを使用して、すべての送信元インターフェイス上のすべてのトラフィックを監視できます。輻輳がある場合、または接続先の帯域幅がすべてのトラフィックを監視するのに十分でない場合、このトラフィック量はパケットドロップを引き起こす可能性があります。

Cisco NX-OS リリース 6.0(2)A4(1) は、監視する必要がある特定の SPAN または ERSPAN トラフィックフローをフィルタ処理する機能を提供します。フィルタ処理は、フィルタを作成し、それを SPAN または ERSPAN セッションにアタッチすることによって実現されます。フィルタにマッチするパケットのみがミラーリングされます。

フィルタ処理には、次のタイプがあります。

- MAC ベース
- IP ベース
- VLAN ベース

## SPAN および ERSPAN フィルタ処理の注意事項および制限事項

SPAN および ERSPAN フィルタリングには、次の注意事項と制限事項があります。

- Cisco Nexus 3500 シリーズ スイッチは、トラフィックの開始時に、あるインターフェイスで rx 方向、別のインターフェイスで tx 方向にスパンしている場合、SPAN コピーをドロップします。これは、デフォルトの SPAN しきい値制限が低く、SPAN のバーストトラフィックを処理できないために発生します。CLI コマンドの **hardware profile buffer span-threshold <xxx>** を使用して、SPAN しきい値を上げてください。



(注) SPAN しきい値を増やすと、共有バッファの割り当てに影響します。割り当て機能は、共有バッファプールから SPAN バッファを割り当てます。

- span-threshold の最小値が 0 から 2 に更新されています。span-threshold を最小値の 2 に設定すると、占有される SPAN バッファは 528 になります。無効化コマンドである **no hardware profile buffer span-threshold 2** を使用すると、span-threshold は 208 になります。デフォルト値は、span-threshold の最小値よりも小さくなっています。
- SPAN セッションの送信元インターフェイスが動作上ダウン状態の場合でも、その SPAN セッションは動作上ダウン状態になりません。この動作は機能に影響しません
- 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。
- SPAN フィルタリングは、16 個のフィルタのみをサポートします。これらのフィルタは、VLAN ベース、IP ベース、および MAC ベースのフィルタの組み合わせにすることができます。
- マルチキャストルータ ポートを送信元ポートとして SPAN セッションが設定されている場合、送信元ポートに実際に転送されているトラフィックがない場合でも、宛先ポートはすべてのマルチキャストトラフィックを認識します。これは、マルチキャスト/SPAN 実装の現在の制限によるものです。
- SPAN フィルタリングは、SPAN 送信元インターフェイストラフィックを除く、スイッチのすべてのトラフィックに適用できます。
- 1 つの SPAN セッションにつき、1 つの IP ベース、1 つの MAC ベース、および 1 つの VLAN ベースのフィルタのみを設定できます。

- フィルタの数は、次のように、SPAN セッションの数とソースのタイプによってさらに制限されます。
  - 最大 8 つの MAC ベース、8 つの IP ベース、または 8 つの VLAN ベースのフィルタを設定できます。
  - すべてのインターフェイス ベースの SPAN セッションには、最大 4 つの IP ベース、4 つの MAC ベース、または 4 つの VLAN ベースのフィルタをアタッチできます。
  - 最大 8 つの IP ベース、8 つの MAC ベース、または 8 つの VLAN ベースのフィルタをすべての VLAN ベースの SPAN セッションにアタッチできます。
- フィルタは、入力方向だけに使用できます。これは設定できません。
- フィルタが機能するには、SPAN セッションがアップ状態である必要があります。
- ERSPAN-dst セッションではフィルタを設定できません。
- ワープ SPAN セッションではフィルタを設定できません。
- 制御パケット フィルタは、常に出力方向に適用されます。
- ERSPAN セッションの送信元インターフェイスと宛先インターフェイスの両方で PTP が有効になっている場合は、制御パケット フィルタが推奨されます。

## SPAN および ERSPAN 制御パケットのフィルタ処理

Cisco NX-OS リリース 6.0(2)A8(9) は、CPU が生成したパケットを SPAN 送信元インターフェイスから除外する機能を提供します。制御パケット フィルタは出力方向に適用されるため、Tx ミラーリングが有効になっている送信元インターフェイスで有効です。

## SPAN および ERSPAN サンプルング

Cisco NX-OS リリース 6.0(2)A4(1) は、各 SPAN または ERSPAN セッションのソースパケットのサンプルングをサポートします。ソースパケットのサンプル数だけを監視すると、SPAN または ERSPAN の帯域幅を削減できます。このサンプルは、構成可能な範囲によって定義されます。たとえば、範囲を 2 に設定すると、2 つのソースパケットごとに 1 つがスパンされます。同様に、範囲を 1023 に設定すると、1023 パケットごとに 1 パケットがスパンされます。この方法では、SPAN または ERSPAN ソースパケットの正確なカウントが得られますが、スパンパケットに関する時間関連の情報は含まれません。

デフォルトでは、SPAN および ERSPAN サンプルングは無効になっています。サンプルングを使用するには、個々の SPAN または ERSPAN セッションで有効にしておく必要があります。

## SPAN および ERSPAN サンプルングの注意事項および制限事項

SPAN および ERSPAN サンプルングには、次の注意事項と制限事項があります。

- サンプルングは、ローカルセッションと ERSPAN-src セッションでのみサポートされます。
- サンプルングは、ERSPAN-dst セッションではサポートされていません。
- サンプルングは、ワープ SPAN セッションではサポートされていません。
- サポートされているサンプルング範囲は 2 ~ 1023 です。

## SPAN および ERSPAN の切り捨て

Cisco NX-OS リリース 6.0(2)A4(1) では、MTU のサイズに基づく、各 SPAN または ERSPAN セッションのソースパケットの切り捨てが導入されています。切り捨てにより、モニタするパケットのサイズを減らすことで、SPAN または ERSPAN の帯域幅を効果的に軽減できます。MTU の切り捨ては、64 バイトから 1518 バイトまで設定できます。指定された MTU サイズよりも大きい SPAN または ERSPAN パケットはすべて、4 バイトのオフセットで指定されたサイズに切り捨てられます。たとえば、MTU を 300 バイトに設定した場合、複製されるパケットの最大サイズは 304 バイトです。

デフォルトでは、SPAN および ERSPAN の切り捨ては無効になっています。切り捨てを使用するには、個々の SPAN または ERSPAN セッションで有効にしておく必要があります。

## SPAN および ERSPAN 切り捨ての注意事項および制限事項

SPAN および ERSPAN 切り捨てには、以下の注意事項および制限事項があります。

- 切り捨てはローカルおよび ERSPAN-src セッションでのみサポートされます。
- ERSPAN-dst セッションでは、切り捨てはサポートされません。
- 切り捨ては、ワープ SPAN セッションではサポートされません。
- サポートされる MTU の範囲は 64 バイトから 1518 バイトです。

## SPAN セッションの作成または削除

**monitor session** コマンドを使用してセッション番号を割り当てることによって、SPAN セッションを作成できます。セッションがすでに存在する場合、既存のセッションにさらに設定情報が追加されます。

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

## 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。

	Command or Action	Purpose
ステップ 2	switch(config)# <b>interface ethernet</b> <i>slot/port</i>	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> 仮想イーサネットポート上で <b>switchport monitor</b> コマンドを有効にするには、 <b>interface vethernet</b> <i>slot/port</i> 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</b> <i>session-number</i>	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 6	switch(config-monitor)# <b>destination interface ethernet</b> <i>slot/port</i>	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</b> <i>slot/port</i> 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

	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、または仮想ファイバチャネルのポート範囲を入力できます。複製するトラフィック方向を、入力 (Rx)、出力 (Tx)、または両方向 (both) として指定できます。デフォルトは both です。

#### Example

```
switch# configure terminal
switch(config) # monitor session 2
switch(config-monitor) # source interface ethernet 1/16
switch(config-monitor) #
```

## 送信元ポート チャネルまたは VLAN の設定

SPANセッションに送信元チャネルを設定できます。これらのポートは、ポートチャネルおよび VLAN に設定できます。モニタリング方向は入力、出力、またはその両方に設定でき、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** | **san-port-channel**} *channel-number* [**rx** | **tx** | **both**] | **vlan** *vlan-range* | **vsan** *vsan-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。
ステップ 2	switch(config) # <b>monitor session</b> <i>session-number</i>	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</b> { <b>interface</b> { <b>port-channel</b>   <b>san-port-channel</b> } <i>channel-number</i> [ <b>rx</b>   <b>tx</b>   <b>both</b> ]   <b>vlan</b> <i>vlan-range</i>   <b>vsan</b> <i>vsan-range</i> }	ポート チャネル、SAN ポート チャネル、VLAN、または VSAN 送信元を設定します。VLAN または VSAN 送信元の場合、監視方向は暗黙的です。

## 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</b> <i>session-number</i>	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</b> <i>description</i>	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

	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>no monitor session</b> { <i>all</i>   <i>session-number</i> } <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**

**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} 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 フィルタの構成

SPAN フィルタは、ローカルセッションおよび ERSPAN 送信元セッションのみに構成できます。

**手順の概要**

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*}
4. switch(config-monitor)# { **source-ip-address** *source-ip-mask* **destination-ip-address** *destination-ip-mask* } **filterip**
5. switch(config-monitor)# **destination interface ethernet** *slot/port*

## 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>monitor session</b> <i>session-number</i>	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</b> { <b>interface</b> { <b>port-channel</b> } <i>channel-number</i> [ <b>rx</b>   <b>tx</b>   <b>both</b> ]   <b>vlan</b> <i>vlan-range</i> }	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。
ステップ 4	switch(config-monitor)# { <b>source-ip-address</b> <i>source-ip-mask</i> <b>destination-ip-address</b> <i>destination-ip-mask</i> } <b>filterip</b>	SPAN フィルタを作成します。
ステップ 5	switch(config-monitor)# <b>destination interface ethernet</b> <i>slot/port</i>	イーサネット SPAN 宛先ポートを設定します。

### 例

次の例は、ローカルセッションに IP ベースの SPAN フィルタを設定する方法を示しています。

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# monitor session 1
switch(config-monitor)# source interface Ethernet 1/7 rx
switch(config-monitor)# filter ip 10.1.1.1 255.255.255.255 20.1.1.1 255.255.255.255
switch(config-monitor)# destination interface Ethernet 1/48
switch(config-monitor)# no shut
switch(config-monitor)#
```

次の例は、ローカルセッションに VLAN ベースの SPAN フィルタを設定する方法を示しています。

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# monitor session 3
switch(config-monitor)# source vlan 200
switch(config-monitor)# destination interface Ethernet 1/4
switch(config-monitor)# no shut
```

```
switch(config-monitor)#
```

## SPAN サンプリングの構成

サンプリングは、ローカルセッションおよびERSPAN送信元セッションのみに構成できます。

### 手順の概要

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}**
4. switch(config-monitor) # **sampling size**
5. switch(config-monitor)# **destination interface ethernet slot/port**

### 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>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。
ステップ 4	switch(config-monitor) # <b>sampling size</b>	スパニングパケットの範囲を構成します。範囲が $n$ として定義されている場合、 $n$ 番目のパケットごとにスパンされます。 サンプリング範囲は 2 ~ 1023 です。
ステップ 5	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。

### 例

次の例は、ローカルセッションのVLANでサンプリングを構成する方法を示しています。

```
switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# monitor session 1
switch(config-monitor)# source vlan 100
switch(config-monitor)# sampling 10
switch(config-monitor)# destination interface ethernet 1/48
switch(config-monitor)# no shut
switch(config-monitor)# show monitor session 1
  session 1
-----
type           : local
state          : up
sampling       : 10
source intf    :
  rx           : Eth1/3          Eth1/7
  tx           :
  both         :
source VLANs   :
  rx           : 100
destination ports : Eth1/48

Legend: f = forwarding enabled, l = learning enabled
```

次の例は、ローカルセッションのイーサネットインターフェイスでサンプリングを構成する方法を示しています。

```
switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# monitor session 3
switch(config-monitor)# source interface ethernet 1/8
switch(config-monitor)# sampling 20
switch(config-monitor)# destination interface ethernet 1/4
switch(config-monitor)# show monitor session 3
  session 3
-----
type           : local
state          : down (No operational src/dst)
sampling       : 20
source intf    :
  rx           : Eth1/8
  tx           : Eth1/8
  both         : Eth1/8
source VLANs   :
  rx           : 200
destination ports : Eth1/4

Legend: f = forwarding enabled, l = learning enabled
```

## SPAN 切り捨ての設定

切り捨ては、ローカルおよび ERSPAN 送信元セッションに対してのみ構成できます。

### 手順の概要

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*}
4. switch(config-monitor) # **mtu size**
5. switch(config-monitor)# **destination interface ethernet** *slot/port*

## 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>monitor session</b> <i>session-number</i>	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</b> { <b>interface</b> { <b>port-channel</b> } <i>channel-number</i> [ <b>rx</b>   <b>tx</b>   <b>both</b> ]   <b>vlan</b> <i>vlan-range</i> }	ポートチャンネルまたは 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。
ステップ 4	switch(config-monitor) # <b>mtu size</b>	MTU の切り捨てサイズを設定します。構成された MTU サイズよりも大きい SPAN パケットはすべて、4 バイトのオフセットで構成されたサイズに切り捨てられます。  MTU 切り捨てサイズは 64 バイトから 1518 バイトです。
ステップ 5	switch(config-monitor)# <b>destination interface ethernet</b> <i>slot/port</i>	イーサネット SPAN 宛先ポートを設定します。

## 例

次の例は、ローカル セッションの MTU 切り捨てを構成する方法を示しています。

```
switch# configure terminal
switch(config)# monitor session 5
switch(config-monitor)# source interface ethernet 1/5 both
switch(config-monitor)# mtu 512
switch(config-monitor)# destination interface Ethernet 1/39
switch(config-monitor)# no shut
switch(config-monitor)# show monitor session 5
  session 5
-----
type           : local
state          : down (No operational src/dst)
mtu            : 512
source intf    :
  rx           : Eth1/5
  tx           : Eth1/5
  both         : Eth1/5
```

```

source VLANs      :
      rx          :
destination ports : Eth1/39

```

Legend: f = forwarding enabled, l = learning enabled

## 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</b> [session {all   session-number   range session-range} [brief]]	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      :
destination ports : Eth3/1

```





## 第 15 章

# ワープ SPAN の構成

この章は、次の内容で構成されています。

- [ワープ SPAN に関する情報 \(221 ページ\)](#)
- [ワープ SPAN の注意事項および制限事項 \(222 ページ\)](#)
- [ワープ SPAN の構成 \(223 ページ\)](#)
- [ワープ SPAN モード構成の確認 \(224 ページ\)](#)
- [ワープ SPAN 機能の履歴 \(226 ページ\)](#)

## ワープ SPAN に関する情報

ワープ SPAN は、専用ポートに着信するトラフィックを非常に低い遅延でポートのグループにスパンする AlgoBoost 機能です。ワープ SPAN では、1 つの専用入力ポートに到着するトラフィックは、出力ポートのユーザー設定可能なグループに複製されます。パケットの複製は、フィルタやルックアップメカニズムなしで実行されます。通常またはワープモードのトラフィック転送とは異なり、着信トラフィックは、トラフィック分類または ACL 処理が発生する前に複製されます。トラフィックはこれらのプロセスをバイパスするため、複製されたパケットの遅延は 50ns と低くなります。ワープ SPAN は、通常のトラフィック転送とは独立して、同時に機能します。たとえば、着信ソーストラフィックでは、スイッチング、ルーティング、マルチキャスト複製などが行われる可能性があります。この着信トラフィックの複数の宛先ポートへのワープ SPAN は同時に行われます。

専用の送信元ポートに入ったオリジナルのトラフィックは、構成された宛先ポートに公称スイッチ遅延で通常転送されます。ワープ SPAN トラフィックのために加わる遅延は約 50ns です。ワープ SPAN は、通常のトラフィック転送モードとワープモードの両方で有効にできます。

ソースは入力方向でのみ監視でき、設定はできません。送信元ポートは、ワープ SPAN セッションを構成するとすぐに自動的に構成されます。

専用のソース レイヤ 2/レイヤ 3 ポート（イーサネットポート 1/36 である必要があります）を、ネットワークの必要に応じて標準構成で構成します。

通常の SPAN 宛先ポートと同様に宛先ポートを設定します。宛先ポートは、通常のレイヤ 2/レイヤ 3 ポートとしては使用できません。宛先ポートは 4 ポートからなるグループにして構成す

る必要があるため、合計 47 の宛先ポートを持つ最大 12 のグループを作成できます（ポート 1/36 は固定送信元ポートです）。次の表を参照してください。

表 29: ワーブ SPAN グループ

グループ	宛先のポート
1	1-4
2	5 ~ 8
3	9-12
4	13 ~ 16
5	17 ~ 20
6	21 ~ 24
7	25 ~ 28
8	29 ~ 32
9	33 ~ 35 <a href="#">1</a>
10	37 ~ 40
11	41 ~ 44
12	45-48

<sup>1</sup> ポート 36 は専用送信元ポートです。

## ワーブ SPAN の注意事項および制限事項

ワーブ SPAN には以下のような構成の注意事項および制限事項があります。

- 送信元と宛先のワーブ SPAN ポートはすべて 10G である必要があります。
- 送信元ポートは構成できず、イーサネット ポート 1/36 として固定されています。
- 合計 47 の宛先ポートを持つ最大 12 のグループを作成できます。すべてのグループに 4 つのポートがありますが、グループ 9 は例外です。ポート 1/36（固定送信元ポート）が含まれないため、3 つのポートしかありません。
- グループ内の 4 つのポートはすべて、SPAN 宛先グループとしてグループ化する前に、**switchport monitor** コマンドで構成する必要があります。

- ワーブ SPAN では、すべてのポートが管理上アップ状態になっていない限り、宛先グループを設定できません。グループの構成が完了したら、SPAN 宛先グループの任意のポートをアップまたはダウン状態にすることができます。1つまたは複数のポートが管理上ダウン状態にある、動作中のワーブ設定をコピーし、その構成を同じスイッチの構成ファイルに貼り付けると、ワーブ SPAN は次のエラーをログに記録します。

```
ERROR: Cannot configure group with member interfaces in admin DOWN state
```

- ワーブ SPAN と ERSPAN で同じ送信元インターフェイスを使用することはサポートされていません。

## ワーブ SPAN の構成

ワーブ SPAN を設定するには、それを有効にしてから、その宛先グループを設定します。

### 手順の概要

1. switch# **configure terminal**
2. switch(config-monitor)# **interface ethernet** *port/slot*
3. switch(config-if)# **switchport monitor**
4. switch(config-if)# **no shutdown**
5. switch(config)# **monitor session warp**
6. switch(config)# **no shutdown**
7. switch(config-monitor)# **destination group** *group-number*
8. (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-monitor)# <b>interface ethernet</b> <i>port/slot</i>	指定したインターフェイスに対してインターフェイス コンフィギュレーション モードを開始します。  (注) 範囲を指定して、複数のインターフェイスを一度に構成できます。
ステップ 3	switch(config-if)# <b>switchport monitor</b>	インターフェイスをモニタ モードに設定します。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無効です。
ステップ 4	switch(config-if)# <b>no shutdown</b>	インターフェイスを管理上アップ状態にします。

	コマンドまたはアクション	目的
ステップ 5	switch(config)# <b>monitor session warp</b>	インターフェイスでワーブ SPAN を有効にします。
ステップ 6	switch(config)# <b>no shutdown</b>	インターフェイスを管理上アップ状態にします。
ステップ 7	switch(config-monitor)# <b>destination group group-number</b>	宛先グループを設定します。  (注) 合計 47 の宛先ポートを持つ最大 12 のグループを作成できます。すべてのグループに 4 つのポートがありますが、グループ 9 は例外です。ポート 1/36 (固定送信元ポート) が含まれないため、3 つのポートしかありません。
ステップ 8	(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、ワーブ SPAN に宛先 SPAN ポート 1/1-4 を設定する例を示します。

```
switch# configure terminal
switch(config-monitor)# interface ethernet 1/1-4
switch(config-if-range)# switchport monitor
switch(config-if-range)# no shutdown
switch(config)# monitor session warp
switch(config)# no shutdown
switch(config-monitor)# destination group 1
switch(config-if-range)# copy running-config startup-config
```

## ワーブ SPAN モード構成の確認

ユーザーはワーブ SPAN モードの構成を確認できます。

### 手順の概要

1. switch(config)# **show monitor session {number | all | range}**
2. switch(config)# **show monitor session warp**

## 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)# <b>show monitor session</b> { <i>number</i>   <b>all</b>   <i>range</i> }	特定の SPAN セッション、すべての SPAN セッション、または一定範囲の SPAN セッションに関する情報を表示します。
ステップ 2	switch(config)# <b>show monitor session warp</b>	ワープ SPAN セッションに関する情報を表示します。

## 例

次に、SPAN セッション 1 に関する情報を表示する例を示します。

```
switch(config)# show monitor session all
session warp
-----
type : local
state : up
source intf :
rx : Eth1/36
tx :
both :
source VLANs :
rx :
destination ports : Eth1/1 Eth1/2 Eth1/3 Eth1/4

Legend: f = forwarding enabled, l = learning enabled
```

```
switch(config)# show monitor session warp
session warp
-----
type : local
state : up
source intf :
rx : Eth1/36
tx :
both :
source VLANs :
rx :
destination ports : Eth1/1 Eth1/2 Eth1/3 Eth1/4

Legend: f = forwarding enabled, l = learning enabled
```

## ワーブ SPAN 機能の履歴

機能名	リリース	機能情報
ワーブ SPAN	5.0(3)A1(1)	この機能が導入されました。



## 第 16 章

# ERSPAN の設定

この章は、次の内容で構成されています。

- [ERSPAN に関する情報 \(227 ページ\)](#)
- [ERSPAN の前提条件 \(229 ページ\)](#)
- [ERSPAN の注意事項および制約事項 \(230 ページ\)](#)
- [ERSPAN のデフォルト設定 \(232 ページ\)](#)
- [ERSPAN の設定 \(232 ページ\)](#)
- [ERSPAN の設定例 \(248 ページ\)](#)
- [その他の参考資料 \(249 ページ\)](#)

## ERSPAN に関する情報

Cisco NX-OS システムは、発信元および宛先ポートの両方で Encapsulated Remote Switching Port Analyzer (ERSPAN) 機能をサポートします。ERSPAN は、IP ネットワークでミラーリングされたトラフィックを転送します。

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。

## ERSPAN タイプ

ERSPAN タイプ III は ERSPAN タイプ II のすべての特徴と機能をサポートするもので、以下の拡張機能が追加されています。

- ERSPAN タイプ III ヘッダーに、エッジ、集約、およびコア スイッチでパケット遅延性を計算するために使用できるタイムスタンプ情報を追加。
- ERSPAN タイプ III ヘッダー フィールドを使用して潜在的なトラフィック ソースを識別可能。

## 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。

- 送信元ポート：送信元ポートは、トラフィック分析のためにモニターされるポートです。任意の VLAN に送信元ポートを設定できます。また、トランクポートを、送信元ポートとして設定したり、非トランク送信元ポートと混在させることができます。
- 送信元 VLAN：送信元 VLAN は、トラフィック分析のためにモニターされる仮想ローカルエリア ネットワーク (VLAN) です。
- 送信元 VSAN：送信元 VSAN は、トラフィック分析のためにモニターされる仮想ストレージエリア ネットワーク (VSAN) です。

## ERSPAN 宛先

ERSPAN 宛先セッションは、イーサネットポートまたはポートチャネル上の ERSPAN 送信元セッションで送信されたパケットを取得し、宛先ポートに送信します。宛先ポートは ERSPAN 送信元からコピーされたトラフィックを受信します。

ERSPAN 宛先セッションは、設定された送信元 IP アドレスおよび ERSPAN ID によって識別されます。これにより、複数の送信元セッションが ERSPAN トラフィックを同じ宛先 IP および ERSPAN ID に送信できるようになり、1つの宛先で同時に終端する複数の送信元を持つことができます。

SPAN 宛先ポートには、次の特性があります。

- 宛先ポートとして設定されたポートは、送信元ポートとして設定できません。
- 宛先ポートは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。
- 入力および入力学習オプションは、モニタ宛先ポートではサポートされていません。
- ホストインターフェイス (HIF) ポートチャネルおよびファブリックポートチャネルポートは、SPAN 宛先ポートとしてはサポートされていません。

## ERSPAN セッション

ERSPAN セッションを作成して、モニタする送信元と接続先を指定することができます。

ERSPAN 送信元セッションを設定する場合、接続先 IP アドレスを構成する必要があります。ERSPAN 接続先セッションを設定する場合、送信元 IP アドレスを構成する必要があります。送信元セッションのプロパティについては [ERSPAN 送信元 \(228 ページ\)](#)、接続先セッションのプロパティについては [ERSPAN 宛先 \(228 ページ\)](#) を参照してください。



- (注) ERSPAN または SPAN 送信元セッションの場合、すべてのスイッチで同時に実行できるのは、8 つまでの単方向、または 4 つまでの双方向セッションです。ERSPAN 接続先セッションの場合、すべてのスイッチで同時に実行できるのは、20 までのセッションです。

次の図は、ERSPAN 構成を示しています。

図 2: ERSPAN の設定



## マルチ ERSPAN セッション

最大で 8 個の単方向 ERSPAN 送信元セッションもしくは SPAN セッション、または 4 個の双方向 ERSPAN 送信元もしくは SPAN セッションを同時に定義できます。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 \(238 ページ\)](#) を参照してください。

## ERSPAN マーカー パケット

タイプ III ERSPAN ヘッダーは、ハードウェアで生成された 32 ビットのタイムスタンプを送信します。このタイムスタンプフィールドは定期的にラップされます。スイッチが 1 ns の最小単位に構成されている場合、このフィールドは 4.29 秒ごとにラップされます。このような時間のラップのため、タイムスタンプの実際の値を解釈する際に問題が生じます。

ERSPAN タイムスタンプの実際の値を回復するために、Cisco NX-OS リリース 6.0(2)A4(1) では、元の UTC タイムスタンプ情報を伝送し、ERSPAN タイムスタンプの参照を提供する定期的なマーカーパケットが導入されています。マーカーパケットは 1 秒間隔で送信されます。したがって、接続先サイトは、参照パケットのタイムスタンプとパケットの順序との違いをチェックすることにより、タイムスタンプが 32 ビットであるために生じたラップを検出できます。

## 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

ERSPAN 設定時の注意事項と制限事項は次のとおりです。

- ERSPAN は次をサポートしています。
  - ERSPAN 送信元セッションタイプ（パケットは、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）。
  - ERSPAN 接続先セッションタイプ（ERSPAN パケットのカプセル化解除のサポートが利用できます。カプセル化されたパケットは接続先ボックスでカプセル化解除され、カプセル化解除されたプレーンパケットは ERSPAN 終端ポイントのフロントパネルポートにスパンされます）。
- ERSPAN 送信元セッションは複数のローカル SPAN セッションで共有されます。1つの方向に最大 8 つの ERSPAN 送信元または SPAN 送信元セッションを構成できます。受信ソースと送信ソースの両方が同じセッションで構成されている場合、2つのセッションとしてカウントされます。一度に構成できるのは 4 つの双方向セッションです。
- Cisco NX-OS 5.0(3)U2(2) をインストールして ERSPAN を設定し、その後でソフトウェアをそれより前のバージョンにダウングレードすると、ERSPAN の設定は失われます。これは、ERSPAN が Cisco NX-OS 5.0(3)U2(2) よりも前のバージョンではサポートされていないためです。

同様の SPAN の制約事項については、[SPAN の注意事項および制約事項（204 ページ）](#)を参照してください。

- ERSPAN 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 セッションは、接続先ルータにおいて同一方式で終了します。
- ERSPAN は、管理ポートではサポートされません。
- 接続先ポートは、一度に 1 つの ERSPAN セッションだけで構成できます。
- 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とができる 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。送信元ポートでこの動作が生じる例の一部を示します。
  - フラディングから発生するトラフィック
  - ブロードキャストおよびマルチキャスト トラフィック
- Nexus 3548 が ERSPAN 接続先の場合、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削除されません。
- ERSPAN は最小単位が 1588 のモードをサポートしていないため、このモードが選択されている場合は拒否されます。
- ERSPAN は、最小単位として 100 マイクロ秒 ( $\mu$ s)、100 ナノ秒 (ns)、および ns をサポートします。
- ERSPAN は、すべてのタイムスタンプを 32 ビット形式で送信します。したがって、タイムスタンプフィールドのラップが定期的が発生します。スイッチの最小単位が ns に設定されている場合、このフィールドは 4.29 秒ごとにラップします。
- レイヤ3サブインターフェイスは、ERSPAN 送信元インターフェイスとして設定できません。
- 単一の接続先ボックスで終端するすべての ERSPAN 送信元は、同じ接続先 IP アドレスを使用する必要があります。
- 異なる ERSPAN 接続先セッションで異なる送信元 IP アドレスを構成することはできません。
- Rx または Tx 方向のいずれかで ERSPAN ソースを介してスパンされる、VLAN X から VLAN Y へのレイヤ3スイッチドトラフィックは、VLAN X (レイヤ3スイッチングまたは入力 VLAN の前の VLAN) の ERSPAN ヘッダーで VLAN 情報を伝送します。
- 出力 (Tx) 方向に設定されている ERSPAN 送信元インターフェイスから送信されないマルチキャストフラッドパケットも、引き続き ERSPAN 接続先に到達できます。これは、Nexus 3548 スイッチの ASIC (特定用途向け集積回路) のスパンがモニターポートのプロパティに基づいているのに対し、出力スパンパケットは、元の出力ポートが特定のフレームを受信して他のフレームをドロップするように選択的に有効化される前にスパンされるためです。その結果、スパンパケットは引き続きリモート接続先に送信されます。これは、マルチキャストフラッドに固有のプラットフォームから予期される動作であり、他のトラフィックストリームでは見られません。

- Tx 方向で ERSPAN 送信元から送信された、複製されたマルチキャストパケットは、ERSPAN 接続先に送信されません。
- 複数の ERSPAN (タイプ 2 またはタイプ 3) セッションで同じ送信元インターフェイス (物理ポートまたはポート チャンネル) を監視できます。
- 送信元として VLAN を使用した ERSPAN またはローカル SPAN での IP フィルタの構成はサポートされていません。

## 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 30: 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 チャンネル、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. **monitor erspan granularity 100\_ns {100\_us|100\_ns|ns}**
4. **no monitor session {session-number | all}**
5. **monitor session {session-number | all} type erspan-source**
6. **header-type version**
7. **description description**

8. **source** {[interface[type slot/port[-port][, type slot/port[-port]]] [port-channel channel-number]] | [vlan {number | range}]} [rx | tx | both]
9. (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。
10. **destination ip** ip-address
11. **erspan-id** erspan-id
12. **vrf** vrf-name
13. (任意) **ip ttl** ttl-number
14. (任意) **ip dscp** dscp-number
15. **no shut**
16. (任意) **show monitor session** {all | session-number | range session-range}
17. (任意) **show running-config monitor**
18. (任意) **show startup-config monitor**
19. (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 ip-address 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>monitor erspan granularity 100_ns {100_us 100_ns ns}</b> 例： switch(config)# monitor erspan granularity 100_ns	すべての ERSPAN セッションの最小単位を構成します。
ステップ 4	<b>no monitor session {session-number   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。
ステップ 5	<b>monitor session {session-number   all} type erspan-source</b> 例： switch(config)# monitor session 3 type erspan-source switch(config-erspan-src)#	ERSPAN 送信元セッションを設定します。

	コマンドまたはアクション	目的
ステップ 6	<b>header-type</b> <i>version</i> 例： <pre>switch(config-erspan-src)# header-type 3</pre>	(任意) ERSPAN 送信元セッションをタイプ II からタイプ III に変更します。
ステップ 7	<b>description</b> <i>description</i> 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 8	<b>source</b> {[ <b>interface</b> [ <i>type slot/port[-port]</i> ], <i>type slot/port[-port]</i> ]} [ <b>port-channel</b> <i>channel-number</i> ]   [ <b>vlan</b> { <i>number</i>   <i>range</i> }] } [ <b>rx</b>   <b>tx</b>   <b>both</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 9	(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 10	<b>destination ip</b> <i>ip-address</i> 例： <pre>switch(config-erspan-src)# destination ip 10.1.1.1</pre>	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	<b>erspan-id</b> <i>erspan-id</i> 例： <pre>switch(config-erspan-src)# erspan-id 5</pre>	ERSPAN 送信元セッションの ERSPAN ID を設定します。ERSPAN の範囲は 1 ~ 1023 です。この ID は、送信元および宛先の ERSPAN セッションのペアを一意に識別します。対応する宛先の ERSPAN セッションに設定される ERSPAN ID は、送信元のセッションで設定されているものと同じにする必要があります。
ステップ 12	<b>vrf</b> <i>vrf-name</i> 例： <pre>switch(config-erspan-src)# vrf default</pre>	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。

	コマンドまたはアクション	目的
ステップ 13	(任意) <b>ip ttl</b> <i>ttl-number</i> 例： switch(config-erspan-src)# ip ttl 25	ERSPAN トラフィックの IP 存続可能時間 (TTL) 値を設定します。範囲は 1 ~ 255 です。
ステップ 14	(任意) <b>ip dscp</b> <i>dscp-number</i> 例： switch(config-erspan-src)# ip dscp 42	ERSPAN トラフィックのパケットの DiffServ コードポイント (DSCP) 値を設定します。範囲は 0 ~ 63 です。
ステップ 15	<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状態で作成されます。  (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 16	(任意) <b>show monitor session</b> {all   <i>session-number</i>   <b>range</b> <i>session-range</i> } 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 17	(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 18	(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 19	(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 宛先セッションの設定

送信元 IP アドレスからローカル デバイス上の宛先ポートにパケットをコピーするように ERSPAN 宛先セッションを構成できます。デフォルトでは、ERSPAN 宛先セッションはシャット状態で作成されます。

## 始める前に

モニタ モードで宛先ポートが設定されていることを確認します。

## 手順の概要

1. **config t**
2. **interface ethernet** *slot/port*[-*port*]
3. **switchport**
4. **switchport mode** [access | trunk]
5. **switchport monitor**
6. ステップ 2 ~ 5 を繰り返して、追加の ERSPAN 宛先でモニタリングを設定します。
7. **no monitor session** {*session-number* | all}
8. **monitor session** {*session-number* | all} **type erspan-destination**
9. **description** *description*
10. **source ip** *ip-address*
11. **destination** {[**interface** [*type slot/port*[-*port*], [*type slot/port* [*port*]]]}
12. **erspan-id** *erspan-id*
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>config t</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>interface ethernet</b> <i>slot/port</i> [- <i>port</i> ] 例： switch(config)# interface ethernet 2/5 switch(config-if)#	選択したスロットおよびポートまたはポート範囲で、インターフェイスコンフィギュレーションモードを開始します。
ステップ 3	<b>switchport</b> 例： switch(config-if)# switchport	選択したスロットおよびポートまたはポート範囲でスイッチポートパラメータを設定します。
ステップ 4	<b>switchport mode</b> [access   trunk] 例：	選択したスロットおよびポートまたはポート範囲で次のスイッチポート モードを設定します。

	コマンドまたはアクション	目的
	<code>switch(config-if)# switchport mode trunk</code>	<ul style="list-style-type: none"> <li>• アクセス</li> <li>• トランク</li> </ul>
ステップ 5	<b>switchport monitor</b> 例 : <code>switch(config-if)# switchport monitor</code>	モニタ モードでスイッチ インターフェイスを設定します。 (destination interface ethernet interface コマンドを使用して) インターフェイスを ERSPAN または SPAN 宛先に設定するには、最初にモニタ モードで設定する必要があります。
ステップ 6	ステップ 2 ~ 5 を繰り返して、追加の ERSPAN 宛先でモニタリングを設定します。	—
ステップ 7	<b>no monitor session {session-number   all}</b> 例 : <code>switch(config-if)# no monitor session 3</code>	指定した ERSPAN セッションの設定を消去します。新しいセッション コンフィギュレーションは、既存のセッション コンフィギュレーションに追加されます。
ステップ 8	<b>monitor session {session-number   all} type erspan-destination</b> 例 : <code>switch(config-if)# monitor session 3 type erspan-destination</code> <code>switch(config-erspan-dst)#</code>	ERSPAN 宛先セッションを設定します。
ステップ 9	<b>description description</b> 例 : <code>switch(config-erspan-dst)# description erspan_dst_session_3</code>	セッションの説明を設定します。デフォルトでは、説明は定義されません。説明には最大 32 の英数字を使用できます。
ステップ 10	<b>source ip ip-address</b> 例 : <code>switch(config-erspan-dst)# source ip 10.1.1.1</code>	ERSPAN セッションの送信元 IP アドレスを設定します。ERSPAN 宛先セッションごとに 1 つの送信元 IP アドレスのみがサポートされます。 この IP アドレスは、対応する ERSPAN 送信元セッションに設定されている宛先 IP アドレスと一致している必要があります。
ステップ 11	<b>destination {[interface [type slot/port[-port], [type slot/port [port]]]}</b> 例 : <code>switch(config-erspan-dst)# destination interface ethernet 2/5</code>	コピーする送信元パケットの宛先を設定します。宛先としては、インターフェイスのみを設定できます。 (注) 宛先ポートをトランク ポートとして設定できません。

	コマンドまたはアクション	目的
ステップ 12	<b>erspan-id erspan-id</b> 例： <pre>switch(config-erspan-dst)# erspan-id 5</pre>	ERSPAN セッションの ERSPAN ID を設定します。指定できる範囲は 1 ～ 1023 です。この ID は、送信元および宛先の ERSPAN セッションのペアを一意に識別します。対応する宛先の ERSPAN セッションに設定される ERSPAN ID は、送信元のセッションで設定されているものと同じにする必要があります。
ステップ 13	<b>no shut</b> 例： <pre>switch(config)# no shut</pre>	ERSPAN 宛先セッションを有効にします。デフォルトでは、セッションはシャット ステートで作成されます。  (注) 同時に実行できるアクティブな ERSPAN 宛先セッションは 16 までです。
ステップ 14	(任意) <b>show monitor session {all   session-number   range session-range}</b> 例： <pre>switch(config)# show monitor session 3</pre>	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： <pre>switch(config-erspan-src)# show running-config monitor</pre>	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： <pre>switch(config-erspan-src)# show startup-config monitor</pre>	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： <pre>switch(config-erspan-src)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

## ERSPAN 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ー 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> 例： switch# configuration terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>monitor session {<i>session-range</i>   all} shut</b> 例： switch(config)# monitor session 3 shut	指定のERSPANセッションをシャットダウンします。セッションの範囲は1～48です。デフォルトでは、セッションはシャットステートで作成されます。
ステップ 3	<b>no monitor session {<i>session-range</i>   all} shut</b> 例： switch(config)# no monitor session 3 shut	指定のERSPANセッションを再開（イネーブルに）します。セッションの範囲は1～48です。デフォルトでは、セッションはシャットステートで作成されます。  (注) モニターセッションがイネーブルで動作状況がダウンの場合、セッションをイネーブルにするには、最初に <b>monitor session shut</b> コマンドを指定してか

	コマンドまたはアクション	目的
		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 <i>session-number</i> type erspan-source</b> 例： <pre>switch(config)# monitor session 3 type erspan-source switch(config-erspan-src)#</pre>	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 <i>session-number</i> type erspan-destination</b> 例： <pre>switch(config-erspan-src)# monitor session 3 type erspan-destination</pre>	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： <pre>switch(config-erspan-src)# shut</pre>	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： <pre>switch(config-erspan-src)# no shut</pre>	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： <pre>switch(config-erspan-src)# show monitor session all</pre>	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： <pre>switch(config-erspan-src)# show running-config monitor</pre>	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： <pre>switch(config-erspan-src)# show startup-config monitor</pre>	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： <pre>switch(config-erspan-src)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

## ERSPAN フィルタリングの設定

SPAN フィルタは、ローカルセッションおよび ERSPAN 送信元セッションのみに構成できません。フィルタの詳細については、[SPAN および ERSPAN フィルタ処理 \(205 ページ\)](#) を参照してください。

### 手順の概要

1. switch# **configure terminal**
2. switch(config)# **monitor session** {*session-number* | **all**} **type erspan-source**
3. switch(config-erspan-src)# **filter** {**ip** *source-ip-address source-ip-mask destination-ip-address destination-ip-mask*}
4. switch(config-erspan-src)# **erspan-id** *erspan-id*
5. switch(config-erspan-src)# **vrf** *vrf-name*
6. switch(config-erspan-src)# **destination ip** *ip-address*
7. switch(config-erspan-src)# **source** [**interface** [*type slot/port*] | **port-channel** *channel-number*] | [**vlan** *vlan-range*] [**rx** | **tx** | **both**]

### 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>monitor session</b> { <i>session-number</i>   <b>all</b> } <b>type erspan-source</b>	ERSPAN 送信元セッションを設定します。
ステップ 3	switch(config-erspan-src)# <b>filter</b> { <b>ip</b> <i>source-ip-address source-ip-mask destination-ip-address destination-ip-mask</i> }	ERSPAN フィルタを作成します。
ステップ 4	switch(config-erspan-src)# <b>erspan-id</b> <i>erspan-id</i>	ERSPAN 送信元セッションの ERSPAN ID を設定します。ERSPAN の範囲は 1 ~ 1023 です。この ID は、送信元および宛先の ERSPAN セッションのペアを一意に識別します。対応する宛先の ERSPAN セッションに設定される ERSPAN ID は、送信元のセッションで設定されているものと同じにする必要があります。
ステップ 5	switch(config-erspan-src)# <b>vrf</b> <i>vrf-name</i>	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 6	switch(config-erspan-src)# <b>destination ip</b> <i>ip-address</i>	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。

	コマンドまたはアクション	目的
ステップ 7	switch(config-erspan-src)# <b>source</b> [interface [type slot/port]   port-channel channel-number]   [vlan vlan-range] [rx   tx   both]	<p>送信元およびパケットをコピーするトラフィックの方向を設定します。イーサネットポート範囲、ポートチャンネル、または VLAN 範囲を入力できます。</p> <p>送信元は 1 つ設定することも、またはカンマで区切った一連のエントリとして、または番号の範囲として、複数設定することもできます。最大 128 のインターフェイスを指定できます。</p> <p>コピーするトラフィックの方向には、入力、出力、または両方を指定できます。デフォルトは双方向です。</p>

### 例

次の例は、ERSPAN 送信元セッションに MAC ベースのフィルタを設定する方法を示しています。

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# monitor session 2 type erspan-source
switch(config-erspan-src) # filter abcd.ef12.3456 1111.2222.3333 1234.5678.9012
1111.2222.3333
switch(config-erspan-src) # erspan-id 20
switch(config-erspan-src) # vrf default
switch(config-erspan-src) # destination ip 200.1.1.1
switch(config-erspan-src) # source interface Ethernet 1/47 rx
switch(config-erspan-src) # no shut
switch(config-erspan-src) #
```

次の例は、ERSPAN 送信元セッションに VLAN ベースのフィルタを設定する方法を示しています。

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# monitor session 2 type erspan-source
switch(config-erspan-src) # filter abcd.ef12.3456 1111.2222.3333 1234.5678.9012
1111.2222.3333
switch(config-erspan-src) # erspan-id 21
switch(config-erspan-src) # vrf default
switch(config-erspan-src) # destination ip 200.1.1.1
switch(config-erspan-src) # source interface Ethernet 1/47 rx
switch(config-erspan-src) # source vlan 315
switch(config-erspan-src) # mtu 200
switch(config-erspan-src) # no shut
switch(config-erspan-src) #
```

## ERSPAN サンプルングの設定

サンプルングは、ローカルセッションおよびERSPAN送信元セッションのみに構成できます。サンプルングの詳細については、[SPAN およびERSPAN サンプルング \(207 ページ\)](#) を参照してください。

### 手順の概要

1. switch# **configure terminal**
2. switch(config)# **monitor session** {*session-number* | **all**} **type erspan-source**
3. switch(config-erspan-src)# **sampling** *sampling-range*
4. switch(config-erspan-src)# **erspan-id** *erspan-id*
5. switch(config-erspan-src)# **vrf** *vrf-name*
6. switch(config-erspan-src)# **destination ip** *ip-address*
7. switch(config-erspan-src)# **source** [**interface** *type slot/port* | **port-channel** *channel-number*] | [**vlan** *vlan-range*] [**rx** | **tx** | **both**]

### 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>monitor session</b> { <i>session-number</i>   <b>all</b> } <b>type erspan-source</b>	ERSPAN 送信元セッションを設定します。
ステップ 3	switch(config-erspan-src)# <b>sampling</b> <i>sampling-range</i>	スパニング パケットの範囲を構成します。範囲が n として定義されている場合、n 番目のパケットごとにスパンされます。  サンプルング範囲は 2 ~ 1023 です。
ステップ 4	switch(config-erspan-src)# <b>erspan-id</b> <i>erspan-id</i>	ERSPAN 送信元セッションの ERSPAN ID を設定します。ERSPAN の範囲は 1 ~ 1023 です。この ID は、送信元および宛先の ERSPAN セッションのペアを一意に識別します。対応する宛先の ERSPAN セッションに設定される ERSPAN ID は、送信元のセッションで設定されているものと同じにする必要があります。
ステップ 5	switch(config-erspan-src)# <b>vrf</b> <i>vrf-name</i>	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。

	コマンドまたはアクション	目的
ステップ 6	switch(config-erspan-src)# <b>destination ip</b> <i>ip-address</i>	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 7	switch(config-erspan-src)# <b>source</b> [ <b>interface</b> <i>type slot/port</i>   <b>port-channel</b> <i>channel-number</i> ]   [ <b>vlan</b> <i>vlan-range</i> ] [ <b>rx</b>   <b>tx</b>   <b>both</b> ]	送信元およびパケットをコピーするトラフィックの方向を設定します。イーサネットポート範囲、ポートチャンネル、または VLAN 範囲を入力できます。  送信元は 1 つ設定することも、またはカンマで区切った一連のエントリとして、または番号の範囲として、複数設定することもできます。最大 128 のインターフェイスを指定できます。  コピーするトラフィックの方向には、入力、出力、または両方を指定できます。デフォルトは双方向です。

## 例

次の例は、ERSPAN 送信元セッションのサンプルングを設定する方法を示しています。

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# monitor session 2 type erspan-source
switch(config-erspan-src)# sampling 40
switch(config-erspan-src)# erspan-id 30
switch(config-erspan-src)# vrf default
switch(config-erspan-src)# destination ip 200.1.1.1
switch(config-erspan-src)# source interface ethernet 1/47
switch(config-erspan-src)# show monitor session 2
session 2
-----
type : erspan-source
state : up
granularity : 100 microseconds
erspan-id : 30
vrf-name : default
destination-ip : 200.1.1.1
ip-ttl : 255
ip-dscp : 0
header-type : 2
mtu : 200
sampling : 40
origin-ip : 150.1.1.1 (global)
source intf :
rx : Eth1/47
tx : Eth1/47
both : Eth1/47
source VLANs :
rx : 315
switch(config-erspan-src)#
```

## ERSPAN 切り捨ての設定

切り捨ては、ローカルおよび ERSPAN 送信元セッションに対してのみ構成できます。切り捨ての詳細については、[SPAN および ERSPAN の切り捨て \(208 ページ\)](#) を参照してください。

### 手順の概要

1. switch# **configure terminal**
2. switch(config)# **monitor session** {*session-number* | **all**} **type erspan-source**
3. switch(config-erspan-src)# **mtu size**
4. switch(config-erspan-src)# **erspan-id** *erspan-id*
5. switch(config-erspan-src)# **vrf** *vrf-name*
6. switch(config-erspan-src)# **destination ip** *ip-address*
7. switch(config-erspan-src)# **source** [**interface** *type slot/port* | **port-channel** *channel-number*] | [**vlan** *vlan-range*] [**rx** | **tx** | **both**]

### 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>monitor session</b> { <i>session-number</i>   <b>all</b> } <b>type erspan-source</b>	ERSPAN 送信元セッションを設定します。
ステップ 3	switch(config-erspan-src)# <b>mtu size</b>	MTU の切り捨てサイズを設定します。構成された MTU サイズよりも大きい SPAN パケットはすべて、4 バイトのオフセットで構成されたサイズに切り捨てられます。  MTU 切り捨てサイズは 64 バイトから 1518 バイトです。
ステップ 4	switch(config-erspan-src)# <b>erspan-id</b> <i>erspan-id</i>	ERSPAN 送信元セッションの ERSPAN ID を設定します。ERSPAN の範囲は 1 ~ 1023 です。この ID は、送信元および宛先の ERSPAN セッションのペアを一意に識別します。対応する宛先の ERSPAN セッションに設定される ERSPAN ID は、送信元のセッションで設定されているものと同じにする必要があります。
ステップ 5	switch(config-erspan-src)# <b>vrf</b> <i>vrf-name</i>	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。

	コマンドまたはアクション	目的
ステップ 6	switch(config-erspan-src)# <b>destination ip</b> <i>ip-address</i>	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 7	switch(config-erspan-src)# <b>source</b> [ <b>interface</b> <i>type slot/port</i>   <b>port-channel</b> <i>channel-number</i> ]   [ <b>vlan</b> <i>vlan-range</i> ] [ <b>rx</b>   <b>tx</b>   <b>both</b> ]	送信元およびパケットをコピーするトラフィックの方向を設定します。イーサネットポート範囲、ポートチャンネル、または VLAN 範囲を入力できます。  送信元は 1 つ設定することも、またはカンマで区切った一連のエントリとして、または番号の範囲として、複数設定することもできます。最大 128 のインターフェイスを指定できます。  コピーするトラフィックの方向には、入力、出力、または両方を指定できます。デフォルトは双方向です。

## 例

次の例は、ERSPAN 送信元セッションの MTU 切り捨てを構成する方法を示しています。

```
switch# configure terminal
switch(config)# monitor session 6 type erspan-source
switch(config-erspan-src)# mtu 1096
switch(config-erspan-src)# erspan-id 40
switch(config-erspan-src)# vrf default
switch(config-erspan-src)# destination ip 200.1.1.1
switch(config-erspan-src)# source interface ethernet 1/40
switch(config-erspan-src)# show monitor session 6
session 6
-----
type : erspan-source
state : down (Session admin shut)
granularity : 100 microseconds
erspan-id : 40
vrf-name : default
destination-ip : 200.1.1.1
ip-ttl : 255
ip-dscp : 0
header-type : 2
mtu : 1096
origin-ip : 150.1.1.1 (global)
source intf :
rx : Eth1/40
tx : Eth1/40
both : Eth1/40
source VLANs :
rx :
```

## ERSPAN マーカー パケットの構成

次のコマンドを使用して、ERSPAN マーカー パケットを構成します。

コマンド	目的
<b>marker-packet</b> 秒	セッションの ERSPAN マーカー パケットを有効にします。 間隔は、1 秒から 4 秒の範囲で指定できます。
<b>marker-packet</b> milliseconds	セッションの ERSPAN マーカー パケットを有効にします。 間隔は 100 ミリ秒から 900 ミリ秒の範囲で、100 の倍数で増やせます。
<b>no marker-packet</b>	セッションの ERSPAN マーカー パケットを無効にします。

### 例

次に、2 秒間隔で ERSPAN マーカー パケットを有効にする例を示します。



- (注) interval パラメータの設定はオプションです。パラメータを指定せずにマーカー パケットを有効にすると、デフォルトまたは既存の間隔が間隔値として使用されます。  
**marker-packet** コマンドは、マーカー パケットのみを有効にします。

```
switch# configure terminal
switch(config)# monitor erspan origin ip-address 172.28.15.250 global
switch(config)# monitor session 1 type erspan-source
switch(config)# header-type 3
switch(config-erspan-src)# erspan-id 1
switch(config-erspan-src)# ip ttl 16
switch(config-erspan-src)# ip dscp 5
switch(config-erspan-src)# vrf default
switch(config-erspan-src)# destination ip 9.1.1.2
switch(config-erspan-src)# source interface e1/15 both
switch(config-erspan-src)# marker-packet 2
switch(config-erspan-src)# no shut
switch(config-erspan-src)# exit
```

## 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</b> {all   <i>session-number</i>   <b>range</b> <i>session-range</i> }	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 erspan granularity 100_ns
switch(config-erspan-src)# header-type 3
switch(config)# monitor session 1 type erspan-source
switch(config-erspan-src)# source interface e14/30
switch(config-erspan-src)# erspan-id 1
switch(config-erspan-src)# ip ttl 16
switch(config-erspan-src)# ip dscp 5
switch(config-erspan-src)# destination ip 9.1.1.2
switch(config-erspan-src)# no shut
switch(config-erspan-src)# exit
switch(config)# show monitor session 1
```



(注) **switch(config)# monitor erspan granularity 100\_ns** および **switch(config-erspan-src)# header-type 3** は、Type III の送信元セッションの設定にだけ使用されます。

### ERSPAN 宛先セッションの設定例

次に、ERSPAN 宛先セッションを設定する例を示します。

```
switch# config t
switch(config)# interface e14/29
switch(config-if)# no shut
switch(config-if)# switchport
switch(config-if)# switchport monitor
switch(config-if)# exit
```

```
switch(config)# monitor session 2 type erspan-destination
switch(config-erspan-dst)# source ip 9.1.1.2
switch(config-erspan-dst)# destination interface e14/29
switch(config-erspan-src)# erspan-id 1
switch(config-erspan-dst)# no shut
switch(config-erspan-dst)# exit
switch(config)# show monitor session 2
```

## その他の参考資料

### 関連資料

関連項目	マニュアルタイトル
ERSPAN コマンド：コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト、使用上の注意事項、および例	ご使用プラットフォームの『 <i>Cisco Nexus NX-OS System Management Command Reference</i> 』。





## 第 17 章

# DNS の設定

この章は、次の内容で構成されています。

- [DNS クライアントに関する情報 \(251 ページ\)](#)
- [DNS クライアントの前提条件 \(252 ページ\)](#)
- [DNS クライアントのデフォルト設定 \(252 ページ\)](#)
- [DNS クライアントの設定 \(252 ページ\)](#)

## DNS クライアントに関する情報

自分で名前の割り当てを管理していないネットワーク内のデバイスとの接続を、ネットワークデバイスが必要とする場合は、DNS を使用して、ネットワーク間でデバイスを特定する一意のデバイス名を割り当てることができます。DNS は、階層方式を使用して、ネットワーク ノードのホスト名を確立します。これにより、クライアントサーバ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、シスコは、インターネットでは `com` ドメインで表される営利団体であるため、そのドメイン名は `cisco.com` です。このドメイン内の特定のホスト名、たとえばファイル転送プロトコル (FTP) システムは `ftp.cisco.com` で識別されます。

## ネーム サーバ

ネーム サーバはドメイン名の動向を把握し、自身が完全な情報を持っているドメイン ツリーの部分を認識しています。ネーム サーバは、ドメイン ツリーの他の部分の情報を格納している場合もあります。Cisco NX-OS 内の IP アドレスにドメイン名をマッピングするには、最初にホスト名を示し、その後にネーム サーバーを指定して、DNS サービスをイネーブルにする必要があります。

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

## DNSクライアントの前提条件

DNSクライアントには次の前提条件があります。

- ネットワーク上にDNSネームサーバが必要です。

## DNSクライアントのデフォルト設定

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

1. switch# **configuration terminal**
2. switch(config)# vrf context management
3. switch(config)# **ip host name address1 [address2... address6]**
4. (任意) switch(config)# **ip domain name name [ use-vrf vrf-name]**
5. (任意) switch(config)# **ip domain-list name [ use-vrf vrf-name]**
6. (任意) switch(config)# **ip name-server server-address1 [server-address2... server-address6] [use-vrf vrf-name]**
7. (任意) switch(config)# **ip domain-lookup**
8. (任意) switch(config)# **show hosts**
9. switch(config)# **exit**
10. (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)# <b>ip host name address1 [address2... address6]</b>	ホスト名キャッシュに、6つまでのスタティック ホスト名/アドレス マッピングを定義します。
ステップ 4	(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。
ステップ 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

	コマンドまたはアクション	目的
		<p>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。</p> <p>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。</p>
ステップ 6	(任意) switch(config)# <b>ip name-server</b> <i>server-address1 [server-address2... server-address6]</i> <b>[use-vrf vrf-name]</b>	<p>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。</p> <p>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。</p>
ステップ 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。
ステップ 8	(任意) switch(config)# <b>show hosts</b>	DNS に関する情報を表示します。
ステップ 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。
ステップ 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 18 章

# トラフィック転送モードの構成

この章は、次の内容で構成されています。

- [ワープモードに関する情報 \(255 ページ\)](#)
- [ワープモードの注意事項および制限事項 \(255 ページ\)](#)
- [ワープモードの有効化と無効化 \(256 ページ\)](#)
- [ワープモードのステータスの確認 \(257 ページ\)](#)
- [ワープモードの機能履歴 \(257 ページ\)](#)

## ワープモードに関する情報

Cisco Nexus デバイスは、アルゴリズムブーストエンジン (Algo Boost Engine) と呼ばれるハードウェア コンポーネントを使用して、ワープモードと呼ばれる転送メカニズムをサポートします。ワープモードでは、転送テーブルを単一のテーブルに統合することによりアクセスパスが短縮されるため、フレームおよびパケットの処理がより高速になります。ワープモードでは、遅延が最大 20 パーセント削減されます。Algo Boost Engine の詳細については、[アクティブバッファモニタリングの概要 \(259 ページ\)](#) を参照してください。

## ワープモードの注意事項および制限事項

ワープモードには以下のような構成の注意事項および制限事項があります。

- ワープモードは、通常の転送より最大で 20% 優れたスイッチ遅延を提供します。
- ワープモードでは、ユニキャストルートテーブルは縮小されます。ルートテーブルは 24000 から 4000 エントリに縮小します。ホストテーブルと MAC テーブルは 64000 から 8000 エントリに縮小します (マルチキャストルートテーブルは 8000 エントリのままです)。
- ワープモードでは、次の機能はサポートされていません。
  - 出力ルーテッドアクセス制御リスト (RACL)
  - ポートアクセス制御リスト (ACL)

- 同等コスト複数パス (ECMP)
- IP リダイレクト

## ワーブモードの有効化と無効化

### 手順の概要

1. switch# **configure terminal**
2. switch(config)# **hardware profile forwarding-mode warp**
3. (任意) switch(config)# **copy running-config startup-config**
4. スイッチをリロードします。

### 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	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>hardware profile forwarding-mode warp</b>	デバイスのワーブモードを有効にします。ワーブモードを無効にするには、このコマンドの <b>no</b> 形式を使用します。デフォルトでは、ワーブモードは無効です。
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。
ステップ 4	スイッチをリロードします。	—

### 例

次に、デバイスのワーブモードを有効にする例を示します。

```
switch# configuration terminal
switch(config)# hardware profile forwarding-mode warp
Warning: This command will take effect only after saving the configuration (copy r s)
switch(config)# copy running-config startup-config
switch(config)#
```

次に、デバイスのワーブモードを無効にする例を示します。

```
switch# configuration terminal
switch(config)# no hardware profile forwarding-mode warp
Warning: This command will take effect only after saving the configuration (copy r s)
switch(config)# copy running-config startup-config
```

## ワーブモードのステータスの確認

### 手順の概要

1. switch# show hardware profile forwarding-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	switch# <b>show hardware profile forwarding-mode</b>	ワーブモードに関する情報と、ホスト、ユニキャスト、マルチキャスト、およびレイヤ 2 の Ternary Content Addressable Memory (TCAM) のサイズを表示します。

### 例

次に、ワーブモードに関する情報を表示する例を示します。

```
switch# show hardware profile forwarding-mode
=====
forwarding-mode : warp
=====
host      size  = 8192
unicast   size  = 4096
multicast size  = 8192
l2        size  = 8192
switch#
```

## ワーブモードの機能履歴

機能名	リリース	機能情報
ワーブモード	5.0(3)A1(1)	この機能が導入されました。





## 第 19 章

# 実行中バッファ監視の構成

この章は、次の内容で構成されています。

- [実行中バッファ監視の構成に付いての情報](#) (259 ページ)
- [実行中バッファ監視の構成](#) (260 ページ)
- [バッファ ヒストグラム データの表示](#) (262 ページ)

## 実行中バッファ監視の構成に付いての情報

### アクティブ バッファ モニタリングの概要

実行中のバッファの監視機能は、詳細なバッファ占有率のデータを提供し、ネットワーク輻輳の検出、ネットワーク輻輳がネットワーク運用にいつどのような影響を与えているかを理解するための過去のイベントの確認、過去の傾向の理解、アプリケーショントラフィックフローのパターンの識別に役立ちます。

Algorithm Boost Engine (Algo Boost Engine) というハードウェア コンポーネントは、個別ポートごとのユニキャストバッファ使用率、バッファ ブロックごとの合計バッファ使用率、およびバッファブロックごとのマルチキャストバッファ使用率の、バッファ ヒストグラム カウンタをサポートします。各ヒストグラム カウンタには、メモリ ブロックにまたがる 18 バケットがあります。Algo Boost Engine はバッファ使用率データを各ハードウェアのサンプリング間隔ごとにポーリングします (デフォルトは 4 ミリ秒ごとですが、10 ナノ秒まで短く設定できます)。バッファ使用率に基づいて、対応するヒストグラム カウンタが増加します。たとえば、イーサネット ポート 1/4 がバッファの 500 KB を消費する場合、イーサネット 1/4 のバケット 2 カウンタ (384 ~ 768 KB を表す) が増加します。

カウンタのオーバーフローを回避するために、Cisco NX-OS ソフトウェアはヒストグラム データをポーリング間隔ごとに収集し、システムメモリに維持します。ソフトウェアは、最小単位 1 秒で、直前の 60 分のシステム メモリのヒストグラム データを維持します。1 時間ごとに、ソフトウェアはバッファのヒストグラム データをシステムメモリからブートフラッシュにバックアップとしてコピーします。

アクティブ バッファ モニタリング機能には 2 つの動作モードがあります。

- ユニキャスト モード：Algo Boost Engine は、バッファ ブロックごとの合計バッファ使用率および 48 ポートすべてのユニキャストバッファ使用率のバッファ ヒストグラムを監視し、維持します。
- マルチキャスト モード：Algo Boost Engine はバッファ ブロックごとの合計バッファ使用率およびバッファ ブロックごとのマルチキャストバッファ使用率のバッファのヒストグラム データを監視し、維持します。

## バッファ ヒストグラム データのアクセスおよび収集

アクティブバッファ モニタリングをイネーブルにすると、デバイスには 70 分のデータが維持されます（ログには最初の 60 分（0 ～ 60 分）、メモリには後の方の 60 分（10 ～ 70 分））。

バッファ ヒストグラム データにはいくつかの方法でアクセスできます。

- **show** コマンドを使用して、システム メモリからアクセスできます。
- アクティブバッファ モニタリング機能を Cisco NX-OS Python スクリプトに統合して、サーバにデータを定期的にコピーして履歴データを収集できます。
- XML インターフェイスを使用してバッファ ヒストグラム データにアクセスできます。
- バッファの占有が、設定されたしきい値を超えるたびに syslog にメッセージを記録するように、Cisco NX-OS を設定できます。

## 実行中バッファ監視の構成



- (注) フロントパネルポートで NX-API を使用する場合は、3000 PPS トラフィックを許可するように CoPP ポリシー（HTTP 用）を増やす必要があります。これにより、パケット ドロップが防止され、CLI はより大きな出力を作成して、予想される時間内に返します。



- (注) 実行中のバッファの監視（ABM）はすべてのフロントポートで有効になっていますが、デフォルトクラスのトラフィックのみを監視できます。

### 手順の概要

1. switch# **configure terminal**
2. switch(config)# **hardware profile buffer monitor {unicast | multicast}**
3. switch(config)# **hardware profile buffer monitor {unicast | multicast} threshold *threshold-value***
4. switch(config)# **hardware profile buffer monitor {unicast | multicast} sampling *sampling-value***
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)# <b>hardware profile buffer monitor {unicast   multicast}</b>	ユニキャストまたはマルチキャストトラフィックのいずれかに対して、ハードウェアプロファイルバッファを有効にします。
ステップ 3	switch(config)# <b>hardware profile buffer monitor {unicast   multicast} threshold <i>threshold-value</i></b>	指定されたバッファサイズの最大値を超えたときに syslog エントリを生成するように指定します。範囲は 384 ~ 6144 KB で、384 KB ずつ増加した値を指定できます。デフォルトは、使用可能な合計共有バッファの 90% です。
ステップ 4	switch(config)# <b>hardware profile buffer monitor {unicast   multicast} sampling <i>sampling-value</i></b>	指定した間隔でデータをサンプリングするように指定します。範囲は 10 ~ 20,000,000 ナノ秒です。デフォルトのサンプリング値は 4 ミリ秒です。
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

この例は、ユニキャストトラフィックの実行中バッファ監視を構成する方法を示しています。384 キロバイトのしきい値と 5000 ナノ秒のサンプリング値が使用されます。

```
switch# configure terminal
switch(config)# hardware profile buffer monitor unicast
switch(config)# hardware profile buffer monitor unicast threshold 384
switch(config)# hardware profile buffer monitor unicast sampling 5000
switch(config)# copy running-config startup-config
```

次の例は、マルチキャストトラフィックの実行中バッファ監視を設定する方法を示しています。384 キロバイトのしきい値と 5000 ナノ秒のサンプリング値が使用されます。

```
switch# configure terminal
switch(config)# hardware profile buffer monitor multicast
switch(config)# hardware profile buffer monitor multicast threshold 384
switch(config)# hardware profile buffer monitor multicast sampling 5000
switch(config)# copy running-config startup-config
```

# バッファ ヒストグラム データの表示

## 手順の概要

1. `switch# show hardware profile buffer monitor [interface ethernet slot/port] {brief | buffer-block | detail | multicast | summary}`
2. (任意) `switch# clear hardware profile buffer monitor`

## 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# show hardware profile buffer monitor [interface ethernet slot/port] {brief   buffer-block   detail   multicast   summary}</code>	<p>バッファについて収集されたデータを表示します。キーワードは次のように定義されます。</p> <ul style="list-style-type: none"> <li>• <b>brief</b> : 各インターフェイスの情報の一部を示すように指定します。</li> <li>• <b>buffer-block</b> 特定のバッファ ブロックに関する情報を表示するように指定します。</li> <li>• <b>detail</b> : 各インターフェイスで収集されたすべての情報を表示するように指定します。</li> <li>• <b>interface</b> : (任意) 特定のポートプロファイルに関する情報を表示するように指定します。</li> <li>• <b>multicast</b> マルチキャスト トラフィックだけのバッファデータを表示するように指定します。</li> <li>• <b>summary</b> : 各バッファ ブロックに関するサマリー情報を表示するように指定します。</li> </ul> <p>(注) show コマンドのオプション <b>interface</b> はユニキャストモードでのみ有効で、<b>multicast</b> オプションはマルチキャストモードでのみ有効です。</p>
ステップ 2	(任意) <code>switch# clear hardware profile buffer monitor</code>	収集されたバッファ データをクリアします。

### 例

次に、各バッファ ブロックと組み合わせたバッファすべてのサマリー情報を表示する例を示します。

```
switch# show hardware profile buffer monitor summary
Summary CLI issued at: 09/18/2012 07:38:39

                Maximum buffer utilization detected
                1sec      5sec      60sec      5min      1hr
-----
Buffer Block 1      0KB      0KB      0KB      0KB      N/A

Total Shared Buffer Available = 5049 Kbytes
Class Threshold Limit = 4845 Kbytes
=====
Buffer Block 2      0KB      0KB      0KB      0KB      N/A

Total Shared Buffer Available = 5799 Kbytes
Class Threshold Limit = 5598 Kbytes
=====
Buffer Block 3      0KB      0KB      5376KB      5376KB      N/A

Total Shared Buffer Available = 5799 Kbytes
Class Threshold Limit = 5598 Kbytes
```

次に、ユニキャストモードの各バッファブロックと各インターフェイスの最大バッファ使用率を表示する例を示します。

```
switch# show hardware profile buffer monitor brief
Brief CLI issued at: 09/18/2012 07:38:29

                Maximum buffer utilization detected
                1sec      5sec      60sec      5min      1hr
-----
Buffer Block 1      0KB      0KB      0KB      0KB      N/A

Total Shared Buffer Available = 5049 Kbytes
Class Threshold Limit = 4845 Kbytes
-----
Ethernet1/45      0KB      0KB      0KB      0KB      N/A
Ethernet1/46      0KB      0KB      0KB      0KB      N/A
Ethernet1/47      0KB      0KB      0KB      0KB      N/A
Ethernet1/48      0KB      0KB      0KB      0KB      N/A
Ethernet1/21      0KB      0KB      0KB      0KB      N/A
Ethernet1/22      0KB      0KB      0KB      0KB      N/A
Ethernet1/23      0KB      0KB      0KB      0KB      N/A
Ethernet1/24      0KB      0KB      0KB      0KB      N/A
Ethernet1/9       0KB      0KB      0KB      0KB      N/A
Ethernet1/10      0KB      0KB      0KB      0KB      N/A
Ethernet1/11      0KB      0KB      0KB      0KB      N/A
Ethernet1/12      0KB      0KB      0KB      0KB      N/A
Ethernet1/33      0KB      0KB      0KB      0KB      N/A
Ethernet1/34      0KB      0KB      0KB      0KB      N/A
Ethernet1/35      0KB      0KB      0KB      0KB      N/A
Ethernet1/36      0KB      0KB      0KB      0KB      N/A
=====
Buffer Block 2      0KB      0KB      0KB      0KB      N/A

Total Shared Buffer Available = 5799 Kbytes
Class Threshold Limit = 5598 Kbytes
-----
Ethernet1/17      0KB      0KB      0KB      0KB      N/A
Ethernet1/18      0KB      0KB      0KB      0KB      N/A
Ethernet1/19      0KB      0KB      0KB      0KB      N/A
Ethernet1/20      0KB      0KB      0KB      0KB      N/A
```

## バッファ ヒストグラム データの表示

```

Ethernet1/5          0KB    0KB    0KB    0KB    N/A
Ethernet1/6          0KB    0KB    0KB    0KB    N/A
Ethernet1/7          0KB    0KB    0KB    0KB    N/A
Ethernet1/8          0KB    0KB    0KB    0KB    N/A
Ethernet1/41         0KB    0KB    0KB    0KB    N/A
Ethernet1/42         0KB    0KB    0KB    0KB    N/A
Ethernet1/43         0KB    0KB    0KB    0KB    N/A
Ethernet1/44         0KB    0KB    0KB    0KB    N/A
Ethernet1/29         0KB    0KB    0KB    0KB    N/A
Ethernet1/30         0KB    0KB    0KB    0KB    N/A
Ethernet1/31         0KB    0KB    0KB    0KB    N/A
Ethernet1/32         0KB    0KB    0KB    0KB    N/A
=====
Buffer Block 3      0KB    0KB   5376KB  5376KB  N/A

Total Shared Buffer Available = 5799 Kbytes
Class Threshold Limit = 5598 Kbytes
-----
Ethernet1/13        0KB    0KB    0KB    0KB    N/A
Ethernet1/14        0KB    0KB    0KB    0KB    N/A
Ethernet1/15        0KB    0KB    0KB    0KB    N/A
Ethernet1/16        0KB    0KB    0KB    0KB    N/A
Ethernet1/37        0KB    0KB    0KB    0KB    N/A
Ethernet1/38        0KB    0KB    0KB    0KB    N/A
Ethernet1/39        0KB    0KB    0KB    0KB    N/A
Ethernet1/40        0KB    0KB    0KB    0KB    N/A
Ethernet1/25        0KB    0KB    0KB    0KB    N/A
Ethernet1/26        0KB    0KB    0KB    0KB    N/A
Ethernet1/27        0KB    0KB    0KB    0KB    N/A
Ethernet1/28        0KB    0KB    0KB    0KB    N/A
Ethernet1/1         0KB    0KB    0KB    0KB    N/A
Ethernet1/2         0KB    0KB    0KB    0KB    N/A
Ethernet1/3         0KB    0KB    0KB    0KB    N/A
Ethernet1/4         0KB    0KB   5376KB  5376KB  N/A

```

次に、マルチキャストモードの各バッファブロックの最大バッファ使用率の情報を表示する例を示します。

```

switch# show hardware profile buffer monitor brief
Brief CLI issued at: 09/18/2012 08:30:08

                Maximum buffer utilization detected
                1sec    5sec    60sec    5min    1hr
                -----
Buffer Block 1    0KB    0KB    0KB    0KB    0KB

Total Shared Buffer Available = 5049 Kbytes
Class Threshold Limit = 4845 Kbytes
Mcast Usage 1    0KB    0KB    0KB    0KB    0KB
=====
Buffer Block 2    0KB    0KB    0KB    0KB    0KB

Total Shared Buffer Available = 5799 Kbytes
Class Threshold Limit = 5598 Kbytes
Mcast Usage 2    0KB    0KB    0KB    0KB    0KB
=====
Buffer Block 3    0KB    0KB    0KB    0KB    0KB

Total Shared Buffer Available = 5799 Kbytes
Class Threshold Limit = 5598 Kbytes
Mcast Usage 3    0KB    0KB    0KB    0KB    0KB

```

次に、マルチキャストモードのバッファブロック 3 の詳細なバッファ使用率の情報を表示する例を示します。

```
switch# show hardware profile buffer monitor multicast 3 detail
Detail CLI issued at: 09/18/2012 08:30:12

Legend -
384KB - between 1 and 384KB of shared buffer consumed by port
768KB - between 385 and 768KB of shared buffer consumed by port
307us - estimated max time to drain the buffer at 10Gbps

Active Buffer Monitoring for Mcast Usage 3 is: Active
KBytes          384  768 1152 1536 1920 2304 2688 3072 3456 3840 4224 4608 4992
5376 5760 6144
us @ 10Gbps      307  614  921 1228 1535 1842 2149 2456 2763 3070 3377 3684 3991
4298 4605 4912
-----
-----
09/18/2012 08:30:12    0  0  0  0  0  0  0  0  0  0  0  0  0  0
 0  0  0
09/18/2012 08:30:11    0  0  0  0  0  0  0  0  0  0  0  0  0  0
 0  0  0
09/18/2012 08:30:10    0  0  0  0  0  0  0  0  0  0  0  0  0  0
 0  0  0
09/18/2012 08:30:09    0  0  0  0  0  0  0  0  0  0  0  0  0  0
 0  0  0
09/18/2012 08:30:08    0  0  0  0  0  0  0  0  0  0  0  0  0  0
 0  0  0
09/18/2012 08:30:07    0  0  0  0  0  0  0  0  0  0  0  0  0  0
 0  0  0
09/18/2012 08:30:06    0  0  0  0  0  0  0  0  0  0  0  0  0  0
 0  0  0
09/18/2012 08:30:05    0  0  0  0  0  0  0  0  0  0  0  0  0  0
 0  0  0
09/18/2012 08:30:04    0  0  0  0  0  0  0  0  0  0  0  0  0  0
 0  0  0
09/18/2012 08:30:03    0  0  0  0  0  0  0  0  0  0  0  0  0  0
 0  0  0
```

次に、イーサネットインターフェイス 1/4 に関する詳細なバッファ データを表示する例を示します。

```
switch# show hardware profile buffer monitor interface ethernet 1/4 detail
Detail CLI issued at: 09/18/2012 07:38:43

Legend -
384KB - between 1 and 384KB of shared buffer consumed by port
768KB - between 385 and 768KB of shared buffer consumed by port
307us - estimated max time to drain the buffer at 10Gbps

Active Buffer Monitoring for port Ethernet1/4 is: Active
KBytes          384  768 1152 1536 1920 2304 2688 3072 3456 3840 4224 4608 4992
5376 5760 6144
us @ 10Gbps      307  614  921 1228 1535 1842 2149 2456 2763 3070 3377 3684 3991
4298 4605 4912
-----
-----
09/18/2012 07:38:42    0  0  0  0  0  0  0  0  0  0  0  0  0  0
 0  0  0
09/18/2012 07:38:41    0  0  0  0  0  0  0  0  0  0  0  0  0  0
 0  0  0
09/18/2012 07:38:40    0  0  0  0  0  0  0  0  0  0  0  0  0  0
 0  0  0
```

バッファ ヒストグラム データの表示

09/18/2012 07:38:39	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0 0 0														
09/18/2012 07:38:38	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0 0 0														
09/18/2012 07:38:37	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0 0 0														
09/18/2012 07:38:36	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0 0 0														
09/18/2012 07:38:35	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0 0 0														
09/18/2012 07:38:34	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0 0 0														
09/18/2012 07:38:33	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0 0 0														
09/18/2012 07:38:32	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0 0 0														
09/18/2012 07:38:31	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0 0 0														
09/18/2012 07:38:30	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0 0 0														
09/18/2012 07:38:29	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0 0 0														
09/18/2012 07:38:28	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0 0 0														
09/18/2012 07:38:27	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0 0 0														
09/18/2012 07:38:26	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0 0 0														
09/18/2012 07:38:25	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0 0 0														
09/18/2012 07:38:24	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0 0 0														
09/18/2012 07:38:23	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0 0 0														
09/18/2012 07:38:22	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0 0 0														
09/18/2012 07:38:21	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0 0 0														
09/18/2012 07:38:20	177	36	0	0	0	0	0	0	0	0	0	0	0	0
0 0 0														
09/18/2012 07:38:19	0	143	107	0	0	0	0	0	0	0	0	0	0	0
0 0 0														
09/18/2012 07:38:18	0	0	72	178	3	0	0	0	0	0	0	0	0	0
0 0 0														
09/18/2012 07:38:17	0	0	0	0	176	74	0	0	0	0	0	0	0	0
0 0 0														
09/18/2012 07:38:16	0	0	0	0	0	105	145	0	0	0	0	0	0	0
0 0 0														
09/18/2012 07:38:15	0	0	0	0	0	0	33	179	38	0	0	0	0	0
0 0 0														
09/18/2012 07:38:14	0	0	0	0	0	0	0	0	140	113	0	0	0	0
0 0 0														
09/18/2012 07:38:13	0	0	0	0	0	0	0	0	0	66	178	6	0	0
0 0 0														
09/18/2012 07:38:12	0	0	0	0	0	0	0	0	0	0	0	173	77	0
0 0 0														
09/18/2012 07:38:11	1	0	0	1	0	0	1	0	0	1	0	0	102	0
42 0 0														
09/18/2012 07:38:10	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0 0 0														



## 第 20 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 \(267 ページ\)](#)
- [パッケージ管理 \(268 ページ\)](#)
- [SMU の前提条件 \(269 ページ\)](#)
- [SMU の注意事項と制約事項 \(269 ページ\)](#)
- [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 \(270 ページ\)](#)
- [パッケージインストールの準備 \(270 ページ\)](#)
- [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 \(272 ページ\)](#)
- [パッケージの追加とアクティブ化 \(273 ページ\)](#)
- [アクティブなパッケージセットのコミット \(274 ページ\)](#)
- [パッケージの非アクティブ化と削除 \(275 ページ\)](#)
- [インストールログ情報の表示 \(276 ページ\)](#)

## SMU について

ソフトウェアメンテナンスアップグレード (SMU) は、特定の障害の修正を含むパッケージファイルです。SMU は、直近の問題に対処するために作成され、新しい機能は含まれていません。通常、SMU がデバイスの動作に大きな影響を及ぼすことはありません。SMU のバージョンは、アップグレードするパッケージのメジャー、マイナー、およびメンテナンスバージョンに同期されます。

SMU の影響は次のタイプによって異なります。

- プロセスの再起動 SMU : アクティベーション時にプロセスまたはプロセスのグループの再起動を引き起こします。
- リロード SMU : スーパーバイザおよびラインカードの平行リロードを引き起こしません。

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 Series NX-OS Software Upgrade and Downgrade Guide』を参照してください。



(注) SMU をアクティブにすると、以前の SMU、または SMU が適用されるパッケージが自動的に非アクティブ化されることはありません。

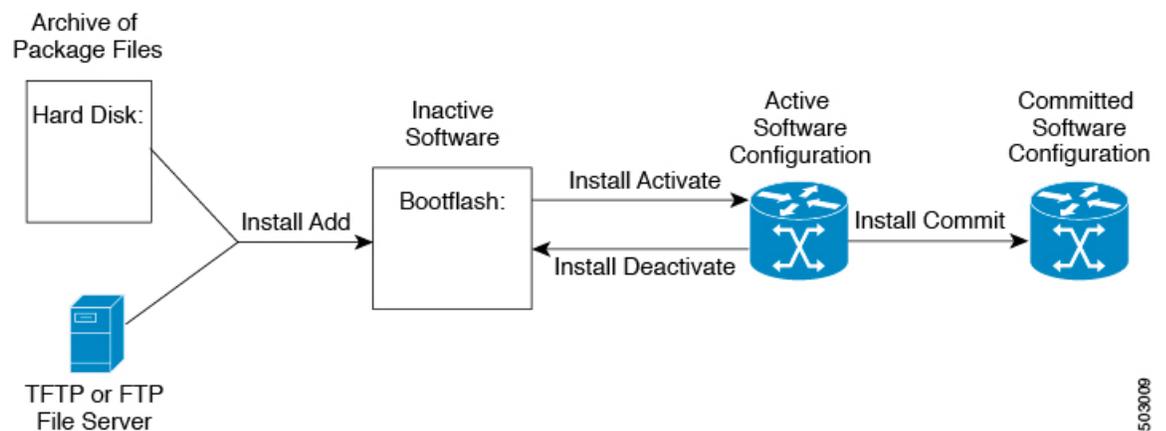
## パッケージ管理

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 3: SMU パッケージを追加、アクティブ化およびコミットするプロセス



503009

## 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。—

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、**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) というメッセージが表示されます。
- 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ます。特定のラインカードのみをサポートするパッケージもあります。

そのリリースに関連する重要な情報についてリリースノートを確認し、そのパッケージとデバイス設定の互換性の有無を判断する。

システムの動作が安定していて、ソフトウェアの変更に対応できることを確認する。

#### 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 : <pre>switch# show install active</pre>	デバイス上のアクティブなソフトウェアを表示します。デバイスに追加する必要があるソフトウェアを決定するため、またインストール操作完了後にアクティブなソフトウェアのレポートと比較するために、このコマンドを使用します。
ステップ 2	<b>show module</b> 例 : <pre>switch# show module</pre>	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 : <pre>switch# show clock</pre>	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するローカルディスクです。デフォルトのブート デバイスは `bootflash:` です。



**ヒント** ローカルストレージ デバイスにパッケージ ファイルをコピーする前に、`dir` コマンドを使用して、必要なパッケージ ファイルがデバイスに存在するかどうかを確認します。

SMU パッケージ ファイルがリモート TFTP、FTP、または SFTP サーバにある場合、ローカルストレージ デバイスにファイルをコピーできます。ファイルがローカルストレージ デバイスに置かれた後、パッケージをそのストレージデバイスからデバイスに追加しアクティブにできます。次のサーバ プロトコルがサポートされます。

- **TFTP** : ネットワークを介して、あるコンピュータから別のコンピュータへファイルを転送できるようにします。通常は、クライアント認証 (たとえば、ユーザ名およびパスワード) を使用しません。これは FTP の簡易版です。



**(注)** パッケージ ファイルによっては、大きさが 32 MB を超える場合もありますが、一部のベンダーにより提供される TFTP サービスではこの大きさのファイルがサポートされていない場合があります。32 MB を超えるファイルをサポートする TFTP サーバにアクセスできない場合は、FTP を使用してファイルをダウンロードします。

- **ファイル転送プロトコル** : FTP は TCP/IP プロトコル スタックの一部であり、ユーザ名とパスワードが必要です。
- **SSH ファイル転送プロトコル** : SFTP は、セキュリティ パッケージの SSHv2 機能の一部で、セキュアなファイル転送を提供します。

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その他のソフトウェアと互換性があることを確認します。競合がある場合は、エラーメッセージが表示されます。アクティブ化が実行されるのは、すべての互換性が確認できた場合だけです。

## 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 : <pre>switch# install add bootflash: n3500-uk9.6.0.2.U6.0.1.CSCab00001.bin</pre>	ローカルストレージデバイスまたはネットワークサーバからパッケージソフトウェア ファイルを解凍してブートフラッシュおよびデバイスにインストールされているすべてのアクティブスーパーバイザおよびスタンバイスーパーバイザに追加します。  <i>filename</i> 引数は、次の形式をとることができます。 <ul style="list-style-type: none"> <li>• <b>bootflash:</b><i>filename</i></li> <li>• <b>tftp://hostname-or-ipaddress/directory-path/</b><i>filename</i></li> <li>• <b>ftp://username:password@hostname-or-ipaddress/directory-path/</b><i>filename</i></li> <li>• <b>sftp://hostname-or-ipaddress/directory-path/</b><i>filename</i></li> </ul>
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。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。

	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す。(install add activate コマンドを使用して、パッケージが前にアクティブにされた場合は、この手順を省略します。)</p> <p>(注) パッケージ名を部分的に入力してから ? を押すと、アクティブ化に使用できるすべての候補が表示されます。候補が 1 つしかない場合に <b>Tab</b> キーを押すと、パッケージ名の残りの部分が自動入力されません。</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。候補が 1 つしかない場合に <b>Tab</b> キーを押すと、パッケージ名の残りの部分が自動入力されます。

	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 : switch# show install inactive	デバイス上の非アクティブなパッケージを表示します。
ステップ 3	(任意) <b>install commit</b>  例 : switch# install commit	現在のパッケージのセットをコミットして、デバイスが再起動したときにこれらのパッケージが使用されるようにします。  (注) パッケージを削除できるのは、非アクティブ化操作がコミットされた場合だけです。
ステップ 4	(任意) <b>install remove {filename   inactive}</b>  例 : 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  例 : switch# install remove inactive Proceed with removing? (y/n)? [n] y	非アクティブなパッケージを削除します。  <ul style="list-style-type: none"> <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> コマンドに <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。
- 引数を指定しない **show install log** コマンドを使用して、すべてのインストール動作のサマリーを表示します。ある動作に固有の情報を表示するには、*request-id* 引数を指定します。ファイルの変更、リロードできなかつたノード、その他プロセスに影響する操作など、特定の操作の詳細を表示するには、**detail** キーワードを使用します。

次に、すべてのインストール要求の情報を表示する例を示します。

```
switch# show install log
Thu Jan 9 01:26:09 2014
Install operation 1 by user 'admin' at Thu Jan 9 01:19:19 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
```





## 第 21 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 \(279 ページ\)](#)
- [概要 \(280 ページ\)](#)
- [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 \(282 ページ\)](#)
- [コンフィギュレーションの置換の推奨ワークフロー \(286 ページ\)](#)
- [コンフィギュレーションの置換の実行 \(287 ページ\)](#)
- [コンフィギュレーションの置換の確認 \(290 ページ\)](#)
- [コンフィギュレーションの置換の例 \(291 ページ\)](#)

## コンフィギュレーションの置換とコミットタイムアウトについて

コンフィギュレーションの置換機能を使用すると、デバイスをリロードすることなく Cisco Nexus スイッチの実行コンフィギュレーションをユーザ指定のコンフィギュレーションに置換できます。コンフィギュレーション自体でリロードが必要な場合にのみ、デバイスのリロードが必要になることがあります。ユーザが提供する実行コンフィギュレーションファイルは、実行ファイルのコピーを使用して取得する必要があります。**copy file: to running** と異なり、コンフィギュレーションの置換機能はマージ操作ではありません。この機能では、実行コンフィギュレーション全体が、ユーザによって提供される新しいコンフィギュレーションに置換されます。コンフィギュレーションの置換に障害がある場合は、元のコンフィギュレーションがスイッチで復元されます。Cisco NX-OS リリース 9.3(1) から、**best-effort** オプションが導入されました。このオプションを使用すると、コマンドでエラーが発生した場合でも、設定の置換によって完全なパッチが実行され、元の設定はスイッチに復元されません。

コミットタイムアウト機能を使用すると、コンフィギュレーションの置換操作の実行に成功した後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** コマンドを使用すると、エラーが発生したコンフィギュレーションそのものを表示できます。
- スイッチを元のコンフィギュレーションに復元するとき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。復元操作中にエラーが発生したコマンドを一覧表示するには、**show config-replace log exec** コマンドを使用します。
- タイマーの期限が切れる前に **configure replace commit** コマンドを入力した場合、コミットタイマーは停止し、コンフィギュレーションの置換機能によって適用されているユーザ指定のコンフィギュレーションでスイッチが稼働します。
- コミットタイマーの期限が切れると、以前のコンフィギュレーションへのロールバックは自動的に開始されます。
- Cisco NX-OS リリース 9.3(1) では、セマンティック検証のサポートが設定の置換に追加されました。このセマンティック検証は、設定置換の事前チェックの一部として実行されます。パッチは、セマンティック検証が成功した場合にのみ適用されます。パッチファイル

を適用すると、コンフィギュレーションの置換によって検証プロセスがトリガーされます。コンフィギュレーションの置換は、検証プロセスで、実行コンフィギュレーションとユーザー構成ファイルを比較します。不一致がある場合、デバイスは元のコンフィギュレーションに復元されます。

コンフィギュレーションの置換と実行コンフィギュレーションへのファイルのコピーとの違いは、次のとおりです。

コンフィギュレーションの置換	ファイルのコピー
<b>configure replace</b> <target-url> コマンドでは、現在の実行コンフィギュレーションにのみ含まれ、置換ファイルには存在しないコマンドは削除されます。また、現在の実行コンフィギュレーションに追加する必要があるコマンドも追加されます。	<b>copy</b> <source-url> <b>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コンフィギュレーションの両方のコマンドがすべて保持されます。このコマンドでは、現在の実行コンフィギュレーションにのみ含まれ、ソースファイルには存在しないコマンドが削除されることはありません。
<b>configure replace</b> <target-url> コマンドの交換ファイルには、完全な Cisco NX-OS コンフィギュレーションファイルを使用する必要があります。	<b>copy</b> <source-url> <b>running-config</b> コマンドのコピー元ファイルとして、部分コンフィギュレーションファイルを使用できます。

## コンフィギュレーションの置換の利点

コンフィギュレーションの置換の利点は次のとおりです。

- スイッチをリロードしたり、CLIで実行コンフィギュレーションファイルに加えた変更を手動で元に戻したりすることなく、現在の実行コンフィギュレーションファイルをユーザ指定のコンフィギュレーションファイルと置換できます。その結果、システムのダウンタイムが減少します。
- 保存済みの Cisco NX-OS コンフィギュレーションの状態に戻すことができます。
- 追加や削除が必要なコマンドだけが影響を受ける場合、デバイスに完全なコンフィギュレーションファイルを適用することができるため、コンフィギュレーションの変更が簡素化されます。その他のサービスおよび変更されていないコンフィギュレーションには影響しません。
- コミットタイムアウト機能を設定すると、コンフィギュレーションの置換操作が成功したときでも以前のコンフィギュレーションにロールバックすることができます。

# コンフィギュレーションの置換に関する注意事項と制限事項

コンフィギュレーションの置換機能には、コンフィギュレーションに関する次のガイドラインと制限事項があります。

- 設定置換機能は、Cisco Nexus 3000 シリーズおよび Cisco Nexus 9000 シリーズ スイッチでサポートされています。
- コンフィギュレーションの置換、チェックポイント、ロールバック操作、または実行コンフィギュレーションからスタートアップコンフィギュレーションへのコピーを同時に実行できるのは、1 ユーザだけです。複数の Telnet、SSH または NX-API セッション経由の操作などのパラレル操作はサポートされていません。複数のコンフィギュレーションの置換またはロールバック要求はシリアル化され、たとえば、最初の要求の完了後にのみ、2 番目の要求の処理が開始されます。
- コミットタイマーの実行中に別のコンフィギュレーションの置換操作を開始することはできません。 **configure replace commit** コマンドを使用してタイマーを停止するか、またはコミットタイマーの期限が切れるまで待機してから別のコンフィギュレーションの置換操作を開始する必要があります。
- **system default switchport shutdown** または **no system default switchport shutdown** を **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。
- Cisco NX-OS Release 9.3 (6) 以降では、**service exclude-bootconfig** の設定によって **boot nxos** イメージ設定を、**show running-config**、**show startup-config**、**copy running-config filename**、および **copy startup-config filename** コマンドで除外できます。
- コミットタイムアウト機能は、コミットタイムアウトを使用してコンフィギュレーションの置換操作を実行する場合にのみ開始されます。タイマーの値の範囲は 30 ~ 3600 秒です。
- ユーザ指定のコンフィギュレーションファイルは、Cisco NX-OS デバイスから取得 (**copy run file**) された有効な **show running-configuration** の出力である必要があります。このコンフィギュレーションは部分コンフィギュレーションにすることはできず、**user admin** などの必須コマンドが含まれている必要があります。
- ソフトウェアバージョン違いで生成されたコンフィギュレーションファイルでコンフィギュレーションの置換操作を実行することは、操作が失敗する可能性があるため推奨されません。ソフトウェアバージョンの変更があるたびに新しいコンフィギュレーションファイルを再生成する必要があります。

- Multichassis EtherChannel トランク (MCT) 設定を仮想ピアリンク設定と置き換えようとした場合、コンフィギュレーションの置換操作はサポートされません。物理 MCT はイーサネットを介した CFS 配信モードを使用し、仮想ピアリンクは IP を介した CFS 配信モードを使用するため、この操作は許可されません。
- コンフィギュレーションの置換操作が進行中の場合、他のセッションからはコンフィギュレーションを変更しないことを推奨します。操作が失敗する可能性があります。
- コンフィギュレーションの置換機能については、次の点に注意してください。
  - 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。
  - Cisco NX-OS リリース 9.3(5) 以降では、FEX インターフェイス コンフィギュレーションの設定置換 (CR) がサポートされています。FEX のプロビジョニングは CR ではサポートされていません。プロビジョニングされた FEX インターフェイスの設定は、CR を使用して変更できます。



(注) このガイドラインは、FEX がサポートされていない Cisco Nexus 3000 シリーズ プラットフォーム スイッチには適用されません。

- FEX ライン カードがオフラインの場合、コンフィギュレーションの置換機能は動作しません。
- Cisco NX-OS リリース 9.3 (5) 以降では、設定置換機能がポートプロファイルでサポートされています。
- Cisco Nexus 92160YC-X および Cisco Nexus 93180LC-EX スイッチのハードウェア プロファイル ポートモード機能では、構成の置換機能はサポートされません。
- コンフィギュレーションの置換機能は、`configure terminal` モード コマンドでのみサポートされます。`configure profile`、`configure jobs`、およびその他のモードはサポートされていません。
- Cisco NX-OS リリース 9.3(5) 以降では、ジョブの設定モードがサポートされています。スケジューラ ジョブ コマンドを含むコンフィギュレーション ファイルは、コンフィギュレーションの置換に使用できます。
- Cisco NX-OS リリース 9.3(4) 以降では、ブレイクアウト インターフェイス コンフィギュレーションの設定置換機能がサポートされています。
- 実行コンフィギュレーションに `feature-set mpls` または `mpls static range` コマンドが含まれていて、MPLS なしでコンフィギュレーションに移動しようとしたり、ラベルの範囲を変更する場合、コンフィギュレーションの置換機能が失敗することがあります。
- コンフィギュレーションの置換機能は、自動設定をサポートしていません。

- コンフィギュレーションの置換機能が適用されるラインカードがオフラインである場合、コンフィギュレーションの置換操作は失敗します。
- 設定置換機能を使用してITDを変更する前に、ITD サービスをシャットダウンする必要があります (**shutdown**) 。
- ユーザ コンフィギュレーションからのメンテナンス モードへの移行はサポートされていません。
- メンテナンス モードから **configure replace** コマンドを使用すると、次の警告でユーザの確認が求められます。

```
Warning: System is in maintenance mode. Please ensure user config won't inadvertently
revert back config in maintenance mode profile.
Do you wish to proceed anyway? (y/n) [n]
```

- `<non-interactive>` オプションを使用してメンテナンス モードから **configure replace** コマンドを使用することはサポートされています。デフォルトでは、`yes` のユーザ確認を受けてから進行します。
- 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。
- 「verify-only」モードでは、TCAM 依存の設定はエラーをスローせず、成功する場合があります。ただし、実際の CR 操作では失敗する可能性があります。これを回避するには、CR を実行する前に TCAM カービング設定を適用してリロードすることをお勧めします。
- 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。

- 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ーション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>使用例 1:</b> 複数のコマンドバリエーション: 最後のコマンドバリエーション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> トラック ID を構成するコマンド: ネクストホップが同じでトラック ID が異なる最後のコマンドバリエーション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ック 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>

## コンフィギュレーションの置換の推奨ワークフロー

コンフィギュレーションの置換の推奨されるワークフローを次に示します。



- (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。
1. Cisco Nexus シリーズ デバイスで最初にコンフィギュレーションを適用してコンフィギュレーション ファイルを生成してから、コンフィギュレーション ファイルとして **show running-configuration** 出力を使用します。このファイルを使用して、必要に応じてコンフィギュレーションを変更します。次に、この生成または更新されたコンフィギュレーション ファイルを使用して、コンフィギュレーションの置換を実行します。
  2. **configure replace <file> show-patch** コマンドを実行してパッチ ファイルを表示し、確認します。この手順は任意です。

3. 構成の置換ファイルを実行するか、**commit-timeout** *<time>* 機能をスキップします。要件に基づいて、次の手順のいずれかを実行できます。
  - コンフィギュレーションの置換で実行されるコマンドをコンソールに表示するには、**configure replace** *<file>* **verbose** を実行します。
  - **configure replace [bootflash/scp/sftp] <user-configuration-file> verbose commit-timeout <time>** コマンドを実行して、コミット時間を構成します。
4. **configure replace commit** コマンドを実行し、コミット タイマーを停止します。この手順は、コミットタイムアウト機能でコンフィギュレーションの置換操作を実行している場合に必要です。
5. コンフィギュレーションのセマンティック検証を含むプレチェックをコンフィギュレーションの置換で実行します。エラーがある場合、コンフィギュレーションの置換操作は失敗します。失敗したコンフィギュレーションの詳細を表示するには、**show config-replace log verify** コマンドを使用します。パッチファイルを適用すると、コンフィギュレーションの置換によって検証プロセスがトリガーされます。コンフィギュレーションの置換は、検証プロセスで、実行コンフィギュレーションとユーザー構成ファイルを比較します。不一致がある場合、デバイスは元のコンフィギュレーションに復元されます。不一致のコンフィギュレーションを表示するには、**show config-replace log verify** コマンドを使用します。
6. Cisco NX-OS リリース9.3(1) では、次のコンフィギュレーションの置換操作を実行できます。
  - セマンティック検証およびベストエフォートモードなしのコンフィギュレーションの置換。
  - セマンティック検証なし、ベストエフォートモードありのコンフィギュレーションの置換。
  - セマンティック検証あり、ベストエフォートモードなしのコンフィギュレーションの置換。
  - セマンティック検証およびベストエフォートモードありのコンフィギュレーションの置換。

## コンフィギュレーションの置換の実行

コンフィギュレーションの置換を実行するには、次の操作を行います。

### 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**
10. (任意) **configure replace** <user-configuration-file > [ **on-failure reload** [ **save-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 replace</b> { <uri_local >   <uri_remote > } [ <b>verbose</b>   <b>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</b> [ <b>bootflash / scp / sftp</b> ] <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。  (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 <b>snmp-server traps</b> コマンドの構成置換が成功した後も、パッチを表示できます。</li> </ul>
ステップ 3	<b>configure replace</b> [ <b>bootflash / scp / sftp</b> ] <user-configuration-file > <b>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

	コマンドまたはアクション	目的
		<p>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。</p>
<p>ステップ 4</p>	<p><b>configure replace</b> &lt;user-configuration-file&gt; [best-effort]</p>	<p>スイッチの設定を新しいユーザ設定に置き換え、セマンティック検証による設定の置き換えを有効にします。</p> <p>best-effort オプションを使用すると、コマンドでエラーが発生した場合でも設定の置換によって完全なパッチが実行され、以前の設定がロールバックされないようになります。</p> <p>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 9300-FX2/FX3/GX シリーズスイッチのパッチ ACL コンフィギュレーションをサポートします。ベストエフォートモードが有効になっている場合、パ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。</p>
<p>ステップ 5</p>	<p><b>configure replace</b> &lt;user-configuration-file&gt; [verify-and-commit]</p>	<p>スイッチの設定を新しいユーザ設定に置き換え、セマンティック検証による設定の置き換えを有効にします。</p> <p>verify-and-commit オプションは、セマンティック検証を有効にするために使用されます。パッチは、完全なパッチのセマンティック検証に合格した場合のみ実行されます。</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>
<p>ステップ 6</p>	<p><b>configure replace</b> &lt;user-configuration-file&gt; [verify-only]</p>	<p>パッチのみを表示し、パッチでセマンティック検証を実行し、結果を表示します。パッチはシステムに適用されません。</p>
<p>ステップ 7</p>	<p>(任意) <b>configure replace</b> [ bootflash / scp / sftp ] &lt; user-configuration-file &gt; verbose commit-timeout &lt;time&gt;</p>	<p>コミット時間を秒単位で設定します。タイマーは、コンフィギュレーションの置換操作が正常に完了した後開始されます。</p>
<p>ステップ 8</p>	<p>(任意) <b>configure replace</b> [ commit ]</p>	<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)</p>

	コマンドまたはアクション	目的
		以前のコンフィギュレーションにロールバックするには、コミットタイマーの期限が切れるまで待機する必要があります。タイマーの期限が切れると、スイッチは自動的に以前のコンフィギュレーションにロールバックされます。
ステップ 9	(任意) <b>configure replace</b> [ <b>bootflash/scp/sftp</b> ] < <i>user-configuration-file</i> > <i>non-interactive</i>	メンテナンスモードでは、ユーザプロンプトはありません。デフォルトでは、 <b>yes</b> のユーザ確認を受けてからロールバックが進行します。非インタラクティブオプションは、メンテナンスモードでのみ使用できます。
ステップ 10	(任意) <b>configure replace</b> < <i>user-configuration-file</i> > [ <b>on-failure reload</b> [ <b>save-startup-config</b> ] ]	このオプションは、設定の置換操作が失敗し、以前の実行コンフィギュレーションへの復元も失敗した場合に、以前に保存したスタートアップコンフィギュレーションにスイッチをリロードします。  このオプションは、次の場合には影響しません。 <ul style="list-style-type: none"> <li>• 設定の置換が正常に行われました</li> <li>• 設定の置換が失敗するが、以前の実行コンフィギュレーションへの復元は成功する</li> </ul> (注) [ <b>save-startup-config</b> ] : このオプションは、設定の置換操作を開始する前に、実行コンフィギュレーションをスタートアップに保存します。

## 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 31: 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> [ <b>bootflash/scp/sftp</b> ] < <i>user-configuration-file</i> > <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。

コマンド	目的
<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。

## コンフィギュレーションの置換の例

以下のコンフィギュレーションの置換の設定例を参照してください。

- **configure replace bootflash:** *<file>* **show-patch** CLI コマンドを使用して、実行コンフィギュレーションとユーザ指定のコンフィギュレーションの違いを表示します。

```
switch(config)# configure replace bootflash:<file> show-patch
Collecting Running-Config
Converting to checkpoint file
#Generating Rollback Patch
!!
no role name abc
```

- **configure replace bootflash:** *<file>* **verbose** CLI コマンドを使用して、スイッチの実行コンフィギュレーション全体をユーザコンフィギュレーションに置換します。

```
switch(config)# configure replace bootflash:<file> verbose
Collecting Running-Config
Generating Rollback patch for switch profile
Rollback Patch is Empty
Note: Applying config parallely may fail Rollback verification
Collecting Running-Config
#Generating Rollback Patch
Executing Rollback Patch
=====
config t
no role name abc
=====
Generating Running-config for verification
Generating Patch for verification

Rollback completed successfully.
```

```

Sample Example with adding of BGP configurations.
switch(config)# sh run | section bgp
switch(config)# sh file bootflash:file | section bgp
feature bgp
router bgp 1
  address-family ipv4 unicast
  neighbor 1.1.1.1
switch(config)#
switch(config)# configure replace bootflash:file verbose
Collecting Running-Config
Generating Rollback patch for switch profile
Rollback Patch is Empty
Note: Applying config 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、パッチを意味的に生成および確認します。

```
switch(config)# configure replace bootflash:user-config.cfg verify-only
```

```
Version match between user file and running configuration.
Pre-check for User config PASSED
Collecting Running-Config
Converting to checkpoint file
Generating Rollback Patch
Validating Patch
=====
`config t `
`interface Ethernet1/1`
`shutdown`
`no switchport trunk allowed vlan`
`no switchport mode`
`no switchport`
`exit`
Skip non dme command for CR validation
`interface Vlan1`
`shutdown`
`interface Ethernet1/1`
`shutdown`
`no switchport`
`ip address 1.1.1.1/24`
`exit`
Skip non dme command for CR validation
=====
Patch validation completed successful
switch(config)#
```

- パッチでセマティック検証を実行した後、**configure replace bootflash:user-config.cfg best-effort verify-and-commit** CLI コマンドを使用して、スイッチの実行コンフィギュレーションを特定のユーザ コンフィギュレーションに置き換えます。

```
switch(config)# configure replace bootflash:user-config.cfg best-effort verify-and-commit
```

```
Version match between user file and running configuration.
Pre-check for User config PASSED
ADVISORY: Config Replace operation started...
Modifying running configuration from another VSH terminal in parallel
is not recommended, as this may lead to Config Replace failure.

Collecting Running-Config
Generating Rollback patch for switch profile
Rollback Patch is Empty
Collecting Running-Config
Generating Rollback Patch

Validating Patch
Patch validation completed successful
Executing Rollback Patch
During CR operation,will retain L3 configuration
when vrf member change on interface
Generating Running-config for verification
Generating Rollback Patch
```

Configure replace completed successfully. Please run 'show config-replace log exec' to see if there is any configuration that requires reload to take effect.

switch(config)#

- **show config-replace log exec** CLI コマンドを使用して、実行したコンフィギュレーションと、存在する場合はエラーをすべて確認します。

```
switch(config)# show config-replace log exec
Operation          : Rollback to Checkpoint File
Checkpoint file name : .replace_tmp_28081
Scheme             : tmp
Rollback done By   : admin
Rollback mode      : atomic
Verbose            : enabled
Start Time         : Wed, 06:39:34 25 Jan 2017
```

```
-----
time: Wed, 06:39:47 25 Jan 2017
Status: SUCCESS
End Time           : Wed, 06:39:47 25 Jan 2017
Rollback Status    : Success
```

```
Executing Patch:
-----
switch#config t
switch#no role name abc
```

- **show config-replace log verify** CLI コマンドを使用して、存在する場合は失敗したコンフィギュレーションを確認します。

```
switch(config)# show config-replace log verify
Operation          : Rollback to Checkpoint File
Checkpoint file name : .replace_tmp_28081
Scheme             : tmp
Rollback done By   : admin
Rollback mode      : atomic
Verbose            : enabled
Start Time         : Wed, 06:39:34 25 Jan 2017
End Time           : Wed, 06:39:47 25 Jan 2017
Status             : Success
```

```
Verification patch contains the following commands:
```

```
-----
!!
! No changes
-----
```

```
time: Wed, 06:39:47 25 Jan 2017
Status: SUCCESS
```

- **show config-replace status** CLI コマンドを使用して、コンフィギュレーションの置換のステータスを確認します。

```
switch(config)# show config-replace status
Last operation : Rollback to file
Details:
  Rollback type: atomic replace_tmp_28081
  Start Time: Wed Jan 25 06:39:28 2017
  End Time: Wed Jan 25 06:39:47 2017
  Operation Status: Success
switch(config)#
```

スイッチから生成された設定の代わりに手動で作成された設定を使用すると、[置換の設定 (Configure Replace)] が失敗することがあります。失敗の原因として考えられるのは、`show running configuration` に示されていないデフォルト設定の潜在的な違いです。次の例を参照してください。

`power redundancy` コマンドがデフォルトのコマンドである場合、デフォルトの設定では表示されません。ただし、`show run all` コマンドを使用すると表示されます。次の例を参照してください。

```
switch# show run all

!Command: show running-config all
!Running configuration last done at: Tue Nov 12 11:07:44 2019
!Time: Tue Nov 12 11:16:09 2019

version 9.3(1) Bios:version 05.39
power redundancy-mode ps-redundant
no hardware module boot-order reverse
no license grace-period
<snip>
hostname n9k13
```

電源冗長コマンドは、`show running configuration` コマンド出力には表示されません。次の例を参照してください。

```
!Command: show running-config
!Running configuration last done at: Tue Nov 12 11:07:44 2019
!Time: Tue Nov 12 11:17:24 2019

version 9.3(1) Bios:version 05.39
hostname n9k13
```

設定置換のユーザ コンフィギュレーションに `power redundancy-mode ps-redundant` コマンドが追加された場合。検証/コミットが失敗する可能性があります。次の例を参照してください。

```
switch# show file bootflash:test

!Command: show running-config
!Running configuration last done at: Tue Nov 12 10:56:49 2019
!Time: Tue Nov 12 11:04:57 2019

version 9.3(1) Bios:version 05.39
power redundancy-mode ps-redundant
hostname n9k13
```

`power redundancy-mode ps-redundant` コマンドは、設定置換の後の `show running` には表示されません。したがって、「欠落」と見なされ、CR は失敗します。次に例を示します。

```
switch# config replace bootflash:test verify-and-commit

Version match between user file and running configuration.
Pre-check for User config PASSED
ADVISORY: Config Replace operation started...
Modifying running configuration from another VSH terminal in parallel
is not recommended, as this may lead to Config Replace failure.

Collecting Running-Config
Generating Rollback patch for switch profile
Rollback Patch is Empty
Collecting Running-Config
.Generating Rollback Patch
```

```

Validating Patch
Patch validation completed successful
Executing Rollback Patch
During CR operation,will retain L3 configuration
when vrf member change on interface
Generating Running-config for verification
Generating Rollback Patch
Executing Rollback Patch
During CR operation,will retain L3 configuration
when vrf member change on interface
Generating Running-config for verification
Generating Patch for verification
Verification failed, Rolling back to previous configuration
Collecting Running-Config
Cleaning up switch-profile buffer
Generating Rollback patch for switch profile
Executing Rollback patch for switch profiles. WARNING - This will change the
configuration of switch profiles and will also affect any peers if configured
Collecting Running-Config
Generating Rollback Patch
Rollback Patch is Empty
Rolling back to previous configuration is successful

Configure replace failed. Use 'show config-replace log verify' or 'show config-replace
log exec' to see reasons for failure

n9k13# show config-replace log verify
Operation : Config-replace to user config
Checkpoint file name : .replace_tmp_31849
Scheme : tmp
Cfg-replace done By : agargula
Cfg-replace mode : atomic
Verbose : disabled
Start Time : Tue, 11:20:59 12 Nov 2019
Start Time UTC : Tue, 10:20:59 12 Nov 2019
-----
End Time : Tue, 11:21:28 12 Nov 2019
End Time UTC : Tue, 10:21:28 12 Nov 2019
Status : Failed

Verification patch contains the following commands:
-----
!!
Configuration To Be Added Missing in Running-config
=====
!
power redundancy-mode ps-redundant

Undo Log
-----
End Time : Tue, 11:21:32 12 Nov 2019
End Time UTC : Tue, 10:21:32 12 Nov 2019
Status : Success
n9k13#

```

上記の例では、CR は欠落しているデフォルトのコマンドを考慮します。



## 第 22 章

# ロールバックの設定

この章は、次の内容で構成されています。

- [ロールバックについて \(297 ページ\)](#)
- [ロールバックの注意事項と制約事項 \(297 ページ\)](#)
- [チェックポイントの作成 \(298 ページ\)](#)
- [ロールバックの実装 \(299 ページ\)](#)
- [ロールバック コンフィギュレーションの確認 \(300 ページ\)](#)

## 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ても、いつでもそのコンフィギュレーションをスイッチに再適用できます。権限のある管理者であれば、チェックポイントで設定されている機能について専門的な知識がなくても、ロールバック機能を使用して、そのチェックポイント コンフィギュレーションを適用できます。

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

実行コンフィギュレーションをロールバックするとき、atomic ロールバックを発生させることができます。atomic ロールバックでは、エラーが発生しなかった場合に限り、ロールバックを実行します。

## ロールバックの注意事項と制約事項

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 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** コマンドを入力すると、チェックポイントが削除されます。**clear checkpoint database** コマンドを使用すると、すべてのチェックポイント ファイルを削除できます。
- ブートフラッシュでチェックポイントを作成した場合、ロールバックの実行前は実行システム コンフィギュレーションとの違いは実行できず、「変更なし」と報告されます。
- チェックポイントはスイッチに対してローカルです。
- **checkpoint** および **checkpoint checkpoint\_name** コマンドを使用して作成されたチェックポイントは、すべてのスイッチの 1 つのスイッチオーバーに対して存在します。
- ブートフラッシュ時のファイルへのロールバックは、**checkpoint checkpoint\_name** コマンドを使用して作成されたファイルでのみサポートされます。他の ASCII タイプのファイルではサポートされません。
- チェックポイントの名前は一意にする必要があります。以前に保存したチェックポイントと同じ名前の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	<pre>switch# <b>checkpoint</b> { [cp-name] [ <b>description descr</b>]   <b>file</b> file-name</pre> <p>例 :</p> <pre>switch# checkpoint stable</pre>	<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 <code>user-checkpoint-&lt;number&gt;</code> に設定します。ここで <code>number</code> は 1 ~ 10 の値です。</p> <p><code>description</code> には、スペースも含めて最大 80 文字の英数字を指定できます。</p>
ステップ 2	<p>(任意) <pre>switch# <b>no checkpoint</b> cp-name</pre></p> <p>例 :</p> <pre>switch# no checkpoint stable</pre>	<p><code>checkpoint</code> コマンドの <code>no</code> 形式を使用すると、チェックポイント名を削除できます。</p> <p><code>delete</code> コマンドを使用して、チェックポイントファイルを削除できます。</p>
ステップ 3	<p>(任意) <pre>switch# <b>show checkpoint</b> cp-name</pre></p> <p>例 :</p> <pre>[ all]</pre> <pre>switch# show checkpoint stable</pre>	<p>チェックポイント名の内容を表示します。</p>

## ロールバックの実装

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



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

手順の概要

1. `show diff rollback-patch { checkpoint src-cp-name | running-config | startup-config | file source-file } { checkpoint dest-cp-name | running-config | startup-config | file dest-file }`
2. `rollback running-config { checkpoint cp-name | file cp-file } atomic`

## 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</b> { <b>checkpoint</b> <i>src-cp-name</i>   <b>running-config</b>   <b>startup-config</b>   <b>file</b> <i>source-file</i> } { <b>checkpoint</b> <i>dest-cp-name</i>   <b>running-config</b>   <b>startup-config</b>   <b>file</b> <i>dest-file</i> }  例： <pre>switch# show diff rollback-patch checkpoint stable running-config</pre>	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</b> { <b>checkpoint</b> <i>cp-name</i>   <b>file</b> <i>cp-file</i> } <b>atomic</b>  例： <pre>switch# rollback running-config checkpoint stable</pre>	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 <b>atomic</b> 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</b> <i>name</i> [ <b>all</b> ]	チェックポイント名の内容を表示します。
<b>show checkpoint all</b> [ <b>user</b>   <b>system</b> ]	現在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</b> [ <b>user</b>   <b>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</b> { <b>checkpoint</b> <i>src-cp-name</i>   <b>running-config</b>   <b>startup-config</b>   <b>file</b> <i>source-file</i> } { <b>checkpoint</b> <i>dest-cp-name</i>   <b>running-config</b>   <b>startup-config</b>   <b>file</b> <i>dest-file</i> }	ソースと宛先のチェックポイント間の差異を表示します。
<b>show rollback log</b> [ <b>exec</b>   <b>verify</b> ]	ロールバック ログの内容を表示します。



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





## 第 23 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 \(303 ページ\)](#)
- [候補構成の完全性チェックの注意事項と制限事項 \(303 ページ\)](#)
- [候補構成の完全性チェックの実行 \(309 ページ\)](#)
- [完全性チェックの例 \(310 ページ\)](#)

## 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 \(309 ページ\)](#) 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。**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。

- 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 (-log-neighbor-warnings; など) があり、そのサブモード (address-family ipv4 unicast または address-family ipv6 unicast) ではなく、router eigrp モードで直接設定されている場合、partial-diff は、diff のデフォルトコマンドの出力に + を付けて表示します (たとえば + log-neighbor-warnings) 。
- 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	show diff のデフォルト コマンド
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	<b>show diff</b> のデフォルト コマンド
PIM6	<pre>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</pre>
IGMP	<pre>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</pre>
MLD	<pre>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</pre>

### **show diff running-config file\_url [unified] [partial] [merged]** コマンドのガイドラインと制限事項

- **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
<pre>route-map rmap1 permit 10   set ip next-hop 1.1.1.1 2.2.2.2 load-share</pre>	<pre>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</pre>	<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のとなつて、コマンドラインの場合と似た結果になります。

候補構成	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、候補構成で単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ーションのみが **partial diff** の出力に表示されます。

例1: この例では、候補構成で、単一のルートマップ **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
```

- **Partial Unified Merged** オプションを使用して、**verify-availability** コマンドのバリエーションの違いを確認する場合、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)。

次の表に、以下に示すさまざまなユースケースのサンプルの候補と実行構成と、**部分的な統合マージ** の出力を示します。

1. 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>

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  
味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味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、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]

## 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>• <b>file_url</b> : 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> : 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、<b>merged</b> を入力します。</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>• <b>file_url</b> : 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-channel500
!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#
```





## 第 24 章

# ユーザアカウントおよび RBAC の設定

この章は、次の内容で構成されています。

- [ユーザーアカウントおよび RBAC の概要, on page 313](#)
- [ユーザーアカウントの注意事項および制約事項 \(317 ページ\)](#)
- [ユーザアカウントの設定, on page 317](#)
- [RBAC の設定 \(319 ページ\)](#)
- [ユーザーアカウントと RBAC の設定の確認, on page 324](#)
- [ユーザーアカウントおよび RBAC のユーザーアカウントデフォルト設定, on page 324](#)

## ユーザーアカウントおよび RBAC の概要

Cisco Nexus シリーズスイッチは、ロールベースアクセスコントロール (RBAC) を使用して、ユーザ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、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。ただし、**network-operator** ロールは **show running-config** コマンドと **show startup-config** コマンドを実行できません。



**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。



**Note** RBAC ロールでチェックポイントまたはロールバックを実行できるのは **network-admin** ユーザーだけです。他のユーザーはこれらのコマンドをロールの許可ルールとして持っていますが、これらのコマンドを実行しようとすると、ユーザー アクセスは拒否されます。

## 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。

### OID

SNMP オブジェクト ID (OID)。

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。

SNMP OID は RBAC でサポートされています。SNMP OID に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つのルールが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

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

ユーザロールポリシーは、ロールに定義されている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設定しないと、ユーザはインターフェイスにアクセスできません。

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

## ユーザ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

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せん。
- 



- 
- (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せん。
- 

パスワードが脆弱な場合（短い、解読されやすいなど）、Cisco Nexus デバイスはパスワードを拒否します。各ユーザ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`、`network-operator`、`san-admin` などの事前定義されたロールは編集不可です。
- ルールの追加、削除、編集は、SAN 管理者ユーザーロールではサポートされません。
- インターフェイス、VLAN、または VSAN 範囲は SAN 管理者ユーザーロールでは変更できません。



- (注) 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。

### 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`

## 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><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 <i>password</i> は定義されていません。</p> <p><b>Note</b> 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>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
```

# 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

	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>role name</b> <i>role-name</i>	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。  <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</b> {deny   permit} <b>command</b> <i>command-string</i>	コマンド ルールを設定します。  <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。

	Command or Action	Purpose
ステップ 4	<code>switch(config-role)# rule number {deny   permit} {read   read-write}</code>	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	<code>switch(config-role)# rule number {deny   permit} {read   read-write} feature feature-name</code>	機能に対して、読み取り専用規則か読み取りと書き込みの規則かを設定します。  機能リストを表示するには、 <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	<code>switch(config-role)# rule number {deny   permit} {read   read-write} feature-group group-name</code>	機能グループに対して、読み取り専用規則か読み取りと書き込みの規則かを設定します。  機能グループのリストを表示するには、 <b>show role feature-group</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 7	(Optional) <code>switch(config-role)# description text</code>	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	<code>switch(config-role)# end</code>	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) <code>switch# show role</code>	ユーザ ロールの設定を表示します。
ステップ 10	(Optional) <code>switch# copy running-config startup-config</code>	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

	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>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、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	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</b> <i>role-name</i>	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>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	switch(config-role-interface) # <b>permit interface</b> <i>interface-list</i>	<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	switch(config-role-interface) # <b>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) switch(config-role) # <b>show role</b>	ロール設定を表示します。
ステップ 7	(Optional) switch(config-role) # <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

	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>role name</b> <i>role-name</i>	ユーザロールを指定し、ロールコンフィギュレーションモードを開始します。
ステップ 3	switch(config-role) # <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</b> <i>vlan-list</i>	ロールがアクセスできるVLANの範囲を指定します。 必要なVLANの数だけこのコマンドを繰り返します。
ステップ 5	switch(config-role-vlan) # <b>exit</b>	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</b> [role-name]	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</b> [all]	実行コンフィギュレーションのユーザアカウント設定を表示します。all キーワードを指定すると、ユーザアカウントのデフォルト値が表示されます。
<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 のユーザーアカウントデフォルト設定

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 32: 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。
VFC ポリシー	すべての VFC にアクセス可能。
VETH ポリシー	すべての VETH にアクセス可能。



## 第 25 章

# 安全な消去の設定

- [安全に消去する（Secure Erase）機能に関する情報（325 ページ）](#)
- [安全な消去を実行するための前提条件（326 ページ）](#)
- [安全な消去の注意事項と制約事項（326 ページ）](#)
- [安全な消去の設定（326 ページ）](#)

## 安全に消去する（Secure Erase）機能に関する情報

Cisco NX-OS リリース 10.2(2)F 以降、Nexus 3548 スイッチのすべての顧客情報を消去する安全に消去する（Secure Erase）機能が導入されました。Secure Erase は、Return Merchandise Authorization（RMA）、アップグレードまたは交換、またはシステムのサポート終了により製品が削除された状態で、Cisco NX-OS デバイス上のすべての識別可能な顧客情報を削除する操作です。

Cisco Nexus 3548 スイッチは、ストレージを消費して、システムソフトウェアイメージ、スイッチ設定、ソフトウェアログ、および動作履歴を保存します。これらの領域には、ネットワークアーキテクチャや設計に関する詳細などの顧客固有の情報や、データ盗難の潜在的な標的が含まれている可能性があります。

安全に消去するプロセスは、次の 2 つのシナリオで使用されます。

- デバイスの返品許可（RMA）：RMA のためにデバイスをシスコに返送する必要がある場合は、そのデバイスの RMA 証明書を取得する前に、お客様固有のデータをすべて削除してください。
- 侵害を受けたデバイスのリカバリ：デバイスに保存されているキーマテリアルまたはクレデンシャルが侵害を受けた場合は、デバイスを初期設定にリセットし、デバイスを再設定してください。



(注) 安全に消去する機能では、外部ストレージのコンテンツは消去されません。

デバイスがリロードされて工場出荷時設定にリセットされ、スイッチがパワーダウンモードになります。初期設定へのリセット後、デバイスは、ソフトウェアの検索とロードに必要な **MAC\_ADDRESS** と **SERIAL\_NUMBER** を含むすべての環境変数をクリアします。

## 安全な消去を実行するための前提条件

- 安全な消去操作を実行する前に、すべてのソフトウェアイメージ、構成、および個人データがバックアップされていることを確認してください。
- プロセスが進行中の場合は、電源の中断がないことを確認してください。
- 安全な消去プロセスを開始する前に、**In-Service Software Upgrade (ISSU)** または **In-Service Software Downgrade (ISSD)** が進行中でないことを確認します。

## 安全な消去の注意事項と制約事項

- FX3 または FX3S または FX3P スイッチは、TOR および FEX モードでサポートされます。安全な消去が FEX モードで実行された場合、スイッチは安全な消去操作後に TOR モードで起動します。
- ソフトウェアパッチは、デバイスにインストールされている場合、初期設定へのリセットプロセス後に復元されません。
- セッションを介して **factory-reset** コマンドが発行された場合、初期設定へのリセットプロセスの完了後にセッションは復元されません。

トップオブラックスイッチとスーパーバイザモジュールは、ローダープロンプトに戻ります。

行端スイッチモジュールは、電源が切断された状態になります。

fex の安全な消去を構成すると、出荷時設定へのリセットが開始され、fex 構成が削除されます。

fex コンソールを使用してモニタリングされる fex 安全な消去。失敗した場合は、再起動して fex を起動し、安全な消去を再度開始します。

## 安全な消去の設定

RMA に発送する前に必要なデータをすべて削除するには、次のコマンドを使用して安全な消去を設定します。

コマンド	目的
<p><b>factory-resetfex module</b><i>mod</i></p> <p>例：</p> <pre>switch(config)# factory-reset [module &lt;3&gt;]</pre>	<p><b>all</b> オプションを有効にしてコマンドを使用してください。<b>factory reset</b> コマンドを使用するために必要なシステム設定はありません。</p> <p>fex の消去を保護するには、<b>factory-resetfex [allfex_no]</b> を使用します。</p> <ul style="list-style-type: none"> <li>一度にすべての fex を安全に消去するには、オプション <b>all</b> を使用します。</li> </ul> <p>(注)</p> <p>安全な消去操作を開始する前に、fex が Active-Active シナリオにないことを確認してください。</p> <p>オプション <b>mod</b> を使用して、起動構成をリセットします。</p> <ul style="list-style-type: none"> <li>top-of-rack (ToR; トップオブラック) スイッチの場合、コマンドは <b>factory-reset</b> または <b>factory-reset module 1</b> です。</li> <li>トップオブラックスイッチの LXC モードでは、コマンドは <b>factory-reset module 1</b> または <b>27</b> です。</li> <li>行末のモジュールスイッチの場合、<b>factory-reset module #module_number</b> コマンドは次のとおりです。</li> </ul> <p>工場出荷時の状態へのリセットプロセスが正常に完了すると、スイッチがリブートして、電源が切れます。</p>



- (注) 並行の安全な消去操作はサポートされていません。単一の EoR シャーシ内の複数のモジュールを消去する場合、推奨される順序は、ラインカード、ファブリック、スタンバイ スーパーバイザ、システムコントローラ、アクティブ スーパーバイザです。

その安全な消去イメージを起動して、データワイブをトリガーできます。

次に、安全な消去による工場出荷時リセット コマンドを設定するための出力例を示します。

```
FX2-2-switch# factory-reset fex all
!!!! WARNING:
This command will perform factory-reset of all FEX modules !!!!
The factory reset operation will erase ALL persistent storage on the specified FEX module.
This includes configuration, all log data, and the full contents of flash and SSDs.
```

```
Special steps are taken in an effort to render data non-recoverable. Please, proceed
with caution and understanding that this operation cannot be undone and will leave the
system in a fresh-from-factory state.
!!!! WARNING !!!!
```

```
Do you want to continue? (y/n) [n] y
Initiating factory-reset for the FEX: 109 --- SUCCESS!!
FEX: 109 is reloading for the reset operation to proceed.
Factory reset may take time...
Please, wait and do not power off the FEX...
Trying to remove the FEX:109 config !!!
Initiating factory-reset for the FEX: 110 --- SUCCESS!!
FEX: 110 is reloading for the reset operation to proceed.
Factory reset may take time...
Please, wait and do not power off the FEX...
Trying to remove the FEX:110 config !!!
Successfully removed FEX:110 config. !!!
```

以下に `fex` ログの例を示します。

```
FX2-2-switch# 2021
FEX console logs:
=====
bgl-ads-4157:138> telnet 10.127.118.15 2007
Trying 10.127.118.15...
Connected to 10.127.118.15.
Escape character is '^]'.

fex-109#
fex-109# [129266.313614] writing reset reason 9, Factory-reset requested by abc
[129266.391801] Restarting system - Factory-reset requested by abc [9]
U-Boot 2011.12 (Jun 25 2014 - 16:28:41) Cisco Systems
CPU0: P1020E, Version: 1.1, (0x80ec0011)
Core: E500, Version: 5.1, (0x80212051)
Clock Configuration:
CPU0:666.667 MHz, CPU1:666.667 MHz,
CCB:333.333 MHz,
DDR:333.333 MHz (666.667 MT/s data rate) (Asynchronous), LBC:83.333 MHz
L1: D-cache 32 kB enabled
I-cache 32 kB enabled
Board: P1020FEX
[MCPSUMR 0x00000000, RSTRSCR 0x00000000, AUTORSTSR 0x0000c000]
I2C buses: ready
Golden image
U-boot retry count 0
Jump to upgradeable image at 0xefd20040
U-Boot 2011.12 (Jun 25 2014 - 16:19:54) Cisco Systems
CPU0: P1020E, Version: 1.1, (0x80ec0011)
Core: E500, Version: 5.1, (0x80212051)
Clock Configuration:
CPU0:666.667 MHz, CPU1:666.667 MHz,
CCB:333.333 MHz,
DDR:333.333 MHz (666.667 MT/s data rate) (Asynchronous), LBC:83.333 MHz
L1: D-cache 32 kB enabled
I-cache 32 kB enabled
Board: P1020FEX
[MCPSUMR 0x00000000, RSTRSCR 0x00000000, AUTORSTSR 0x0000c000]
I2C buses: ready
Upgradeable image
DRAM: Configuring DDR for 666.667 MT/s data rate
Time-out count = 480
DDR configuration get done
1 GiB (DDR3, 32-bit, CL=6, ECC on)
Memory test from 0x40000 to 0x1fdfffff
Data line test..... OK
```

```
Address line test..... OK
OK
Flash: 288 MiB
L2: 256 KB enabled
Set dbglevel to its default value (0x1)
PCIE1: Root Complex of mini PCIe SLOT, x1, regs @ 0xffe0a000
PCIE1: Bus 00 - 01
PCIE2: Root Complex of PCIe SLOT, no link, regs @ 0xffe09000
PCIE2: Bus 02 - 02
Net: eTSEC1, eTSEC3
Hit Ctrl-L to stop autoboot: 0
WARN: user forced bootcmd="run sysboot"
.. WARNING: adjusting available memory to 30000000
## Booting kernel from Legacy Image at 01000000 ...
Image Name: Linux-2.6.27.47
Created: 2015-11-20 10:22:39 UTC
Image Type: PowerPC Linux Kernel Image (gzip compressed)
Data Size: 8936305 Bytes = 8.5 MiB
Load Address: 00000000
Entry Point: 00000000
Verifying Checksum ... OK
## Flattened Device Tree blob at 00c00000
Booting using the fdt blob at 0x00c00000
Uncompressing Kernel Image ... OK
Loading Device Tree to 03ffb000, end 03ffff82 ... OK
setup_arch: bootmem
mpc85xx_fex_setup_arch()
arch: exit
[0.436112] Host controller irq 17
[0.477490] pci 0000:00:00.0: ignoring class b20 (doesn't match header type 01)
[0.566841] Assign root port irq 17 for 0000:00:00.0
[2.210329] Enabling all PCI devices
[2.802226] FSL:i2c-mpc - probing i2c controller
modprobe: FATAL: Could not load /lib/modules/2.6.27.47/modules.dep: No such file or
directory
[2.975494] FSL:i2c-mpc - probing i2c controller
modprobe: FATAL: Could not load /lib/modules/2.6.27.47/modules.dep: No such file or
directory
modprobe: FATAL: Could not load /lib/modules/2.6.27.47/modules.dep: No such file or
directory
modprobe: FATAL: Could not load /lib/modules/2.6.27.47/modules.dep: No such file or
directory
modprobe: FATAL: Could not load /lib/modules/2.6.27.47/modules.dep: No such file or
directory
modprobe: FATAL: Could not load /lib/modules/2.6.27.47/modules.dep: No such file or
directory
modprobe: FATAL: Could not load /lib/modules/2.6.27.47/modules.dep: No such file or
directory
modprobe: FATAL: Could not load /lib/modules/2.6.27.47/modules.dep: No such file or
directory
modprobe: FATAL: Could not load /lib/modules/2.6.27.47/modules.dep: No such file or
directory
[3.889037]
[3.889041] Watchdog init<0>
Mount failed for selinuxfs on /selinux: No such file or directory
INIT: version 2.86 booting
Setting system clock: [ OK ]
Mounting all filesystems: [ OK ]
/sbin/dhclient-script: configuration for eth1 not found. Continuing with defaults.
/etc/sysconfig/network-scripts/network-functions: line 78: eth1: No such file or directory
Mounting system image: [ OK ]
Unpacking system image: [ OK ]
Uncompressing system image: [ OK ]
Loading system image: [ OK ]
net.ipv4.ip_forward = 0
net.ipv4.ip_default_ttl = 64
```

```
net.ipv4.ip_no_pmtu_disc = 1
Starting internet superserver: inetd [ OK ]
net.core.rmem_max = 524288
net.core.wmem_max = 524288
net.core.rmem_default = 524288
net.core.wmem_default = 524288
net.core.somaxconn = 1024
net.core.netdev_max_backlog = 1024
modprobe: FATAL: Could not load /lib/modules/2.6.27.47/modules.dep: No such file or
directory
[23.255118] Device eth0 configured with sgmii interface
Non issu restart
[24.151321]
[24.151327] base_addr is 26524<0>
Secure erase requested! Please, do not power off module!
Starting the secure erase. !!
This may take time. Please wait !!
>>>> Wiping all storage devices ...
[28.706882] NX-OS starts punching watchdog
grep: Backu: No such file or directory
+++ Starting mtd secure erase for the partition /dev/mtd2 +++
Erasing /dev/mtd2 ...
Erasing 128 Kibyte @ 17e0000 -- 99 % complete.
---> SUCCESS
Writing random data onto /dev/mtd2
Filling /dev/mtd2 using random data ...
Erasing blocks: 192/192 (100%)
Writing data: 24576k/24576k (100%)
Verifying data: 24576k/24576k (100%)
---> SUCCESS
Erasing /dev/mtd2 ...
Erasing 128 Kibyte @ 17e0000 -- 99 % complete.
---> SUCCESS
+++ Skipping cmos secure erase +++
>>>> Done
+++ Skipping nvram secure erase +++
>>>> Done
>>>> Iniatilzing system to factory defaults ...
+++ Starting init-system +++
Initializing /dev/mtd5
/isan/bin/mount_jffs2.sh: line 68: ${LOG_FILE}: ambiguous [ 651.954326] Restarting system.
U-Boot 2011.12 (Jun 25 2014 - 16:28:41) Cisco Systems
CPU0: P1020E, Version: 1.1, (0x80ec0011)
Core: E500, Version: 5.1, (0x80212051)
Clock Configuration:
CPU0:666.667 MHz, CPU1:666.667 MHz,
CCB:333.333 MHz,
DDR:333.333 MHz (666.667 MT/s data rate) (Asynchronous), LBC:83.333 MHz
L1: D-cache 32 kB enabled
I-cache 32 kB enabled
Board: P1020FEX
[MCPSUMR 0x00000000, RSTRSCR 0x00000000, AUTORSTSR 0x0000c000]
I2C buses: ready
Golden image
U-boot retry count 1
Jump to upgradeable image at 0xefd20040
U-Boot 2011.12 (Jun 25 2014 - 16:19:54) Cisco Systems
CPU0: P1020E, Version: 1.1, (0x80ec0011)
Core: E500, Version: 5.1, (0x80212051)
Clock Configuration:
CPU0:666.667 MHz, CPU1:666.667 MHz,
CCB:333.333 MHz,
DDR:333.333 MHz (666.667 MT/s data rate) (Asynchronous), LBC:83.333 MHz
L1: D-cache 32 kB enabled
```

```
I-cache 32 kB enabled
Board: P1020FEX
[MCPSUMR 0x00000000, RSTRSCR 0x00000000, AUTORSTSR 0x0000c000]
I2C buses: ready
Upgradeable image
DRAM: Configuring DDR for 666.667 MT/s data rate
Time-out count = 480
DDR configuration get done
1 GiB (DDR3, 32-bit, CL=6, ECC on)
Memory test from 0x40000 to 0x1fdfffff
Data line test..... OK
Address line test..... OK
OK
Flash: 288 MiB
L2: 256 KB enabled
Set dbglevel to its default value (0x1)
PCIE1: Root Complex of mini PCIe SLOT, x1, regs @ 0xffe0a000
PCIE1: Bus 00 - 01
PCIE2: Root Complex of PCIe SLOT, no link, regs @ 0xffe09000
PCIE2: Bus 02 - 02
Net: eTSEC1, eTSEC3
Hit Ctrl-L to stop autoboot: 0
WARN: user forced bootcmd="run sysboot"
.. WARNING: adjusting available memory to 30000000
## Booting kernel from Legacy Image at 01000000 ...
Image Name: Linux-2.6.27.47
Created: 2015-11-20 10:22:39 UTC
Image Type: PowerPC Linux Kernel Image (gzip compressed)
Data Size: 8936305 Bytes = 8.5 MiB
Load Address: 00000000
Entry Point: 00000000
Verifying Checksum ... OK
## Flattened Device Tree blob at 00c00000
Booting using the fdt blob at 0x00c00000
Uncompressing Kernel Image ... OK
Loading Device Tree to 03ffb000, end 03fffe82 ... OK
setup_arch: bootmem
mpc85xx_fex_setup_arch()
arch: exit
[ 0.436112] Host controller irq 17
[ 0.477490] pci 0000:00:00.0: ignoring class b20 (doesn't match header type 01)
[ 0.566841] Assign root port irq 17 for 0000:00:00.0
[ 2.210556] Enabling all PCI devices
[ 2.804559] FSL:i2c-mpc - probing i2c controller
modprobe: FATAL: Could not load /lib/modules/2.6.27.47/modules.dep: No such file or
directory
[ 2.975502] FSL:i2c-mpc - probing i2c controller
modprobe: FATAL: Could not load /lib/modules/2.6.27.47/modules.dep: No such file or
directory
modprobe: FATAL: Could not load /lib/modules/2.6.27.47/modules.dep: No such file or
directory
modprobe: FATAL: Could not load /lib/modules/2.6.27.47/modules.dep: No such file or
directory
modprobe: FATAL: Could not load /lib/modules/2.6.27.47/modules.dep: No such file or
directory
modprobe: FATAL: Could not load /lib/modules/2.6.27.47/modules.dep: No such file or
directory
modprobe: FATAL: Could not load /lib/modules/2.6.27.47/modules.dep: No such file or
directory
modprobe: FATAL: Could not load /lib/modules/2.6.27.47/modules.dep: No such file or
directory
modprobe: FATAL: Could not load /lib/modules/2.6.27.47/modules.dep: No such file or
directory
[ 3.889014]
[ 3.889018] Watchdog init<0>
Mount failed for selinuxfs on /selinux: No such file or directory
```

```

INIT: version 2.86 booting
Setting system clock: [ OK ]
Mounting all filesystems: [ OK ]
/sbin/dhclient-script: configuration for eth1 not found. Continuing with defaults.
/etc/sysconfig/network-scripts/network-functions: line 78: eth1: No such file or directory
Mounting system image: [ OK ]
Unpacking system image: [ OK ]
Uncompressing system image: [ OK ]
Loading system image: [ OK ]
net.ipv4.ip_forward = 0
net.ipv4.ip_default_ttl = 64
net.ipv4.ip_no_pmtu_disc = 1
Starting internet superserver: inetd [ OK ]
net.core.rmem_max = 524288
net.core.wmem_max = 524288
net.core.rmem_default = 524288
net.core.wmem_default = 524288
net.core.somaxconn = 1024
net.core.netdev_max_backlog = 1024
modprobe: FATAL: Could not load /lib/modules/2.6.27.47/modules.dep: No such file or
directory
[ 22.630994] Device eth0 configured with sgmi interface
Non issu restart
[ 23.535827]
[ 23.535832] base_addr is 26524<0>
INIT: Entering runlevel: 3
fex login: Sorry, user root is not allowed to execute '/sbin/sysctl -q -w vm.drop_caches=3'
as root on fex.
[ 28.090052] NX-OS starts punching watchdog
fex login:

```

次に、モジュールで安全な消去による工場出荷時リセットコマンドを設定するための出力例を示します。

```

switch# factory-reset [all | module <mod>]
switch# factory-reset [module <3>]
!!!! WARNING !!!!
The factory reset operation will erase ALL persistent storage on the specified module.
This includes configuration, all log data, and the full contents of flash and SSDs.
Special steps are taken to render data non-recoverable. Please, proceed with caution and
understanding that this operation cannot be undone and will leave the system in a
fresh-from-factory state.
!!!! WARNING !!!!
Continue? (y/n) [n] y
A module reload is required for the reset operation to proceed. Please, wait...
...truncated...
Secure erase requested! Please, do not power off module!
>>>> Wiping all storage devices ...
+++ Starting mmc secure erase for /dev/mmcblk0 +++
*** Please, wait - this may take several minutes ***
\
---> SUCCESS
+++ Starting SSD secure erase for /dev/sda +++
*** Please, wait - this may take several minutes ***
\
---> SUCCESS
+++ Starting cmos secure erase +++
\
---> SUCCESS
>>>> Done
+++ Starting nvram secure erase +++
\
---> SUCCESS
>>>> Done

```







## 索引

### C

- Call Home の通知 [106–107](#)
  - syslog の XML 形式 [107](#)
  - syslog のフルテキスト形式 [106](#)
- cfs を使用した ntp [44](#)

### E

- EEM [166–171, 173, 176, 179–180, 182](#)
  - syslog スクリプト [182](#)
  - VSH スクリプト [179](#)
    - 登録およびアクティブ化 [179](#)
  - VSH スクリプト ポリシー [168](#)
  - アクション文 [168](#)
  - アクション文、設定 [176](#)
  - イベント文 [167](#)
  - イベント文、設定 [173](#)
  - システム ポリシー、上書き [180](#)
  - デフォルト設定 [170](#)
  - ポリシー [166](#)
  - ユーザー ポリシー、定義 [171](#)
  - 環境変数の定義 [170](#)
  - 前提条件 [169](#)
- EEM ポリシーの定義 [179](#)
  - VSH スクリプト [179](#)
- ERSPAN [227–229, 232, 235, 248–249](#)
  - セッション [229](#)
    - multiple [229](#)
  - タイプ [227](#)
  - デフォルトパラメータ [232](#)
  - 宛先 [228, 248](#)
    - 設定例 [248](#)
  - 宛先セッション [235](#)
    - ERSPAN の設定 [235](#)
  - 宛先セッションの設定 [235](#)
  - 概要 [227](#)
  - 関連資料 [249](#)
  - 高可用性 [229](#)
  - 前提条件 [229](#)

### ERSPAN (続き)

- 送信元 [228, 248](#)
  - 設定例 [248](#)
- 送信元セッション [232](#)
  - ERSPAN の設定 [232](#)
- 送信元セッションの設定 [232](#)

### G

- GOLD 診断 [159–161](#)
  - ヘルス モニタリング [160](#)
  - ランタイム [159](#)
  - 拡張モジュール [161](#)
  - 構成 [161](#)

### I

- ID [86](#)
  - シリアル ID [86](#)

### L

- linkDown 通知 [147–148](#)
- linkUp 通知 [147–148](#)
- logging [68](#)
  - ファシリティメッセージ [68](#)
  - モジュールメッセージ [68](#)

### N

- ntp [43–46, 50, 59–60](#)
  - cfs の使用 [44](#)
  - アクセス制限、設定 [50](#)
  - ガイドライン [45](#)
  - クロック マネージャ [44](#)
  - タイム サーバ [44](#)
  - デフォルト設定 [46](#)
  - 仮想化 [45](#)
  - 関連資料 [60](#)
  - 機能の履歴 [60](#)
  - 情報 [43](#)

## ntp (続き)

設定例 59

## NTP 構成 55

変更のコミット 55

## P

## PTP 17, 19–20, 23, 26

インターフェイス、設定 26

グローバル設定 23

デバイス タイプ 19

デフォルト設定 23

プロセス 20

概要 17

## R

## RBAC 313–315, 317, 319–321, 323–324

ユーザ ロールおよびルール、設定 319

ユーザー アカウント、設定 317

ユーザー アカウントの制限事項 315

ユーザー ロール VLAN ポリシー、変更 323

ユーザー ロール インターフェイス ポリシー、変更 321

ユーザーロール 313

ルール 314

確認 324

機能グループ、作成 320

## rollback 114

デフォルト設定 114

## S

## scheduler 117–124, 126–127, 129

ジョブ、削除 123

タイムテーブル、定義 124

ディセーブル化 127

デフォルト設定 119

リモートユーザー認証、設定 121–122

リモートユーザ認証 118

ログ ファイル 118

ログ ファイル サイズ、定義 120

ログ ファイル、消去 126

概要 117

規格 129

設定、確認 127

注意事項と制約事項 118

有効化 119

## Session Manager 111, 113–114

ACL セッションの設定例 114

ガイドライン 111

セッションのコミット 113

## Session Manager (続き)

セッションの確認 113

セッションの廃棄 114

セッションの保存 114

構成の確認 114

制限事項 111

説明 111

## show コマンドの追加、アラート グループ 99

smart call home 99

## smart call home 81–83, 91–93, 95–96, 98–100, 102–106

show コマンドの追加、アラート グループ 99

アラート グループ 83

アラート グループのアソシエート 98

デフォルト設定 91

メッセージフォーマット オプション 82

宛先プロファイル 82

宛先プロファイル、作成 95

宛先プロファイル、変更 96

確認 106

重複メッセージ抑制、ディセーブル化 103–104

設定のテスト 105

説明 81

前提条件 91

担当者情報、設定 93

注意事項と制約事項 91

定期的なインベントリ通知 102

電子メールの詳細、設定 100

登録 92

## Smart Call Home のメッセージ 82, 85

フォーマット オプション 82

レベルの設定 85

## SMU 267–270, 273–276

アクティブなパッケージセットのコミット 274

ガイドライン 269

パッケージ インストールの準備 270

パッケージのアクティブ化 273

パッケージの削除 275

パッケージの追加 273

パッケージの非アクティブ化 275

パッケージ管理 268

制限事項 269

説明 267

前提条件 269

## SNMP 131–132, 134–137, 139–140, 143, 151

CLI を使用したユーザの同期 135

アクセス グループ 136

インバンドアクセス 143

グループ ベースのアクセス 136

セキュリティ モデル 134

デフォルト設定 137

## SNMP (続き)

- トラップ通知 **132**
- バージョン3のセキュリティ機能 **132**
- メッセージの暗号化 **139**
- ユーザベースのセキュリティ **134**
  - SNMP **134**
- ユーザーの構成 **137**
- 機能の概要 **131**
- 注意事項と制約事項 **136**
- 通知レシーバ **140**
- 無効化 **151**
- 要求のフィルタリング **140**
- SNMP のデフォルト設定 **137**
- SNMP 通知 **143**
  - VRF に基づくフィルタリング **143**
- SNMP 通知レシーバ **142**
  - VRF による設定 **142**
- SNMP 要求のフィルタリング **140**
- snmp-server name **138**
- SNMP (簡易ネットワーク管理プロトコル) **133**
  - バージョン **133**
- SNMPv3 **132, 139**
  - セキュリティ機能 **132**
  - 複数のロールの割り当て **139**
- SPAN **203–205, 208–209, 211–213, 219**
  - VLAN、設定 **211**
  - イーサネット宛先ポート、設定 **209**
  - セッションのアクティブ化 **213**
  - モニタリングの送信元 **203**
  - 宛先 **205**
  - 宛先ポート、特性 **205**
  - 作成、セッションの削除 **208**
  - 出力送信元 **204**
  - 情報の表示 **219**
  - 説明、設定 **212**
  - 送信元ポート チャンネル、設定 **211**
  - 送信元ポート、設定 **211**
  - 特性、送信元ポート **204**
  - 入力送信元 **204**
- SPAN 送信元 **204**
  - 出力 **204**
  - 入力 **204**
- syslog **72, 182**
  - 構成 **72**
  - 組み込みイベント マネージャ (EEM) **182**

## V

- VRF **142–143**
  - SNMP 通知のフィルタリング **143**
  - SNMP 通知レシーバの設定 **142**

- VSH スクリプト **179**
  - EEM ポリシーの定義 **179**
- VSH スクリプト ポリシー **168, 179**
  - EEM **168**
  - 登録およびアクティブ化 **179**

## あ

- アクション文 **168**
  - EEM **168**
- アクション文、設定 **176**
  - 組み込みイベント マネージャ (EEM) **176**
- アクセス制限、設定 **50**
  - ntp **50**
- アラート グループ **83**
  - smart call home **83**
- アラート グループのアソシエート **98**
  - smart call home **98**

## い

- イーサネット宛先ポート、設定 **209**
  - SPAN **209**
- イベント文 **167**
  - EEM **167**
- イベント文、設定 **173**
  - 組み込みイベント マネージャ (EEM) **173**
- インストール ログ情報の表示 **276**
- インターフェイス、設定 **26**
  - PTP **26**

## か

- ガイドライン **45**
  - ntp **45**

## く

- クロック マネージャ **44**
  - ntp **44**

## さ

- サーバー ID **86**
  - 説明 **86**

## し

- システム ポリシー、上書き **180**
  - 組み込みイベント マネージャ (EEM) **180**

システム メッセージ ログの設定 **63**

デフォルト **63**

システム メッセージのログ **61-62**

概要 **61**

注意事項と制約事項 **62**

ジョブ スケジュール、表示 **128**

例 **128**

ジョブ、削除 **123**

スケジューラ **123**

シリアル ID **86**

説明 **86**

## す

スイッチド ポート アナライザ **203**

スケジューラ ジョブ、スケジューリング **128**

例 **128**

スケジューラ ジョブ、結果の表示 **129**

例 **129**

スケジューラ ジョブ、作成 **128**

例 **128**

## せ

セッションのアクティブ化 **213**

SPAN **213**

セッションの実行 **113**

## た

タイム サーバ **44**

ntp **44**

タイムテーブル、定義 **124**

スケジューラ **124**

## て

ディセーブル化 **127**

スケジューラ **127**

デバイス ID **86**

Call Home の形式 **86**

デフォルト パラメータ **232**

ERSPAN **232**

デフォルトの ntp 設定 **46**

デフォルト設定 **91, 114, 119, 170**

EEM **170**

rollback **114**

smart call home **91**

スケジューラ **119**

## と

トラップ通知 **132**

## は

パスワード要件 **316**

バッファ ヒストグラム データ **260, 262**

アクセス **260**

バッファ ヒストグラム データ **260**

収集 **260**

表示 **262**

バッファ監視 **260**

構成 **260**

## ふ

ファシリティ メッセージのログイン **68**

構成 **68**

## へ

ヘルス モニタリング診断 **160**

情報 **160**

## ほ

ポリシー **166**

組み込みイベント マネージャ (EEM) **166**

## め

メッセージの暗号化 **139**

SNMP **139**

## も

モジュール メッセージのログイン **68**

構成 **68**

## ゆ

ユーザ ロールおよびルール、作成 **319**

RBAC **319**

ユーザー **313**

説明 **313**

ユーザー アカウント **317**

注意事項と制約事項 **317**

ユーザー アカウントの制限事項 **315**

RBAC **315**

ユーザー ポリシー、定義 **171**  
 組み込みイベント マネージャ (EEM) **171**  
 ユーザー ロール VLAN ポリシー、変更 **323**  
 RBAC **323**  
 ユーザー ロール インターフェイス ポリシー、変更 **321**  
 RBAC **321**  
 ユーザーアカウント **316, 324**  
 パスワード **316**  
 確認 **324**  
 ユーザーロール **313**  
 RBAC **313**

## ら

ランタイム診断 **159**  
 情報 **159**

## り

リモート ユーザー 認証、設定 **121-122**  
 スケジューラ **121-122**  
 リモート ユーザ 認証 **118**  
 scheduler **118**

## る

ルール **314**  
 RBAC **314**

## ろ

ロール **313**  
 認証 **313**  
 ロールバック **111, 114**  
 ガイドライン **111**  
 チェックポイントのコピー **111**  
 チェックポイント コピーの作成 **111**  
 チェックポイント ファイルの削除 **111**  
 チェックポイント ファイルへの復帰 **111**  
 ロールバックの実装 **111**  
 構成の確認 **114**  
 高可用性 **111**  
 制限事項 **111**  
 設定例 **111**  
 説明 **111**  
 ログ ファイル **118**  
 scheduler **118**  
 ログ ファイル サイズ、定義 **120**  
 スケジューラ **120**  
 ログ ファイル、消去 **126**  
 スケジューラ **126**

## わ

ワープ モード **255-257**  
 ステータスの確認 **257**  
 概要 **255**  
 無効化 **256**  
 有効化 **256**



## 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。