Cisco Nexus 3548 スイッチ NX-OS システム管理構成ガイド、リリース 10.3(x)

初版：2022 年 8 月 19 日

最終更新：2022 年 8 月 25 日

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

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

目 次

はじめに

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
bold	太字の文字は、表示どおりにユーザが入力するコマンドおよびキーワードです。
italic	イタリック体の文字は、ユーザが値を入力する引数です。
[x]	省略可能な要素（キーワードまたは引数）は、角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。イタリック体が使用できない場合に使用されます。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。

例では、次の表記法を使用しています。

表記法	説明
`screen フォント`	スイッチが表示する端末セッションおよび情報は、スクリーンフォントで示しています。

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

Cisco Nexus 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

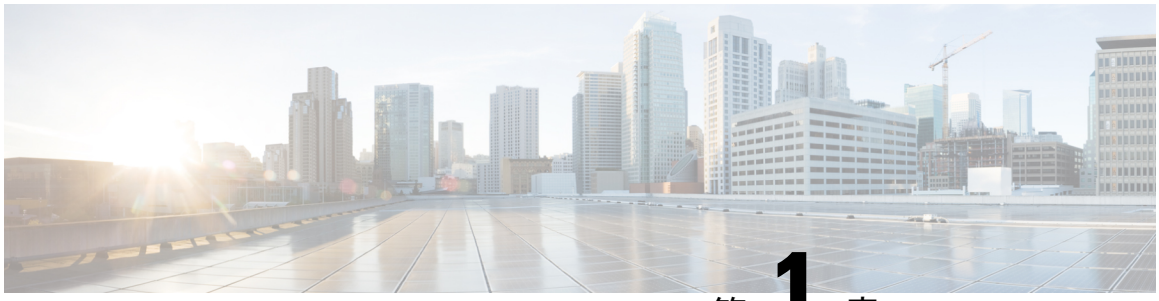
- シスコからタイムリーな関連情報を受け取るには、Cisco Profile Manager でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、シスコサービスにアクセスしてください。
- サービス リクエストを送信するには、シスコサポートにアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、Cisco Marketplace にアクセスしてください。
- 一般的なネットワーク、トレーニング、認定関連の出版物を入手するには、Cisco Press にアクセスしてください。

- 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 バグ検索ツール（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。

はじめに



第 1 章

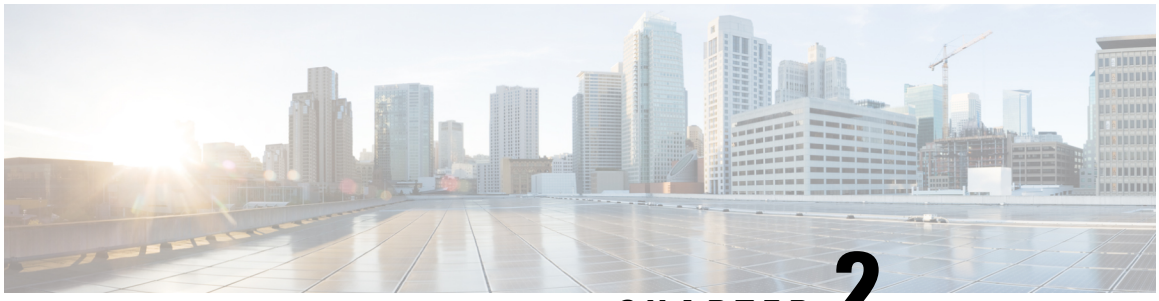
新機能と変更情報

新機能と変更情報

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 *10.3(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

新機能と変更情報



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

このマニュアルに記載されているシステム管理機能について説明します。

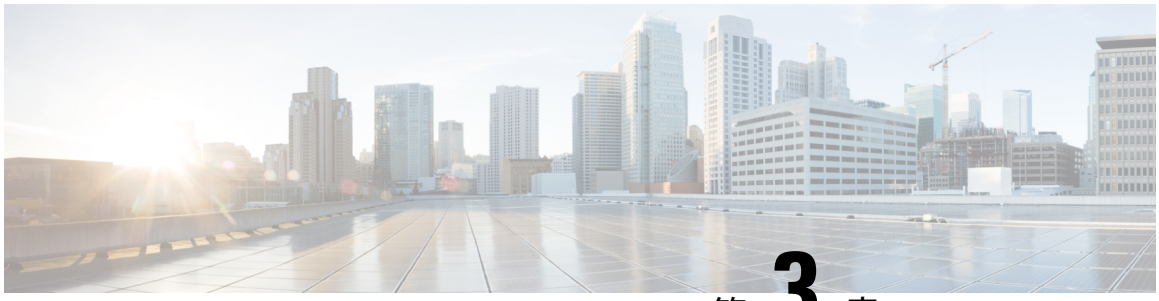
機能	説明
実行中のバッファの監視	実行中のバッファの監視機能は、詳細なバッファ占有率のデータを提供し、ネットワーク輻輳の検出、ネットワーク輻輳がネットワーク運用にいつどのような影響を与えているかを理解するための過去のイベントの確認、過去の傾向の理解、アプリケーショントラフィック フローのパターンの識別に役立ちます。
ワープ モード	ワープモードでは、転送テーブルを単一のテーブルに統合することによりアクセス パスが短縮されるため、フレームおよびパケットの処理がより高速になります。ワープモードでは、遅延が最大 20 パーセント削減されます。
ユーザー アカウントおよび RBAC	ユーザーアカウン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

機能	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。

機能	説明
設定のロール バック	設定のロールバック機能を使用すると、Cisco NX-OS のコンフィギュレーションのスナップショットまたはユーザー 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用メッセージ フォーマットを提供する、アプリケーションレイヤプロトコルです。SNMP では、ネットワーク内のデバイスのモニタリングと管理に使用する標準フレームワークと共通言語が提供されます。
RMON	RMON は、各種のネットワーク エージェントおよびコンソール システムがネットワーク モニタリング データを交換できるようにするための、Internet Engineering Task Force（IETF）標準モニタリング仕様です。Cisco NX-OS では、Cisco NX-OS デバイスをモニターするための、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）プローブです。

ライセンス要件

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



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。

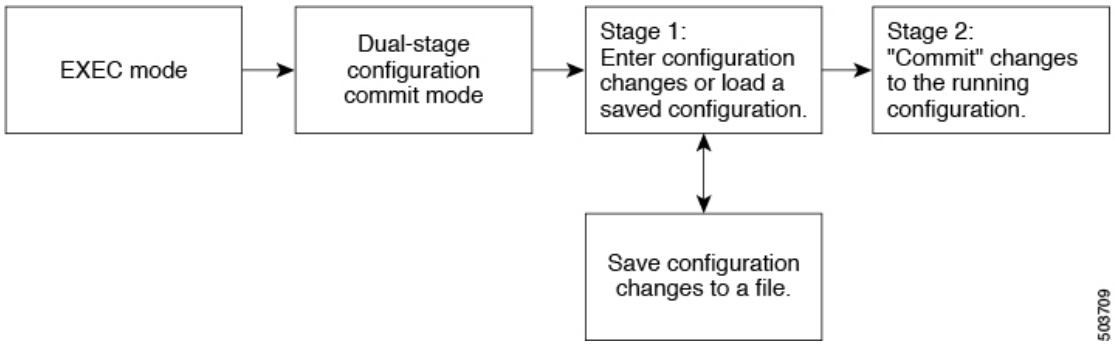
この章は、次の項で構成されています。

2 段階構成のコミットについて

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



ガイドラインと制約事項

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	**configure dual-stage**
	例：
	`switch# configure dual-stage`
	`switch(config-dual-stage)#`
		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	**feature** *feature_name*
	例：
	`switch(config-dual-stage)# feature bgp`
	`switch(config-dual-stage)#`
		機能を有効にします。
		（注）
		• 2 ステージ コンフィギュレーション コミット モードを開始する前でも、この機能を有効にできます。
		• 機能が有効になっていない場合は、機能関連のコマンドを組み合わせて使用することはできません。

ステップ 3	**commit** [**confirmed***seconds*]
	例：
	`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)#`
	例：
		実行コンフィギュレーションに変更をコミットします。
		• **confirmed**：実行コンフィギュレーションに変更をコミットします。
		• 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。
		（注） トライアル期間を入力する場合は、commit コマンドを実行して設定を確認します。commit コマンドを実行しないと、トライアル期間後に以前の設定に戻ります。

	コマンドまたはアクション	目的
	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)#	
ステップ 4	**例：** 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)#	このコンフィギュレーション モードでサポートされている機能関連のコマンドを実行します。
ステップ 5	**show configuration** **例：** switch(config-dual-stage-router)# show configuration ! Cached configuration ! router bgp 64515.46 router-id 141.8.139.131	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。 **（注）** 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	**commit** [**confirmed** *seconds*] **例：** 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	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	（任意） **show configuration commit** [**changes**] *commit-id* **例：** 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	コミット関連情報を表示します。 最後の 50 個のコミットまたは予約済みディスク領域に保存されたコミット ファイルのみが保存されます。予約済みディスク領域は20MB です。スイッチをリロードすると、すべてのコミット セッションが削除されます。ただし、コミット ID は削除されません。 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、**show configuration commit changes** *commit-id* コマンドを使用します。

	コマンドまたはアクション	目的
	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 **例：** switch(config-dual-stage)# show configuration commit 1000000003 feature bgp router bgp 64515.46 router-id 141.8.139.131 . . .	指定したコミットの完全な設定を表示するには、**show configuration commit** *commit-id* コマンドを使用します。
ステップ 8	（任意） **save configuration** *filename* **例：** switch(config-dual-stage)# save configuration bootflash:test.cfg	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。 （注） • 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ます。ファイルはブートフラッシュに保存されます。 • 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、**show configuration file***filename* コマンドを実行します。 • 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。
ステップ 9	（任意） **load** *filename* **例：** 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)#	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、**save configuration** *filename* コマンドを使用します。 **save configuration** *filename* 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。
ステップ 10	（任意） **clear configuration** **例：**	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

	コマンドまたはアクション	目的

	`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)#`
		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。

ステップ 11	**end**
	例：
	`switch(config-dual-stage-if)# end`
	`Uncommitted changes found, commit them before exiting (yes/no/cancel)? [cancel]`
		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。
		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。
		• 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。
		• 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。
		• 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。
		（注）
		• 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。
		• 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。

2ステージコンフィギュレーション コミット モードの中止

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

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

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

version 10.1(2) Bios:version
feature bgp


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

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

version 10.1(2) Bios:version
feature bgp

switch#
```

コミット ID の表示

コミットが成功するたびに、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

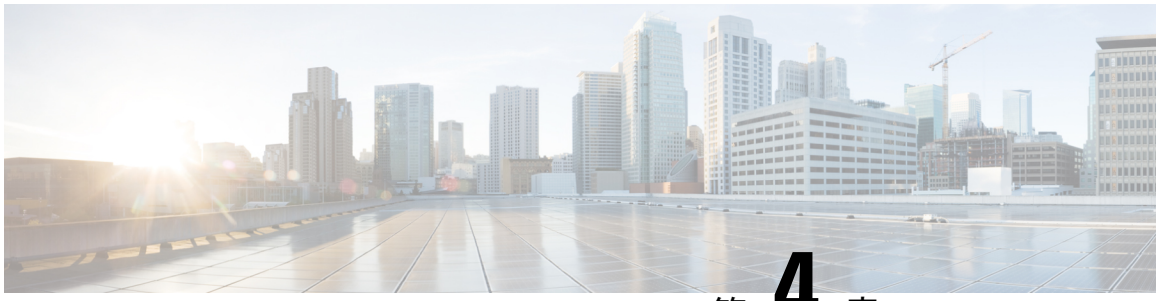
以前に成功したコミットのいずれかに設定をロールバックできます。**rollback configuration** コマンドを使用して、最後の 50 のコミットのいずれかにロールバックします。

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

If there is no configuration, the following message appears:

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



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

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 デバイス タイプ

次のクロックは、一般的な PTP デバイスです。

オーディナリ クロック

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

境界クロック

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

トランスペアレント クロック

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

次の 2 種類のトランスペアレント クロックがあります。

エンドツーエンド トランスペアレント クロック

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

ピアツーピア トランスペアレント クロック

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

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

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

PTP プロセス

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

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

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

マスター/スレーブ階層が確立されると、クロックは次のように同期されます。

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

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>` 設定で使用される送信元 IP アドレスが、BC デバイスの物理または論理インターフェイスでも設定されている必要があります。推奨されるベストプラクティスは、デバイスのループバック インターフェイスを使用することです。
- Cisco Nexus 3500 シリーズ スイッチは、最大 48 の PTP セッションをサポートします。

- 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 はネットワークごとに 1 つのドメインに制限されます。
- PTP 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 として設定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。

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 パラメータを設定できます。

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） **show ptp brief**
8. （任意） **show ptp clock**
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal`	グローバル設定モードを開始します。
ステップ 2	[**no**] **feature ptp** 例： `switch(config) # feature ptp`	デバイス上でPTPをイネーブルまたはディセーブルにします。 （注） スイッチのPTPをイネーブルにしても、各インターフェイスの PTP はイネーブルになりません。
ステップ 3	[**no**] **ptp source** *ip-address* 例： `switch(config) # ptp source 10.2.3.4`	すべての PTP パケットのソース IP アドレスを設定します。 *ip-address*：IPv4 形式。
ステップ 4	（任意） [**no**] **ptp domain** *number* 例： `switch(config) # ptp domain 24`	このクロックで使用するドメイン番号を設定します。PTP ドメインを使用すると、1 つのネットワーク上で、複数の独立した PTP クロッキング サブドメインを使用できます。 *number*：有効な範囲は 0 ～ 128 です。
ステップ 5	（任意） [**no**] **ptp priority1** *value* 例： `switch(config) # ptp priority1 10`	このクロックをアドバタイズするときに使用する priority1 の値を設定します。この値はベスト マスタークロック選択のデフォルトの基準（クロック品質、クロック クラスなど）を上書きします。低い値が優先されます。 *value*：範囲は 0 ～ 255 です。
ステップ 6	（任意） [**no**] **ptp priority2** *value* 例： `switch(config) # ptp priority2 20`	このクロックをアドバタイズするときに使用する priority2 の値を設定します。この値は、デフォルトの基準では同等に一致する 2 台のデバイスのうち、どちらを優先するかを決めるために使用されます。たとえば、priority2 値を使用して、特定のスイッチが他の同等のスイッチよりも優先されるようにすることができます。 *value*：範囲は 0 ～ 255 です。

	コマンドまたはアクション	目的
ステップ 7	（任意） **show ptp brief** 例： `switch(config) # show ptp brief`	PTP のステータスを表示します。
ステップ 8	（任意） **show ptp clock** 例： `switch(config) # show ptp clock`	ローカル クロックのプロパティを表示します。
ステップ 9	**copy running-config startup-config** 例： `switch(config) # copy running-config startup-config`	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

例

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

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

インターフェイスでの PTP の設定

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

始める前に

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

手順の概要

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

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 7	（任意） switch(config-if) # [**no**] **ptp vlan** *vlan-id*	PTP をイネーブルにするインターフェイスの VLAN を指定します。インターフェイスの 1 つの VLAN でイネーブルにできるのは、1 つの PTP のみです。 指定できる範囲は 1 ～ 4094 です。
ステップ 8	（任意） switch(config-if) # **show ptp brief**	PTP のステータスを表示します。
ステップ 9	（任意） switch(config-if) # **show ptp port interface** *interface slot/port*	PTP ポートのステータスを表示します。
ステップ 10	（任意） switch(config-if)# **copy running-config startup-config**	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。

例

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

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# ptp
switch(config-if)# ptp announce interval 3
switch(config-if)# ptp announce timeout 2
switch(config-if)# ptp delay-request minimum interval 4
switch(config-if)# ptp sync interval -1
switch(config-if)# show ptp brief
PTP port status
-----------------------
Port State
------- --------------
Eth2/1 Master
switch(config-if)# show ptp port interface ethernet 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)#
```

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

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config) # [**no**] **feature ptp**	デバイス上で PTP をイネーブルまたはディセーブルにします。 （注） スイッチの PTP をイネーブルにしても、各インターフェイスの PTP はイネーブルになりません。
ステップ 3	switch(config) # [**no**] **ptp source** *ip-address* [**vrf** *vrf*]	すべての PTP パケットのソース IP アドレスを設定します。 *ip-address* には IPv4 形式を使用できます。
ステップ 4	switch(config) # [**no**] **ptp multi-domain**	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**] **ptp domain** *value* **priority** *value*	ドメインおよび優先度の値を指定します。 domain の *value* の範囲は 0 ～ 127 です。domain のデフォルト値は 0 です。 priority の *value* の範囲は 0 ～ 255 です。priority のデフォルト値は 255 です。

	コマンドまたはアクション	目的
ステップ 6	switch(config) # [**no**] **ptp domain** *value* **clock-class-threshold** *value*	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。 domain の *value* の範囲は 0 ～ 127 です。 clock-class-threshold の *value* の範囲は 0 ～ 255 です。 （注） 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。
ステップ 7	switch(config) # [**no**] **ptp domain** *value* **clock-accuracy-threshold** *value*	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。 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 8	switch(config) # [**no**] **ptp multi-domain transition-attributes priority1** *value*	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 *domain transition-attributes priority1* 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 *priority1* 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、*domain transition-attributes priority1* の値で置き換えられます。デフォルト値は 255 です。 transition-attributes priority1 の *value* の範囲は 0 ～ 255 です。
ステップ 9	switch(config) # [**no**] **ptp multi-domain transition-attributes priority2** *value*	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 *domain transition-attributes priority2* 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 *priority2* 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、

	コマンドまたはアクション	目的
		その値がスレーブ インターフェイスの値と異なる場合、*domain transition-attributes priority2* の値で置き換えられます。デフォルト値は 255 です。 transition-attributes priority2 の *value* の範囲は 0 ～ 255 です。
ステップ 10	switch(config-if) # [**no**] **ptp domain** *value*	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

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config) # [**no**] **feature ptp**	デバイス上でPTPをイネーブルまたはディセーブルにします。 （注） スイッチのPTPをイネーブルにしても、各インターフェイスの PTP はイネーブルになりません。
ステップ 3	switch(config) # [**no**] **ptp source** *ip-address* [**vrf** *vrf*]	すべての PTP パケットのソース IP アドレスを設定します。 *ip-address* には IPv4 形式を使用できます。
ステップ 4	switch(config) # **no ptp grandmaster-capable** [*convergence-time*]	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**] **ptp domain** *value* **clock-class-threshold** *value*	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。 domain の *value* の範囲は 0 ～ 127 です。 clock-class-threshold の *value* の範囲は 0 ～ 255 です。

	コマンドまたはアクション	目的
		（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	switch(config) # [**no**] **ptp domain** *value* **clock-accuracy-threshold** *value*	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	switch(config) # **ptp grandmaster-capable**	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-if) # [**no**] **feature ptp**
5. switch(config-if) # [**no**] **ptp cost** *value*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config) # [**no**] **feature ptp**	デバイス上でPTPをイネーブルまたはディセーブルにします。 （注） スイッチのPTPをイネーブルにしても、各インターフェイスの PTP はイネーブルになりません。
ステップ 3	switch(config) # [**no**] **ptp source** *ip-address* [**vrf** *vrf*]	すべての PTP パケットのソース IP アドレスを設定します。 *ip-address* には IPv4 形式を使用できます。
ステップ 4	switch(config-if) # [**no**] **feature ptp**	インターフェイスのPTPをディセーブル、またはイネーブルにします。
ステップ 5	switch(config-if) # [**no**] **ptp cost** *value*	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

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config) # [**no**] **feature ptp**	デバイス上でPTPをイネーブルまたはディセーブルにします。 （注） スイッチのPTPをイネーブルにしても、各インターフェイスの PTP はイネーブルになりません。
ステップ 3	switch(config-if) # **ptp clock-identity** *MAC Address*	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）。

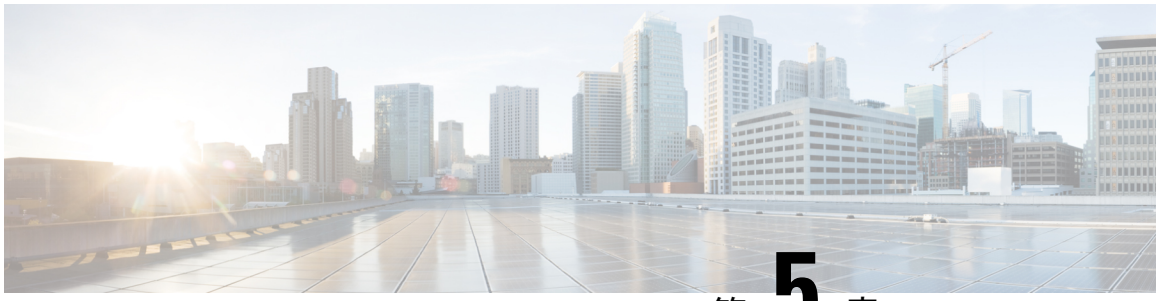
PTP 設定の確認

次のいずれかのコマンドを使用して、設定を確認します。

表 *3 : PTP Show* コマンド

コマンド	目的
show ptp brief	PTP のステータスを表示します。
show ptp clock	ローカルクロックのプロパティ（クロック ID など）を表示します。

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



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

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

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 ロギング	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

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# [**no**] **ntp server** {*ip-address* | *ipv6-address* | *dns-name*} [**key** *key-id*] [**maxpoll** *max-poll*] [**minpoll** *min-poll*] [**prefer**] [**use-vrf** *vrf-name*]	1 つのサーバと 1 つのサーバ アソシエーションを形成します。 NTP サーバとの通信で使用するキーを設定するには、**key** キーワードを使用します。key-id 引数の範囲は 1 ～ 65535 です。 サーバをポーリングする最大および最小の間隔を設定するには、 **maxpoll** および **minpoll** キーワードを使用します。 *max-poll* および *min-poll* 引数の範囲は4ー16（2の累乗として設定されます。つまり、実質的に16ー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）。 これをデバイスの優先 NTP サーバーにするには、**prefer** キーワードを使用します。 指定された VRF を介して通信するように NTP サーバを設定するには、**use-vrf** キーワードを使用します。**vrf-name** 引数として、default、management、または 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）。 （注） NTPサーバとの通信で使用するキーを設定する場合は、そのキーが、デバイス上の信頼できるキーとして存在していることを確認してください。
ステップ 3	switch(config)# [**no**] **ntp peer** {*ip-address* | *ipv6-address* | *dns-name*} [**key** *key-id*] [**maxpoll** *max-poll*] [**minpoll** *min-poll*] [**prefer**] [**use-vrf** *vrf-name*]	1 つのピアと 1 つのピア アソシエーションを形成します。複数のピア アソシエーションを指定できます。 NTP ピアとの通信で使用するキーを設定するには、**key** キーワードを使用します。key-id 引数の範囲は 1 ～ 65535 です。 サーバをポーリングする最大および最小の間隔を設定するには、 **maxpoll** および **minpoll** キーワードを使用します。 *max-poll* および *min-poll* 引数の範囲は4ー16（2の累乗として設定されます。つまり、実質的に 16ー131072 秒）で、デフォルト値はそれ

	コマンドまたはアクション	目的
		ぞれ 6 と 4 です（*maxpoll* デフォルト = 64秒、*minpoll* デフォルト= 16秒）。 これをデバイスの優先 NTP サーバーにするには、**prefer** キーワードを使用します。 指定された VRF を介して通信するように NTP サーバを設定するには、**use-vrf** キーワードを使用します。**vrf-name** 引数として、default、management、または 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）。
ステップ 4	（任意） switch(config)# **show ntp peers**	設定されたサーバおよびピアを表示します。 （注） ドメイン名が解決されるのは、DNS サーバが設定されている場合だけです。
ステップ 5	（任意） switch(config)# **copy running-config startup-config**	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

例

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

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# [**no**] **ntp authentication-key** *number* **md5** *md5-string*	認証キーを定義します。デバイスが時刻源と同期するのは、時刻源がこれらの認証キーのいずれかを持ち、**ntp trusted-key** *number* コマンドによってキー番号が指定されている場合だけです。
ステップ 3	（任意） switch(config)# **show ntp authentication-keys**	設定済みの NTP 認証キーを表示します。
ステップ 4	switch(config)# [**no**]**ntp trusted-key** *number*	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)# **show ntp trusted-keys**	設定済みの NTP の信頼されているキーを表示します。
ステップ 6	switch(config)# [**no**] **ntp authenticate**	NTP 認証機能をイネーブルまたはディセーブルにします。NTP 認証はデフォルトでディセーブルになっています。
ステップ 7	（任意） switch(config)# **show ntp authentication-status**	NTP 認証の状況を表示します。

	コマンドまたはアクション	目的
ステップ 8	（任意） switch(config)# **copy running-config startup-config**	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

例

次に、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

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# [**no**] **ntp access-group** {**peer** | **serve** | **serve-only** | **query-only**} *access-list-name*	NTP のアクセスを制御し、基本の IP アクセス リストを適用するためのアクセス グループを作成または削除します。 アクセス グループのオプションは、次の順序で制限の緩いものから厳しいものへとスキャンされます。

	コマンドまたはアクション	目的
		ただし、ピアに設定された拒否 ACL ルールに NTP が一致した場合、ACL 処理は停止し、次のアクセス グループ オプションへと継続しません。 • **peer** キーワードは、デバイスが時刻要求と NTP 制御クエリーを受信し、アクセス リストで指定されているサーバと同期するようにします。 • **serve** キーワードは、アクセス リストに指定されているサーバからの時刻要求と NTP 制御クエリーをデバイスが受信できるようにしますが、指定されたサーバとは同期しないようにします。 • **serve-only** キーワードは、デバイスがアクセス リストで指定されたサーバからの時刻要求だけを受信するようにします。 • **query-only** キーワードは、デバイスがアクセス リストで指定されたサーバからの NTP 制御クエリーのみを受信するようにします。
ステップ 3	（任意） switch(config)# **show ntp access-groups**	NTP アクセス グループのコンフィギュレーションを表示します。
ステップ 4	（任意） switch(config)# **copy running-config startup-config**	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

例

次に、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

	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。*ip-address* 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

	コマンドまたはアクション	目的
ステップ 1	switch(config)# [**no**] **ntp source-interface** *interface*	すべての NTP パケットに対してソースインターフェイスを設定します。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

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# [**no**] **ntp logging**	重要な NTP イベントでシステム ログを生成することをイネーブルまたはディセーブルにします。NTP ロギングはデフォルトでディセーブルになっています。
ステップ 3	（任意） switch(config)# **show ntp logging-status**	NTP ロギングのコンフィギュレーション状況を表示します。
ステップ 4	（任意） switch(config)# **copy running-config startup-config**	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

例

次に、重要な NTP イベントによってシステム ログを生成するよう、NTP ロギングをイネーブルにする例を示します。

```
switch# 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

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# [**no**] **ntp distribute**	CFS を介して配信される NTP コンフィギュレーションのアップデートをデバイスが受信することを、イネーブルまたはディセーブルにします。
ステップ 3	（任意） switch(config)# **show ntp status**	NTP CFS の配信状況を表示します。
ステップ 4	（任意） switch(config)# **copy running-config startup-config**	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

例

次に、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

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **ntp commit**	ネットワーク内のすべての Cisco NX-OS デバイスに NTP コンフィギュレーションの変更を配信し、CFS ロックを解放します。このコマンドは、保留データベースに対して行われた変更によって、有効なデータベースを上書きします。

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

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

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

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

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

	コマンドまたはアクション	目的
ステップ 1	**show ntp access-groups**	NTP アクセス グループのコンフィギュレーションを表示します。
ステップ 2	**show ntp authentication-keys**	設定済みの NTP 認証キーを表示します。
ステップ 3	**show ntp authentication-status**	NTP 認証の状況を表示します。
ステップ 4	**show ntp logging-status**	NTP のロギング状況を表示します。
ステップ 5	**show ntp peer-status**	すべての NTP サーバおよびピアのステータスを表示します。
ステップ 6	**show ntp peers**	すべての NTP ピアを表示します。
ステップ 7	**show ntp pending**	NTP 用の一時 CFS データベースを表示します。
ステップ 8	**show ntp pending-diff**	保留 CFS データベースと現行の NTP コンフィギュレーションの差異を表示します。
ステップ 9	**show ntp rts-update**	RTS アップデートの状況を表示します。
ステップ 10	**show ntp session status**	NTP CFS 配信セッションの情報を表示します。
ステップ 11	**show ntp source**	設定済みの NTP ソース IP アドレスを表示します。

	コマンドまたはアクション	目的
ステップ 12	**show ntp source-interface**	設定済みの NTP ソース インターフェイスを表示します。
ステップ 13	**show ntp statistics** {**io** | **local** | **memory** | **peer** {**ipaddr** {*ipv4-addr* | *ipv6-addr*} | **name** *peer-name*}}	NTP 統計情報を表示します。
ステップ 14	**show ntp status**	NTP CFS の配信状況を表示します。
ステップ 15	**show ntp trusted-keys**	設定済みの NTP の信頼されているキーを表示します。
ステップ 16	**show running-config ntp**	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
```

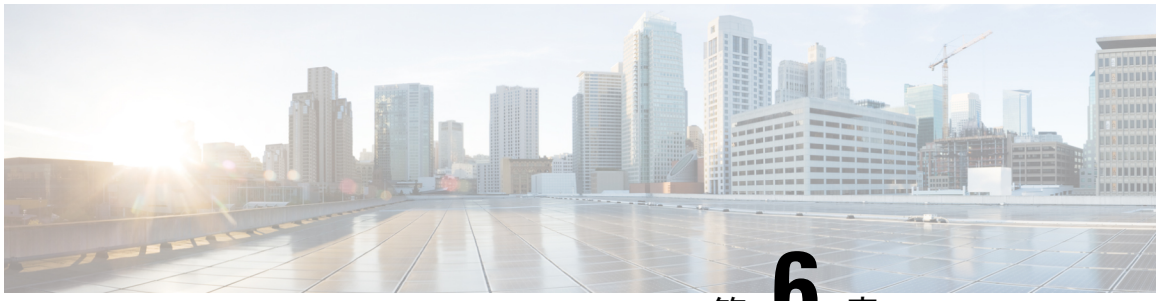
NTP の関連資料

関連項目	マニュアル タイトル
NTP CLI コマンド	*Cisco Nexus 3548* スイッチ *NX-OS* 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

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

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

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

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

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

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 スイッチを設定できます。

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

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 メッセージは、デフォルトでコンソールおよびログ ファイルに記録されます。

システム メッセージ ロギングのデフォルト設定

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

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

パラメータ	デフォルト
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	ディセーブル

システム メッセージ ロギングの設定

ターミナル セッションへのシステム メッセージ ロギングの設定

コンソール、Telnet、およびセキュア シェル セッションに対するシビラティ（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

	Command or Action	Purpose
ステップ 1	switch# **terminal monitor**	コンソールから現在の端末セッションに syslog メッセージをコピーします。
ステップ 2	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。

	Command or Action	Purpose
ステップ 3	switch(config)# **logging console** [*severity-level*]	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。 • 0：緊急 • 1：アラート • 2：クリティカル • 3：エラー • 4：警告 • 5：通知 • 6：情報 • 7：デバッグ 重大度が指定されていない場合、デフォルトの 2 が使用されます。
ステップ 4	(Optional) switch(config)# **no logging console** [*severity-level*]	コンソールへのロギング メッセージをディセーブルにします。
ステップ 5	switch(config)# **logging monitor** [*severity-level*]	指定されたシビラティ（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。 • 0：緊急 • 1：アラート • 2：クリティカル • 3：エラー • 4：警告 • 5：通知 • 6：情報 • 7：デバッグ 重大度が指定されていない場合、デフォルトの 2 が使用されます。

	Command or Action	Purpose
		設定は Telnet および SSH セッションに適用されます。
ステップ 6	(Optional) switch(config)# **no logging monitor** [*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# **show logging console**	コンソール ロギング設定を表示します。
ステップ 8	(Optional) switch# **show logging monitor**	モニタ ロギング設定を表示します。
ステップ 9	(Optional) switch# **copy running-config startup-config**	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

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

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **logging logfile** *logfile-name severity-level* [**size** *bytes*]	システム メッセージを保存するのに使用するログ ファイルの名前と、記録する最小シビラティ（重大度）を設定します。任意で最大ファイルサイズを指定できます。デフォルトの重大度は 5 です。ファイル サイズは 4194304 です。 重大度は 0 ～ 7 の範囲です。 • 0：緊急 • 1：アラート • 2：クリティカル • 3：エラー • 4：警告 • 5：通知 • 6：情報 • 7：デバッグ ファイル サイズは 4096 ～ 10485760 バイトです。
ステップ 3	(Optional) switch(config)# **no logging logfile** [*logfile-name severity-level* [**size** *bytes*]]	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。

	Command or Action	Purpose
ステップ 4	(Optional) switch# **show logging info**	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# **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。

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 メッセージのロギングの設定

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

SUMMARY STEPS

1. 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

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **logging module** [*severity-level*]	指定された重大度またはそれ以上の重大度であるモジュール ログ メッセージをイネーブルにします。重大度は 0 ～ 7 の範囲です。 • 0：緊急 • 1：アラート • 2：クリティカル • 3：エラー • 4：警告 • 5：通知 • 6：情報 • 7：デバッグ 重大度が指定されていない場合、デフォルトの 5 が使用されます。
ステップ 3	switch(config)# **logging level** *facility severity-level*	指定された重大度またはそれ以上の重大度である指定のファシリティからのロギング メッセージをイネーブルにします。重大度は 0 ～ 7 です。 • 0：緊急 • 1：アラート • 2：クリティカル • 3：エラー • 4：警告 • 5：通知 • 6：情報 • 7：デバッグ

	Command or Action	Purpose
		同じ重大度をすべてのファシリティに適用するには、allファシリティを使用します。デフォルト値については、**show logging level** コマンドを参照してください。 **Note** 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。
ステップ 4	(Optional) switch(config)# **no logging module** [*severity-level*]	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) switch(config)# **no logging level** [*facility severity-level*]	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。
ステップ 6	(Optional) switch# **show logging module**	モジュール ロギング設定を表示します。
ステップ 7	(Optional) switch# **show logging level** [*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# **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。

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

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **logging timestamp** {**microseconds** | **milliseconds** | **seconds**}	ロギング タイムスタンプ単位を設定します。デフォルトでは、単位は秒です。
ステップ 3	(Optional) switch(config)# **no logging timestamp** {**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# **show logging timestamp**	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# **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。

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
```

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 サーバーを最大で 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

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**logging server** *host* [*severity-level* [**use-vrf** *vrf-name* [**facility** *facility*]]] **Example:** `switch(config)# logging server 172.28.254.254 5 use-vrf default facility local3`	ホストが syslog メッセージを受信するように設定します。 • *host* 引数は、syslog サーバー ホストのホスト名または IPv4 または IPv6 アドレスを示します。 • *severity-level* 引数は、指定したレベルに syslog サーバー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 51を参照してください。 • **use vrf** *vrf-name* キーワードと引数は、Virtual Routing and Forwarding（VRF）名の *default* または *management* 値を示します。特定の VRF が指定されない場合は、management がデフォルトです。ただし、management が設定されているときは、それがデフォルトであるため、**show-running** コマンドの出力には表示されません。特定の VRF が設定されている場合、**show-running** コマンドの出力には、各サーバーの VRF が表示されます。 **Note** 現在の Cisco Fabric Services（CFS）配信では VRF をサポートしていません。CFS 配信がイネーブルの場合、デフォルト VRF で設定されているロギング サーバーは管理 VRF として配布されます。 • facility 引数は syslog ファシリティ タイプを指定します。デフォルトの発信ファシリティは local7 です。 ファシリティは、使用している Cisco Nexus シリーズ ソフトウェアのコマンド リファレンスに記載されています。

	Command or Action	Purpose
		Note 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。
ステップ 3	(Optional) **no logging server** *host* **Example:** `switch(config)# no logging server 172.28.254.254 5`	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) **show logging server** **Example:** `switch# show logging server`	Syslog サーバー設定を表示します。
ステップ 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	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。 **Note** 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

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

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **logging distribute**	CFS インフラストラクチャを使用して、ネットワーク スイッチへの syslog サーバ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)# **logging commit**	ファブリック内のスイッチへ配布するための Syslog サーバ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)# **logging abort**	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。

	Command or Action	Purpose
ステップ 5	(Optional) switch(config)# **no logging distribute**	CFS インフラストラクチャを使用して、ネットワーク スイッチへの syslog サーバ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。**logging commit** および **logging abort** コマンドを参照してください。デフォルトでは、配布はディセーブルです。
ステップ 6	(Optional) switch# **show logging pending**	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# **show logging pending-diff**	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# **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。

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

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

	Command or Action	Purpose
ステップ 5	switch# **clear logging nvram**	NVRAM の記録されたメッセージをクリアします。

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

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **system ethernet dom polling**	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

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **no system ethernet dom polling**	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

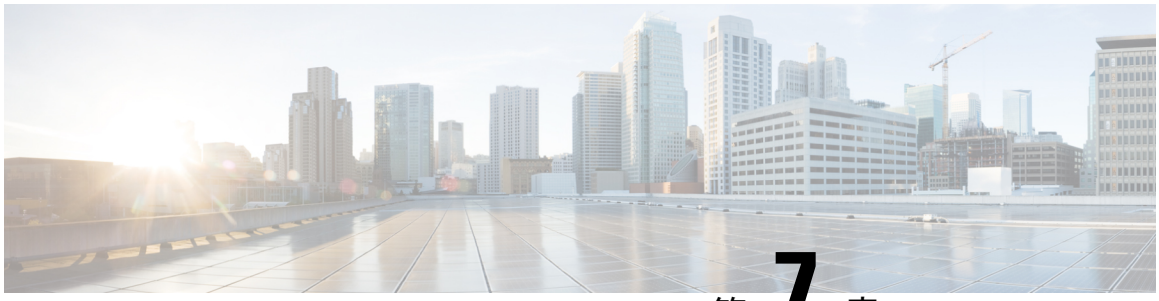
コマンド	目的
show system ethernet dom polling status	トランシーバのデジタル オプティカル モニタリングの定期的なポーリング ステータスを表示します。

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
show logging console	コンソール ロギング設定を表示します。
show logging info	ロギング設定を表示します。
show logging ip access-list cache	IP アクセス リスト キャッシュを表示します。
show logging ip access-list cache detail	IP アクセス リスト キャッシュに関する詳細情報を表示します。

コマンド	目的
show logging ip access-list status	IP アクセス リスト キャッシュのステータスを表示します。
show logging last *number-lines*	ログ ファイルの末尾から指定行数を表示します。
show logging level [*facility*]	ファシリティ ロギング シビラティ（重大度）設定を表示します。
show logging logfile [**start-time** *yyyy mmm dd hh:mm:ss*] [**end-time** *yyyy mmm dd hh:mm:ss*]	ログ ファイルのメッセージを表示します。
show logging module	モジュール ロギング設定を表示します。
show logging monitor	モニタ ロギング設定を表示します。
show logging nvram [**last** *number-lines*]	NVRAM ログのメッセージを表示します。
show logging pending	Syslog サーバーの保留中の配布設定を表示します。
show logging pending-diff	Syslog サーバーの保留中の配布設定の違いを表示します。
show logging server	Syslog サーバー設定を表示します。
show logging session	ロギング セッションのステータスを表示します。
show logging status	ロギング ステータスを表示します。
show logging timestamp	ロギング タイムスタンプ単位設定を表示します。



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

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 宛ての、他のアラート グループからのすべてのクリティカル アラート。	アラートを発信するアラート グループに基づいてコマンドを実行します。
診断	診断によって生成されたイベント。	**show diagnostic result module all detail** **show moduleshow version** **show tech-support platform callhome**

アラートグループ	説明	実行されるコマンド
スーパーバイザ ハードウェア	スーパーバイザ モジュールに関連するイベント。	**show diagnostic result module all detail** **show moduleshow version** **show tech-support platform callhome**
ラインカード ハードウェア	標準またはインテリジェント スイッチング モジュールに関連するイベント。	**show diagnostic result module all detail** **show moduleshow version** **show tech-support platform callhome**
設定	設定に関連した定期的なイベント。	**show version** **show module** **show running-config all** **show startup-config**
システム	装置の動作に重要なソフトウェア システムの障害によって生成されるイベント	**show system redundancy status** **show tech-support**
環境	電源、ファン、および温度アラームなどの環境検知要素に関連するイベント。	**show environment** **show logging last 1000** **show module show version** **show tech-support platform callhome**
インベントリ	装置がコールド ブートした場合、またはFRU の取り付けまたは取り外しを行った場合に示されるコンポーネント ステータス。このアラートは重要でないイベントであり、情報はステータスおよび使用権に使用されます。	**show module** **show version** **show license usage** **show inventory** **show sprom all** **show system uptime**

Smart Call Home は、syslog のシビラティ（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 *YYYY-MM-DD HH:MM:SS GMT+HH:MM*	/aml/header/time
メッセージ名	メッセージの名前。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	メッセージを生成したエンドデバイスの固有デバイス識別情報（UDI）。メッセージがデバイスに対して固有でない場合は、このフィールドを空にする必要があります。形式は、*type@Sid@serial*。 • *type* は、バックプレーン IDPROM からの製品の型番。 • @ は区切り文字です。 • *Sid* は C で、シリアル ID をシャーシ シリアル番号として特定します。 • *serial* は、Sid フィールドによって識別される番号です。 例：WS-C6509@C@12345678	/aml/ header/deviceID
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	デバイスからメッセージが生成された場合、これはデバイスの Unique Device Identifier（UDI）フォーマットです。 形式は、*type@Sid@serial*。 • *type* は、バックプレーン IDPROM からの製品の型番。 • @ は区切り文字です。 • *Sid* は C で、シリアル ID をシャーシ シリアル番号として特定します。 • *serial* は、Sid フィールドによって識別される番号です。 例：WS-C6509@C@12345678	/aml/header/serverID
メッセージの説明	エラーを説明するショート テキスト。	/aml/body/msgDesc
デバイス名	イベントが発生したノード（デバイスのホスト名）。	/aml/body/sysName
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

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

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **snmp-server contact** *sys-contact*	SNMP sysContact を設定します。
ステップ 3	switch(config)# **callhome**	Smart Call Home コンフィギュレーション モードを開始します。
ステップ 4	switch(config-callhome)# **email-contact** *email-address*	スイッチの担当者の電子メール アドレスを設定します。 *email-address* には、電子メール アドレスの形式で、最大 255 の英数字を使用できます。 **Note** 任意の有効な E メール アドレスを使用できます。アドレスには、空白を含めることはできません。
ステップ 5	switch(config-callhome)# **phone-contact** *international-phone-number*	デバイスの担当者の電話番号を国際電話フォーマットで設定します。*international-phone-number* は、最大 17 文字の英数字で、国際電話フォーマットにする必要があります。

	Command or Action	Purpose
		Note 電話番号には、空白を含めることはできません。番号の前にプラス（+）プレフィックスを使用します。
ステップ 6	switch(config-callhome)# **streetaddress** *address*	スイッチの主担当者の住所を設定します。 *address* には、最大 255 の英数字を使用できます。スペースを使用できます。
ステップ 7	(Optional) switch(config-callhome)# **contract-id** *contract-number*	サービス契約からこのスイッチの契約番号を設定します。 *contract-number* には最大 255 の英数字を使用できます。
ステップ 8	(Optional) switch(config-callhome)# **customer-id** *customer-number*	サービス契約からこのスイッチのカスタマー番号を設定します。 *customer-number* には最大 255 の英数字を使用できます。
ステップ 9	(Optional) switch(config-callhome)# **site-id** *site-number*	このスイッチのサイト番号を設定します。 *site-number* は、最大 255 文字の英数字を自由なフォーマットで指定できます。
ステップ 10	(Optional) switch(config-callhome)# **switch-priority** *number*	このスイッチのスイッチ プライオリティを設定します。 指定できる範囲は 0 ～ 7 です。0 は最高のプライオリティを、7は最低のプライオリティを示します。デフォルト値は 7 です。 **Note** 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。
ステップ 11	(Optional) switch# **show callhome**	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)# **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、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

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **callhome**	Smart Call Home コンフィギュレーション モードを開始します。
ステップ 3	switch(config-callhome)# **destination-profile** {**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**	新しい宛先プロファイルを作成し、そのプロファイルのメッセージ フォーマットを設定します。プロファイル名は、最大 31 文字の英数字で指定できます。

	Command or Action	Purpose
	{**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**}}}	このコマンドについての詳細は、プラットフォームのコマンド リファレンスを参照してください。
ステップ 4	(Optional) switch# **show callhome destination-profile** [**profile** *name*]	1 つまたは複数の宛先プロファイルに関する情報を表示します。
ステップ 5	(Optional) 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、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

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **callhome**	Smart Call Home コンフィギュレーション モードを開始します。
ステップ 3	switch(config-callhome)# **destination-profile** {*name* | **full-txt-destination** | **short-txt-destination**} **email-addr** *address*	ユーザ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	**destination-profile** {*name* | **full-txt-destination** | **short-txt-destination**} **message-level** *number*	この宛先プロファイルの Smart Call Home メッセージのシビラティ（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。*number* 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)# **destination-profile** {*name* | **full-txt-destination** | **short-txt-destination**} **message-size** *number*	この宛先プロファイルの最大メッセージサイズを設定します。full-txt-destination の値の範囲は 0 ～ 5000000 で、デフォルトは 2500000 です。short-txt-destination の値の範囲は 0 ～ 100000 で、デフォルトは 4000 です。CiscoTAC-1 では、値は 5000000 で、これは変更不可能です。
ステップ 6	(Optional) switch# **show callhome destination-profile** [**profile** *name*]	1 つまたは複数の宛先プロファイルに関する情報を表示します。
ステップ 7	(Optional) switch(config)# **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、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

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **callhome**	Smart Call Home コンフィギュレーション モードを開始します。
ステップ 3	switch(config-callhome)# **destination-profile** *name* **alert-group** {**All** | **Cisco-TAC** | **Configuration** | **Diagnostic** | **Environmental** | **Inventory** | **License** | **Linecard-Hardware** | **Supervisor-Hardware** | **Syslog-group-port** | **System** | **Test**}	アラート グループをこの宛先プロファイルにアソシエートします。キーワード **All** を使用して、すべてのアラート グループをこの宛先プロファイルにアソシエートします。
ステップ 4	(Optional) switch# **show callhome destination-profile** [**profile** *name*]	1 つまたは複数の宛先プロファイルに関する情報を表示します。
ステップ 5	(Optional) 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、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

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **callhome**	Smart Call Home コンフィギュレーション モードを開始します。
ステップ 3	switch(config-callhome)# **alert-group** {**Configuration** | **Diagnostic** | **Environmental** | **Inventory** | **License** | **Linecard-Hardware** | **Supervisor-Hardware** | **Syslog-group-port** | **System** | **Test**} **user-def-cmd** *show-cmd*	**show** コマンド出力を、このアラート グループに送信された Call Home メッセージに追加します。有効な **show** コマンドだけが受け入れられます。 **Note** CiscoTAC-1 宛先プロファイルには、ユーザー定義の **show** コマンドを追加できません。

	Command or Action	Purpose
ステップ 4	(Optional) switch# **show callhome user-def-cmds**	アラート グループに追加されたすべてのユーザー定義 **show** コマンドに関する情報を表示します。
ステップ 5	(Optional) 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、**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

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **callhome**	Smart Call Home コンフィギュレーション モードを開始します。

	Command or Action	Purpose
ステップ 3	switch(config-callhome)# **transport email smtp-server** *ip-address* [**port** *number*] [**use-vrf** *vrf-name*]	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)# **transport email from** *email-address*	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)# **transport email reply-to** *email-address*	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# **show callhome transport-email**	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)# **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、Smart Call Home メッセージの電子メール オプションを設定する例を示します。

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

What to do next

定期的なインベントリ通知を設定します。

定期的なインベントリ通知の設定

ハードウェアのインベントリ情報に加えて、デバイス上で現在イネーブルになっているすべてのソフトウェア サービスおよび実行中のすべてのソフトウェア サービスのインベントリに関するメッセージを定期的に送信するようにスイッチを設定できます。スイッチは 2 つの Smart Call Home 通知（定期的な設定メッセージと定期的なインベントリ メッセージ）を生成します。

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **callhome**	Smart Call Home コンフィギュレーション モードを開始します。
ステップ 3	switch(config-callhome)# **periodic-inventory notification** [**interval** *days*] [**timeofday** *time*]	定期的なインベントリ メッセージを設定します。 **interval** *days* の範囲は 1 ～ 30 日です。 デフォルトは 7 日です。 **timeofday** *time* は HH:MM の形式です。
ステップ 4	(Optional) switch# **show callhome**	Smart Call Home に関する情報を表示します。
ステップ 5	(Optional) 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、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

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **callhome**	Smart Call Home コンフィギュレーション モードを開始します。
ステップ 3	switch(config-callhome) # **no duplicate-message throttle**	Smart Call Home の重複メッセージ抑制をディセーブルにします。 重複メッセージ抑制はデフォルトでイネーブルです。
ステップ 4	（任意） switch(config)# **copy running-config startup-config**	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

例

次に、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

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **callhome**	Smart Call Home コンフィギュレーション モードを開始します。
ステップ 3	switch(config-callhome) # [**no**] **enable**	Smart Call Home をイネーブルまたはディセーブルにします。 Smart Call Home は、デフォルトでディセーブルです。
ステップ 4	（任意） switch(config)# **copy running-config startup-config**	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

例

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

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

次のタスク

任意でテスト メッセージを生成します。

Smart Call Home 設定のテスト

始める前に

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

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **callhome**	Smart Call Home コンフィギュレーション モードを開始します。
ステップ 3	switch(config-callhome) # **callhome send diagnostic**	設定されたすべての宛先に指定の Smart Call Home テスト メッセージを送信します。
ステップ 4	switch(config-callhome) # **callhome test**	設定されたすべての宛先にテスト メッセージを送信します。
ステップ 5	（任意） switch(config)# **copy running-config startup-config**	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

例

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

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

Smart Call Home 設定の確認

次のいずれかのコマンドを使用して、設定を確認します。

コマンド	目的
show callhome	Smart Call Home のステータスを表示します。
show callhome destination-profile *name*	1 つまたは複数の Smart Call Home 宛先プロファイルを表示します。

コマンド	目的
show callhome pending-diff	保留中の Smart Call Home 設定と実行中の Smart Call Home 設定の違いを表示します。
show callhome status	Smart Call Home ステータスを表示します。
show callhome transport-email	Smart Call Home の電子メール設定を表示します。
show callhome user-def-cmds	任意のアラート グループに追加された CLI コマンドを表示します。
show running-config [**callhome** | **callhome-all**]	Smart Call Home の実行コンフィギュレーションを表示します。
show startup-config callhome	Smart Call Home のスタートアップ コンフィギュレーションを表示します。
show tech-support callhome	Smart Call Home のテクニカル サポート出力を表示します。

フル テキスト形式での syslog アラート通知の例

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

```
source:MDS9000
Switch Priority:7
Device Id:WS-C6509@C@FG@07120011
Customer Id:Example.com
Contract Id:123
Site Id:San Jose
Server Id:WS-C6509@C@FG@07120011
Time of Event: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

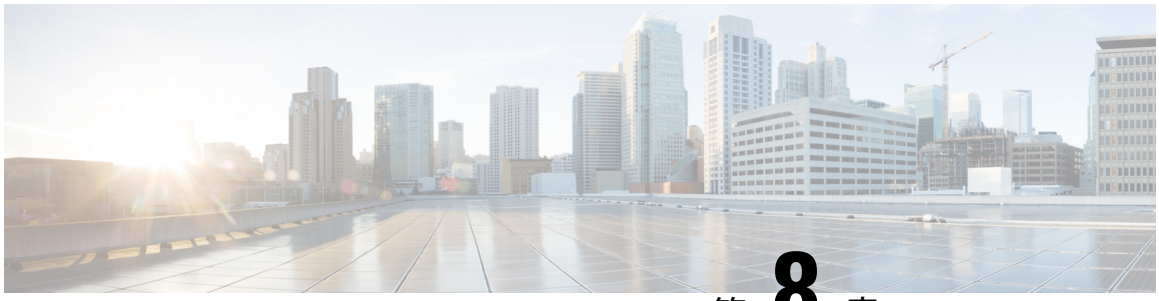
次の例では、Syslog ポート アラート グループ通知の XML を示します。

```
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>abcdefg12345</ch:ContractId>
```

```
<ch:DeviceId>WS-C6509@C@69000101</ch:DeviceId>
</ch:ContractData>
<ch:SystemInfo>
<ch:Name>Router</ch:Name>
<ch:Contact>
</ch:Contact>
<ch:ContactEmail>user@example.com</ch:ContactEmail>
<ch:ContactPhoneNumber>+1-408-555-1212</ch:ContactPhoneNumber>
<ch:StreetAddress>#1234 Any Street, Any City, Any State, 12345
</ch:StreetAddress>
</ch:SystemInfo>
</ch:CustomerData>
<ch:Device>
<rme:Chassis xmlns:rme="http://www.example.com/rme/4.0">
<rme:Model>WS-C6509</rme:Model>
<rme:HardwareVersion>1.0</rme:HardwareVersion>
<rme:SerialNumber>69000101</rme:SerialNumber>
<rme:AdditionalInformation>
<rme:AD name="PartNumber" value="73-3438-03 01" />
<rme:AD name="SoftwareVersion" value="4.0(20080421:012711)" />
</rme:AdditionalInformation>
</rme:Chassis>
</ch:Device>
</ch:Call Home>
</aml-block:Content>
<aml-block:Attachments>
<aml-block:Attachment type="inline">
<aml-block:Name>show logging</aml-block:Name>
<aml-block:Data encoding="plain">
<![CDATA[Syslog logging: enabled (0 messages dropped, 0 messages
rate-limited, 0 flushes, 0 overruns, xml disabled, filtering disabled)
    Console logging: level debugging, 53 messages logged, xml disabled,
filtering disabled    Monitor logging: level debugging, 0 messages logged,
xml disabled,filtering disabled    Buffer logging: level debugging,
53 messages logged, xml disabled,      filtering disabled    Exception
Logging: size (4096 bytes)    Count and timestamp logging messages: disabled
    Trap logging: level informational, 72 message lines logged
Log Buffer (8192 bytes):
00:00:54: curr is 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

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

	Command or Action	Purpose
ステップ 1	switch# **configure session** *name*	コンフィギュレーションセッションを作成し、セッション コンフィギュレーション モードを開始します。名前は任意の英数字ストリングです。 セッションの内容を表示します。
ステップ 2	(Optional) switch(config-s)# **show configuration session** [*name*]	セッションの内容を表示します。
ステップ 3	(Optional) switch(config-s)# **save** *location*	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

	Command or Action	Purpose
ステップ 1	switch# **configure session** *name*	コンフィギュレーションセッションを作成し、セッション コンフィギュレーション モードを開始します。名前は任意の英数字ストリングです。
ステップ 2	switch(config-s)# **ip access-list** *name*	ACL を作成します。
ステップ 3	(Optional) switch(config-s-acl)# **permit** *protocol source destination*	ACL に許可文を追加します。
ステップ 4	switch(config-s-acl)# **interface** *interface-type number*	インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	switch(config-s-if)# **ip port access-group** *name* **in**	インターフェイスにポート アクセス グループを追加します。
ステップ 6	(Optional) switch# **show configuration session** [*name*]	セッションの内容を表示します。

セッションの確認

セッションを確認するには、セッション モードで次のコマンドを使用します。

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

セッションのコミット

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

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

セッションの保存

セッションを保存するには、セッション モードで次のコマンドを使用します。

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

セッションの廃棄

セッションを廃棄するには、セッション モードで次のコマンドを使用します。

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

Session Manager のコンフィギュレーション例

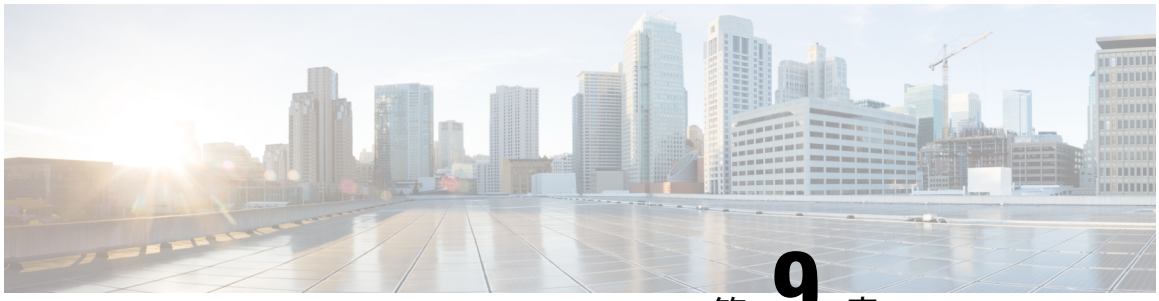
次に、ACL 用のコンフィギュレーション セッションを作成する例を示します。

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

Session Manager 設定の確認

Session Manager の設定情報を確認するには、次の作業のいずれかを行います。

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



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

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コマンドや中断を伴うコマンド（例：**copy bootflash:** *file* **ftp:***URI*、**write erase**、その他類似のコマンド）が指定されていないことを確認してください。

スケジューラのデフォルト設定

表 *16*：コマンド スケジューラのパラメータのデフォルト

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

スケジューラの設定

スケジューラのイネーブル化

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

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config) # **feature scheduler**	スケジューラをイネーブルにします。
ステップ 3	（任意） switch(config) # **show scheduler config**	スケジューラ設定を表示します。
ステップ 4	（任意） switch(config)# **copy running-config startup-config**	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

例

次に、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

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config) # **scheduler logfile size** *value*	スケジューラ ログ ファイル サイズをキロバイト（KB）で定義します。 範囲は 16 ～ 1024 です。デフォルトのログ 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)# **copy running-config startup-config**	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

例

次に、スケジューラ 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

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config) # **scheduler aaa-authentication password** [**0** | **7**] *password*	現在ログインしているユーザ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、**0** を入力します。 暗号化されたパスワードを設定するには、**7** を入力します。
ステップ 3	switch(config) # **scheduler aaa-authentication username** *name* **password** [**0** | **7**] *password*	リモート ユーザーのクリア テキスト パスワードを設定します。
ステップ 4	（任意） switch(config) # **show running-config | include "scheduler aaa-authentication"**	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） switch(config)# **copy running-config startup-config**	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

例

次に、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

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config) # **scheduler job name** *name*	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。 *name* は 31 文字までに制限されています。
ステップ 3	switch(config-job) # *command1* **;** [*command2* **;***command3* **;** ...	特定のジョブに対応するコマンドシーケンスを定義します。複数のコマンドは、スペースとセミコロンで（;）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) # **show scheduler job** [*name*]	ジョブ情報を表示します。 *name* は 31 文字までに制限されています。
ステップ 5	（任意） switch(config-job) # **copy running-config startup-config**	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

例

次の例は、次の方法を示します。

- 「backup-cfg」という名前のスケジューラ ジョブを作成示します。

- 実行中の構成をブートフラッシュ上のファイルに保存します。
- 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

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config) # **no scheduler job name** *name*	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。 *name* は 31 文字までに制限されています。
ステップ 3	（任意） switch(config-job) # **show scheduler job** [*name*]	ジョブ情報を表示します。
ステップ 4	（任意） switch(config-job) # **copy running-config startup-config**	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

例

次に、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

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

	コマンドまたはアクション	目的
ステップ 2	switch(config) # **scheduler schedule name** *name*	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。 *name* は 31 文字までに制限されています。
ステップ 3	switch(config-schedule) # **job name** *name*	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。 *name* は 31 文字までに制限されています。
ステップ 4	switch(config-schedule) # **time daily** *time*	ジョブが毎日 HH:MM の形式で指定された時刻に開始することを意味します。
ステップ 5	switch(config-schedule) # **time weekly** [[*day-of-week*:] *HH*:] *MM*	ジョブが週の指定された曜日に開始することを意味します。 曜日は整数（たとえば、日曜日は **1**、月曜日は **2**）または略語（たとえば、**sun**、 **mon**）で表します。 引数全体の最大長は 10 文字です。
ステップ 6	switch(config-schedule) # **time monthly** [[*day-of-month*:] *HH*:] *MM*	ジョブが月の特定の日に開始することを意味します。 29、30 または 31 のいずれかを指定した場合、そのジョブは各月の最終日に開始されます。
ステップ 7	switch(config-schedule) # **time start** { **now repeat** *repeat-interval* | *delta-time* [**repeat** *repeat-interval*]}	ジョブが定期的に開始することを意味します。 start-time の形式は [[[[yyyy:]mmm:]dd:]HH]:MM です。 • *delta-time*：スケジュールの設定後、ジョブの開始までの待機時間を指定します。 • **now**：ジョブが今から 2 分後に開始することを指定します。 • **repeat** *repeat-interval*：ジョブを反復する回数を指定します。
ステップ 8	（任意） switch(config-schedule) # **show scheduler config**	スケジューラの情報を表示します。
ステップ 9	（任意） switch(config-schedule) # **copy running-config startup-config**	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

例

次に、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

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config) # **clear scheduler logfile**	スケジューラ ログ ファイルを消去します。

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

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config) # **no feature scheduler**	スケジューラをディセーブルにします。
ステップ 3	（任意） switch(config) # **show scheduler config**	スケジューラ設定を表示します。
ステップ 4	（任意） switch(config)# **copy running-config startup-config**	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

例

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

スケジューラの設定例

スケジューラ ジョブの作成

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

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

スケジューラ ジョブのスケジューリング

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

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

ジョブ スケジュールの表示

次に、ジョブ スケジュールを表示する例を示します。

```
switch# show scheduler schedule
Schedule Name       : daily
---------------------------
User Name            : admin
Schedule Type        : Run every day at 1 Hrs 00 Mins
Last Execution Time  : Fri Jan 2 1:00:00 2009
Last Completion Time: Fri Jan 2 1:00:01 2009
Execution count      : 2
----------------------------------------------
     Job Name            Last Execution Status
----------------------------------------------
back-cfg                            Success (0)
switch(config)#
```

スケジューラ ジョブの実行結果の表示

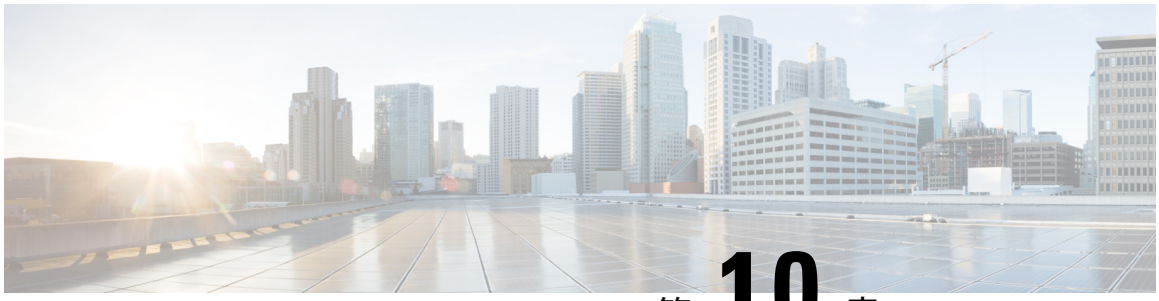
次に、スケジューラによって実行されたスケジューラ ジョブの結果を表示する例を示します。

```
switch# show scheduler logfile
Job Name       : back-cfg                          Job Status: Failed (1)
```

```
Schedule Name  : daily                              User Name : admin
Completion time: Fri Jan 1  1:00:01 2009
------------------------------ Job Output ---------------------------------
`cli var name timestamp 2009-01-01-01.00.00`
`copy running-config bootflash:/$(HOSTNAME)-cfg.$(timestamp)`
`copy bootflash:/switch-cfg.2009-01-01-01.00.00 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#
```

スケジューラの標準

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



第 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

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、または HMAC-SHA	未対応	Hash-Based Message Authentication Code（HMAC）メッセージ ダイジェスト 5（MD5）アルゴリズムまたは HMAC Secure Hash Algorithm（SHA）アルゴリズムに基づいて認証します。
v3	authPriv	HMAC-MD5、または HMAC-SHA	DES	HMAC-MD5 アルゴリズムまたは HMAC-SHA アルゴリズムに基づいて認証します。データ暗号規格（DES）の 56 ビット暗号化、および暗号ブロック連鎖（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

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

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

Cisco NX-OS は、次のようにユーザ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 を使用してユーザを作成または削除すると、SNMP と CLI の両方でユーザが作成または削除されます。
- ユーザとロールの対応関係の変更は、SNMP と CLI で同期化されます。
- ロール変更（CLI からの削除または変更）は、SNMP と同期化されます。

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

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、 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。

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 ユーザーを設定するために使用するコマンドは、Cisco IOS でユーザーを設定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. switch(config)# **snmp-server user** *name* [**auth** {**md5** | **sha**} *passphrase* [**auto**] [**priv** [**aes-128**] *passphrase*] [**engineID** *id*] [**localizedkey**]]
3. (Optional) switch# **show snmp user**
4. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	switch(config)# **snmp-server user** *name* [**auth** {**md5** | **sha**} *passphrase* [**auto**] [**priv** [**aes-128**] *passphrase*] [**engineID** *id*] [**localizedkey**]] **Example:** `switch(config)# snmp-server user Admin auth sha abcd1234 priv abcdefgh`	認証およびプライバシー パラメータのある SNMP ユーザを設定します。 パスフレーズには最大 64 文字の英数字を使用できます。大文字と小文字が区別されます。 **localizedkey** キーワードを使用する場合は、パスフレーズに大文字と小文字を区別した英数字を 130 文字まで使用できます。 engineID の形式は、12 桁のコロンで区切った 10 進数字です。
ステップ 3	(Optional) switch# **show snmp user** **Example:** `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。

	Command or Action	Purpose
ステップ 4	(Optional) **copy running-config startup-config** **Example:** `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 ユーザーを設定する例を示します。

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

SNMP メッセージ暗号化の適用

着信要求に認証または暗号化が必要となるよう SNMP を設定できます。デフォルトでは、SNMP エージェントは認証および暗号化を行わないでも SNMPv3 メッセージを受け付けます。プライバシーを適用する場合、Cisco NX-OS は、**noAuthNoPriv** または **authNoPriv** のいずれかのセキュリティ レベル パラメータを使用するすべての SNMPv3 PDU 要求に対して、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)# **snmp-server user** *name* **enforcePriv**	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)# **snmp-server globalEnforcePriv**	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)# **snmp-server user** *name group*	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)# **snmp-server community** *name group* {**ro** | **rw**}	SNMP コミュニティ ストリングを作成します。

SNMP 要求のフィルタリング

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

ACL は次のパラメータで作成します。

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

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

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

IPv4 または IPv6 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
switch(config)# **snmp-server community** *name* [**use-ipv4acl** *ipv4acl-name*] [**use-ipv6acl** *ipv6acl-name*] `switch(config)# snmp-server community public use-ipv4acl myacl`	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)# **snmp-server host** *ip-address* **traps version 1** *community* [**udp_port** *number*]	SNMPv1 トラップのホスト レシーバを設定します。*ip-address* は IPv4 または IPv6 アドレスを使用できます。コミュニティは、最大 255 文字の英数字で指定できます。UDP ポート番号の範囲は 0 ～ 65535 です。

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

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

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

コマンド	目的
switch(config)# **snmp-server host** *ip-address* {**traps** | **informs**} **version 3** {**auth** | **noauth** | **priv**} *username* [**udp_port** *number*]	SNMPv2c トラップまたはインフォームのホスト レシーバを設定します。*ip-address* は IPv4 または IPv6 アドレスを使用できます。ユーザー名は、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 にエントリが追加されます。

（注） VRF 到達可能性またはフィルタリング オプションを設定する前に、ホストを設定する必要があります。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch# **snmp-server host** *ip-address* **use-vrf** *vrf_name* [**udp_port** *number*]	特定の VRF を使用してホスト レシーバと通信するように SNMP を設定します。IP アドレスは、IPv4 または IPv6 アドレスを使用できます。VRF 名には最大 255 の英数字を使用できます。UDP ポート番号の範囲は 0 ～ 65535 です。このコマンドによって、

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

例

次に、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

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **snmp-server host** *ip-address* **filter-vrf** *vrf_name* [**udp_port** *number*]	設定された VRF に基づいて、通知ホスト レシーバへの通知をフィルタリングします。IP アドレスは、IPv4 または IPv6 アドレスを使用できます。VRF 名には最大 255 の英数字を使用できます。UDP ポート番号の範囲は 0 ～ 65535 です。 このコマンドによって、CISCO-SNMP-TARGET-EXT-MB の ExtSnmpTargetVrfTable にエントリが追加されます。

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

例

次に、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

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

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

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

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

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

リンクの通知の設定

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

- cieLinkDown：シスコ拡張リンク ステート ダウン通知をイネーブルにします。
- cieLinkUp：シスコ拡張リンク ステート アップ通知をイネーブルにします。
- cisco-xcvr-mon-status-chg：シスコ インターフェイス トランシーバ モニター 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

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**snmp-server enable traps link** [**cieLinkDown**	**cieLinkUp**	**cisco-xcvr-mon-status-chg**	**delayed-link-state-change**]	**extended-linkUp**	**extended-linkDown**	**linkDown**	**linkUp**] 例： `switch(config)# snmp-server enable traps link cieLinkDown`	リンク SNMP 通知をイネーブルにします。

インターフェイスでのリンク通知のディセーブル化

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

手順の概要

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

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

TCP での SNMP に対するワンタイム認証のイネーブル化

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

コマンド	目的
switch(config)# **snmp-server tcp-session** [**auth**]	TCP セッション上で SNMP に対するワンタイム認証をイネーブルにします。この機能はデフォルトで無効に設定されています。

SNMP スイッチの連絡先および場所の情報の割り当て

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

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

	Command or Action	Purpose
ステップ 1	switch# **configuration terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **snmp-server contact** *name*	sysContact（SNMP 担当者名）を設定します。
ステップ 3	switch(config)# **snmp-server location** *name*	sysLocation（SNMP ロケーション）を設定します。
ステップ 4	(Optional) switch# **show snmp**	1 つまたは複数の宛先プロファイルに関する情報を表示します。
ステップ 5	(Optional) switch# **copy running-config startup-config**	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

	Command or Action	Purpose
ステップ 1	switch# **configuration terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **snmp-server context** *context-name* [**instance** *instance-name*] [**vrf** *vrf-name*] [**topology** *topology-name*]	SNMP コンテキストをプロトコル インスタンス、VRF、またはトポロジにマッピングします。名前には最大 32 の英数字を使用できます。
ステップ 3	switch(config)# **snmp-server mib community-map** *community-name* **context** *context-name*	SNMPv2c コミュニティを SNMP コンテキストにマッピングします。名前には最大 32 の英数字を使用できます。
ステップ 4	(Optional) switch(config)# **no snmp-server context** *context-name* [**instance** *instance-name*] [**vrf** *vrf-name*] [**topology** *topology-name*]	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。

	Command or Action	Purpose
		Note コンテキスト マッピングを削除する目的で、インスタンス、VRF、またはトポロジを入力しないでください。**instance**、**vrf**、または **topology** キーワードを使用すると、コンテキストとゼロ長ストリング間のマッピングが設定されます。

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

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

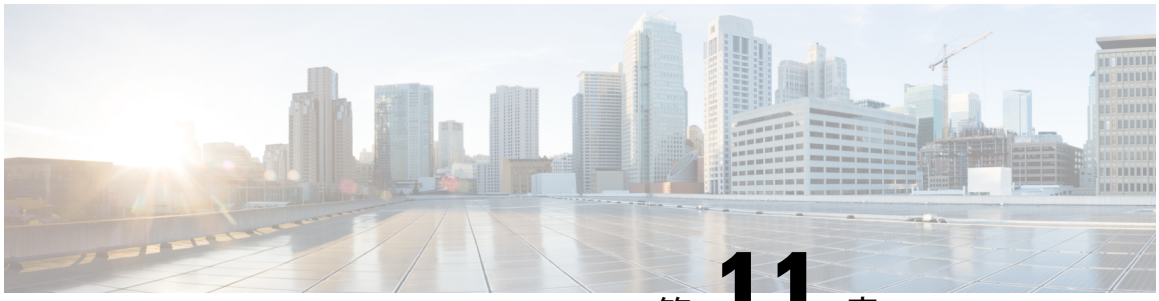
ステップ 2	switch(config) # **no snmp-server protocol enable** 例： `no snmp-server protocol enable`	SNMP をディセーブルにします。 SNMP は、デフォルトでディセーブルになっています。

SNMP 設定の確認

SNMP 設定情報を表示するには、次の作業を行います。

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

コマンド	目的
show snmp trap	イネーブルまたはディセーブルである SNMP 通知を表示します。
show snmp user	SNMPv3 ユーザを表示します。



第 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

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

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

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

RMON アラーム

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

アラームを作成する場合、次のパラメータを指定します。

- モニタリングする MIB オブジェクト

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

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*] [**storagetype** *type*]
4. (Optional) switch# **show rmon** {**alarms** | **hcalarms**}
5. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

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

	Command or Action	Purpose
ステップ 2	switch(config)# **rmon alarm** *index mib-object sample-interval* {**absolute** | **delta**} **rising-threshold** *value* [*event-index*] **falling-threshold** *value* [*event-index*] [**owner** *name*]	RMON アラームを作成します。値の範囲は -2147483647 ～ 2147483647 です。オーナー名は任意の英数字ストリングです。
ステップ 3	switch(config)# **rmon hcalarm** *index mib-object sample-interval* {**absolute** | **delta**} **rising-threshold-high** *value* **rising-threshold-low** *value* [*event-index*] **falling-threshold-high** *value* **falling-threshold-low** *value* [*event-index*] [**owner** *name*] [**storagetype** *type*]	RMON 高容量アラームを作成します。値の範囲は -2147483647 ～ 2147483647 です。オーナー名は任意の英数字ストリングです。 ストレージ タイプの範囲は 1 ～ 5 です。
ステップ 4	(Optional) switch# **show rmon** {**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# **copy running-config startup-config**	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。

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

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **rmon event** *index* [**description** *string*] [**log**] [**trap**] [**owner** *name*]	RMONイベントを設定します。説明のストリングおよびオーナー名は、任意の英数字ストリングです。
ステップ 3	(Optional) switch(config)# **show rmon** {**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# **copy running-config startup-config**	この設定変更を保存します。

RMON 設定の確認

RMON の設定情報を確認するには、次のコマンドを使用します。

コマンド	目的
show rmon alarms	RMON アラームに関する情報を表示します。
show rmon events	RMON イベントに関する情報を表示します。
show rmon hcalarms	RMON高容量アラームに関する情報を表示します。
show rmon logs	RMON ログに関する情報を表示します。

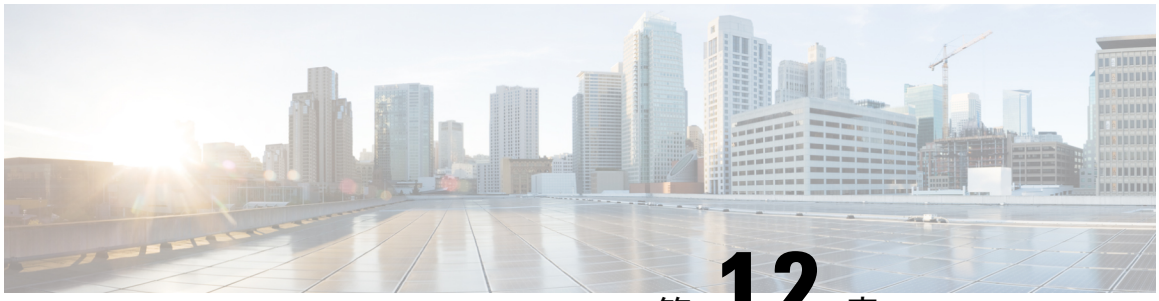
デフォルトの RMON 設定

次の表に、RMON パラメータのデフォルト設定を示します。

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

パラメータ	デフォルト
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

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。
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。

診断	説明
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。
転送エンジン	転送エンジン ASIC をテストします。

診断	説明
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

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **diagnostic bootup level** [**complete** | **bypass**]	デバイスの起動時に診断を実行するよう起動時診断レベルを次のように設定します。 • **complete**：すべての起動時診断を実行します。これはデフォルト値です。 • **bypass**：起動時診断を実行しません。
ステップ 3	(Optional) switch# **show diagnostic bootup level**	現在、スイッチで実行されている起動時診断レベル（bypass または complete）を表示します。

Example

次に、完全な診断を実行するよう起動時診断レベルを設定する例を示します。

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

オンライン診断設定の確認

オンライン診断の設定情報を確認するには、次のコマンドを使用します。

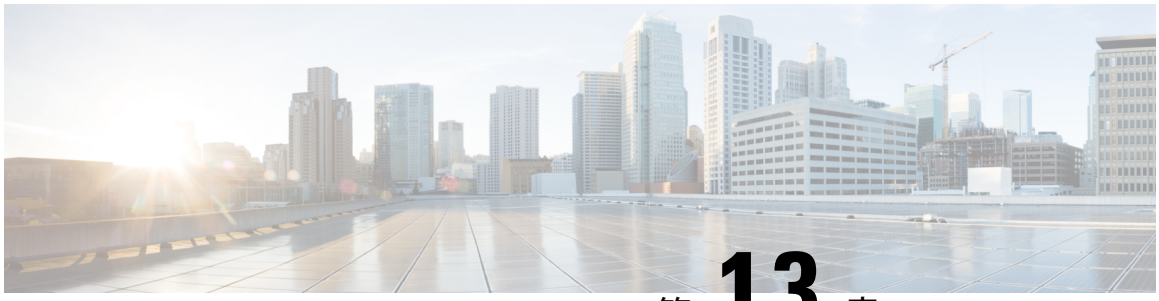
コマンド	目的
show diagnostic bootup level	起動時診断レベルを表示します。
show diagnostic result module *slot*	診断テストの結果を表示します。

オンライン診断のデフォルト設定

次の表に、オンライン診断パラメータのデフォルト設定を示します。

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

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。
- イベント文が指定されていて、アクション文が指定されていない上書きポリシーを設定した場合、アクションは開始されません。また、障害も通知されません。
- 上書きポリシーにイベント文が含まれていないと、システムポリシーで可能性のあるイベントがすべて上書きされます。
- 通常コマンドの表現の場合：すべてのキーワードを拡張する必要があり、アスタリスク（*）記号のみが引数の置換に使用できます。
- EEM イベント相関は 1 つのポリシーに最大 4 つのイベント文をサポートします。イベント タイプは同じでも別でもかまいませんが、サポートされるイベント タイプは、cli、カウンタ、snmp、syslog、追跡だけです。
- 複数のイベント文が EEM ポリシーに存在する場合は、各イベント文に **tag** キーワードと一意な tag 引数が必要です。
- EEM イベント相関はシステムのデフォルト ポリシーを上書きしません。
- デフォルトアクション実行は、タグ付きのイベントで設定されているポリシーではサポートされません。
- 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

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**event manager environment** *variable-name variable-value*	EEM 用の環境変数を作成します。

	コマンドまたはアクション	目的
	例： `switch(config) # event manager environment emailto "admin@anyplace.com"`	*variable-name* は大文字と小文字を区別し、最大 29 文字の英数字を使用できます。 *variable-value* 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） **show event manager environment** {*variable-name* | **all**} 例： `switch(config) # show event manager environment all`	設定した環境変数に関する情報を表示します。
ステップ 4	（任意） **copy running-config startup-config** 例： `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

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

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

	コマンドまたはアクション	目的

ステップ 2	**event manager applet** *applet-name*
	例：
	`switch(config)# event manager applet monitorShutdown`
	`switch(config-applet)#`
		EEM にアプレットを登録し、アプレット コンフィギュレーション モードを開始します。
		applet-name は大文字と小文字を区別し、最大 29 文字の英数字を使用できます。

ステップ 3	（任意） **description** *policy-description* 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。 string には最大 80 文字の英数字を使用できます。ストリングは引用符で囲みます。
ステップ 4	**event** *event-statement* 例： `switch(config-applet)# event cli match "shutdown"`	ポリシーのイベント文を設定します。
ステップ 5	（任意） **tag** *tag* {**and** | **andnot** | **or**} *tag* [**and** | **andnot** | **or** {*tag*}] { **happens** *occurs* **in** *seconds*} 例： `switch(config-applet)# tag one or two happens 1 in 10000`	ポリシー内の複数のイベントを相互に関連付けます。 *occurs* 引数の範囲は 1 ～ 4294967295 です。 *seconds* 引数の範囲は 0 ～ 4294967295 秒です。
ステップ 6	**action** *number*[.*number2*] *action-statement* 例： `switch(config-applet)# action 1.0 cli show interface e 3/1`	ポリシーのアクション文を設定します。アクション文が複数ある場合、このステップを繰り返します。
ステップ 7	（任意） **show event manager policy-state** *name* [**module** *module-id*] 例： `switch(config-applet)# show event manager policy-state monitorShutdown`	設定したポリシーの状態に関する情報を表示します。
ステップ 8	（任意） **copy running-config startup-config** 例： `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

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

	コマンドまたはアクション	目的
ステップ 1	**event cli** [**tag** *tag*] **match** *expression* [**count** *repeats* | **time** *seconds* 例： `switch(config-applet) # event cli match "shutdown"`	正規表現と一致するコマンドが入力された場合に、イベントを発生させます。 **tag** *tag* キーワードと引数のペアは、複数のイベントがポリシーに含まれている場合、この特定のイベントを識別します。 *repeats* の範囲は 1 ～ 65000 です。 *time* の範囲は 0 ～ 4294967295 です。0 は無制限を示します。
ステップ 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**} 例： `switch(config-applet) # event counter name mycounter entry-val 20 gt`	カウンタが、開始演算子に基づいて開始のしきい値を超えた場合にイベントを発生させます。イベントはただちにリセットされます。任意で、カウンタが終了のしきい値を超えたあとでリセットされるように、イベントを設定できます。

	コマンドまたはアクション	目的
		tag *tag* キーワードと引数のペアは、複数のイベントがポリシーに含まれている場合、この特定のイベントを識別します。 *counter* name は大文字と小文字を区別し、最大 28 の英数字を使用できます。 *entry* および *exit* の値の範囲は 0 ～ 2147483647 です。
ステップ 3	**event fanabsent** [**fan** *number*] **time** *seconds* 例： `switch(config-applet) # event fanabsent time 300`	秒数で設定された時間を超えて、ファンがデバイスから取り外されている場合に、イベントを発生させます。 *number* の範囲はモジュールに依存します。 *seconds* の範囲は 10 ～ 64000 です。
ステップ 4	**event fanbad** [**fan** *number*] **time** *seconds* 例： `switch(config-applet) # event fanbad time 3000`	秒数で設定された時間を超えて、ファンが故障状態の場合に、イベントを発生させます。 *number* の範囲はモジュールに依存します。 *seconds* の範囲は 10 ～ 64000 です。
ステップ 5	**event memory** {**critical** | **minor** | **severe**} 例： `switch(config-applet) # event memory critical`	メモリのしきい値を超えた場合にイベントを発生させます。
ステップ 6	**event policy-default count** *repeats* [**time** *seconds*] 例： `switch(config-applet) # event policy-default count 3`	システム ポリシーで設定されているイベントを使用します。このオプションは、ポリシーを上書きする場合に使用します。 *repeats* の範囲は 1 ～ 65000 です。 *seconds* の範囲は 0 ～ 4294967295 秒です。0 は無制限を示します。
ステップ 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* 例： `switch(config-applet) # event snmp oid 1.3.6.1.2.1.31.1.1.1.6 get-type next entry-op lt 300 entry-val 0 exit-op eq 400 exit-time 30 polling-interval 300`	SNMP OID が、開始演算子に基づいて開始のしきい値を超えた場合にイベントを発生させます。イベントはただちにリセットされます。または任意で、カウンタが終了のしきい値を超えたあとでリセットされるように、イベントを設定できます。OID はドット付き 10 進表記です。 **tag** *tag* キーワードと引数のペアは、複数のイベントがポリシーに含まれている場合、この特定のイベントを識別します。

	コマンドまたはアクション	目的
		entry および *exit* の値の範囲は 0 ～ 18446744073709551615 です。 *time* の範囲は 0 ～ 2147483647 秒です。 *interval* の範囲は 0 ～ 2147483647 秒です。
ステップ 8	**event sysmgr memory** [**module** *module-num*] **major** *major-percent* **minor** *minor-percent* **clear** *clear-percent* 例： `switch(config-applet) # event sysmgr memory minor 80`	指定したシステム マネージャのメモリのしきい値を超えた場合にイベントを発生させます。 *percent* の範囲は 1 ～ 99 です。
ステップ 9	**event temperature** [**module** *slot*] [**sensor** *number*] **threshold** {**any** | **down** | **up**} 例： `switch(config-applet) # event temperature module 2 threshold any`	温度センサーが設定されたしきい値を超えた場合に、イベントを発生させます。 *sensor* の範囲は 1 ～ 18 です。
ステップ 10	**event track** [**tag** *tag*] *object-number* **state** {**any** | **down** | **up** 例： `switch(config-applet) # event track 1 state down`	トラッキング対象オブジェクトが設定された状態になった場合に、イベントを発生させます。 **tag** *tag* キーワードと引数のペアは、複数のイベントがポリシーに含まれている場合、この特定のイベントを識別します。 指定できる *object-number* の範囲は 1 ～ 500 です。

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

	コマンドまたはアクション	目的
ステップ 1	**action** *number*[.*number2*] **cli** *command1*[*command2.*] [**local**] 例： `switch(config-applet) # action 1.0 cli "show interface e 3/1"`	設定済みコマンドを実行します。任意で、イベントが発生したモジュール上でコマンドを実行できます。 アクション ラベルのフォーマットは number1.number2 です。 *number* には 1 ～ 16 桁の任意の番号を指定できます。 *number2* の範囲は 0 ～ 9 です。
ステップ 2	**action** *number*[.*number2*] **counter name** *counter* **value** *val* **op** {**dec**	**inc**	**nop**	**set**} 例： `switch(config-applet) # action 2.0 counter name mycounter value 20 op inc`	設定された値および操作でカウンタを変更します。 アクション ラベルのフォーマットは number1.number2 です。 *number* には 1 ～ 16 桁の任意の番号を指定できます。 *number2* の範囲は 0 ～ 9 です。 *counter* 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。

	コマンドまたはアクション	目的
		val には 0 ～ 2147483647 の整数または置換パラメータを指定できます。
ステップ 3	**action** *number*[.*number2*] **event-default** 例： `switch(config-applet) # action 1.0 event-default`	関連付けられたイベントのデフォルトアクションを実行します。 アクション ラベルのフォーマットは number1.number2 です。 *number* には 1 ～ 16 桁の任意の番号を指定できます。 *number2* の範囲は 0 ～ 9 です。
ステップ 4	**action** *number*[.*number2*] **policy-default** 例： `switch(config-applet) # action 1.0 policy-default`	上書きしているポリシーのデフォルトアクションを実行します。 アクション ラベルのフォーマットは number1.number2 です。 *number* には 1 ～ 16 桁の任意の番号を指定できます。 *number2* の範囲は 0 ～ 9 です。
ステップ 5	**action** *number*[.*number2*] **reload** [**module** *slot* [**-** *slot*]] 例： `switch(config-applet) # action 1.0 reload module 3-5`	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。 アクション ラベルのフォーマットは number1.number2 です。 *number* には 1 ～ 16 桁の任意の番号を指定できます。 *number2* の範囲は 0 ～ 9 です。
ステップ 6	**action** *number*[.*number2*] **snmp-trap** [**intdata1** *integer-data1*] [**intdata2** *integer-data2*] [**strdata** *string-data*] 例： `switch(config-applet) # action 1.0 snmp-trap strdata "temperature problem"`	設定されたデータを使用して SNMP トラップを送信します。アクション ラベルのフォーマットは number1.number2 です。 *number* には 1 ～ 16 桁の任意の番号を指定できます。 *number2* の範囲は 0 ～ 9 です。 *data* 要素には 80 桁までの任意の数を指定できます。 *string* には最大 80 文字の英数字を使用できます。
ステップ 7	**action** *number*[.*number2*] **syslog** [**priority** *prio-val*] **msg** *error-message* 例： `switch(config-applet) # action 1.0 syslog priority notifications msg "cpu high"`	設定されたプライオリティで、カスタマイズした syslog メッセージを送信します。 アクション ラベルのフォーマットは number1.number2 です。 *number* には 1 ～ 16 桁の任意の番号を指定できます。 *number2* の範囲は 0 ～ 9 です。

	コマンドまたはアクション	目的
		error-message には最大 80 文字の英数字を引用符で囲んで使用できます。

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

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

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**event manager policy** *policy-script* 例： `switch(config)# event manager policy moduleScript`	EEM スクリプト ポリシーを登録してアクティブにします。 *policy-script* は大文字と小文字を区別し、最大 29 文字の英数字を使用できます。
ステップ 3	（任意） **event manager policy internal** *name* 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。 *policy-script* は大文字と小文字を区別し、最大 29 の英数字を使用できます。
ステップ 4	（任意） **copy running-config startup-config** 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

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	（任意） **show event manager policy-state** *system-policy*
	例：
	`switch(config-applet)# show event manager policy-state __ethpm_link_flap`
	`Policy __ethpm_link_flap`
	`Cfg count : 5`
	`Cfg time interval : 10.000000 (seconds)`
	`Hash default, Count 0`
		上書きするシステム ポリシーの情報をしきい値を含めて表示します。**show event manager system-policy** 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	**event manager applet** *applet-name* **override** *system-policy*
	例：
	`switch(config-applet)# event manager applet ethport override __ethpm_link_flap`
	`switch(config-applet)#`
		システム ポリシーを上書きし、アプレット コンフィギュレーション モードを開始します。
		applet-name は大文字と小文字を区別し、最大 80 文字の英数字を使用できます。
		system-policy 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	**description** *policy-description* 例：	ポリシーの説明になるストリングを設定します。

	コマンドまたはアクション	目的
	`switch(config-applet)# description "Overrides link flap policy"`	*policy-description* 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	**event** *event-statement* 例： `switch(config-applet)# event policy-default count 2 time 1000`	ポリシーのイベント文を設定します。
ステップ 6	**section** *number action-statement* 例： `switch(config-applet)# action 1.0 syslog priority warnings msg "Link is flapping."`	ポリシーのアクション文を設定します。複数のアクション文では、この手順を繰り返します。
ステップ 7	（任意） **show event manager policy-state** *name* 例： `switch(config-applet)# show event manager policy-state ethport`	設定したポリシーに関する情報を表示します。
ステップ 8	（任意） **copy running-config startup-config** 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

	コマンドまたはアクション	目的

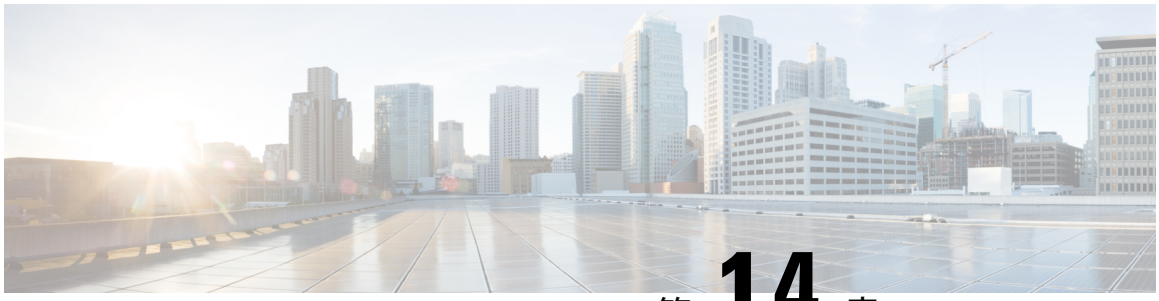
ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**event manager applet** *applet-name*
	例：
	`switch(config)# event manager applet abc`
	`switch (config-appliet)#`
		EEM にアプレットを登録し、アプレット コンフィギュレーション モードを開始します。

ステップ 3	**event syslog** [**tag** *tag*] { **occurs** *number*	**period** *seconds*	**pattern** *msg-text*	**priority** *priority*} 例： `switch(config-applet)# event syslog occurs 10`	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） **copy running-config startup-config** 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

EEM 設定を確認します。



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

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 ソース

SPAN 送信元とは、トラフィックをモニタリングできるインターフェイスを表します。Cisco Nexus デバイスは、SPAN 送信元として、イーサネット、ポート チャネル、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 <xx>** 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 サンプリング

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 パケットのサンプリ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 サンプリングは無効になっています。サンプリ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 サンプリングの注意事項および制限事項

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

- サンプリングは、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。
- サンプリングは、ERSPAN-dst セッションではサポートされていません。
- サンプリングは、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リング範囲は 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

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **monitor session** *session-number*	モニター 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

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface ethernet** *slot*/*port*	指定されたスロットとポートでイーサネット インターフェイスのインターフェイス コンフィギュレーション モードを開始します。

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

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config) # **monitor session** *session-number*	指定したモニタリング セッションのモニター 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) # **source interface** *type slot*/*port* [**rx**	**tx**	**both**]	イーサネット SPAN の送信元ポートを追加し、パケットを複製するトラフィック方向を指定します。イーサネット、ファイバチャネル、または仮想ファイバチャネルのポート範囲を入力できます。複製するトラフィック方向を、入力（Rx）、出力（Tx）、または両方向（both）として指定できます。デフォルトは both です。

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

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config) # **monitor session** *session-number*	指定した SPAN セッションのモニター 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) # **source** {**interface** {**port-channel** | **san-port-channel**} *channel-number* [**rx** | **tx**| **both**] | **vlan** *vlan-range* | **vsan** *vsan-range* }	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

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config) # **monitor session** *session-number*	指定した SPAN セッションのモニター 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-monitor) # **description** *description*	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

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config) # **no monitor session** {**all** | *session-number*} **shut**	指定された SPAN セッションまたはすべてのセッションを開始します。

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

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config) # **monitor session** {**all**	*session-number*} **shut**	指定された SPAN セッションまたはすべてのセッションを一時停止します。

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

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **monitor session** *session-number*	指定した SPAN セッションのモニター コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	switch(config-monitor)# **source** {**interface** {**port-channel**} *channel-number* [**rx** | **tx** | **both**] | **vlan** *vlan-range*}	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)# { source-ip-address source-ip-mask destination-ip-address destination-ip-mask } **filterip**	SPAN フィルタを作成します。
ステップ 5	switch(config-monitor)# **destination interface ethernet** *slot/port*	イーサネット SPAN 宛先ポートを設定します。

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

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **monitor session** *session-number*	指定した SPAN セッションのモニター 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)# **source** {**interface** {**port-channel**} *channel-number* [**rx** | **tx** | **both**] | **vlan** *vlan-range*}	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) # **sampling** *size*	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)# **destination interface ethernet** *slot/port*	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

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **monitor session** *session-number*	指定した SPAN セッションのモニター 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) # **source** {**interface** {**port-channel**} *channel-number* [**rx** | **tx** | **both**] | **vlan** *vlan-range*}	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) # **mtu** *size*	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、

	コマンドまたはアクション	目的
		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)# **destination interface ethernet** *slot/port*	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

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

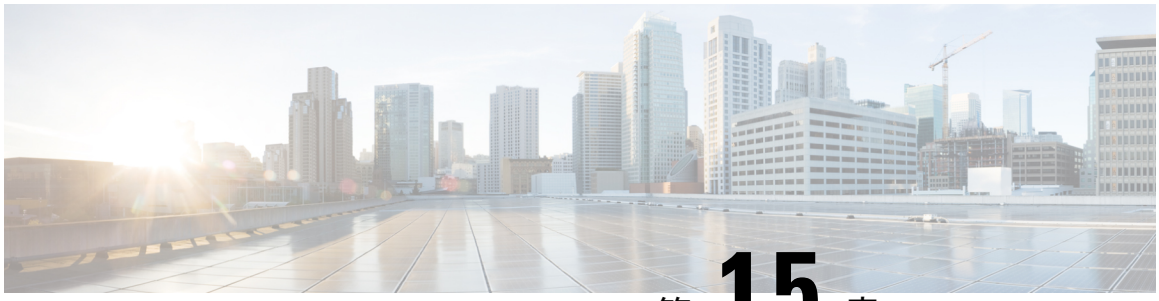
Example

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

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が、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 :* ワープ *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 [1]
10	37 ～ 40
11	41 ～ 44
12	45-48

[1] ポート 36 は専用送信元ポートです。

ワープ SPAN の注意事項および制限事項

ワープ 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プ 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。

- ワープ 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、動作中のワープ設定をコピーし、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、ワープ 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
```

- ワープ 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。

ワープ SPAN の構成

ワープ 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(conifig-monitor)# **destination group** *group-number*
8. （任意） switch(config-if)# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config-monitor)# **interface ethernet** *port/slot*	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)# **switchport monitor**	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)# **no shutdown**	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 5	switch(config)# **monitor session warp**	インターフェイスでワープ SPAN を有効にします。
ステップ 6	switch(config)# **no shutdown**	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 7	switch(conifig-monitor)# **destination group** *group-number*	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)# **copy running-config startup-config**	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

例

次に、ワープ 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
```

ワープ SPAN モード構成の確認

ユーザーはワープ 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

	コマンドまたはアクション	目的
ステップ 1	switch(config)# **show monitor session** {*number* | **all** | *range*}	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)# **show monitor session warp**	ワープ SPAN セッションに関する情報を表示します。

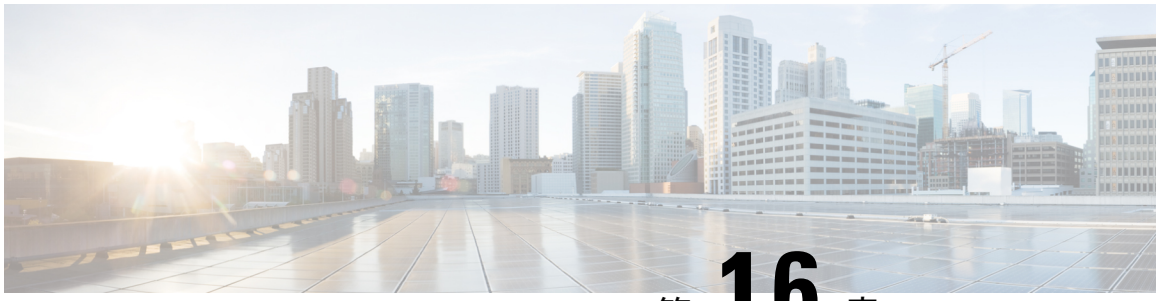
例

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
```

ワープ SPAN 機能の履歴

機能名	リリース	機能情報
ワープ 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

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。

- イーサネット ポートおよびポート チャネル。
- VLAN：VLAN が ERSPAN 送信元として指定されている場合、VLAN でサポートされているすべてのインターフェイスが ERSPAN 送信元となります。

ERSPAN 送信元ポートには、次の特性があります。

- 送信元ポートとして設定されたポートを宛先ポートとしても設定することはできません。
- ERSPANは送信元に関係なく、スーパーバイザによって生成されるパケットをモニターしません。

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

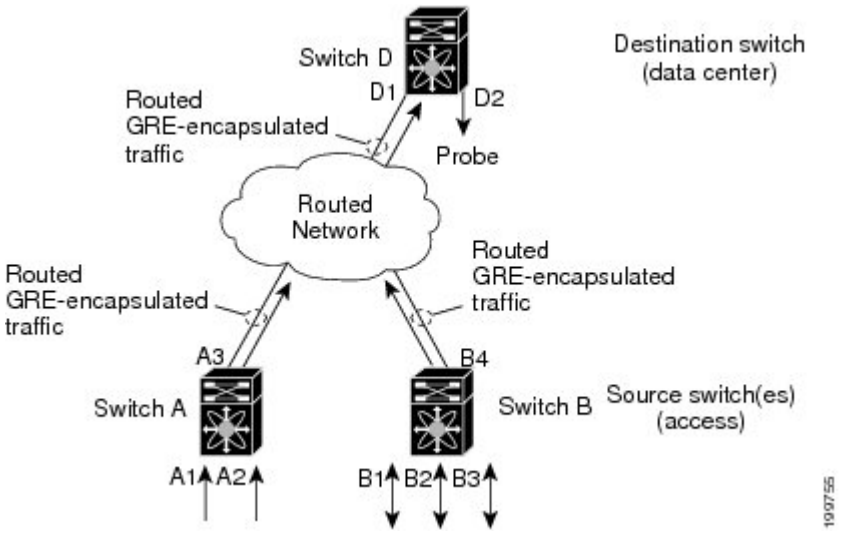
ERSPAN セッションを作成して、モニタする送信元と接続先を指定することができます。

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 （194 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 （194 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 （205 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伝送します。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 （170 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て使用できます。
  - イーサネット ポートまたはポート チャネル（サブ インターフェイスを除く）。
  - ポート チャネル サブインターフェイスに割り当てることのできる 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。
  - フラッディングから発生するトラフィック
  - ブロードキャストおよびマルチキャスト トラフィック
- 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 (µs)、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に発生します。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 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

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# config t`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**monitor erspan origin ip-address** *ip-address* **global** 例： `switch(config)# monitor erspan origin ip-address 10.0.0.1 global`	ERSPAN のグローバルな送信元 IP アドレスを設定します。
ステップ 3	**monitor erspan granularity 100_ns**{**100_us**|**100_ns**|**ns**} 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。

	コマンドまたはアクション	目的
ステップ 4	**no monitor session** {*session-number* | **all**} 例： `switch(config)# no monitor session 3`	指定したERSPANセッションの設定を消去します。新しいセッション コンフィギュレーションは、既存のセッション コンフィギュレーションに追加されます。

ステップ 5	**monitor session** {*session-number* | **all**} **type erspan-source**
	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。

ステップ 6	**header-type** *version* 例： `switch(config-erspan-src)# header-type 3`	（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	**description** *description* 例： `switch(config-erspan-src)# description erspan_src_session_3`	セッションの説明を設定します。デフォルトでは、説明は定義されません。説明には最大 32 の英数字を使用できます。

ステップ 8	**source** {[**interface**[*type slot/port*[*-port*][, *type slot/port[-port*]]] [**port-channel** *channel-number*]] | [**vlan** {*number* | *range*}]} [**rx** | **tx** | **both**]
	例：
	`switch(config-erspan-src)# source interface ethernet 2/1-3, ethernet 3/1 rx`
	例：
	`switch(config-erspan-src)# source interface port-channel 2`
	例：
	`switch(config-erspan-src)# source interface sup-eth 0 both`
	例：
	`switch(config-monitor)# source interface ethernet 101/1/1-3`	

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	**destination ip** *ip-address* 例： `switch(config-erspan-src)# destination ip 10.1.1.1`	ERSPAN セッションの宛先 IP アドレスを設定します。ERSPAN 送信元セッションごとに 1 つの宛先 IP アドレスのみがサポートされます。

	コマンドまたはアクション	目的
ステップ 11	**erspan-id** *erspan-id* 例： `switch(config-erspan-src)# erspan-id 5`	ERSPAN 送信元セッションの ERSPAN ID を設定します。ERSPAN の範囲は 1 ～ 1023 です。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	**vrf** *vrf-name* 例： `switch(config-erspan-src)# vrf default`	ERSPAN 送信元セッションがトラフィックの転送に使用する VRF を設定します。
ステップ 13	（任意） **ip ttl** *ttl-number* 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） **ip dscp** *dscp-number* 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	**no shut** 例： `switch(config-erspan-src)# no shut`	ERSPAN送信元セッションをイネーブルにします。デフォルトでは、セッションはシャット ステートで作成されます。 （注） 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） **show monitor session** {**all** | *session-number* | **range** *session-range*} 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） **show running-config monitor** 例： `switch(config-erspan-src)# show running-config monitor`	ERSPAN の実行コンフィギュレーションを表示します。
ステップ 18	（任意） **show startup-config monitor** 例： `switch(config-erspan-src)# show startup-config monitor`	ERSPAN のスタートアップ コンフィギュレーションを表示します。

	コマンドまたはアクション	目的
ステップ 19	（任意） **copy running-config startup-config** 例： `switch(config-erspan-src)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ERSPAN 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 ステートで作成されます。

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

	コマンドまたはアクション	目的

ステップ 1	**config t**
	例：
	`switch# config t`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します

	コマンドまたはアクション	目的

ステップ 2	**interface ethernet** *slot/port*[*-port*]
	例：
	`switch(config)# interface ethernet 2/5`
	`switch(config-if)#`
		選択したスロットおよびポートまたはポート範囲で、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**switchport** 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	**switchport mode** [**access** | **trunk**] 例： `switch(config-if)# switchport mode trunk`	選択したスロットおよびポートまたはポート範囲で次のスイッチポート モードを設定します。 • アクセス • トランク
ステップ 5	**switchport monitor** 例： `switch(config-if)# switchport monitor`	モニタ モードでスイッチ インターフェイスを設定します。 （**destination interface ethernet** *interface* コマンドを使用して）インターフェイスを ERSPAN または SPAN 宛先に設定するには、最初にモニタ モードで設定する必要があります。
ステップ 6	ステップ 2 ～ 5 を繰り返して、追加の ERSPAN 宛先でモニタリングを設定します。	—
ステップ 7	**no monitor session** {*session-number* | **all**} 例： `switch(config-if)# no monitor session 3`	指定した ERSPAN セッションの設定を消去します。新しいセッション コンフィギュレーションは、既存のセッション コンフィギュレーションに追加されます。

ステップ 8	**monitor session** {*session-number* | **all**} **type erspan-destination**
	例：
	`switch(config-if)# monitor session 3 type erspan-destination`
	`switch(config-erspan-dst)#`
		ERSPAN 宛先セッションを設定します。

ステップ 9	**description** *description* 例： `switch(config-erspan-dst)# description erspan_dst_session_3`	セッションの説明を設定します。デフォルトでは、説明は定義されません。説明には最大 32 の英数字を使用できます。
ステップ 10	**source ip** *ip-address* 例： `switch(config-erspan-dst)# source ip 10.1.1.1`	ERSPAN セッションの送信元 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。

	コマンドまたはアクション	目的
		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	**destination** {[**interface** [*type slot/port*[*-port*], [*type slot/port* [*port*]]]} 例： `switch(config-erspan-dst)# destination interface ethernet 2/5`	コピーする送信元パケットの宛先を設定します。宛先としては、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す。
ステップ 12	**erspan-id** *erspan-id* 例： `switch(config-erspan-dst)# erspan-id 5`	ERSPAN セッションの ERSPAN ID を設定します。指定できる範囲は 1 ～ 1023 です。この ID は、送信元および宛先の ERSPAN セッションのペアを一意に識別します。対応する宛先の ERSPAN セッションに設定される ERSPAN ID は、送信元のセッションで設定されているものと同じにする必要があります。
ステップ 13	**no shut** 例： `switch(config)# no shut`	ERSPAN 宛先セッションを有効にします。デフォルトでは、セッションはシャット ステートで作成されます。 （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） **show monitor session** {**all** | *session-number* | **range** *session-range*} 例： `switch(config)# show monitor session 3`	ERSPAN セッション設定を表示します。
ステップ 15	（任意） **show running-config monitor** 例： `switch(config-erspan-src)# show running-config monitor`	ERSPAN の実行コンフィギュレーションを表示します。
ステップ 16	（任意） **show startup-config monitor** 例： `switch(config-erspan-src)# show startup-config monitor`	ERSPAN のスタートアップ コンフィギュレーションを表示します。
ステップ 17	（任意） **copy running-config startup-config** 例： `switch(config-erspan-src)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ERSPAN セッションのシャットダウンまたはアクティブ化

ERSPANセッションをシャットダウンすると、送信元から宛先へのパケットのコピーを切断できます。同時に実行できる ERSPAN セッション数は限定されているため、あるセッションをシャットダウンしてハードウェア リソースを解放することによって、別のセッションが使用できるようになります。デフォルトでは、ERSPAN セッションはシャット ステートで作成されます。

ERSPANセッションをイネーブルにすると、送信元から宛先へのパケットのコピーをアクティブ化できます。すでにイネーブルになっていて、動作状況がダウンの ERSPAN セッションをイネーブルにするには、そのセッションをいったんシャットダウンしてから、改めてイネーブルにする必要があります。ERSPAN セッション ステートをシャットダウンおよびイネーブルにするには、グローバルまたはモニタ コンフィギュレーション モードのいずれかのコマンドを使用できます。

手順の概要

1. **configuration terminal**
2. **monitor session** {*session-range* | **all**} **shut**
3. **no monitor session** {*session-range* | **all**} **shut**
4. **monitor session** *session-number* **type erspan-source**
5. **monitor session** *session-number* **type erspan-destination**
6. **shut**
7. **no shut**
8. （任意） **show monitor session all**
9. （任意） **show running-config monitor**
10. （任意） **show startup-config monitor**
11. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configuration terminal**
	例：
	`switch# configuration terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**monitor session** {*session-range*	**all**} **shut** 例： `switch(config)# monitor session 3 shut`	指定の ERSPAN セッションをシャットダウンします。セッションの範囲は 1 ～ 48 です。デフォルトでは、セッションはシャット ステートで作成されます。
ステップ 3	**no monitor session** {*session-range*	**all**} **shut** 例：	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。。

	コマンドまたはアクション	目的
	`switch(config)# no monitor session 3 shut`	（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 **monitor session shut** コマンドを指定してから、**no monitor session shut** コマンドを続ける必要があります。

ステップ 4	**monitor session** *session-number* **type erspan-source**
	例：
	`switch(config)# monitor session 3 type erspan-source`
	`switch(config-erspan-src)#`
		ERSPAN 送信元タイプのモニタ コンフィギュレーション モードを開始します。新しいセッション コンフィギュレーションは、既存のセッション コンフィギュレーションに追加されます。

ステップ 5	**monitor session** *session-number* **type erspan-destination** 例： `switch(config-erspan-src)# monitor session 3 type erspan-destination`	ERSPAN 宛先タイプのモニター 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	**shut** 例： `switch(config-erspan-src)# shut`	ERSPAN セッションをシャットダウンします。デフォルトでは、セッションはシャット ステートで作成されます。
ステップ 7	**no shut** 例： `switch(config-erspan-src)# no shut`	ERSPANセッションをイネーブルにします。デフォルトでは、セッションはシャット ステートで作成されます。
ステップ 8	（任意） **show monitor session all** 例： `switch(config-erspan-src)# show monitor session all`	ERSPAN セッションのステータスを表示します。
ステップ 9	（任意） **show running-config monitor** 例： `switch(config-erspan-src)# show running-config monitor`	ERSPAN の実行コンフィギュレーションを表示します。
ステップ 10	（任意） **show startup-config monitor** 例： `switch(config-erspan-src)# show startup-config monitor`	ERSPAN のスタートアップ コンフィギュレーションを表示します。
ステップ 11	（任意） **copy running-config startup-config** 例： `switch(config-erspan-src)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ERSPAN 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す。フィルタの詳細については、SPAN および ERSPAN フィルタ処理 （171 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

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **monitor session** {*session-number* | **all**} **type erspan-source**	ERSPAN 送信元セッションを設定します。
ステップ 3	switch(config-erspan-src)# **filter** {**ip** *source-ip-address source-ip-mask destination-ip-address destination-ip-mask*}	ERSPAN フィルタを作成します。
ステップ 4	switch(config-erspan-src)# **erspan-id** *erspan-id*	ERSPAN 送信元セッションの ERSPAN ID を設定します。ERSPAN の範囲は 1 ～ 1023 です。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)# **vrf** *vrf-name*	ERSPAN 送信元セッションがトラフィックの転送に使用する VRF を設定します。
ステップ 6	switch(config-erspan-src)# **destination ip** *ip-address*	ERSPAN セッションの宛先 IP アドレスを設定します。ERSPAN 送信元セッションごとに 1 つの宛先 IP アドレスのみがサポートされます。

	コマンドまたはアクション	目的
ステップ 7	switch(config-erspan-src)# **source** [**interface** [*type slot/port*] | **port-channel** *channel-number*] | [**vlan** *vlan-range*] [**rx** | **tx** | **both**]	送信元およびパケットをコピーするトラフィックの方向を設定します。イーサネット ポート範囲、ポート チャネル、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 サンプリングの設定

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。サンプリングの詳細については、SPAN および ERSPAN サンプリング （173 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

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **monitor session** {*session-number* | **all**} **type erspan-source**	ERSPAN 送信元セッションを設定します。
ステップ 3	switch(config-erspan-src)# **sampling** *sampling-range*	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 4	switch(config-erspan-src)# **erspan-id** *erspan-id*	ERSPAN 送信元セッションの ERSPAN ID を設定します。ERSPAN の範囲は 1 ～ 1023 です。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)# **vrf** *vrf-name*	ERSPAN 送信元セッションがトラフィックの転送に使用する VRF を設定します。
ステップ 6	switch(config-erspan-src)# **destination ip** *ip-address*	ERSPAN セッションの宛先 IP アドレスを設定します。ERSPAN 送信元セッションごとに 1 つの宛先 IP アドレスのみがサポートされます。

	コマンドまたはアクション	目的
ステップ 7	switch(config-erspan-src)# **source** [**interface** *type slot/port* | **port-channel** *channel-number*] | [**vlan** *vlan-range*] [**rx** | **tx** | **both**]	送信元およびパケットをコピーするトラフィックの方向を設定します。イーサネットポート範囲、ポートチャネル、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リ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 （174 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

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **monitor session** {*session-number* | **all**} **type erspan-source**	ERSPAN 送信元セッションを設定します。
ステップ 3	switch(config-erspan-src)# **mtu** *size*	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)# **erspan-id** *erspan-id*	ERSPAN 送信元セッションの ERSPAN ID を設定します。ERSPAN の範囲は 1 ～ 1023 です。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)# **vrf** *vrf-name*	ERSPAN 送信元セッションがトラフィックの転送に使用する VRF を設定します。
ステップ 6	switch(config-erspan-src)# **destination ip** *ip-address*	ERSPAN セッションの宛先 IP アドレスを設定します。ERSPAN 送信元セッションごとに 1 つの宛先 IP アドレスのみがサポートされます。

	コマンドまたはアクション	目的
ステップ 7	switch(config-erspan-src)# **source** [**interface** *type slot/port* | **port-channel** *channel-number*] | [**vlan** *vlan-range*] [**rx** | **tx** | **both**]	送信元およびパケットをコピーするトラフィックの方向を設定します。イーサネット ポート範囲、ポート チャネル、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
marker-packet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。
marker-packetmilliseconds	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。
no marker-packet	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
show monitor session {**all** | *session-number* | **range** *session-range*}	ERSPAN セッション設定を表示します。

コマンド	目的
show running-config monitor	ERSPAN の実行コンフィギュレーションを表示します。
show startup-config monitor	ERSPAN のスタートアップ コンフィギュレーションを表示します。

ERSPAN の設定例

ERSPAN 送信元セッションの設定例

次に、ERSPAN 送信元セッションを設定する例を示します。

```
switch# 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『*Cisco Nexus NX-OS System Management Command Reference*』。

関連資料

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

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 managment
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

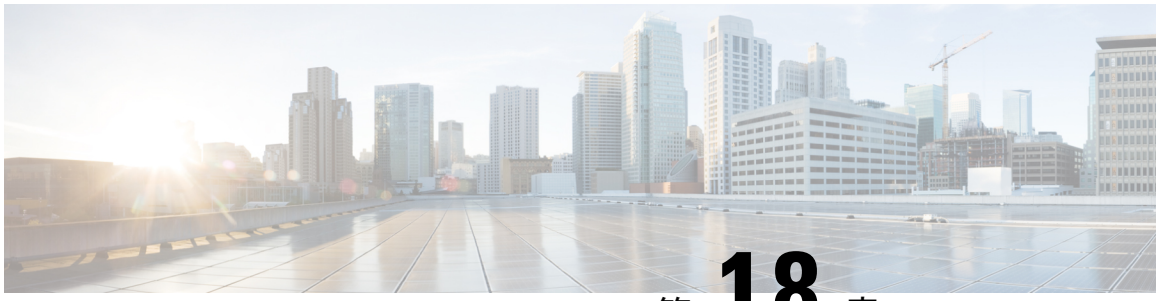
	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# vrf context managment	設定可能な仮想およびルーティング（VRF）名を指定します。
ステップ 3	switch(config)# **ip host** *name address1 [address2... address6]*	ホスト名キャッシュに、6つまでのスタティック ホスト名/アドレス マッピングを定義します。
ステップ 4	（任意） switch(config)# **ip domain name** *name* [**use-vrf** *vrf-name*]	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)# **ip domain-list** *name* [**use-vrf** *vrf-name*]	Cisco NX-OS が非完全修飾ホスト名に使用できる追加のドメイン ネーム サーバーを定義します。このドメイン名を設定した VRF でこのドメイン ネーム サーバーを解決できない場合は、任意で、Cisco

	コマンドまたはアクション	目的
		NX-OS がこのドメイン ネーム サーバーを解決するために使用する VRF を定義することもできます。 Cisco NX-OS はドメイン リスト内の各エントリを使用して、ドメイン名ルックアップを開始する前に、完全なドメイン名を含まないあらゆるホスト名にこのドメイン名を追加します。Cisco NX-OS は、一致するものが見つかるまで、ドメイン リストの各エントリにこれを実行します。
ステップ 6	（任意） switch(config)# **ip name-server** *server-address1 [server-address2... server-address6]* **[use-vrf** *vrf-name*]	最大 6 台のネーム サーバを定義します。使用可能なアドレスは、IPv4 アドレスまたは IPv6 アドレスです。 このネーム サーバを設定した VRF でこのネーム サーバに到達できない場合は、任意で、Cisco NX-OS がこのネーム サーバに到達するために使用する VRF を定義することもできます。
ステップ 7	（任意） switch(config)# **ip domain-lookup**	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)# **show hosts**	DNS に関する情報を表示します。
ステップ 9	switch(config)# **exit**	コンフィギュレーション モードを終了し、EXEC モードに戻ります。
ステップ 10	（任意） switch# **copy running-config startup-config**	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

例

次に、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

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 （225 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

ワープ 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

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **hardware profile forwarding-mode warp**	デバイスのワープ モードを有効にします。ワープ モードを無効にするには、このコマンドの **no** 形式を使用します。デフォルトでは、ワープモードは無効です。
ステップ 3	（任意） switch(config)# **copy running-config startup-config**	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。
ステップ 4	スイッチをリロードします。	—

例

次に、デバイスのワープ 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、デバイスのワープ 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
```

ワープ 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

	コマンドまたはアクション	目的
ステップ 1	switch# **show hardware profile forwarding-mode**	ワープ 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。

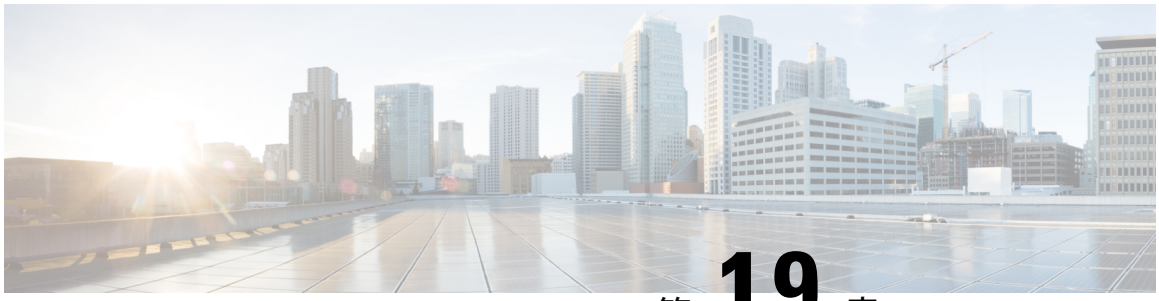
例

次に、ワープ 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#
```

ワープモードの機能履歴

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



第 19 章

アクティブ バッファ モニタリングの設定

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

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

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

例

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

	コマンドまたはアクション	目的
ステップ 1	switch# **show hardware profile buffer monitor** [**interface ethernet** *slot/port*] {**brief** | **buffer-block** | **detail** | **multicast** | **summary**}	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。 • **brief**：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。 • **buffer-block**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。 • **detail**：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 • **interface**：（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。 • **multicast**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。 • **summary**：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。 （注） show コマンドのオプション **interface** はユニキャスト モードでのみ有効で、**multicast** オプションはマルチキャスト モードでのみ有効です。
ステップ 2	（任意） switch# **clear hardware profile buffer monitor**	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 Avaliable = 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 Avaliable = 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
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 Avaliable = 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 Avaliable = 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 Avaliable = 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 Avaliable = 5799 Kbytes
Class Threshold Limit = 5598 Kbytes
Mcast Usage 3         0KB       0KB       0KB       0KB       0KB
```

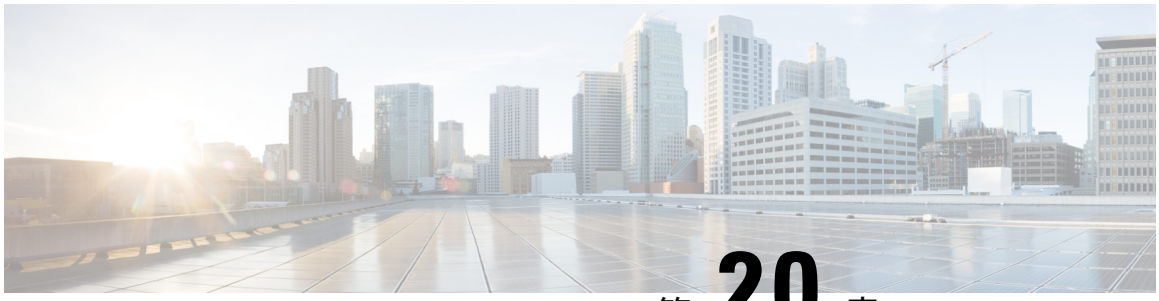
次に、マルチキャストモードのバッファブロック 3 の詳細なバッファ使用率の情報を表示する例を示します。

```
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
09/18/2012 08:30:11      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
09/18/2012 08:30:09      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
09/18/2012 08:30:07      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
09/18/2012 08:30:05      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
09/18/2012 08:30:03      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
09/18/2012 07:38:41      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
09/18/2012 07:38:39      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
09/18/2012 07:38:37      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
09/18/2012 07:38:35      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
09/18/2012 07:38:33      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
09/18/2012 07:38:31      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
09/18/2012 07:38:29      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
09/18/2012 07:38:27      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
09/18/2012 07:38:25      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
09/18/2012 07:38:23      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
09/18/2012 07:38:21      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
09/18/2012 07:38:19      0  143  107    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
09/18/2012 07:38:17      0    0    0    0  176   74    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
09/18/2012 07:38:15      0    0    0    0    0    0   33  179   38    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
09/18/2012 07:38:13      0    0    0    0    0    0    0    0    0   66  178    6    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
09/18/2012 07:38:11      1    0    0    1    0    0    1    0    0    1    0    0  102
  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
```



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

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

SMU の影響は次のタイプによって異なります。

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

SMU は、メンテナンス リリースの代わりになるものではありません。直近の問題に対する迅速な解決策を提供します。SMU で修正された障害は、メンテナンス リリースにすべて統合されます。

デバイスを新しい機能やメンテナンス リリースにアップグレードする詳細については、『*Cisco Nexus 3500 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。

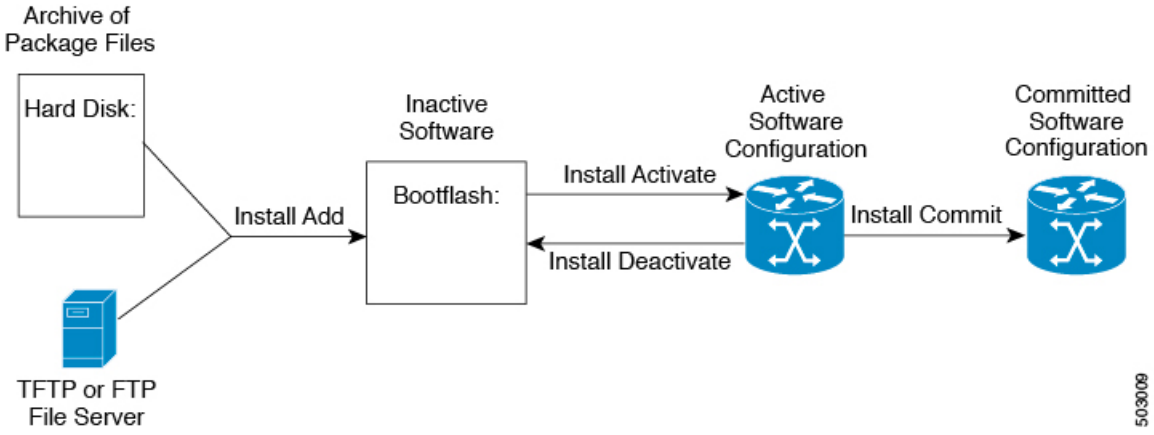
パッケージ管理

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



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 のソフトウェア メンテナンス アップグレードの実行

パッケージ インストールの準備

SMU パッケージのインストールの準備に関する情報を収集するには、複数の **show** コマンドを使用する必要があります。

始める前に

ソフトウェアの変更が必要かどうかを確認します。

使用中のシステムで新しいパッケージがサポートされていることを確認する。ソフトウェア パッケージによっては、他のパッケージまたはパッケージバージョンをアクティブにする必要があり、特定のライン カードのみをサポートするパッケージもあります。

そのリリースに関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

	コマンドまたはアクション	目的
ステップ 1	**show install active** 例： `switch# show install active`	デバイス上のアクティブなソフトウェアを表示します。デバイスに追加する必要があるソフトウェアを決定するため、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	**show module** 例： `switch# show module`	すべてのモジュールが安定状態であることを確認します。
ステップ 3	**show clock** 例： `switch# show clock`	システム クロックが正しいことを確認します。ソフトウェア操作は、デバイス クロックの時刻に基づいて証明書を使用します。

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

	コマンドまたはアクション	目的
ステップ 1	**install add** *filename* [**activate**] 例：	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

	コマンドまたはアクション	目的
	`switch# install add bootflash: n3500-uk9.6.0.2.U6.0.1.CSCab00001.bin`	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。 *filename* 引数は、次の形式をとることができます。 • **bootflash:***filename* • **tftp://***hostname-or-ipaddress*/*directory-path*/*filename* • **ftp://***username***:***password***@***hostname-or-ipaddress*/*directory-path*/*filename* • **sftp://***hostname-or-ipaddress*/*directory-path*/*filename*
ステップ 2	（任意） **show install inactive** **例**： `switch# show install inactive`	デバイス上の非アクティブなパッケージを表示します。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。

ステップ 3	必須: **install activate** *filename* [**test**]
	例：
	`switch# install activate n3500-uk9.6.0.2.U6.0.1.CSCab00001.bin`
	例：
	`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`
	例：
	`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`
		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。）
		（注） パッケージ名を部分的に入力してから **?** を押すと、アクティブ化に使用できるすべての候補が表示されます。候補が1つしかない場合に **Tab** キーを押すと、パッケージ名の残りの部分が自動入力されます。

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	（任意） **show install active** **例**： `switch# show install active`	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

	コマンドまたはアクション	目的
ステップ 1	**install commit** *filename* 例： `switch# install commit 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） **show install committed** 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

	コマンドまたはアクション	目的
ステップ 1	**install deactivate** *filename* 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 **Tab** キーを押すと、パッケージ名の残りの部分が自動入力されます。

	コマンドまたはアクション	目的
ステップ 2	（任意） **show install inactive** 例： `switch# show install inactive`	デバイス上の非アクティブなパッケージを表示します。
ステップ 3	（任意） **install commit** 例： `switch# install commit`	現在のパッケージのセットをコミットして、デバイスが再起動したときにこれらのパッケージが使用されるようにします。 （注） パッケージを削除できるのは、非アクティブ化操作がコミットされた場合だけです。

ステップ 4	（任意） **install remove** {*filename* | **inactive**}
	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。
		• 削除できるのは非アクティブなパッケージだけです。
		• パッケージは、デバイスのすべてのライン カードから非アクティブにされた場合にのみ削除できます。
		• パッケージの非アクティブ化はコミットする必要があります。
		• ストレージデバイスから特定の非アクティブなパッケージを削除するには、**install remove** コマンドに *filename* 引数を指定して使用します。
		• システムのすべてのノードから非アクティブなパッケージをすべて削除するには、**install remove** コマンドと **inactive** キーワードを使用します。

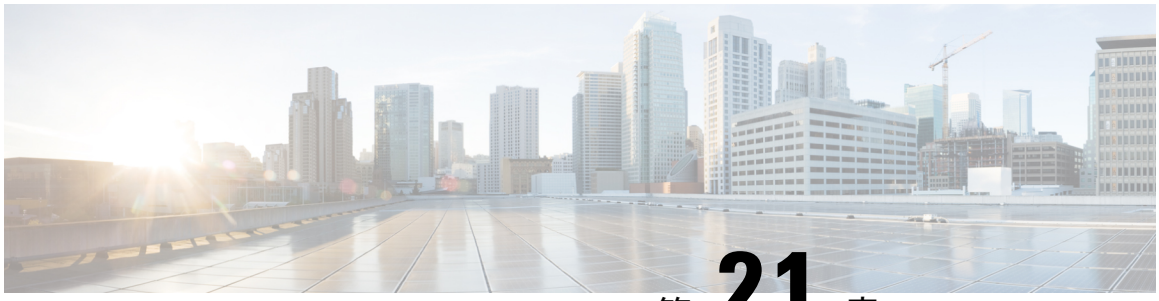
インストール ログ情報の表示

インストール ログは、インストール動作の履歴についての情報を提供します。インストール動作が実行されるたびに、その動作に対して番号が割り当てられます。

- **show install log** コマンドを使用して、インストール動作の成功および失敗の両方について情報を表示します。
- 引数を指定しない **show install log** コマンドを使用して、すべてのインストール動作のサマリーを表示します。ある動作に固有の情報を表示するには、*request-id* 引数を指定します。ファイルの変更、リロードできなかったノード、その他プロセスに影響する操作など、特定の操作の詳細を表示するには、**detail** キーワードを使用します。

次に、すべてのインストール要求の情報を表示する例を示します。

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

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

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を同じ名前で上書きすることはできません。
- Cisco NX-OS コマンドは Cisco IOS コマンドと異なる場合があります。

チェックポイントの作成

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

手順の概要

1. switch# **checkpoint** { [*cp-name*] [**description** *descr*] | **file** *file-name*
2. （任意） switch# **no checkpoint***cp-name*
3. （任意） switch# **show checkpoint***cp-name*

手順の詳細

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

ロールバックの実装

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

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

手順の概要

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

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

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
```

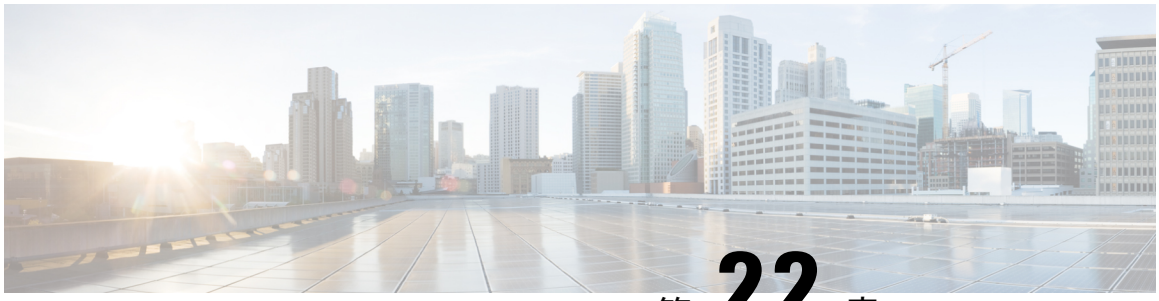
ロールバック コンフィギュレーションの確認

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
show checkpoint *name* [**all**]	チェックポイント名の内容を表示します。
show checkpoint all [**user** | **system**]	現行のスイッチ内のすべてのチェックポイントの内容を表示します。表示されるチェックポイントを、ユーザ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。
show checkpoint summary [**user** | **system**]	現在のスイッチ内のすべてのチェックポイントのリストを表示します。表示されるチェックポイントを、ユーザ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。
show diff rollback-patch { **checkpoint** *src-cp-name* | **running-config** | **startup-config** | **file** *source-file*} {	ソースと宛先のチェックポイント間の差異を表示します。

コマンド	目的
checkpoint *dest-cp-name* | **running-config** | **startup-config** | **file** *dest-file*}	
show rollback log [**exec** | **verify**]	ロールバック ログの内容を表示します。

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



第 22 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

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つのロールが3つのルールを持っている場合、ルール 3 がルール 2 よりも前に適用され、ルール 2 はルール 1 よりも前に適用されます。

ユーザー ロール ポリシー

ユーザ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、ユーザーがそのユーザーに関連付けられたユーザー ロール ポリシーに含まれていなくても、ユーザーはこれらのリソースへのアクセスを許可されます。

ユーザー アカウントの設定の制限事項

次の語は予約済みであり、ユーザー設定に使用できません。

- adm
- bin
- daemon
- ftp
- ftpuser
- games
- gdm
- gopher
- halt
- lp
- mail
- mailnull
- man
- mtsuser
- news
- nobody

- san-admin
- shutdown
- sync
- sys
- uucp
- xfs

ユーザ パスワードの要件

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。

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 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

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	(Optional) switch(config)# **show role**	使用可能なユーザ ロールを表示します。必要に応じて、他のユーザ ロールを設定できます。
ステップ 3	switch(config) # **username** *user-id* [**password** *password*] [**expire** *date*] [**role** *role-name*]	ユーザー アカウントを設定します。 *user-id* は、最大 28 文字の英数字の文字列で、大文字と小文字が区別されます。 デフォルトの *password* は定義されていません。 **Note** 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。 **expire** *date* 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。
ステップ 4	switch(config) # **exit**	グローバル コンフィギュレーション モードを終了します。
ステップ 5	(Optional) switch# **show user-account**	ロール設定を表示します。
ステップ 6	(Optional) switch# **copy running-config startup-config**	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

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

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config) # **role name** *role-name*	ユーザー 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。 *role-name* 引数は、最大 16 文字の英数字の文字列で、大文字と小文字が区別されます。
ステップ 3	switch(config-role) # **rule** *number* {**deny** | **permit**} **command** *command-string*	コマンド ルールを設定します。 *command-string* には、スペースおよび正規表現を含めることができます。たとえば、「interface ethernet *」は、すべてのイーサネット インターフェイスが含まれます。 必要な規則の数だけこのコマンドを繰り返します。
ステップ 4	switch(config-role)# **rule** *number* {**deny** | **permit**} {**read** | **read-write**}	すべての操作の読み取り専用ルールまたは読み取り/書き込みルールを設定します。

	Command or Action	Purpose
ステップ 5	switch(config-role)# **rule** *number* {**deny** | **permit**} {**read** | **read-write**} **feature** *feature-name*	機能に対して、読み取り専用規則か読み取りと書き込みの規則かを設定します。 機能リストを表示するには、**show role feature** コマンドを使用します。 必要な規則の数だけこのコマンドを繰り返します。
ステップ 6	switch(config-role)# **rule** *number* {**deny** | **permit**} {**read** | **read-write**} **feature-group** *group-name*	機能グループに対して、読み取り専用規則か読み取りと書き込みの規則かを設定します。 機能グループのリストを表示するには、**show role feature-group** コマンドを使用します。 必要な規則の数だけこのコマンドを繰り返します。
ステップ 7	(Optional) switch(config-role)# **description** *text*	ロールの説明を設定します。説明にはスペースも含めることができます。
ステップ 8	switch(config-role)# **end**	ロール コンフィギュレーション モードを終了します。
ステップ 9	(Optional) switch# **show role**	ユーザ ロールの設定を表示します。
ステップ 10	(Optional) switch# **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、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

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config) # **role feature-group** *group-name*	ユーザー 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。 *group-name* は、最大 32 文字の英数字の文字列で、大文字と小文字が区別されます。
ステップ 3	switch(config) # **exit**	グローバル コンフィギュレーション モードを終了します。
ステップ 4	(Optional) switch# **show role feature-group**	ロール機能グループ設定を表示します。
ステップ 5	(Optional) switch# **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、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

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config) # **role name** *role-name*	ユーザー 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) # **interface policy deny**	ロール インターフェイス ポリシー コンフィギュレーション モードを開始します。
ステップ 4	switch(config-role-interface) # **permit interface** *interface-list*	ロールがアクセスできるインターフェイスのリストを指定します。 必要なインターフェイスの数だけこのコマンドを繰り返します。 このコマンドでは、イーサネット インターフェイスを指定できます。
ステップ 5	switch(config-role-interface) # **exit**	ロール インターフェイス ポリシー コンフィギュレーション モードを終了します。
ステップ 6	(Optional) switch(config-role) # **show role**	ロール設定を表示します。
ステップ 7	(Optional) switch(config-role) # **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。

Example

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

```
switch# configure terminal
switch(config)# role name UserB
switch(config-role)# interface policy deny
switch(config-role-interface)# permit interface ethernet 2/1
switch(config-role-interface)# permit interface fc 3/1
switch(config-role-interface)# permit interface vfc 30/1
```

ユーザ ロール VLAN ポリシーの変更

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

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config) # **role name** *role-name*
3. switch(config-role)# **vlan policy deny**
4. switch(config-role-vlan # **permit vlan** *vlan-list*
5. switch(config-role-vlan) # **exit**
6. (Optional) switch# **show role**
7. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config) # **role name** *role-name*	ユーザー 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)# **vlan policy deny**	ロール VLAN ポリシー コンフィギュレーション モードを開始します。
ステップ 4	switch(config-role-vlan # **permit vlan** *vlan-list*	ロールがアクセスできる VLAN の範囲を指定します。 必要な VLAN の数だけこのコマンドを繰り返します。
ステップ 5	switch(config-role-vlan) # **exit**	ロール VLAN ポリシー コンフィギュレーション モードを終了します。
ステップ 6	(Optional) switch# **show role**	ロール設定を表示します。
ステップ 7	(Optional) switch# **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。

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
show role [*role-name*]	ユーザー ロールの設定を表示します。
show role feature	機能リストを表示します。
show role feature-group	機能グループの設定を表示します。

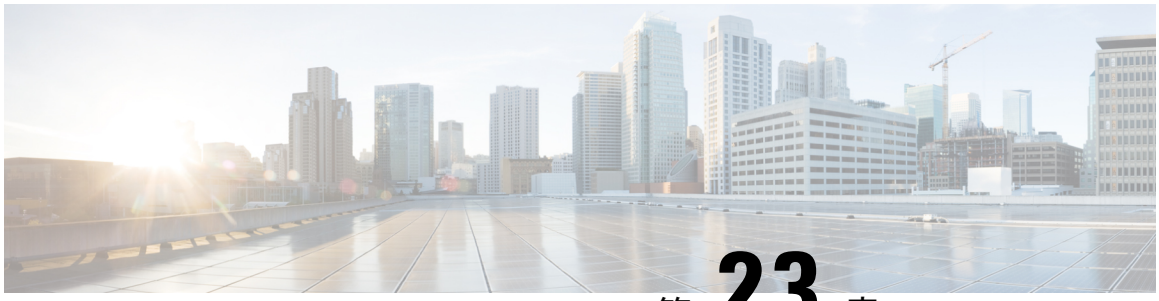
コマンド	目的
show startup-config security	スタートアップ コンフィギュレーションのユーザ アカウント設定を表示します。
show running-config security [**all**]	実行コンフィギュレーションのユーザ アカウント設定を表示します。**all** キーワードを指定すると、ユーザ アカウントのデフォルト値が表示されます。
show user-account	ユーザ アカウント情報を表示します。

ユーザー 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 31: 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 23 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

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
factory-resetfex module*mod* 例： `switch(config)# factory-reset [module <3>]`	**all** オプションを有効にしてコマンドを使用してください。**factory reset** 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。 fex の消去を保護するには、**factory-resetfex** [*allfex_no*] を使用します。 • 一度にすべての fex を安全に消去するには、オプション **all** を使用します。 （注） 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。 オプション **mod** を使用して、起動構成をリセットします。 • top-of-rack（ToR; トップオブラック）スイッチの場合、コマンドは **factory-reset** または **factory-reset module 1** です。 • トップ オブ ラック スイッチの LXC モードでは、コマンドは **factory-reset module 1** または **27** です。 • 行末のモジュール スイッチの場合、**factory-reset module #module_number** コマンドは次のとおりです。 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。

（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 ワイプ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 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
[2.210329] 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
[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
```

安全な消去の設定

```
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
[ 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 sgmii 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
```

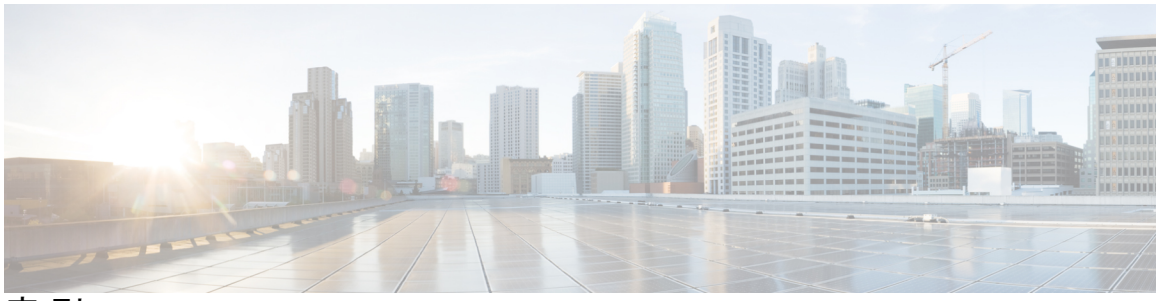
次に、LC で安全な消去による工場出荷時リセット コマンドを設定するための出力ログの例を示します。

```
switch#
switch# factory-reset mod 1
!!!! 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 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 !!!!
Continue? (y/n) [n] y
A module reload is required for the reset operation to proceed. Please, wait...
reloading module 1 ...
.....................................................................
SUCCESS! All persistent storage devices detected on the specified module have been purged.
switch#
```

次に、modでの安全な消去による工場出荷時リセットコマンドを設定した場合の出力ログの例を示します。

```
switch# factory-reset mod 26
!!!! 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 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 !!!!
Continue? (y/n) [n] y
A module reload is required for the reset operation to proceed. Please, wait...
reloading module 26 ...
.....................................................................
.......................
.....................................................................
.......................
.....................................................................
.......................
.....................................................................
.......................
.....................................................................
.......................
.....................................................................
.......................
.....................................................................
SUCCESS! All persistent storage devices detected on the specified module have been
cleared.
>>>> Please, note - multiple write passes were required to remove data from one or more
 devices. <<<<
switch#
```

安全な消去の設定



索 引

P

R

S

V

あ

い

か

き

く

こ

さ

し

す

せ

そ

た

ち

つ

て

と

は

ひ

ふ

へ

ほ

む

め

も

ゆ

よ

ら

り

る

れ

ろ

わ

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。