Cisco Nexus 5000 シリーズ NX-OS システム管理コンフィギュレーション ガイド リリース 5.1(3)N1(1)

初版：2011 年 12 月 05 日

最終更新：2012 年 02 月 26 日

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

Text Part Number: OL-25846-01-J

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

目 次

はじめに

ここでは、次の項について説明します。

対象読者

この出版物は Cisco Nexus シリーズ デバイスおよび Cisco Nexus 2000 シリーズ ファブリック エクステンダの設定と保守を行う経験豊富な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]	角カッコで囲まれているものは、省略可能な要素（キーワードまたは引数）です。
[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。

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

例では、次の表記法を使用しています。

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

このマニュアルでは、次の表記法を使用しています。

（注） 「注釈」です。 役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

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

関連資料

完全な Cisco NX-OS 5000 シリーズ マニュアル セットは、次の URL で入手できます。
http://www.cisco.com/en/US/products/ps9670/tsd_products_support_series_home.html

リリース ノート

リリース ノートは、次の URL で入手できます。
http://www.cisco.com/en/US/products/ps9670/prod_release_notes_list.html

コンフィギュレーション ガイド

これらのガイドは、次の URL で入手できます。
http://www.cisco.com/en/US/products/ps9670/products_installation_and_configuration_guides_list.html
このカテゴリのマニュアルは次のとおりです。

- 『*Adapter-FEX Configuration Guide*』
- 『*Cisco Fabric Manager Configuration Guide*』
- 『*Cisco Nexus 5000 Series NX-OS Software Configuration Guide*』
- 『*Configuration Limits for Cisco NX-OS*』
- 『*FabricPath Configuration Guide*』
- 『*Fibre Channel over Ethernet Configuration Guide*』
- 『*Layer 2 Switching Configuration Guide*』
- 『*Multicast Routing Configuration Guide*』
- 『*Operations Guide*』
- 『*SAN Switching Configuration Guide*』
- 『*Quality of Service Configuration Guide*』
- 『*Security Configuration Guide*』
- 『*System Management Configuration Guide*』
- 『*Unicast Routing Configuration Guide*』

メンテナンスおよび操作ガイド

さまざまな機能に対応する『Cisco Nexus 5000 Series NX-OS Operations Guide』は、http://www.cisco.com/en/US/products/ps9670/prod_maintenance_guides_list.html で入手できます。

インストレーション ガイドおよびアップグレード ガイド

これらのガイドは、次の URL で入手できます。

http://www.cisco.com/en/US/products/ps9670/prod_installation_guides_list.html

このカテゴリのマニュアルは次のとおりです。

- 『*FabricPath Command Reference*』
- 『*Software Upgrade and Downgrade Guides*』
- 『*Regulatory Compliance and Safety Information*』

ライセンス ガイド

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

コマンド リファレンス

これらのガイドは、次の URL で入手できます。

http://www.cisco.com/en/US/products/ps9670/prod_command_reference_list.html

このカテゴリのマニュアルは次のとおりです。

- 『*Command Reference Master Index*』
- 『*Fabric Extender Command Reference*』
- 『*FabricPath Command Reference*』
- 『*Fibre Channel Command Reference*』
- 『*Fundamentals Command Reference*』
- 『*Layer 2 Interfaces Command Reference*』
- 『*Multicast Routing Command Reference*』
- 『*QoS Command Reference*』
- 『*Security Command Reference*』
- 『*System Management Command Reference*』
- 『*TrustSec Command Reference*』
- 『*Unicast Routing Command Reference*』
- 『*vPC Command Reference*』

テクニカル リファレンス

『*Cisco Nexus 5000 and Cisco Nexus 2000 MIBs Reference*』は、http://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/mib/reference/NX5000_MIBRef.html で入手できます。

エラー メッセージおよびシステム メッセージ

『*Nexus 5000 Series NX-OS System Message Reference*』は、http://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/system_messages/reference/sl_nxos_book.html で入手できます。

トラブルシューティング ガイド

『*Cisco Nexus 5000 Series Troubleshooting Guide*』は、http://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/troubleshooting/guide/N5K_Troubleshooting_Guide.html で入手できます。

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』は Really Simple Syndication（RSS）フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。 RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

第 1 章

新機能および変更された機能に関する情報

この章では、『*Cisco Nexus 3000 Series NX-OS Fundamentals Configuration Guide*』の新機能および変更された機能に関するリリース固有の情報を示します。

このリリースの新規および変更情報

次の表に、最新リリースに関するこのガイドでの重要な変更点の概要を示します。 この表は、実行コンフィギュレーション ガイドへのすべての変更や、またはこのリリースの新機能の詳細なリストを提供しません。

表 *1*：新機能

機能	説明	参照先
設定の同期	スイッチプロファイルで設定されたポートチャネル メンバ ポートの設定の同期の改善。	スイッチプロファイルの設定，（9 ページ）
システム メッセージ ロギング	8 台の syslog サーバのサポート。	システム メッセージ ロギングの設定，（101 ページ）
ERSPAN	Encapsulated Remote Switched Port Analyzer（ERSPAN）機能の設定のサポート。	ERSPAN の設定，（207 ページ）
IPv6 の SNMP サポート	IPv6 をサポートするための SNMP の機能拡張。	SNMP の設定，（163 ページ）

第 2 章

概要

この章の内容は、次のとおりです。

システム管理機能

このマニュアルに記載されているシステム管理機能について説明します。

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

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

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

機能	説明
設定のロール バック	設定のロールバック機能を使用すると、Cisco NX-OS のコンフィギュレーションのスナップショットまたはユーザ チェックポイントを使用して、スイッチをリロードしなくても、いつでもそのコンフィギュレーションをスイッチに再適用できます。 権限のある管理者であれば、チェックポイントで設定されている機能について専門的な知識がなくても、ロールバック機能を使用して、そのチェックポイント コンフィギュレーションを適用できます。
SNMP	簡易ネットワーク管理プロトコル（SNMP）は、SNMP マネージャとエージェントの間の通信のメッセージフォーマットを提供するアプリケーション層プロトコルです。 SNMP は、ネットワーク内のデバイスのモニタリングおよび管理に使用する標準フレームワークと共通言語を提供します。
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インターネット技術特別調査委員会（IETF）標準モニタリング仕様です。 Cisco NX-OS では、Cisco NX-OS デバイスをモニタするための、RMON アラーム、イベント、およびログをサポートします。
SPAN	スイッチド ポート アナライザ（SPAN）機能（ポート ミラーリングまたはポート モニタリングとも呼ばれる）は、ネットワーク アナライザによる分析のためのネットワーク 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。

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

第 3 章

スイッチ プロファイルの設定

この章の内容は、次のとおりです。

スイッチ プロファイルに関する情報

複数のアプリケーションは、ネットワーク内のCisco Nexusシリーズスイッチ間で整合性のある設定が必要です。 たとえば、仮想ポート チャネル（vPC）を使用する場合、同じ設定にする必要があります。 設定の不一致により、エラーや設定ミスが発生し、サービスが中断されることがあります。

設定の同期（config-sync）機能では、1 つのスイッチ プロファイルを設定し、設定を自動的にピア スイッチに同期させることができます。 スイッチ プロファイルには、次の利点があります。

- 設定をスイッチ間で同期できます。
- 2 台のスイッチ間で接続が確立されると、設定がマージされます。
- 同期される設定を正確に制御できます。
- マージおよび相互排除チェックを通じて、ピア全体の設定の一貫性を保証します。
- 確認とコミットのセマンティックが提供されます。
- ポート プロファイル コンフィギュレーションの設定と同期をサポートします。
- 既存の vPC 設定をスイッチ プロファイルに移行するためのインポート コマンドが提供されます。

スイッチ プロファイル コンフィギュレーション モード

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

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

コンフィギュレーション同期モード

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

スイッチ プロファイル モード

スイッチプロファイルモードでは、後でピアスイッチと同期化されるスイッチプロファイルに、サポートされているコンフィギュレーション コマンドを追加できます。 スイッチ プロファイルモードで入力したコマンドは、**commit** コマンドを入力するまでバッファに格納されます。

スイッチ プロファイル インポート モード

以前のリリースからアップグレードするとき、スイッチ プロファイルに、サポートされている実行コンフィギュレーション コマンドをコピーするため、**import** コマンドを入力できます。 **import** コマンドを入力した後、スイッチプロファイルモード（config-sync-sp）は、スイッチプロファイル インポート モード（config-sync-sp-import）に変わります。 スイッチ プロファイル インポート モードでは、既存のスイッチ設定を実行コンフィギュレーションからインポートし、どのコマンドをスイッチ プロファイルに含めるかを指定できます。

異なるトポロジで、スイッチ プロファイルに含まれる異なるコマンドが必要になるため、**import** コマンド モードでは、特定のトポロジに合うようにインポートされたコマンドを変更できます。 たとえば、デュアルホームファブリックエクステンダ（FEX）トポロジでは、大部分の設定が同期している必要があります。 他の vPC トポロジでは、同期する必要がある設定は、かなり小さいコマンドのセットである可能性があります。

インポート プロセスを完了し、スイッチ プロファイルにコンフィギュレーションを移動するには、**commit** コマンドを入力する必要があります。 インポート プロセス中の設定変更がサポートされないため、新しいコマンドを **commit** コマンドを入力する前に追加すると、スイッチプロファイルが保存されないまま残り、スイッチはスイッチ プロファイル インポート モードのままになります。 追加したコマンドを削除するか、またはインポートを中断します。 未保存のコンフィギュレーションは、プロセスが中断されると失われます。 インポートの完了後、スイッチ プロファイルに新しいコマンドを追加できます。

設定の確認

2 種類の設定の有効性検査により、2 種類のスイッチ プロファイルの障害を識別できます。

- 相互排除チェック
- マージ チェック

相互排除チェック

スイッチプロファイルに含まれる設定を上書きする可能性を減らすため、相互排除（mutex）は、スイッチ プロファイルのコマンドを、ローカル スイッチ上に存在するコマンドと、ピア スイッチ上のコマンドに対してチェックします。 あるスイッチプロファイルに含まれるコマンドをそのスイッチ プロファイルの外部やピア スイッチで設定することはできません。 この要件は、既存のコマンドが意図せず上書きされる可能性を減らします。

mutex チェックは、コミット プロセスの一部として、ピア スイッチに到達できる場合は両方のスイッチで行われ、そうでない場合はローカルで実行されます。 設定端末から行われた設定変更は、ローカル スイッチだけで発生します。

mutex チェックがエラーを識別すると、mutex の障害として報告され、手動で修正する必要があります。

次の例外は相互排除ポリシーに適用されます。

- インターフェイス設定：Release 5.1(3) よりも前のリリースでは、競合がない限り、インターフェイス設定の一部がスイッチプロファイルに存在し、一部が実行コンフィギュレーションに存在できました。 Release 5.1(3) 以降では、ポート チャネル インターフェイスは、スイッチ プロファイル モードまたはグローバル コンフィギュレーション モードのいずれかで完全に設定する必要があります。

（注） 一部のポート チャネル サブコマンドは、スイッチ プロファイル モードで設定できません。 これらのコマンドは、ポート チャネルがスイッチプロファイル モードで作成および設定されている場合でも、グローバル コンフィギュレーション モードで設定できます。

たとえば、次のコマンドはグローバル コンフィギュレーション モードでしか設定できません。

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

- shutdown/no shutdown
- システム QoS

マージ チェック

マージ チェックは設定を受信するピア スイッチで行われます。 マージ チェックによって、受信したコンフィギュレーションが受信側スイッチ上の既存のスイッチ プロファイル コンフィギュレーションと競合しないことが確認されます。 マージ チェックは、マージまたはコミット プロセスで実行されます。 マージが失敗した場合はエラーが報告され、手動で修正する必要があります。

いずれかまたは両方のスイッチがリロードされ、コンフィギュレーションが最初に同期されると、マージチェックは、スイッチプロファイルの設定が両方のスイッチで同じであることを確認します。 スイッチプロファイルの違いは、マージ障害として報告され、手動で修正する必要があります。

スイッチプロファイルを使用したソフトウェアのアップグレードおよびダウングレード

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

以前のリリースからアップグレードする場合、スイッチ プロファイルに一部の実行コンフィギュレーション コマンドを移動することを選択できます。 **import** コマンドでは、関連するスイッチ プロファイルコマンドをインポートできます。アップグレードは、バッファされた設定（コミットされていない）がある場合に実行できます。ただし、コミットされていない設定は失われます。

スイッチ プロファイルに含まれるスイッチの 1 つで、In Service Software Upgrade（ISSU）を実行すると、ピアが到達不能であるため、設定の同期は実行できません。

スイッチ プロファイルの前提条件

スイッチ プロファイルには次の前提条件があります。

- **cfs ipv4 distribute** コマンドを入力して、両方のスイッチで mgmt0 上の IP を介した Cisco Fabric Series（CFSoIP）配布をイネーブルにする必要があります。
- **config sync** コマンドと **switch-profile** コマンドを入力して、両方のピア スイッチで同じ名前を持つスイッチ プロファイルを設定する必要があります。
- **sync-peers destination** コマンドを入力して、各スイッチをピア スイッチとして設定します

スイッチ プロファイルの注意事項および制約事項

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

- mgmt0 インターフェイスを使用してのみ設定同期化をイネーブルにできます。
- 設定の同期は、mgmt 0 インターフェイスを使用して実行され、管理 SVI を使用して実行できません。
- 同じスイッチ プロファイル名で同期されたピアを設定する必要があります。
- スイッチ プロファイル設定で使用可能なコマンドを、設定スイッチ プロファイル（config-sync-sp）モードで設定できます。
- サポートされているスイッチ プロファイル コマンドは、vPC コマンドに関連します。 FCoE コマンドはサポートされません。
- 1 つのスイッチ プロファイル セッションが一度に進行できます。 別のセッションの開始を試みると失敗します。
- スイッチ プロファイル セッションの進行中は、コンフィギュレーション端末モードから実行されたサポートされているコマンドの変更はブロックされます。 スイッチ プロファイル セッションが進行しているときは、コンフィギュレーション端末モードからサポートされていないコマンドの変更を行わないでください。
- **commit** コマンドを入力し、ピア スイッチに到達可能である場合、設定は、両方のピア スイッチに適用されるか、いずれのスイッチにも適用されません。 コミットの障害が発生した場合、コマンドは、スイッチプロファイルバッファに残ります。 その場合、必要な修正をし、コミットを再試行します。
- シスコでは、インターフェイス コンフィギュレーションが設定同期機能を使用して同期される、すべての Generic Expansion Module（GEM）モジュールおよび Cisco Nexus ファブリック エクステンダ モジュールで事前プロビジョニングをイネーブルにすることを推奨します。 ファブリック エクステンダが 1 台のスイッチでオンラインでない可能性があり、その設定が変更され、他のスイッチで同期される、Cisco Nexus ファブリック エクステンダ アクティブ/アクティブ トポロジでは、次の注意事項に従ってください。 このシナリオでは、事前プロ

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

- ポート チャネルがスイッチ プロファイル モードを使用して設定されている場合、グローバル コンフィギュレーション（config 端末）モードを使用して設定できません。

（注） 一部のポート チャネル サブコマンドは、スイッチ プロファイル モードで設定できません。 これらのコマンドは、ポート チャネルがスイッチ プロファイル モードで作成および設定されている場合でも、グローバル コンフィギュレーション モードで設定できます。

たとえば、次のコマンドはグローバル コンフィギュレーション モードでしか設定できません。

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

- shutdown および no shutdown はグローバル コンフィギュレーション モードまたはスイッチ プロファイル モードで設定できます。
- ポート チャネルがグローバル コンフィギュレーション モードで作成されている場合、メンバ インターフェイスを含むチャネル グループも、グローバル コンフィギュレーション モードを使用して作成する必要があります。
- スイッチ プロファイル モードで設定されたポート チャネルでは、スイッチ プロファイルの内側と外側の両方にメンバを持つ場合があります。
- スイッチ プロファイルにメンバ インターフェイスをインポートする場合、メンバ インターフェイスを含むポート チャネルもスイッチ プロファイル内に存在する必要があります。

リブート、接続損失、または障害後の同期化に関する注意事項

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

  設定変更を 1 台のスイッチだけで実行する場合、マージは、mgmt0 インターフェイスが起動し、設定が他のスイッチに適用されると実行されます。
- ISSU が 1 台のスイッチで実行され、設定変更がピア スイッチで行われる場合の設定の同期化：vPC トポロジでは、ピア スイッチの設定変更は、ISSU が他のスイッチで実行される場

合は許可されません。 vPC のないトポロジでは、設定変更は許可され、アップグレードが完了すると、ISSU を実行しているスイッチは新しい設定を同期します。

スイッチ プロファイルの設定

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

はじめる前に

各スイッチに同じ名前を持つスイッチ プロファイルを作成し、スイッチを互いにピアとして設定する必要があります。 同じアクティブ スイッチ プロファイルを持つスイッチ間で接続が確立されると、スイッチ プロファイルが同期されます。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的

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

ステップ 2	**cfs ipv4 distribute**
	
	例：
	`switch(config)# cfs ipv4 distribute`
	`switch(config)#`
		ピア スイッチ間の CFS 配信をイネーブルにします。

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

	コマンドまたはアクション	目的

ステップ 4	**switch-profile** *name*
	
	例：
	`switch(config-sync)# switch-profile abc`
	`switch(config-sync-sp)#`
		スイッチプロファイルを設定し、スイッチプロファイルの名前を設定し、スイッチプロファイル同期コンフィギュレーション モードを開始します。

ステップ 5	**sync-peers destination** *IP-address*
	
	例：
	`switch(config-sync-sp)# sync-peers destination 10.1.1.1`
	`switch(config-sync-sp)#`
		ピア スイッチを設定します。

ステップ 6	**show switch-profile** *name* **status**
	
	例：
	`switch(config-sync-sp)# show switch-profile abc status`
	`switch(config-sync-sp)#`
		（任意）
		ローカルスイッチのスイッチプロファイルおよびピア スイッチ情報を表示します。

ステップ 7	**exit**
	
	例：
	`switch(config-sync-sp)# exit`
	`switch#`
		スイッチプロファイルコンフィギュレーションモードを終了し、EXEC モードに戻ります。

ステップ 8	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

次に、スイッチプロファイルを設定し、スイッチプロファイルのステータスを表示する例を示します。

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

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

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

Peer information:
----------------
IP-address: 10.1.1.1
Sync-status: In Sync.
```

```
Status: Commit Success
Error(s):
switch(config-sync-sp)# exit
switch#
```

スイッチ プロファイルへのスイッチの追加

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

スイッチを追加する場合は、次の注意事項に従ってください。

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

  スイッチ プロファイルにメンバ インターフェイスをインポートする場合、メンバ インターフェイスを含むポート チャネルもスイッチ プロファイル内に存在する必要があります。

はじめる前に

ローカル スイッチでスイッチ プロファイルを作成した後、同期に含まれる 2 番めのスイッチを追加する必要があります。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config sync**
	
	例：
	`switch# config sync`
	`switch(config-sync)#`
		コンフィギュレーション同期モードを開始します。

	コマンドまたはアクション	目的

ステップ 2	**switch-profile** *name*
	
	例：
	`switch(config-sync)# switch-profile abc`
	`switch(config-sync-sp)#`
		スイッチプロファイルを設定し、スイッチプロファイルの名前を設定し、スイッチプロファイル同期コンフィギュレーション モードを開始します。

ステップ 3	**sync-peers destination** *destination IP*
	
	例：
	`switch(config-sync-sp)# sync-peers destination 10.1.1.1`
	`switch(config-sync-sp)#`
		スイッチ プロファイルにスイッチを追加します。

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

ステップ 5	**show switch-profile peer** 例： `switch# show switch-profile peer`	（任意） スイッチプロファイルのピアの設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

スイッチ プロファイルのコマンドの追加または変更

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

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

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

はじめる前に

ローカルおよびピア スイッチでスイッチ プロファイルを設定したら、スイッチ プロファイルにサポートされているコマンドを追加し、コミットする必要があります。 コマンドは、**commit** コマンドを入力するまでスイッチ プロファイル バッファに追加されます。 **commit** コマンドは次を行います。

- mutex チェックとマージ チェックを起動し、同期を確認します。
- ロールバック インフラストラクチャでチェックポイントを作成します。
- ローカル スイッチおよびピア スイッチのコンフィギュレーションを適用します。
- スイッチプロファイル内の任意のスイッチでアプリケーション障害がある場合は、すべてのスイッチでロール バックを実行します。
- チェックポイントを削除します。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config sync**
	
	例：
	`switch# config sync`
	`switch(config-sync)#`
		コンフィギュレーション同期モードを開始します。

ステップ 2	**switch-profile** *name*
	
	例：
	`switch(config-sync)# switch-profile abc`
	`switch(config-sync-sp)#`
		スイッチプロファイルを設定し、スイッチプロファイルの名前を設定し、スイッチ プロファイル同期コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的

ステップ 3	**command** *argument*
	
	例：
	`switch(config-sync-sp)# interface Port-channel100`
	`switch(config-sync-sp-if)# speed 1000`
	`switch(config-sync-sp-if)# interface Ethernet1/1`
	`switch(config-sync-sp-if)# speed 1000`
	`switch(config-sync-sp-if)# channel-group 100`
		スイッチ プロファイルにコマンドを追加します。

ステップ 4	**show switch-profile** *name* **buffer**
	
	例：
	`switch(config-sync-sp)# show switch-profile abc buffer`
	`switch(config-sync-sp)#`
		（任意）
		スイッチ プロファイル バッファ内のコンフィギュレーション コマンドを表示します。

ステップ 5	**verify** 例： `switch(config-sync-sp)# verify`	スイッチ プロファイル バッファ内のコマンドを確認します。
ステップ 6	**commit** 例： `switch(config-sync-sp)# commit`	スイッチ プロファイルにコマンドを保存し、ピア スイッチと設定を同期します。

ステップ 7	**show switch-profile** *name* **status**
	
	例：
	`switch(config-sync-sp)# show switch-profile abc status`
	`switch(config-sync-sp)#`
		（任意）
		ローカルスイッチのスイッチプロファイルのステータスとピア スイッチのステータスを表示します。

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

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

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

```
switch# configuration terminal
switch(config)# cfs ipv4 distribute
switch(config-sync)# switch-profile abc
switch(config-sync-sp)# sync-peers destination 10.1.1.1
switch(config-sync-sp)# interface port-channel100
switch(config-sync-sp-if)# speed 1000
```

```
switch(config-sync-sp-if)# interface Ethernet1/1
switch(config-sync-sp-if)# speed 1000
switch(config-sync-sp-if)# channel-group 100
switch(config-sync-sp)# verify
switch(config-sync-sp)# commit
switch(config-sync-sp)# exit
switch#
```

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

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

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

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

スイッチ プロファイルのインポート

インポートするコマンドのセットに基づいてスイッチプロファイルをインポートできます。 コンフィギュレーション端末モードの使用：

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

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

新しいコマンドがインポート中に追加されると、スイッチ プロファイルが保存されていないままになり、スイッチはスイッチプロファイル インポート モードのままになります。 **abort** コマンドを入力してインポートを停止します。 スイッチ プロファイルのインポートの詳細については、「スイッチ プロファイル インポート モード」の項を参照してください。

手順の概要

1. **config sync**
2. **switch-profile** *name*
3. **import** {*interface port/slot* | *running-config* [**exclude interface ethernet**]}
4. **commit**
5. （任意） **abort**
6. **exit**
7. （任意） **show switch-profile**
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	**config sync**
	
	例：
	`switch# config sync`
	`switch(config-sync)#`
		コンフィギュレーション同期モードを開始します。

ステップ 2	**switch-profile** *name*
	
	例：
	`switch(config-sync)# switch-profile abc`
	`switch(config-sync-sp)#`
		スイッチ プロファイルを設定し、スイッチ プロファイルの名前を設定し、スイッチプロファイル同期コンフィギュレーション モードを開始します。

ステップ 3	**import** {*interface port/slot* | *running-config* [**exclude interface ethernet**]}
	
	例：
	`switch(config-sync-sp)# import ethernet 1/2`
	`switch(config-sync-sp-import)#`
		インポートするコマンドを識別し、スイッチプロファイルインポート モードを開始します。
		• <CR>：選択したコマンドを追加します。
		• **interface**：指定したインターフェイスのサポートされるコマンドを追加します。
		• **running-config**：サポートされるシステムレベル コマンドを追加します。
		• **running-config exclude interface ethernet**：物理インターフェイス コマンドを除く、サポートされるシステムレベル コマンドを追加します。

ステップ 4	**commit** 例： `switch(config-sync-sp-import)# commit`	コマンドをインポートし、スイッチプロファイルにコマンドを保存します。

	コマンドまたはアクション	目的
ステップ 5	**abort** 例： `switch(config-sync-sp-import)# abort`	（任意） インポート プロセスを中止します。

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

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

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

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

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

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

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

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

vPC トポロジでの設定のインポート

2 スイッチ vPC トポロジで設定をインポートできます。

（注） 次の手順の詳細については、この章の該当する項を参照してください。

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

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

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

スイッチ プロファイルのコマンドの確認

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

手順の概要

1. **config sync**
2. **switch-profile** *name*
3. **verify**
4. **exit**
5. （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 sync**
	
	例：
	`switch# config sync`
	`switch(config-sync)#`
		コンフィギュレーション同期モードを開始します。

	コマンドまたはアクション	目的

ステップ 2	**switch-profile** *name*
	
	例：
	`switch(config-sync)# switch-profile abc`
	`switch(config-sync-sp)#`
		スイッチプロファイルを設定し、スイッチプロファイルの名前を設定し、スイッチ プロファイル同期コンフィギュレーション モードを開始します。

ステップ 3	**verify** 例： `switch(config-sync-sp)# verify`	スイッチプロファイルバッファ内のコマンドを確認します。

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

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

ピア スイッチの分離

スイッチ プロファイルを変更するためにピア スイッチを分離できます。 このプロセスは、設定の同期をブロックする場合、または設定をデバッグするときに使用できます。

ピア スイッチを分離するには、スイッチプロファイルからスイッチを削除し、スイッチプロファイルにピア スイッチを追加する必要があります。

（注） 次の手順の詳細については、この章の該当する項を参照してください。

一時的にピア スイッチを分離するには、次の手順を実行します。

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

スイッチ プロファイルの削除

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

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config sync**
	
	例：
	`switch# config sync`
	`switch(config-sync)#`
		コンフィギュレーション同期モードを開始します。

ステップ 2	**no switch-profile name** {**all-config** | **local-config**}
	
	例：
	`switch(config-sync)# no switch-profile abc local-config`
	`switch(config-sync-sp)#`
		次の手順に従って、スイッチプロファイルを削除します。
		• **all-config**：ローカル スイッチおよびピア スイッチのスイッチ プロファイルを削除します。 ピア スイッチが到達可能でない場合は、ローカルスイッチプロファイルだけが削除されます。
		• **local-config**：スイッチ プロファイルおよびローカル コンフィギュレーションを削除します。

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

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

スイッチ プロファイルからのスイッチの削除

スイッチ プロファイルからスイッチを削除できます。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config sync**
	
	例：
	`switch# config sync`
	`switch(config-sync)#`
		コンフィギュレーション同期モードを開始します。

ステップ 2	**switch-profile** *name*
	
	例：
	`switch(config-sync)# switch-profile abc`
	`switch(config-sync-sp)#`
		スイッチプロファイルを設定し、スイッチプロファイルの名前を設定し、スイッチ プロファイル同期コンフィギュレーション モードを開始します。

ステップ 3	**no sync-peers destination** *destination IP*
	
	例：
	`switch(config-sync-sp)# no sync-peers destination 10.1.1.1`
	`switch(config-sync-sp)#`
		スイッチ プロファイルから指定のスイッチを削除します。

	コマンドまたはアクション	目的

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

ステップ 5	**show switch-profile** 例： `switch# show switch-profile`	（任意） スイッチプロファイルコンフィギュレーションを表示します。
ステップ 6	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

スイッチ プロファイル バッファの表示

手順の概要

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

手順の詳細

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

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

```
switch# configure sync
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config-sync)# switch-profile sp
Switch-Profile started, Profile ID is 1
switch(config-sync-sp)# show switch-profile sp buffer
-----------------------------------------------------------
Seq-no  Command
-----------------------------------------------------------
1       vlan 101
1.1       ip igmp snooping querier 10.101.1.1
2       mac address-table static 0000.0000.0001 vlan 101 drop
3       interface Ethernet1/2
3.1       switchport mode trunk
3.2       switchport trunk allowed vlan 101

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

スイッチのリブート後のコンフィギュレーションの同期化

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

手順の概要

1. リブート中にピア スイッチ上で変更された設定を再適用します。
2. **commit** コマンドを入力します。
3. 設定が正しく適用されており、両方のピアが同期されていることを確認します。

手順の詳細

ステップ 1 リブート中にピア スイッチ上で変更された設定を再適用します。

ステップ 2 **commit** コマンドを入力します。

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

スイッチ プロファイル設定の show コマンド

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

コマンド	目的
show switch-profile *name*	スイッチ プロファイル中のコマンドを表示します。
show switch-profile *name* **buffer**	スイッチ プロファイル中のコミットされていないコマンド、移動されたコマンド、削除されたコマンドを表示します。
show switch-profile *name* **peer** *IP-address*	ピア スイッチの同期ステータスが表示されます。
show switch-profile *name* **session-history**	最後の 20 のスイッチ プロファイル セッションのステータスを表示します。
show switch-profile *name* **status**	ピア スイッチのコンフィギュレーション同期ステータスを表示します。
show running-config expand-port-profile	ポート プロファイルについての詳細が表示されます。
show running-config exclude-provision	オフラインで事前プロビジョニングされた非表示のインターフェイスの設定を表示します。
show running-config switch-profile	ローカル スイッチのスイッチプロファイルの実行コンフィギュレーションを表示します。
show startup-config switch-profile	ローカル スイッチのスイッチプロファイルのスタートアップ コンフィギュレーションを表示します。

これらのコマンドの出力フィールドの詳細については、『*Cisco Nexus 5000 Series Command Reference*』を参照してください。

スイッチ プロファイルの設定例

ローカルおよびピア スイッチでのスイッチ プロファイルの作成例

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

手順の概要

1. ローカルおよびピア スイッチで CFSoIP 配信をイネーブルにします。
2. ローカルおよびピア スイッチでスイッチ プロファイルを作成します。
3. スイッチ プロファイルが、ローカルおよびピア スイッチで同じであることを確認します。
4. ローカル スイッチでスイッチプロファイルにコンフィギュレーションコマンドを追加します。コマンドがコミットされたときに、コマンドがピア スイッチに適用されます。
5. バッファ リングされたコマンドを表示します。
6. スイッチ プロファイルのコマンドを検証します。
7. スイッチ プロファイルにコマンドを適用し、ローカルとピア スイッチ間の設定を同期させます。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	ローカルおよびピア スイッチで CFSoIP 配信をイネーブルにします。 例： switch# **configuration terminal** switch(config)# **cfs ipv4 distribute**	
ステップ 2	ローカルおよびピア スイッチでスイッチ プロファイルを作成します。 例： switch(config-sync)# **switch-profile abc** switch(config-sync-sp)# **sync-peers destination 10.1.1.1**	
ステップ 3	スイッチ プロファイルが、ローカルおよびピア スイッチで同じであることを確認します。 例： switch(config-sync-sp)# **show switch-profile abc status** Start-time: 15801 usecs after Mon Aug 23 06:21:08 2010 End-time: 6480 usecs after Mon Aug 23 06:21:13 2010 Profile-Revision: 1 Session-type: Initial-Exchange Peer-triggered: Yes Profile-status: Sync Success Local information: ---------- Status: Commit Success Error(s): Peer information: ---------- IP-address: 10.1.1.1 Sync-status: In Sync. Status: Commit Success Error(s):	

	コマンドまたはアクション	目的

ステップ 4	ローカル スイッチでスイッチプロファイルにコンフィギュレーション コマンドを追加します。コマンドがコミットされたときに、コマンドがピア スイッチに適用されます。
	
	例：
	`switch(config-sync-sp)# class-map type qos c1`
	`switch(config-sync-sp-cmap-qos)# match cos 2`
	`switch(config-sync-sp-cmap-qos)# class-map type qos c2`
	`switch(config-sync-sp-cmap-qos)# match cos 5`
	`switch(config-sync-sp-cmap-qos)# policy-map type qos p1`
	`switch(config-sync-sp-pmap-qos)# class c1`
	`switch(config-sync-sp-pmap-c-qos)# set qos-group 2`
	`switch(config-sync-sp-pmap-c-qos)# class c2`
	`switch(config-sync-sp-pmap-c-qos)# set qos-group 3`
	`switch(config-sync-sp-pmap-c-qos)# system qos`
	`switch(config-sync-sp-sys-qos)# service-policy type qos input p1`
	`switch(config-sync-sp-sys-qos)# vlan 1-50`
	`switch(config-sync-sp-vlan)# interface port-channel 100`
	`switch(config-sync-sp-if)# vpc peer-link`
	`switch(config-sync-sp-if)# switchport mode trunk`
	`switch(config-sync-sp-if)# interface port-channel 10`
	`switch(config-sync-sp-if)# vpc 1`
	`switch(config-sync-sp-if)# switchport mode trunk`
	`switch(config-sync-sp-if)# switchport trunk allowed vlan 1, 10-50`	

ステップ 5	バッファ リングされたコマンドを表示します。
	
	例：
	`switch(config-sync-sp-if)# show switch-profile switch-profile buffer`
	`----------`
	`Seq-no  Command`
	`----------`
	`1  class-map type qos match-all c1`
	`1.1  match cos 2`
	`2  class-map type qos match-all c2`
	`2.1  match cos 5`
	`3  policy-map type qos p1`
	`3.1  class c1`
	`3.1.1  set qos-group 2`
	`3.2  class c2`
	`3.2.1  set qos-group 3`
	`4  system qos`
	`4.1  service-policy type qos input p1`
	`5  vlan 2-50`
	`6  interface port-channel100`
	`6.1  vpc peer-link`
	`6.2  switchport mode trunk`
	`7  interface port-channel10`
	`7.1  vpc 1`
	`7.2  switchport mode trunk`
	`7.3  switchport trunk allowed vlan 1, 10-50`	

ステップ 6	スイッチ プロファイルのコマンドを検証します。	

	コマンドまたはアクション	目的

	例：
	`switch(config-sync-sp-if)# verify`
	`Verification Successful`	

ステップ 7	スイッチ プロファイルにコマンドを適用し、ローカルとピア スイッチ間の設定を同期させます。
	
	例：
	`switch(config-sync-sp)# commit`
	`Commit Successful`
	`switch(config-sync)#`	

同期ステータスの確認例

次に、ローカルとピア スイッチ間の同期ステータスを確認する例を示します。

手順の概要

1. **show switch-profile switch-profile status** コマンドを入力します。

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**show switch-profile switch-profile status** コマンドを入力します。
	
	例：
	`switch(config-sync)# show switch-profile switch-profile status`
	
	`Start-time: 804935 usecs after Mon Aug 23 06:41:10 2010`
	`End-time: 956631 usecs after Mon Aug 23 06:41:20 2010`
	
	`Profile-Revision: 2`
	`Session-type: Commit`
	`Peer-triggered: No`
	`Profile-status: Sync Success`
	
	`Local information:`
	`----------`
	`Status: Commit Success`
	`Error(s):`
	
	`Peer information:`
	`----------`
	`IP-address: 10.1.1.1`
	`Sync-status: In Sync.`
	`Status: Commit Success`
	`Error(s):`	

	コマンドまたはアクション	目的
	`switch(config-sync)#`	

実行コンフィギュレーションの表示

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

```
switch# configure sync
switch(config-sync)# show running-config switch-profile
switch-profile sp
  sync-peers destination 10.1.1.1
  class-map type qos match-all c1
    match cos 2
  class-map type qos match-all c2
    match cos 5
  policy-map type qos p1
    class c1
      set qos-group 2
    class c2
      set qos-group 3
  system qos
    service-policy type qos input p1
  vlan 2-50

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

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

ローカル スイッチとピア スイッチ間のスイッチ プロファイルの同期の表示

次に、2 台のピア スイッチの同期ステータスを表示する例を示します。

```
switch1# show switch-profile sp status

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

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

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

Peer information:
```

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

switch1#


switch2# show switch-profile sp status

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

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

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

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

switch2#
```

ローカル スイッチとピア スイッチでの確認とコミットの表示

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

```
switch1# configure sync
Enter configuration commands, one per line.  End with CNTL/Z.
switch1(config-sync)# switch-profile sp
Switch-Profile started, Profile ID is 1
switch1(config-sync-sp)# interface ethernet1/1
switch1(config-sync-sp-if)# description foo
switch1(config-sync-sp-if)# verify
Verification Successful
switch1(config-sync-sp)# commit
Commit Successful
switch1(config-sync)# show running-config switch-profile
switch-profile sp
  sync-peers destination 10.193.194.52
  interface Ethernet1/1
    description foo
switch1(config-sync)# show switch-profile sp status

Start-time: 171513 usecs after Wed Aug 11 17:51:28 2010
End-time: 676451 usecs after Wed Aug 11 17:51:43 2010

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

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

Peer information:
----------------
```

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

switch1(config-sync)#


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

Start-time: 265716 usecs after Wed Aug 11 16:51:28 2010
End-time: 734702 usecs after Wed Aug 11 16:51:43 2010

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

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

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

switch2#
```

同期の成功と失敗の例

次に、ピア スイッチでのスイッチ プロファイルの同期の成功例を示します。

```
switch# show switch-profile abc peer

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

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

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

スイッチ プロファイル バッファの設定、バッファ移動、およびバッファの削除

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

```
switch# configure sync
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config-sync)# switch-profile sp
Switch-Profile started, Profile ID is 1
switch(config-sync-sp)# vlan 101
switch(config-sync-sp-vlan)# ip igmp snooping querier 10.101.1.1
switch(config-sync-sp-vlan)# exit
switch(config-sync-sp)# mac address-table static 0000.0000.0001 vlan 101 drop
switch(config-sync-sp)# interface ethernet1/2
switch(config-sync-sp-if)# switchport mode trunk
switch(config-sync-sp-if)# switchport trunk allowed vlan 101
switch(config-sync-sp-if)# exit
switch(config-sync-sp)# show switch-profile sp buffer
-----------------------------------------------------------
Seq-no  Command
-----------------------------------------------------------
1       vlan 101
1.1       ip igmp snooping querier 10.101.1.1
2       mac address-table static 0000.0000.0001 vlan 101 drop
3       interface Ethernet1/2
3.1       switchport mode trunk
3.2       switchport trunk allowed vlan 101

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

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

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

設定のインポート

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

```
switch# show running-config interface ethernet1/3

!Command: show running-config interface Ethernet1/3
!Time: Wed Aug 11 18:12:44 2010
```

```
version 5.0(2)N1(1)

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

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

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

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

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

```
switch(config-sync)# switch-profile sp
Switch-Profile started, Profile ID is 1
switch(config-sync-sp)# import running-config
switch(config-sync-sp-import)# show switch-profile sp buffer
-----------------------------------------------------------
Seq-no  Command
-----------------------------------------------------------
1       logging event link-status default
2       vlan 1
3       port-profile type ethernet pp1
3.1       bandwidth 5000
3.2       bandwidth inherit
3.3       speed 10000
3.4       state enabled
4       interface port-channel3
4.1       switchport mode trunk
4.2       vpc peer-link
4.3       spanning-tree port type network
5       interface port-channel30
5.1       switchport mode trunk
5.2       vpc 30
5.3       switchport trunk allowed vlan 2-10
6       interface port-channel31
6.1       switchport mode trunk
6.2       vpc 31
6.3       switchport trunk allowed vlan 11-20
7       interface port-channel101
7.1       switchport mode fex-fabric
7.2       fex associate 101
8       interface port-channel102
8.1       switchport mode fex-fabric
8.2       vpc 102
8.3       fex associate 102
9       interface port-channel103
9.1       switchport mode fex-fabric
9.2       vpc 103
9.3       fex associate 103
10      interface Ethernet1/1
11      interface Ethernet1/2
12      interface Ethernet1/3
13      interface Ethernet1/4
13.1      switchport mode trunk
13.2      channel-group 3
14      interface Ethernet1/5
14.1      switchport mode trunk
```

```
14.2      channel-group 3
15      interface Ethernet1/6
15.1      switchport mode trunk
15.2      channel-group 3
16      interface Ethernet1/7
16.1      switchport mode trunk
16.2      channel-group 3
17      interface Ethernet1/8
18      interface Ethernet1/9
18.1      switchport mode trunk
18.2      switchport trunk allowed vlan 11-20
18.3      channel-group 31 mode active
19      interface Ethernet1/10
19.1      switchport mode trunk
19.2      switchport trunk allowed vlan 11-20
19.3      channel-group 31 mode active
20      interface Ethernet1/11
21      interface Ethernet1/12
...
45      interface Ethernet2/4
45.1      fex associate 101
45.2      switchport mode fex-fabric
45.3      channel-group 101
46      interface Ethernet2/5
46.1      fex associate 101
46.2      switchport mode fex-fabric
46.3      channel-group 101
47      interface Ethernet2/6
47.1      fex associate 101
47.2      switchport mode fex-fabric
47.3      channel-group 101
48      interface Ethernet2/7
48.1      fex associate 101
48.2      switchport mode fex-fabric
48.3      channel-group 101
49      interface Ethernet2/8
49.1      fex associate 101
...
89      interface Ethernet100/1/32
90      interface Ethernet100/1/33
91      interface Ethernet100/1/34
92      interface Ethernet100/1/35
93      interface Ethernet100/1/36
...
105     interface Ethernet100/1/48
switch(config-sync-sp-import)#
```

次に、選択したサポートされているコマンドをインポートする例を示します。 最初に、インポートしようとしているコンフィギュレーションを識別するため、ポート プロファイルの実行コンフィギュレーションを表示します。

```
switch# show running-config port-profile

!Command: show running-config port-profile
!Time: Thu Aug 12 12:09:11 2010

version 5.0(2)N1(1)
port-profile type ethernet pp1
  bandwidth 5000
  bandwidth inherit
  speed 10000
  state enabled

switch#

switch# configure sync
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config-sync)# switch-profile sp
Switch-Profile started, Profile ID is 1
switch(config-sync-sp)# import
switch(config-sync-sp-import)# port-profile type ethernet pp1
switch(config-sync-sp-import-if)# bandwidth 5000
```

```
switch(config-sync-sp-import-if)# bandwidth inherit
switch(config-sync-sp-import-if)# speed 10000
switch(config-sync-sp-import-if)# state enabled
switch(config-sync-sp-import-if)# show switch-profile sp buffer
-----------------------------------------------------------
Seq-no  Command
-----------------------------------------------------------
1       port-profile type ethernet pp1
1.1       bandwidth 5000
1.2       bandwidth inherit
1.3       speed 10000
1.4       state enabled

switch(config-sync-sp-import-if)# verify
Verification Successful
switch(config-sync-sp-import)# commit
Commit Successful
switch(config-sync)# show running-config switch-profile
switch-profile sp
  sync-peers destination 10.193.194.52
  port-profile type ethernet pp1
    bandwidth 5000
    bandwidth inherit
    speed 10000
    state enabled
switch(config-sync)#
```

import コマンドを使用したサンプル移行

ファブリック エクステンダ A-A トポロジでの Cisco NX-OS Release 5.0(2)N1(1) の移行例

次に、ファブリック エクステンダ A-A トポロジで Cisco NX-OS Release 5.0(2)N1(1) に移行するために使用するタスクを示します。 タスクの詳細については、この章の該当する項を参照してください。

手順の概要

1. 設定が両方のスイッチで同じであることを確認します。
2. 両方のスイッチで、同じ名前を持つスイッチ プロファイルを設定します。
3. 両方のスイッチで **import running config** コマンドを入力します。
4. **switch-profile** *name* **buffer** コマンドを入力し、すべての設定が両方のスイッチで正しくインポートされていることを確認します。
5. バッファを編集して不要な設定を削除します。
6. 両方のスイッチで **commit** コマンドを入力します。
7. 両方のスイッチでピア スイッチを設定するには、**sync-peers destination** *IP-address* コマンドを入力します。
8. 両方のスイッチが同期されていることを確認するには、**switch-profile** *name* **status** コマンドを入力します。

手順の詳細

ステップ 1 設定が両方のスイッチで同じであることを確認します。

ステップ 2 両方のスイッチで、同じ名前を持つスイッチ プロファイルを設定します。

ステップ 3 両方のスイッチで **import running config** コマンドを入力します。

ステップ 4 **switch-profile** *name* **buffer** コマンドを入力し、すべての設定が両方のスイッチで正しくインポートされていることを確認します。

ステップ 5 バッファを編集して不要な設定を削除します。
詳細については、例：スイッチ プロファイル バッファの設定、バッファ移動、およびバッファの削除を参照してください。

ステップ 6 両方のスイッチで **commit** コマンドを入力します。

ステップ 7 両方のスイッチでピア スイッチを設定するには、**sync-peers destination** *IP-address* コマンドを入力します。

ステップ 8 両方のスイッチが同期されていることを確認するには、**switch-profile** *name* **status** コマンドを入力します。

ファブリックエクステンダのストレート型トポロジでのCiscoNX-OSRelease5.0(2)N1(1)の移行例

次に、ファブリック エクステンダのストレート型トポロジで Cisco NX-OS Release 5.0(2)N1(1) に移行するために使用するタスクを示します。 タスクの詳細については、この章の該当する項を参照してください。

手順の概要

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

手順の詳細

ステップ 1 vPC ポートチャネルの設定が、両方のスイッチで同じであることを確認します。

ステップ 2 両方のスイッチで、同じ名前を持つスイッチ プロファイルを設定します。

ステップ 3 両方のスイッチのすべての vPC ポートチャネルについて、**import interface port-channel** *x-y*, **port-channel** *z* コマンドを入力します。

ステップ 4 show switch-profile *name* buffer コマンドを入力し、すべての設定が両方のスイッチで正しくインポートされていることを確認します。

ステップ 5 バッファを編集して不要な設定を削除します。
詳細については、例：スイッチ プロファイル バッファの設定、バッファ移動、およびバッファの削除を参照してください。

ステップ 6 両方のスイッチで **commit** コマンドを入力します。

ステップ 7 両方のスイッチでピア スイッチを設定するには、**sync-peers destination** *IP-address* コマンドを入力します。

ステップ 8 両方のスイッチが同期されていることを確認するには、**show switch-profile** *name* **status** コマンドを入力します。

第 4 章

モジュールの事前プロビジョニングの設定

この章の内容は、次のとおりです。

モジュールの事前プロビジョニングに関する情報

事前プロビジョニング機能では、モジュールを挿入または取り付ける前にインターフェイスを事前に設定できます。 また、モジュールがオフラインになった場合に、事前プロビジョニングを使用して、オフラインモジュールのインターフェイス設定を変更できます。 事前にプロビジョニングされたモジュールがオンラインになると、事前プロビジョニングの設定が適用されます。 どの設定も適用されなかった場合は、syslog が生成されます。 syslog には、受け入れられなかった設定の一覧が記録されます。

一部の仮想ポート チャネル（vPC）トポロジでは、設定の同期機能に事前プロビジョニングが必要です。 事前プロビジョニングでは、あるピアでオンラインでも別のピアでオフラインであるインターフェイスの設定を同期させることができます。

サポートされているハードウェア

ご使用のソフトウェアバージョンでサポートされるハードウェアについては、リリース ノートを参照してください。

アップグレードおよびダウングレード

Cisco NX-OS Release 4.2(1)N2(1) 以前から Cisco NX-OS Release 5.0(2)N1(1) にアップグレードする場合には、設定の影響はありません。 事前プロビジョニングをサポートするリリースから、In-Service Software Upgrade（ISSU）を含む機能をサポートする別のリリースにアップグレードする場合、アップグレード全体で事前プロビジョニングされた設定が維持されます。

事前プロビジョニングをサポートするイメージから、事前プロビジョニングをサポートしないイメージにダウングレードする場合、事前プロビジョニングされた設定を削除するように要求されます。

注意事項および制約事項

事前プロビジョニング設定時の注意事項と制限事項は次のとおりです。

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

モジュールの事前プロビジョニングのイネーブル化

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

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

手順の概要

1. **configuration terminal**
2. **slot** *slot*
3. **provision model** *model*
4. **exit**
5. （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# config t`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**slot** *slot*
	
	例：
	`switch(config)# slot 101`
	`switch(config-slot)#`
		事前プロビジョニングするスロットを選択し、スロット コンフィギュレーション モードを開始します。

ステップ 3	**provision model** *model*
	
	例：
	`switch(config-slot)# provision model N2K-C2248T`
	`switch(config-slot)#`
		事前プロビジョニングするモジュールを選択します。

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

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

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

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

モジュールの事前プロビジョニングの削除

事前プロビジョニングされたモジュールを削除できます。

手順の概要

1. **configuration terminal**
2. **slot** *slot*
3. **no provision model** *model*
4. **exit**
5. （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# config t`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**slot** *slot*
	
	例：
	`switch(config)# slot 101`
	`switch(config-slot)#`
		事前プロビジョニングするスロットを選択し、スロット コンフィギュレーション モードを開始します。

ステップ 3	**no provision model** *model*
	
	例：
	`switch(config-slot)# no provision model N2K-C2248T`
	`switch(config-slot)#`
		モジュールから事前プロビジョニングを削除します。

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

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

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

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

事前プロビジョニングした設定の確認

事前プロビジョニングした設定を表示するには、次のいずれかの作業を行います。

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

事前プロビジョニングの設定例

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

```
switch# configure terminal
switch(config)# slot 110
switch(config-slot)# provision model N2K-C2232P
switch(config-slot)# exit

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

version 5.0(2)N1(1)

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

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

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

interface Ethernet101/1/1
  service-policy input test


interface Ethernet101/1/2
  service-policy input test


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

次に、スロットから事前プロビジョニングされたすべてのモジュールを取り外す例を示します。

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

第 5 章

CFS の使用

この章の内容は、次のとおりです。

CFS について

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

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

Cisco Nexus シリーズ スイッチは、ファイバ チャネルおよび IPv4 または IPv6 ネットワークを介した CFS メッセージ配信をサポートします。 ファイバ チャネル ポートにスイッチがプロビジョニングされている場合、デフォルトではファイバ チャネルを介した CFS はイネーブルです。 これに対し、IP を介した CFS は明示的にイネーブルにする必要があります。

CFS には次の機能があります。

- CFS レイヤでクライアント/サーバ関係を持たないピアツーピア プロトコル。

- ファイバ チャネルおよび IPv4 または IPv6 ネットワークを介した CFS メッセージ配信。
- 3 つの配信モード。
  - 協調型配信：ネットワーク内でいつでも使用できる配信は 1 つだけです。
  - 非協調型配信：協調型配信が実行中の場合を除き、ネットワーク内で複数の同時配信を使用できます。
  - 無制限の非協調型配信：既存の協調型配信がある場合にネットワーク内で複数の同時配信が許可されます。 無制限の非協調型配信は他のすべてのタイプの配信と同時に実行できます。

IP を介した CFS 配信では、次の機能がサポートされます。

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

ファイバ チャネル SAN を介した CFS 配信では、次の機能がサポートされます。

- SAN ファブリックを介した配信の 3 つの範囲：
  - 論理範囲：VSAN の範囲内で配信されます。
  - 物理範囲：物理トポロジ全体に配信されます。
  - 選択した VSAN セット間：一部の機能では、特定の VSAN 間で設定配信を必要とします。 これらの機能では、CFS に対して、配信を制限する VSAN のセットを指定できます。
- ファブリックの結合イベント時（2 つの独立したファブリックが結合する場合）に機能設定の結合を実現する結合プロトコルのサポート。

CFS 配信

CFS 配信機能は、下位層の転送とは無関係です。 Cisco Nexus シリーズ スイッチは、IP およびファイバ チャネル上の CFS 配信をサポートします。 CFS を使用する機能は、下位層の転送を認識しません。

CFS の配信モード

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

- 非協調型配信
- 協調型配信
- 無制限の非協調型配信

常に 1 つのモードだけを適用できます。

非協調型配信

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

協調型配信

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

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

協調型配信には、次の 2 種類があります。

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

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

無制限の非協調型配信

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

スイッチ上での CFS 配信のディセーブル化またはイネーブル化

ファイバチャネルポートにスイッチがプロビジョニングされている場合、デフォルトではファイバ チャネルを介した CFS はイネーブルです。 IP を介した CFS は明示的にイネーブルにする必要があります。

物理接続を維持したまま、スイッチ上で CFS をグローバルにディセーブルにし、ネットワーク全体の配信から CFS を使用する機能を隔離できます。 スイッチ上で CFS がグローバルにディセーブルにされている場合、CFS 動作はそのスイッチに限定されます。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **no cfs distribute**
3. （任意） switch(config)# **cfs distribute**

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**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **no cfs distribute**	スイッチ上のすべてのアプリケーションに対して、CFS 配信（ファイバ チャネルまたは IP を介した CFS）をグローバルにディセーブルにします。
ステップ 3	switch(config)# **cfs distribute**	（任意） スイッチ上の CFS 配信をイネーブルにします。 これはデフォルトです。

CFS 配信ステータスの確認

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

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

IP を介した CFS 配信

IP を介した CFS 配信は次の機能をサポートしています。

- IP ネットワーク全体での物理的配信。
- ファイバ チャネルまたは IP を介して到達可能なすべてのスイッチに配信が到達する、ハイブリッド ファイバ チャネルおよび IP ネットワークでの物理的配信。

（注） スイッチはまずファイバ チャネルを介して情報を配信し、ファイバ チャネルでの最初の試みが失敗すると IP ネットワークを介して配信します。 IP およびファイバ チャネルの両方を介した配信がイネーブルの場合、CFS は重複メッセージを送信しません。

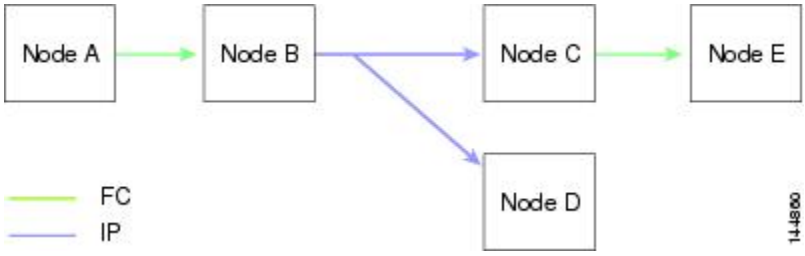
- IP バージョン 4（IPv4）または IP バージョン 6（IPv6）を介した配信。

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

- 設定可能なマルチキャストアドレスを使用してネットワーク トポロジの変更を検出するキープアライブ メカニズム。
- Release 2.x 以降を実行する Cisco MDS 9000 ファミリ スイッチとの互換性

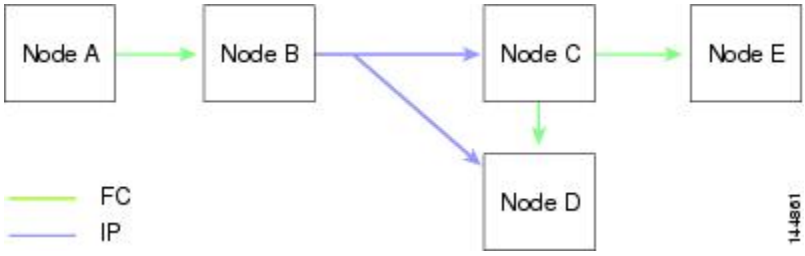
次の図（ネットワーク例 *1*）は、ファイバ チャネル接続と IP 接続の両方を使用したネットワークを示します。 ノード A はファイバ チャネルを介してノード B にイベントを転送します。 ノード B はユニキャスト IP を使用してノード C とノード D にイベントを転送します。 ノード C はファイバ チャネルを介してノード E にイベントを転送します。

図 *1*：ファイバ チャネル接続と *IP* 接続を使用するネットワーク例 *1*



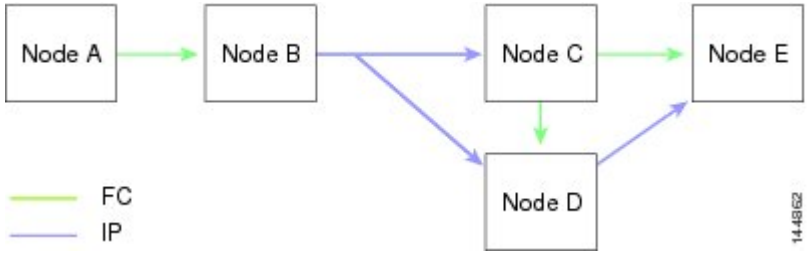
次の図（ネットワーク例 *2*）は前の図と同じです。ただし、ノード C とノード D はファイバ チャネルを使用して接続しています。 ノード B にはノード C とノード D の IP 用配信リストがあるので、この例のすべてのプロセスは同じです。 ノード D はすでにノード B からの配信リストに入っているため、ノード C はノード D に転送しません。

図 *2*：ファイバ チャネル接続と *IP* 接続を使用するネットワーク例 *2*



次の図（ネットワーク例 *3*）は前の図と同じです。ただし、ノード D とノード E が IP を使用して接続しています。 ノード E はノード B からの配信リストに入っていないため、ノード C とノード D はイベントをノード E に転送します。

図 *3*：ファイバ チャネル接続と *IP* 接続を使用するネットワーク例 *3*



ファイバ チャネルを介した CFS 配信

ファイバ チャネルを介した CFS 配信の場合、CFS プロトコル レイヤが FC2 レイヤの上位に存在します。 CFS は FC2 転送サービスを使用して、他のスイッチに情報を送信します。 CFS はすべての CFS パケットに対して独自の SW_ILS（0x77434653）プロトコルを使用します。 CFS パケットはスイッチ ドメイン コントローラ アドレスとの間で送受信されます。

CFS 配信の範囲

Cisco Nexus シリーズ スイッチの各種アプリケーションは、次のさまざまなレベルで設定を配信する必要があります。 ファイバ チャネルを介した CFS 配信を使用する場合、次のレベルが使用できます。

- VSAN レベル（論理スコープ）

  VSAN の範囲内で動作するアプリケーションは、設定の配信が VSAN に限定されます。 アプリケーション例は、VSAN 内だけでコンフィギュレーションデータベースを適用できる場合のポート セキュリティです。

  （注） IP を介した CFS 配信では、論理範囲はサポートされません。

- 物理トポロジ レベル（物理スコープ）

  一部のアプリケーション（NTP など）は、物理トポロジ全体に設定を配信する必要があります。

- 選択された 2 つのスイッチ間

  一部のアプリケーションはネットワーク内の選択したスイッチ間でだけ動かせます。

CFS 結合のサポート

CFS 結合は、ファイバ チャネルを介した CFS 配信でサポートされます。

アプリケーションは、CFS を通じて SAN ファブリック内の同期化された設定を保ちます。 このような 2 つのファブリック間で ISL を起動すると、これらのファブリックがマージされることがあります。 これらの 2 つのファブリック内の設定情報セットが異なっている時は、マージ イベント中に調整する必要があります。 CFS は、アプリケーション ピアがオンラインになるたびに通知を送信します。 M のアプリケーション ピアを持つファブリックが N のアプリケーション ピアを持つ別のファブリックと結合し、アプリケーションが通知のたびに結合アクションを行うと、リンク アップ イベントがファブリック内の MxN 結合をもたらします。

CFS は、CFS レイヤでマージの複雑性に対処することで、必要とされるマージ数を 1 つに減らすプロトコルをサポートしています。 このプロトコルは、スコープ単位でアプリケーションごとに稼働します。 プロトコルには、ファブリックのマージマネージャとしてそのファブリック内から 1 つのスイッチを選択する作業が伴います。 他のスイッチは、結合プロセスにおいて役割を担いません。

マージ時、2 つのファブリック内のマージ マネージャは相互にコンフィギュレーション データベースを交換します。 一方のアプリケーションが情報をマージし、マージが正常に行われたかどうかを確認し、結合されたファブリック内のすべてのスイッチにマージ ステータスを通知します。

マージに成功した場合、マージしたデータベースは結合ファブリック内のすべてのスイッチに配信され、新規ファブリック全体が一貫したステートになります。 マージ障害から回復するには、新規ファブリック内の任意のスイッチから配信を開始します。 この配信により、ファブリック内のすべてのピアが同じコンフィギュレーション データベースに復元されます。

アプリケーションの CFS サポート

CFS のアプリケーション要件

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

- CFS の暗黙的な使用：CFS 対応アプリケーションの CFS 作業を初めて行う場合、設定変更プロセスが開始され、アプリケーションがネットワークをロックします。
- 保留データベース：保留データベースはコミットされていない情報を保持する一時的なバッファです。 データベースが、ネットワーク内の他のスイッチのデータベースと確実に同期するために、コミットされていない変更はすぐには適用されません。 変更をコミットすると、保留データベースはコンフィギュレーション データベース（別名、アクティブ データベースまたは有効データベース）を上書きします。

- アプリケーション単位でイネーブル化またはディセーブル化される CFS 配信：CFS 配信ステートのデフォルト（イネーブルまたはディセーブル）は、アプリケーション間で異なります。 アプリケーションでCFSの配信がディセーブルにされている場合、そのアプリケーションは設定を配信せず、またネットワーク内の他のスイッチからの配信も受け入れません。
- 明示的なCFSコミット：大半のアプリケーションでは、新しいデータベースをネットワークに配信したりネットワーク ロックを解除したりするために、一時的なバッファ内の変更をアプリケーション データベースにコピーする明示的なコミット操作が必要です。 コミット操作を実行しないと、一時的バッファ内の変更は適用されません。

アプリケーションに対する CFS のイネーブル化

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

アプリケーションでは、配信はデフォルトでイネーブルにされています。

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

アプリケーション登録スターテスの確認

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

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

```
switch# show cfs application

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

show cfs application name コマンドは、特定のアプリケーションの詳細を表示します。 表示されるのは、イネーブル/ディセーブル ステート、CFS に登録されているタイムアウト、結合可能であるか（結合のサポートに対して CFS に登録されているか）、および配信範囲です。

```
switch# show cfs application name fscm

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

ネットワークのロック

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

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

CFS ロック ステータスの確認

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

```
switch# show cfs lock

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

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

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

```
switch# show cfs lock name ntp

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

 Total number of entries = 1
```

変更のコミット

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

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

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

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

commit コマンドを入力すると、指定した機能の変更をコミットできます。

変更の廃棄

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

abort コマンドを入力すると、指定した機能の変更を廃棄できます。

設定の保存

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

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

ロック済みセッションのクリア

ネットワーク内の任意のスイッチからアプリケーションが保持しているロックをクリアすると、ロックが取得されているにもかかわらず解除されていない状態から回復できます。 この機能には、Admin 権限が必要になります。

注意　この機能を使用してネットワーク内のロックを解除する場合は、注意が必要です。 ネットワーク内の任意のスイッチの保留中設定がフラッシュされ、内容が失われます。

CFS リージョン

CFS リージョンの概要

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

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

シナリオ例

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

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

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

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

CFS リージョンの管理

CFS リージョンの作成

CFS リージョンを作成できます。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **cfs region** *region-id*

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**	コンフィギュレーションモードを開始します。
ステップ 2	switch(config)# **cfs region** *region-id*	リージョンを作成します。

CFS リージョンへのアプリケーションの割り当て

スイッチでリージョンにアプリケーションを割り当てることができます。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **cfs region** *region-id*
3. switch(config-cfs-region)# *application*

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

次に、リージョンにアプリケーションを割り当てる例を示します。

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

別の CFS リージョンへのアプリケーションの移動

あるリージョンから別のリージョンにアプリケーションを移動できます。

手順の概要

1. switch# **configure**
2. switch(config)# **cfs region** *region-id*
3. switch(config-cfs-region)# *application*

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

	コマンドまたはアクション	目的

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

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

リージョンからのアプリケーションの削除

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

手順の概要

1. switch# **configure**
2. switch(config)# **cfs region** *region-id*
3. switch(config-cfs-region)# **no** *application*

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**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **cfs region** *region-id*	CFS リージョン サブモードを開始します。
ステップ 3	switch(config-cfs-region)# **no** *application*	リージョンに属しているアプリケーションを削除します。

CFS リージョンの削除

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

手順の概要

1. switch# **configure**
2. switch(config)# **no cfs region** *region-id*

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**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **no cfs region** *region-id*	リージョンを削除します。 （注） 「All the applications in the region will be moved to the default region」という警告が表示されます。

IP を介した CFS の設定

IPv4 を介した CFS のイネーブル化

IPv4 を介した CFS をイネーブルまたはディセーブルにできます。

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

手順の概要

1. switch# **configure**
2. switch(config)# **cfs ipv4 distribute**
3. （任意） switch(config)# **no cfs ipv4 distribute**

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**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **cfs ipv4 distribute**	スイッチのすべてのアプリケーションに対して IPv6 を介した CFS をグローバルでイネーブルにします。

	コマンドまたはアクション	目的
ステップ 3	switch(config)# **no cfs ipv4 distribute**	（任意） スイッチの IPv6 を介した CFS をディセーブルにします（デフォルト）。

IPv6 を介した CFS のイネーブル化

IPv6 を介した CFS をイネーブルまたはディセーブルにできます。

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

手順の概要

1. switch# **configure**
2. switch(config)# **cfs ipv6 distribute**
3. （任意） switch(config)# **no cfs ipv6 distribute**

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**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **cfs ipv6 distribute**	スイッチのすべてのアプリケーションに対して IPv6 を介した CFS をグローバルでイネーブルにします。
ステップ 3	switch(config)# **no cfs ipv6 distribute**	（任意） スイッチの IPv6 を介した CFS をディセーブルにします（デフォルト）。

IP を介した CFS 設定の確認

次に、IP を介した CFS の設定を確認する例を示します。**show cfs status** コマンドを使用します。

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

IP を介した CFS の IP マルチキャスト アドレスの設定

類似のマルチキャスト アドレスを持つ IP を介した CFS 対応スイッチのすべては、IP ネットワークを介した 1 つの CFS を形成します。 ネットワーク トポロジ変更を検出するためのキープアライブ メカニズムのような CFS プロトコル特有の配信は、IP マルチキャスト アドレスを使用して情報を送受信します。

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

CFS の IPv4 マルチキャスト アドレスの設定

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

手順の概要

1. switch# **configure**
2. switch(config)# **cfs ipv4 mcast-address** *ipv4-address*
3. （任意） switch(config)# **no cfs ipv4 mcast-address** *ipv4-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**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **cfs ipv4 mcast-address** *ipv4-address*	IPv4 を介した CFS 配信の IPv4 マルチキャスト アドレスを設定します。 有効な IPv4 アドレスの範囲は 239.255.0.0 ～ 239.255.255.255 および 239.192/16 ～ 239.251/16 です。

	コマンドまたはアクション	目的
ステップ 3	switch(config)# **no cfs ipv4 mcast-address** *ipv4-address*	（任意） IPv4 を介した CFS 配信のデフォルトの IPv4 マルチキャスト アドレスに戻します。 CFS のデフォルトの IPv4 マルチキャスト アドレスは 239.255.70.83 です。

CFS の IPv6 マルチキャスト アドレスの設定

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

手順の概要

1. switch# **configure**
2. switch(config)# **cfs ipv6 mcast-address** *ipv4-address*
3. （任意） switch(config)# **no cfs ipv6 mcast-address** *ipv4-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**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **cfs ipv6 mcast-address** *ipv4-address*	IPv6 を介した CFS 配信の IPv6 マルチキャスト アドレスを設定します。 有効な IPv6 アドレスの範囲は ff15::/16（ff15::0000:0000 ～ ff15::ffff:ffff）および ff18::/16（ff18::0000:0000 ～ ff18::ffff:ffff）です。
ステップ 3	switch(config)# **no cfs ipv6 mcast-address** *ipv4-address*	（任意） IPv6 を介した CFS 配信のデフォルトの IPv6 マルチキャスト アドレスに戻します。 IP を介した CFS のデフォルトの IPv6 マルチキャスト アドレスは ff15::efff:4653 です。

IP を介した CFS の IP マルチキャスト アドレス設定の確認

次に、IP を介した CFS の IP マルチキャスト アドレス設定を確認する例を示します。**show cfs status** コマンドを使用します。

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

CFS 配信情報の表示

show cfs merge status name コマンドを実行すると、指定したアプリケーションの結合ステータスが表示されます。 次に、論理範囲内のアプリケーション配信の出力例を示します。 この例は、スイッチ上のすべての有効な VSAN におけるマージ ステータスを示しています。 コマンドの出力は、結合ステータスを Success、Waiting、Failure、または In Progress のいずれかで示します。 結合が正常に行われた場合は、ネットワーク内のすべてのスイッチがローカル ネットワークの下に表示されます。 結合が失敗した場合、結合が進行中である場合は、結合に関わったローカルネットワークとリモートネットワークが別個に表示されます。 各ネットワーク内の結合で主体となったアプリケーション サーバには、Merge Master の用語が表示されます。

```
switch# show cfs merge status name port-security

Logical [VSAN 1] Merge Status: Failed
Local Fabric
-----------------------------------------------------------------
 Domain Switch WWN               IP Address
-----------------------------------------------------------------
 238    20:00:00:05:30:00:6b:9e  10.76.100.167   [Merge Master]

Remote Fabric
-----------------------------------------------------------------
 Domain Switch WWN               IP Address
-----------------------------------------------------------------
 236    20:00:00:0e:d7:00:3c:9e  10.76.100.169    [Merge Master]

Logical [VSAN 2] Merge Status: Success
Local Fabric
-----------------------------------------------------------------
 Domain Switch WWN               IP Address
-----------------------------------------------------------------
 211    20:00:00:05:30:00:6b:9e  10.76.100.167    [Merge Master]
 1      20:00:00:0e:d7:00:3c:9e  10.76.100.169

Logical [VSAN 3] Merge Status: Success
Local Fabric
-----------------------------------------------------------------
 Domain Switch WWN               IP Address
-----------------------------------------------------------------
 221    20:00:00:05:30:00:6b:9e  10.76.100.167    [Merge Master]
 103    20:00:00:0e:d7:00:3c:9e  10.76.100.169
```

次の **show cfs merge status name** コマンドの出力例は、物理範囲において結合が失敗したアプリケーションを示します。 このコマンドは、指定されたアプリケーション名を使用し、アプリケーション範囲に基づいた結合ステータスを表示します。

```
switch# show cfs merge status name ntp
```

```
Physical  Merge Status: Failed
Local Fabric
------------------------------------------------------------
 Switch WWN               IP Address
------------------------------------------------------------
 20:00:00:05:30:00:6b:9e  10.76.100.167    [Merge Master]

Remote Fabric
------------------------------------------------------------
 Switch WWN               IP Address
------------------------------------------------------------
 20:00:00:0e:d7:00:3c:9e  10.76.100.169    [Merge Master]
```

show cfs peers コマンドの出力例は、物理ネットワーク内のすべてのスイッチをスイッチ WWN および IP アドレスの観点から表示します。 ローカル スイッチには Local が表示されます。

```
switch# show cfs peers

Physical Fabric
--------------------------------------------------
 Switch WWN               IP Address
--------------------------------------------------
 20:00:00:05:30:00:6b:9e  10.76.100.167   [Local]
 20:00:00:0e:d7:00:3c:9e  10.76.100.169

 Total number of entries = 2
```

show cfs peers name コマンドは、特定のアプリケーションが CFS に登録されているすべてのピアを表示します。 コマンド出力には、アプリケーション範囲に応じて物理範囲のすべてのピア、またはスイッチ上の有効な各 VSAN のすべてのピアが表示されます。 物理範囲では、すべてのピアのスイッチ WWN が表示されます。 ローカル スイッチには Local が表示されます。

```
switch# show cfs peers name ntp

Scope      : Physical

--------------------------------------------------

Switch WWN               IP Address

--------------------------------------------------

20:00:00:44:22:00:4a:9e  172.22.92.27    [Local]

20:00:00:05:30:01:1b:c2  172.22.92.215
```

次の **show cfs peers name** コマンドの出力例は、すべてのアプリケーション ピアを表示します（アプリケーションが登録されているすべてのスイッチ）。 ローカル スイッチには Local が表示されます。

```
switch# show cfs peers name port-security
Scope      : Logical [VSAN 1]

------------------------------------------------------------

Domain   Switch WWN               IP Address

------------------------------------------------------------

124      20:00:00:44:22:00:4a:9e  172.22.92.27    [Local]

98       20:00:00:05:30:01:1b:c2  172.22.92.215


Total number of entries = 2
```

```
Scope      : Logical [VSAN 3]
-----------------------------------------------------------
Domain   Switch WWN               IP Address
-----------------------------------------------------------
224      20:00:00:44:22:00:4a:9e  172.22.92.27    [Local]
151      20:00:00:05:30:01:1b:c2  172.22.92.215

Total number of entries = 2
```

CFS のデフォルト設定

次の表に、CFS のデフォルト設定を示します。

表 2：デフォルトの *CFS* パラメータ

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

CISCO-CFS-MIB には CFS 関連機能の SNMP 設定情報が含まれます。『*Cisco Nexus 5000 and Nexus 2000 MIBs Reference*』を参照してください。次の URL で入手できます。http://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/mib/reference/NX5000_MIBRef.htmlを参照してください。

第 6 章

ユーザ アカウントと RBAC の設定

この章の内容は、次のとおりです。

ユーザ アカウントと RBAC の概要

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

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

ユーザ ロール

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

スイッチには、次のデフォルト ユーザ ロールが用意されています。

network-admin（スーパーユーザ）

スイッチ全体に対する完全な読み取りと書き込みのアクセス権。

ネットワーク オペレータ

スイッチに対する完全な読み取りアクセス権。

san-admin

SNMP または CLI を使用したファイバ チャネルおよび FCoE 管理タスクへの完全な読み取りと書き込みのアクセス権。

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

事前定義された SAN 管理者ユーザ ロール

SAN 管理者ユーザ ロールは、LAN および SAN の管理タスクを分離するように設計された、編集不可能な事前定義されたユーザ ロールです。 SAN 管理者ユーザ ロールを割り当てられたユーザは、別のユーザ ロールによって割り当てられていない限り、イーサネット機能に対する書き込みまたは読み取りアクセス権を持ちません。

SAN 管理者ユーザには、次の機能が許可されます。

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

- FCoE-NPV
- FPORT-CHANNEL-TRUNK
- PORT-TRACK
- FABRIC-BINDING

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

ルール

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

コマンド

正規表現で定義されたコマンドまたはコマンド グループ

機能

Cisco Nexus 5000 Series スイッチにより提供される機能に適用されるコマンド。 **show role feature** コマンドを入力すれば、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** コマンドを入力すれば、このパラメータに指定できるデフォルトの機能グループが表示されます。

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

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

SAN 管理者ロール機能のルール マッピング

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

表 *3*：*SAN* 管理者ユーザロールのロール機能のルール

機能	権限
copy	コピー関連コマンドに対する読み取りおよび書き込み権限
fabric-binding	ファブリック バインディング関連コマンドに対する読み取りおよび書き込み権限
fcdomain	ファイバ チャネル ドメイン関連コマンドに対する読み取りおよび書き込み権限
fcfe	ファイバ チャネル FE 関連コマンドに対する読み取りおよび書き込み権限
fcmgmt	ファイバチャネル管理関連コマンドに対する読み取りおよび書き込み権限
fcns	ファイバチャネル関連サービス FCNS コマンドに対する読み取りおよび書き込み権限
fcoe	Fibre Channel over Ethernet 関連コマンドに対する読み取りおよび書き込み権限
fcsp	Fibre Channel Security Protocol（FCSP）関連コマンドに対する読み取りおよび書き込み権限
fdmi	Fabric Device Management Interface（FDMI）関連コマンドに対する読み取りおよび書き込み権限
fspf	Fabric Shortest Path First（FSPF）関連コマンドに対する読み取りおよび書き込み権限
interface	インターフェイス関連コマンドに対する読み取りおよび書き込み権限。 これには、ファイバチャネルインターフェイスだけでなく、すべてのインターフェイスが含まれます。
port-track	ポートトラック関連コマンドに対する読み取りおよび書き込み権限
port-security	ポートセキュリティ関連コマンドに対する読み取りおよび書き込み権限

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

ユーザ ロール ポリシー

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

ユーザ ロール ポリシーは、ロールに定義されている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、または VSAN）へのアクセスを許可した場合、ユーザがそのユーザに関連付けられたユーザ ロール ポリシーに表示されていなくても、ユーザはこれらのリソースへのアクセスを許可されます。

ユーザ アカウントの設定の制限事項

次の語は予約済みであり、ユーザ設定に使用できません。

- adm
- bin
- daemon
- ftp
- ftpuser
- games
- gdm
- gopher
- halt
- lp
- mail
- mailnull
- man
- mtsuser
- news
- nobody
- san-admin
- shutdown
- sync
- sys

- uucp
- xfs

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

ユーザ パスワードの要件

Cisco Nexus 5000 Series パスワードには大文字小文字の区別があり、英数字だけを含むことができます。 ドル記号（$）やパーセント記号（%）などの特殊文字は使用できません。

パスワードが脆弱な場合（短い、解読されやすいなど）、Cisco Nexus 5000 Series スイッチはパスワードを拒否します。 各ユーザ アカウントには強力なパスワードを設定するようにしてください。 強固なパスワードは、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
- 固有名詞を含んでいない
- 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

強固なパスワードの例を次に示します。

- If2CoM18
- 2009AsdfLkj30
- Cb1955S21

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

ユーザ アカウントの注意事項および制約事項

ユーザ アカウントおよびRBACを設定する場合、次の注意事項および制約事項を考慮してください。

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

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

ユーザ アカウントの設定

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

手順の概要

1. switch# **configure terminal**
2. （任意） switch(config)# **show role**
3. switch(config) # **username** *user-id* [**password** *password*] [**expire** *date*] [**role** *role-name*]
4. switch(config) # **exit**
5. （任意） switch# **show user-account**
6. （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# **configure terminal**	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	switch(config)# **show role**	（任意） 使用可能なユーザ ロールを表示します。 必要に応じて、他のユーザ ロールを設定できます。
ステップ 3	switch(config) # **username** *user-id* [**password** *password*] [**expire** *date*] [**role** *role-name*]	ユーザ アカウントを設定します。 *user-id* は、最大 28 文字の英数字のストリングで、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。 （注） パスワードを指定しなかった場合、ユーザはスイッチにログインできない場合があります。 **expire** *date* オプションの形式は、YYYY-MM-DD です。 デフォルトでは、失効日はありません。
ステップ 4	switch(config) # **exit**	グローバル コンフィギュレーション モードを終了します。
ステップ 5	switch# **show user-account**	（任意） ロール設定を表示します。
ステップ 6	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、ユーザ アカウントを設定する例を示します。

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

SAN 管理者ユーザの設定

手順の概要

1. switch# **configure terminal**
2. switch(config) # **username** *user-id* **role san-admin password** *password*
3. （任意） switch(config) # **show user-account**
4. （任意） switch(config) # **show snmp-user**
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) # **username** *user-id* **role san-admin password** *password*	指定したユーザに対する SAN 管理者ユーザ ロールのアクセス権を設定します。
ステップ 3	switch(config) # **show user-account**	（任意） ロール設定を表示します。
ステップ 4	switch(config) # **show snmp-user**	（任意） SNMP ユーザの設定を表示します。
ステップ 5	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

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

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

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

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

User     Auth   Priv
____     ____   ____

switch(config) #
```

RBAC の設定

ユーザ ロールおよびルールの作成

指定するルール番号は、適用したルールの順序を決めます。ルールは降順で適用されます。たとえば、1 つのロールが 3 つのルールを持っている場合、ルール 3 がルール 2 よりも前に適用され、ルール 2 はルール 1 よりも前に適用されます。

手順の概要

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. （任意） switch(config-role)# **description** *text*
8. switch(config-role)# **end**
9. （任意） switch# **show role**
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# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config) # **role name** *role-name*	ユーザ ロールを指定し、ロール コンフィギュレーション モードを開始します。 *role-name* 引数は、最大 16 文字の長さの英数字のストリングで、大文字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。 必要なルール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。

	コマンドまたはアクション	目的
ステップ 5	switch(config-role)# **rule** *number* {**deny** | **permit**} {**read** | **read-write**} **feature** *feature-name*	機能に対して、読み取り専用ルールか読み取りと書き込みのルールかを設定します。 **show role feature** コマンドを使用すれば、機能のリストが表示されます。 必要なルール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、読み取り専用ルールか読み取りと書き込みのルールかを設定します。 **show role feature-group** コマンドを使用すれば、機能グループのリストが表示されます。 必要なルールの数だけこのコマンドを繰り返します。
ステップ 7	switch(config-role)# **description** *text*	（任意） ロールの説明を設定します。 説明にはスペースも含めることができます。
ステップ 8	switch(config-role)# **end**	ロール コンフィギュレーション モードを終了します。
ステップ 9	switch# **show role**	（任意） ユーザ ロールの設定を表示します。
ステップ 10	switch# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

次に、ユーザ ロールを作成してルールを指定する例を示します。

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

機能グループの作成

手順の概要

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

次に、機能グループを作成する例を示します。

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

ユーザ ロール インターフェイス ポリシーの変更

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

手順の概要

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. （任意） switch(config-role) # **show role**
7. （任意） switch(config-role) # **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) # **role name** *role-name*	ユーザ ロールを指定し、ロール コンフィギュレーション モードを開始します。
ステップ 3	switch(config-role) # **interface policy deny**	ロール インターフェイス ポリシー コンフィギュレーション モードを開始します。
ステップ 4	switch(config-role-interface) # **permit interface** *interface-list*	ロールがアクセスできるインターフェイスのリストを指定します。 必要なインターフェイスの数だけこのコマンドを繰り返します。 このコマンドの場合、イーサネットインターフェイス、ファイバ チャネル インターフェイス、および仮想ファイバ チャネル インターフェイスを指定できます。
ステップ 5	switch(config-role-interface) # **exit**	ロール インターフェイス ポリシー コンフィギュレーション モードを終了します。
ステップ 6	switch(config-role) # **show role**	（任意） ロール設定を表示します。

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

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

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

ユーザ ロール VLAN ポリシーの変更

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

手順の概要

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. （任意） switch# **show role**
7. （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# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config) # **role name** *role-name*	ユーザ ロールを指定し、ロール コンフィギュレーション モードを開始します。
ステップ 3	switch(config-role)# **vlan policy deny**	ロール VLAN ポリシー コンフィギュレーション モードを開始します。
ステップ 4	switch(config-role-vlan # **permit vlan** *vlan-list*	ロールがアクセスできる VLAN の範囲を指定します。 必要な VLAN の数だけこのコマンドを繰り返します。

	コマンドまたはアクション	目的
ステップ 5	switch(config-role-vlan) # **exit**	ロール VLAN ポリシー コンフィギュレーション モードを終了します。
ステップ 6	switch# **show role**	（任意） ロール設定を表示します。
ステップ 7	switch# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

ユーザ ロール VSAN ポリシーの変更

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

手順の概要

1. switch# **configure terminal**
2. switch(config-role) # **role name** *role-name*
3. switch(config-role) # **vsan policy deny**
4. switch(config-role-vsan) # **permit vsan** *vsan-list*
5. switch(config-role-vsan) # **exit**
6. （任意） switch# **show role**
7. （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# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config-role) # **role name** *role-name*	ユーザ ロールを指定し、ロール コンフィギュレーション モードを開始します。
ステップ 3	switch(config-role) # **vsan policy deny**	ロール VSAN ポリシー コンフィギュレーション モードを開始します。
ステップ 4	switch(config-role-vsan) # **permit vsan** *vsan-list*	ロールがアクセスできる VSAN 範囲を指定します。 必要な VSAN の数だけ、このコマンドを繰り返します。

	コマンドまたはアクション	目的
ステップ 5	switch(config-role-vsan) # **exit**	ロール VSAN ポリシー コンフィギュレーション モードを終了します。
ステップ 6	switch# **show role**	（任意） ロール設定を表示します。
ステップ 7	switch# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

ユーザ アカウントと RBAC の設定の確認

設定を確認するには、次のいずれかのコマンドを使用します。

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

ユーザ アカウントおよび RBAC のユーザ アカウント デフォルト設定

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

表 *4*：デフォルトのユーザ アカウントと *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 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 7 章

Session Manager の設定

この章の内容は、次のとおりです。

Session Manager の概要

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

- コンフィギュレーション セッション：セッション マネージャ モードで実装するコマンドのリストを作成します。
- 検証：設定の基本的なセマンティクス検査を行います。 Cisco NX-OS は、設定の一部でセマンティクス検査が失敗した場合にエラーを返します。
- 確認：既存のハードウェア/ソフトウェア構成およびリソースに基づいて、設定を全体として確認します。 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：実装しないで設定の変更を破棄します。

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 がサポートするのは、アクセス コントロール リスト（ACL）機能だけです。
- 作成できるコンフィギュレーション セッションの最大数は 32 です。
- すべてのセッションで設定できるコマンドの最大数は 20,000 です。

Session Manager の設定

セッションの作成

作成できるコンフィギュレーション セッションの最大数は 32 です。

手順の概要

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

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 session** *name*	コンフィギュレーション セッションを作成し、セッション コンフィギュレーション モードを開始します。 名前は任意の英数字ストリングです。 セッションの内容を表示します。
ステップ 2	switch(config-s)# **show configuration session** [*name*]	（任意） セッションの内容を表示します。
ステップ 3	switch(config-s)# **save** *location*	（任意） セッションをファイルに保存します。 保存場所には、bootflash または volatile を指定できます。

セッションでの ACL の設定

コンフィギュレーション セッションで ACL を設定できます。

手順の概要

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

セッションの確認

セッションを確認するには、セッション モードで次のコマンドを使用します。

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

セッションのコミット

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

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

セッションの保存

セッションを保存するには、セッション モードで次のコマンドを使用します。

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

セッションの廃棄

セッションを廃棄するには、セッション モードで次のコマンドを使用します。

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

Session Manager のコンフィギュレーション例

この例では、ACL 用の設定セッションを作成する方法を示します。

```
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 8 章

オンライン診断の設定

この章の内容は、次のとおりです。

オンライン診断について

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モニタします。

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。

起動時診断

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

表 *5*：起動時診断

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

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

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

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

起動時診断をバイパスするか、完全な起動時診断セットを実行するよう Cisco Nexus 5000 Series スイッチを設定できます。

ヘルス モニタリング診断

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

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

次の表に、スイッチのヘルス モニタリング診断を示します。

表 *6*： 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 をモニタします。
電源装置	電源装置のヘルス ステータスをモニタします。
温度センサー	温度センサーの読み取り値をモニタします。
テスト ファン	ファンの速度およびファンの制御をモニタします。

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

表 *7*: ヘルス モニタリングおよび起動時診断テスト

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

拡張モジュール診断

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

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

表 *8*: 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。

診断	説明
前面ポート	前面ポート上のコンポーネント（PHY および MAC など）をテストします。

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

表 *9*：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 をモニタします。
温度センサー	温度センサーの読み取り値をモニタします。

オンライン診断の設定

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

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

手順の概要

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

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**	コン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。

	コマンドまたはアクション	目的
		• complete：すべての起動時診断を実行します。 これがデフォルト値です。 • bypass：起動時診断を実行しません。
ステップ **3**	switch# **show diagnostic bootup level**	（任意） 現在、スイッチで実行されている起動時診断レベル（bypass または complete）を表示します。

次に、完全な診断を実行するよう起動時診断レベルを設定する例を示します。

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

オンライン診断設定の確認

オンライン診断設定情報を表示するには、次の作業を行います。

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

オンライン診断のデフォルト設定

次の表に、オンライン診断パラメータのデフォルト設定を示します。

表 *10*：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 9 章

システム メッセージ ロギングの設定

この章の内容は、次のとおりです。

システム メッセージ ロギングの概要

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 5000 Seriesスイッチはメッセージをターミナル セッションへ出力します。

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

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

表 *11*： システム メッセージの重大度

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

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

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

syslog サーバ

syslog サーバは、syslog プロトコルに基づいてシステム メッセージを記録するよう設定されたリモート システムで稼働します。 最大 8 台の syslog サーバにログを送信するように Cisco Nexus シリーズスイッチを設定できます。

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

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

システム メッセージ ロギングのライセンス要件

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

システムメッセージロギングの注意事項および制約事項

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

システム メッセージ ロギングのデフォルト設定

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

表 *12*： デフォルトのシステム メッセージ ロギング パラメータ

パラメータ	デフォルト
コンソール ロギング	重大度 2 でイネーブル
モニタ ロギング	重大度 2 でイネーブル
ログ ファイル ロギング	重大度 5 でメッセージのロギングをイネーブル
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重大度によって、メッセージを記録するようスイッチを設定できます。

デフォルトでは、ターミナル セッションでロギングはイネーブルです。

手順の概要

1. switch# **terminal monitor**
2. switch# **configure terminal**
3. switch(config)# **logging console** [*severity-level*]
4. （任意） switch(config)# **no logging console** [*severity-level*]
5. switch(config)# **logging monitor** [*severity-level*]
6. （任意） switch(config)# **no logging monitor** [*severity-level*]
7. （任意） switch# **show logging console**
8. （任意） switch# **show logging monitor**
9. （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# **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**	コンフィギュレーション モードを開始します。
ステップ 3	switch(config)# **logging console** [*severity-level*]	指定された重大度（またはそれ以上）に基づくコンソール セッションへのメッセージの記録をイネーブルにします（数字が小さいほうが大きい重大度を示します）。 重大度は 0 ～ 7 の範囲です。 • 0：緊急 • 1：アラート • 2：クリティカル • 3：エラー • 4：警告 • 5：通知

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

次に、コンソールのロギング レベルを 3 に設定する例を示します。

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

次に、コンソールのロギングの設定を表示する例を示します。

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

次に、コンソールのロギングをディセーブルにする例を示します。

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

次に、ターミナル セッションのロギング 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。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **logging logfile** *logfile-name severity-level* [**size** *bytes*]
3. （任意） switch(config)# **no logging logfile** [*logfile-name severity-level* [**size** *bytes*]]
4. （任意） switch# **show logging info**
5. （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# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **logging logfile** *logfile-name severity-level* [**size** *bytes*]	システム メッセージを保存するのに使用するログ ファイルの名前と、記録する最小重大度を設定します。 任意で最大ファイル サイズを指定できます。 デフォルトの重大度は 5 です。ファイル サイズは 4194304 です。

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

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

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

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

```
switch# show logging info
Logging console:                enabled (Severity: debugging)
Logging monitor:                enabled (Severity: debugging)
Logging linecard:               enabled (Severity: notifications)
Logging fex:                    enabled (Severity: notifications)
Logging timestamp:              Seconds
Logging server:                 disabled
Logging logfile:                enabled
        Name - my_log: Severity - informational Size - 4194304
Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
```

```
aaa                     3                       3
aclmgr                  3                       3
afm                     3                       3
altos                   3                       3
auth                    0                       0
authpriv                3                       3
bootvar                 5                       5
callhome                2                       2
capability              2                       2
cdp                     2                       2
cert_enroll             2                       2
...
```

モジュールおよびファシリティ メッセージのロギングの設定

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

手順の概要

1. switch# **configure terminal**
2. switch(config)# **logging module** [*severity-level*]
3. switch(config)# **logging level** *facility severity-level*
4. （任意） switch(config)# **no logging module** [*severity-level*]
5. （任意） switch(config)# **no logging level** [*facility severity-level*]
6. （任意） switch# **show logging module**
7. （任意） switch# **show logging level** [*facility*]
8. （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# **configure terminal**	コン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

	コマンドまたはアクション	目的
		• 7：デバッグ 重大度が指定されていない場合、デフォルトの 5 が使用されます。
ステップ 3	switch(config)# **logging level** *facility severity-level*	指定された重大度またはそれ以上の重大度である指定のファシリティからのロギング メッセージをイネーブルにします。 重大度は 0 ～ 7 です。 • 0：緊急 • 1：アラート • 2：クリティカル • 3：エラー • 4：警告 • 5：通知 • 6：情報 • 7：デバッグ 同じ重大度をすべてのファシリティに適用するには、all ファシリティを使用します。 デフォルト値については、**show logging level** コマンドを参照してください。
ステップ 4	switch(config)# **no logging module** [*severity-level*]	（任意） モジュール ログ メッセージをディセーブルにします。
ステップ 5	switch(config)# **no logging level** [*facility severity-level*]	（任意） 指定されたファシリティのロギング重大度をデフォルト レベルにリセットします。 ファシリティおよび重大度を指定しないと、スイッチはすべてのファシリティをデフォルト レベルにリセットします。
ステップ 6	switch# **show logging module**	（任意） モジュール ロギング設定を表示します。
ステップ 7	switch# **show logging level** [*facility*]	（任意） ファシリティごとに、ロギング レベル設定およびシステムのデフォルト レベルを表示します。 ファシリティを指定しないと、スイッチはすべてのファシリティのレベルを表示します。
ステップ 8	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

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

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

ロギング タイムスタンプの設定

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

手順の概要

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

次に、メッセージのタイムスタンプ単位を設定する例を示します。

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

ACL ロギング キャッシュの設定

手順の概要

1. switch# **configure terminal**
2. switch(config)#**logging ip access-list cache entries** *num_entries*
3. switch(config)# **logging ip access-list cache interval** *seconds*
4. switch(config)# **logging ip access-list cache threshold** *num_packets*
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)#**logging ip access-list cache entries** *num_entries*	ソフトウェア内にキャッシュする最大ログエントリ数を設定します。 範囲は0～1048576エントリです。 デフォルト値は8000エントリです。
ステップ 3	switch(config)# **logging ip access-list cache interval** *seconds*	ログの更新の間隔を秒数で設定します。 この時間中エントリが非アクティブの場合、キャッシュから削除されます。 指定できる範囲は 5 ～ 86400 秒です。 デフォルト値は 300 秒です。
ステップ 4	switch(config)# **logging ip access-list cache threshold** *num_packets*	エントリがログに記録されるまでに一致するパケット数を設定します。 範囲は 0 ～ 1000000 パケットです。 デフォルト値は 0 パケットです。つまり、パケットの一致数によってロギングはトリガーされません。
ステップ 5	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を永続的に保存します。

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

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

インターフェイスにログインする ACL の設定

mgmt0 インターフェイスのみで ACL ロギングを設定できます。

はじめる前に

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

手順の概要

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

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

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

ACL ログの一致レベルの設定

手順の概要

1. switch# **configure terminal**
2. switch(config)# **acllog match-log-level** *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)# **acllog match-log-level** *number*	ACL ログ（acllog）で記録するエントリと一致するようにログ レベルを指定します。 *number* は 0 ～ 7 までの値です。 デフォルト値は 6 です。 （注） ログに入力するログ メッセージでは、ACL ログ ファシリティ（acllog）のログ レベルとログ ファイルのロギング重大度は、ACL ログの一致ログ レベル設定よりも大きいか、同じです。詳細については、モジュールおよびファシリティ メッセージのロギングの設定，（108 ページ）とファイルへのシステム メッセージ ロギングの設定，（106 ページ）を参照してください。
ステップ 3	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

syslog サーバの設定

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

手順の概要

1. **configure terminal**
2. **logging server** *host* [*severity-level* [**use-vrf** *vrf-name* [**facility** *facility*]]]
3. （任意） **no logging server** *host*
4. （任意） **show logging server**
5. （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	**logging server** *host* [*severity-level* [**use-vrf** *vrf-name* [**facility** *facility*]]] 例： `switch(config)# logging server 172.28.254.254 5 use-vrf default facility local3`	ホストが syslog メッセージを受信するように設定します。 • *host* 引数は、syslog サーバ ホストのホスト名または IPv4 または IPv6 アドレスを示します。 • *severity-level* 引数は、指定したレベルに syslog サーバへのメッセージのロギングを制限します。 重大度は 0 ～ 7 の範囲です。 表 11：システム メッセージの重大度，（102 ページ）を参照してください。 • **use vrf** *vrf-name* キーワードと引数は、仮想ルーティングおよび転送（VRF）名の *default* または *management* 値を示します。 特定の VRF が指定されない場合は、management がデフォルトです。 ただし、management が設定されているときは、それがデフォルトであるため、**show running** コマンドの出力には表示されません。 特定の VRF が設定されている場合、**show-running** コマンドの出力には、各サーバの VRF が表示されます。 （注） 現在 CFS 配信は VRF をサポートしていません。 CFS 配信がイネーブルの場合、デフォルト VRF で設定されているロギング サーバは管理 VRF として配布されます。 • facility 引数は syslog ファシリティ タイプを指定します。 デフォルトの発信ファシリティは local7 です。 ファシリティは、使用している Cisco Nexus シリーズ ソフトウェアのコマンド リファレンスに記載されています。 Nexus 5000 用の入手可能なコマンド リファレンスは http://www.cisco.com/en/US/products/ps9670/prod_command_reference_list.html にあります。 （注） デバッグは CLI ファシリティですが、デバッグの syslog にはサーバに送信されません。
ステップ 3	**no logging server** *host* 例： `switch(config)# no logging server 172.28.254.254 5`	（任意） 指定されたホストのロギング サーバを削除します。

	コマンドまたはアクション	目的
ステップ 4	**show logging server** 例： `switch# show logging server`	（任意） Syslog サーバ設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

次に、syslog サーバを設定する例を示します。

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

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

UNIX または Linux システムでの syslog の設定

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

```
facility.level <five tab characters> action
```

次の表に、設定可能な syslog フィールドを示します。

表 13： ***syslog.conf* の *Syslog* フィールド**

フィールド	説明
Facility	メッセージの作成者。auth、authpriv、cron、daemon、kern、lpr、mail、mark、news、syslog、user、local0 ～ local7 です。アスタリスク（*）を使用するとすべてを指定します。 これらのファシリティ指定により、発信元に基づいてメッセージの宛先を制御できます。 （注） ローカル ファシリティを使用する前に設定をチェックします。

フィールド	説明
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 リストです。アスタリスク（*）を使用するとすべてのログインユーザを指定します。

手順の概要

1. /etc/syslog.conf ファイルに次の行を追加して、ファイル /var/log/myfile.log に local7 ファシリティのデバッグ メッセージを記録します。
2. シェル プロンプトで次のコマンドを入力して、ログ ファイルを作成します。
3. 次のコマンドを入力して、システム メッセージ ロギング デーモンが myfile.log をチェックして、新しい変更を取得するようにします。

手順の詳細

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

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

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

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

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

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

Syslog サーバ設定の配布の設定

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

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

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

はじめる前に

1 つまたは複数の syslog サーバを設定しておく必要があります。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **logging distribute**
3. switch(config)# **logging commit**
4. switch(config)# **logging abort**
5. （任意） switch(config)# **no logging distribute**
6. （任意） switch# **show logging pending**
7. （任意） switch# **show logging pending-diff**
8. （任意） switch# **show logging internal info**
9. （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# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **logging distribute**	CFS インフラストラクチャを使用して、ネットワーク スイッチへの syslog サーバ設定の配布をイネーブルにします。 デフォルトでは、配布はディセーブルです。
ステップ 3	switch(config)# **logging commit**	ファブリック内のスイッチへ配布するための Syslog サーバ設定に対する保留中の変更をコミットします。
ステップ 4	switch(config)# **logging abort**	Syslog サーバ設定に対する保留中の変更をキャンセルします。
ステップ 5	switch(config)# **no logging distribute**	（任意） CFS インフラストラクチャを使用して、ネットワーク スイッチへの syslog サーバ設定の配布をディセーブルにします。 設定変更が保留中の場合は、配布をディセーブルにできません。 **logging commit** および **logging abort** コマンドを参照してください。 デフォルトでは、配布はディセーブルです。

	コマンドまたはアクション	目的
ステップ 6	switch# **show logging pending**	（任意） Syslog サーバ設定に対する保留中の変更を表示します。
ステップ 7	switch# **show logging pending-diff**	（任意） syslog サーバ設定の保留中の変更に対して、現在の syslog サーバ設定との違いを表示します。
ステップ 8	switch# **show logging internal info**	（任意） syslog サーバ配布の現在の状態と最後に実行したアクションに関する情報を表示します。
ステップ 9	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ログ ファイルの表示およびクリア

ログ ファイルおよび NVRAM のメッセージを表示したりクリアしたりできます。

手順の概要

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**

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 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。 month time フィールドには 3 文字を、year フィールドと day time フィールドには数値を入力します。

	コマンドまたはアクション	目的
ステップ 3	switch# **show logging nvram** [**last** *number-lines*]	NVRAM のメッセージを表示します。 表示される行数を制限するには、表示する最終行番号を入力できます。 最終行番号には 1 ～ 100 を指定できます。
ステップ 4	switch# **clear logging logfile**	ログ ファイルの内容をクリアします。
ステップ 5	switch# **clear logging nvram**	NVRAM の記録されたメッセージをクリアします。

次に、ログ ファイルのメッセージを表示する例を示します。

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

次に、ログ ファイルのメッセージをクリアする例を示します。

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

システム メッセージ ロギングの設定確認

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

コマンド	目的
show logging console	コンソール ロギング設定を表示します。
show logging info	ロギング設定を表示します。
show logging internal info	syslog 配布情報を表示します。
show logging last *number-lines*	ログ ファイルの末尾から指定行数を表示します。
show logging level [*facility*]	ファシリティ ロギング重大度設定を表示します。
show logging logfile [**start-time** *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。

コマンド	目的
show logging pending	syslog サーバの保留中の配布設定を表示します。
show logging pending-diff	syslog サーバの保留中の配布設定の違いを表示します。
show logging server	syslog サーバ設定を表示します。
show logging session	ロギング セッションのステータスを表示します。
show logging status	ロギング ステータスを表示します。
show logging timestamp	ロギング タイムスタンプ単位設定を表示します。

第 10 章

Smart Call Home の設定

この章の内容は、次のとおりです。

Smart Call Home に関する情報

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

シスコと直接サービス契約を結んでいる場合は、Smart Call Home サービス用のデバイスを登録できます。 Smart Call Home は、ご使用のデバイスから送信された Smart Call Home メッセージを分析し、背景情報および推奨事項を提供して、システムの問題を迅速に解決します。 既知と特定できる問題、特に GOLD 診断エラーについては、Cisco Technical Assistance Center（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; トランスポート ゲートウェイ）集約ポイントを経由して行われます。複数のデバイスでサポートを必要としている場合、またはセキュリティ要件の関係でご使用のデバイスをインターネットに直接接続できない場合は、TG集約ポイントを使用できます。
- Smart Call Home メッセージと推奨事項、すべての Smart Call Home デバイスのインベントリおよび設定情報、および Field Notice、セキュリティ勧告、およびサポート終了日情報への Web ベースのアクセス。

Smart Call Home の概要

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

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

Smart Call Home 機能には、次のものがあります。

- 関連する CLI コマンド出力の実行および添付が自動化されます。
- 次のような、複数のメッセージ フォーマット オプションがあります。
  - ショート テキスト：ポケットベルまたは印刷形式のレポートに最適。
  - フルテキスト：人間が判読しやすいように完全にフォーマットされたメッセージ情報です。
  - XML：Extensible Markup Language（XML）および Adaptive Messaging Language（AML）XML 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、Cisco 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。 それぞれの宛先プロファイルには、最大 50 個の E メール宛先アドレスを設定できます。

Smart Call Home 宛先プロファイル

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

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

- 1 つ以上の電子メール宛先：この宛先プロファイルに割り当てられたアラート グループによって生成された Smart Call Home メッセージの受信者リスト。
- メッセージ フォーマット：Smart Call Home メッセージのフォーマット（ショート テキスト、フル テキスト、または XML）
- メッセージ重大度：スイッチが宛先プロファイル内のすべての電子メールアドレスに対して Smart Call Home メッセージを生成するまで、アラートが満たす必要がある Smart Call Home 重大度。 アラートの Smart Call Home 重大度が、宛先プロファイルに設定されたメッセージ重大度よりも低い場合、スイッチはアラートを生成しません。

定期メッセージを日別、週別、月別で送信するコンポーネントアラートグループを使用して、定期的なコンポーネントアップデートメッセージを許可するよう宛先プロファイルを設定することもできます。

Cisco Nexus スイッチは、次の定義済み宛先プロファイルをサポートします。

- CiscoTAC-1：XML メッセージ フォーマットの Cisco-TAC アラート グループをサポートします。
- full-text-destination：フル テキスト メッセージ フォーマットをサポートします。
- short-text-destination：ショート テキスト メッセージ フォーマットをサポートします。

Smart Call Home アラート グループ

アラート グループは、すべての Cisco Nexus 5000 Series スイッチでサポートされる Smart Call Home アラートの定義済みサブセットです。 アラート グループを使用すると、定義済みまたはカスタム宛先プロファイルに送信する一連の Smart Call Home アラートを選択できます。 Smart Call Home アラートが宛先プロファイルにアソシエートされたいずれかのアラート グループに属する場合、およびアラートで、Smart Call Home メッセージ重大度が宛先プロファイルに設定されているメッセージ重大度と同じか、それ以上である場合のみ、スイッチは Smart Call Home アラートは宛先プロファイルの電子メールの宛先に送信されます。

次の表に、サポートされるアラート グループと、アラート グループ用に生成された Smart Call Home メッセージに含まれるデフォルトの CLI コマンド出力を示します。

表 *14*： アラート グループおよび実行されるコマンド

アラート グループ	説明	実行されるコマンド
Cisco-TAC	Smart Call Home 宛ての、他のアラート グループからのすべてのクリティカル アラート	アラートを発信するアラート グループに基づいてコマンドを実行します。

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

Smart Call Home は、syslog の重大度を、syslog ポート グループ メッセージの対応する Smart Call Home の重大度に対応させます

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

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

Smart Call Home のメッセージ レベル

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

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

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

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

表 *15*： 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	N/A	ネットワーク全体に及ぶ深刻な障害。
8	Disaster	N/A	ネットワークへの重大な影響。
7	Fatal	緊急（0）	システムは使用不能。
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	クリティカル（2）	メジャー状態です。
4	Minor	エラー（3）	マイナーな状態。

Smart Call Home レベル	キーワード	Syslog レベル	説明
3	Warning	警告（4）	警告状態。
2	Notification	通知（5）	基本的な通知および情報メッセージです。 他と関係しない、重要性の低い障害です。
1	Normal	情報（6）	標準状態に戻ることを示す標準イベントです。
0	Debugging	デバッグ（7）	デバッグ メッセージ。

Call Home のメッセージ形式

Call Home では、次のメッセージ フォーマットがサポートされます。

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

次の表に、すべてのメッセージ タイプのショート テキスト書式設定オプションを示します。

表 *16*：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
エラー切り分けメッセージ	起動イベントの簡単な説明（英語）
アラーム緊急度	システム メッセージに適用されるようなエラー レベル

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

表 *17*：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とタイム 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
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。 • *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特定される数字。 例：WS-C6509@C@12345678	/aml/ header/deviceID

データ項目（プレーン テキストおよび XML）	説明（プレーン テキストおよび XML）	XML タグ（XML のみ）
カスタマー ID	サポート サービスによって契約情報やその他の ID に使用されるオプションのユーザ設定可能なフィールド。	/aml/ header/customerID
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
サーバ ID	デバイスからメッセージが生成された場合、これはデバイスの Unique Device Identifier（UDI）フォーマットです。 形式は、*type@Sid@serial*。 • *type* は、バックプレーン IDPROM からの製品の型番。 • @ は区切り文字。 • *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特定される数字。 例：WS-C6509@C@12345678	/aml/header/serverID
メッセージの説明	エラーを説明するショート テキスト	/aml/body/msgDesc
デバイス名	イベントが発生したノード（デバイスのホスト名）。	/aml/body/sysName

データ項目（プレーン テキストおよび XML）	説明（プレーン テキストおよび XML）	XML タグ（XML のみ）
担当者名	イベントが発生したノード関連の問題について問い合わせる担当者名	/aml/body/sysContact
連絡先電子メール	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 Return Materials Authorization（RMA; 返品許可）部品の送付先住所を保存するオプション フィールド	/aml/body/sysStreetAddress
モデル名	デバイスのモデル名（製品ファミリ名に含まれる具体的なモデル）	/aml/body/chassis/name
シリアル番号	ユニットのシャーシのシリアル番号。	/aml/body/chassis/serialNo
シャーシの部品番号	シャーシの最上アセンブリ番号。	/aml/body/chassis/partNo
特定のアラート グループ メッセージの固有のフィールドは、ここに挿入されます。		
このアラート グループに対して複数の CLI コマンドが実行されると、次のフィールドが繰り返される場合があります。		
コマンド出力名	実行された CLI コマンドの正確な名前	/aml/attachments/attachment/name
添付ファイルの種類	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。

表 *18*：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	最上位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 の部品番号	影響のある FRU の部品番号。	/aml/body/fru/partNo
FRU スロット	イベントメッセージを生成する FRU のスロット番号	/aml/body/fru/slot
FRU ハードウェアバージョン	影響のある 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。

表 *19*：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	最上位ソフトウェアバージョン。	/aml/body/chassis/swVersion

データ項目（プレーン テキストおよび XML）	説明（プレーン テキストおよび XML）	XML タグ（XML のみ）
FRU 名	イベント メッセージを生成する関連 FRU の名前	/aml/body/fru/name
FRU s/n	FRU のシリアル番号。	/aml/body/fru/serialNo
FRU 部品番号	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 のユーザが作成したテスト メッセージ形式について説明します。

表 *20*： ユーザが作成したテスト メッセージの挿入フィールド

データ項目（プレーン テキストおよび XML）	説明（プレーン テキストおよび XML）	XML タグ（XML のみ）
プロセス ID	固有のプロセス ID。	/aml/body/process/id
プロセス ステート	プロセスの状態（実行中、中止など）。	/aml/body/process/processState
プロセス例外	例外または原因コード。	/aml/body/process/exception

Smart Call Home の注意事項および制約事項

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

Smart Call Home の前提条件

- 電子メール サーバの接続。
- コンタクト名（SNMP サーバの連絡先）、電話番号、および住所情報へのアクセス。
- スイッチと電子メール サーバ間の IP 接続。
- 設定するデバイス用の有効なサービス契約。

Call Home のデフォルト設定

表 *21*： デフォルトの *Call Home* パラメータ

パラメータ	デフォルト
フルテキストフォーマットで送信するメッセージの宛先メッセージ サイズ	4000000
XML フォーマットで送信するメッセージの宛先メッセージ サイズ	4000000
ショートテキストフォーマットで送信するメッセージの宛先メッセージ サイズ	4000
ポートを指定しなかった場合の SMTP サーバ ポート	25
プロファイルとアラート グループの関連付け	フルテキスト宛先プロファイルおよびショートテキスト宛先プロファイルの場合はすべて。CiscoTAC-1 宛先プロファイルの場合は cisco-tac アラート グループ
フォーマット タイプ	XML
Call Home のメッセージ レベル	0（ゼロ）

Smart Call Home の設定

Smart Call Home の登録

はじめる前に

- ご使用のスイッチの SMARTnet 契約番号
- 電子メール アドレス
- Cisco.com ID

手順の概要

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

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

次の作業

連絡先情報を設定します。

担当者情報の設定

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

手順の概要

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. （任意） switch(config-callhome)# **contract-id** *contract-number*
8. （任意） switch(config-callhome)# **customer-id** *customer-number*
9. （任意） switch(config-callhome)# **site-id** *site-number*
10. （任意） switch(config-callhome)# **switch-priority** *number*
11. （任意） switch# **show callhome**
12. （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 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 E 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。 （注） 任意の有効な E メール アドレスを使用できます。 アドレスには、空白を含めることはできません。
ステップ 5	switch(config-callhome)# **phone-contact** *international-phone-number*	デバイスの担当者の電話番号を国際電話フォーマットで設定します。 *international-phone-number* は、最大 17 文字の英数字で、国際電話フォーマットにする必要があります。 （注） 電話番号には、空白を含めることはできません。 番号の前にプラス（+）プレフィックスを使用します。
ステップ 6	switch(config-callhome)# **streetaddress** *address*	スイッチの主担当者の住所を設定します。 *address* には、最大 255 の英数字を使用できます。 スペースを使用できます。
ステップ 7	switch(config-callhome)# **contract-id** *contract-number*	（任意） サービス契約からこのスイッチの契約番号を設定します。

	コマンドまたはアクション	目的
		contract-number には最大 255 の英数字を使用できます。
ステップ 8	switch(config-callhome)# **customer-id** *customer-number*	（任意） サービス契約からこのスイッチのカスタマー番号を設定します。 *customer-number* には最大 255 の英数字を使用できます。
ステップ 9	switch(config-callhome)# **site-id** *site-number*	（任意） このスイッチのサイト番号を設定します。 *site-number* は、最大 255 文字の英数字を自由なフォーマットで指定できます。
ステップ 10	switch(config-callhome)# **switch-priority** *number*	（任意） このスイッチのスイッチ プライオリティを設定します。 指定できる範囲は 0 ～ 7 です。0 は最高のプライオリティを、7 は最低のプライオリティを示します。 デフォルトは 7 です。
ステップ 11	switch# **show callhome**	（任意） Smart Call Home コンフィギュレーションの概要を表示します。
ステップ 12	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

次に、Call Home に関する契約情報を設定する例を示します。

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

次の作業

宛先プロファイルを作成します。

宛先プロファイルの作成

ユーザ定義の宛先プロファイルを作成し、新しい宛先プロファイルにメッセージ フォーマットを設定する必要があります。

手順の概要

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**}} | *profile-name* {**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. （任意） switch# **show callhome destination-profile** [**profile** *name*]
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)# **destination-profile** {**ciscoTAC-1** {**alert-group** *group* | **email-addr** *address* | **http** *URL* | **transport-method** {**email** | **http**}} | *profile-name* {**alert-group** *group* | **email-addr** *address* | **format** {**XML** | **full-txt** | **short-txt**} | **http** *URL* | **message-level** *level* | **message-size** *size* | **transport-method** {**email** | **http**}} | **full-txt-destination** {**alert-group** *group* | **email-addr** *address* | **http** *URL* | **message-level** *level* | **message-size** *size* | **transport-method** {**email** | **http**}} | **short-txt-destination** {**alert-group** *group* | **email-addr** *address* | **http** *URL* | **message-level** *level* | **message-size** *size* | **transport-method** {**email** | **http**}}}	新しい宛先プロファイルを作成し、そのプロファイルのメッセージ フォーマットを設定します。 プロファイル名は、最大 31 文字の英数字で指定できます。 このコマンドの詳細については、使用している Cisco Nexus シリーズ ソフトウェアのコマンド リファレンスを参照してください。 Nexus 5000 用の入手可能なコマンド リファレンスは http://www.cisco.com/en/US/products/ps9670/prod_command_reference_list.html にあります。
ステップ 4	switch# **show callhome destination-profile** [**profile** *name*]	（任意） 1 つまたは複数の宛先プロファイルに関する情報を表示します。
ステップ 5	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

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

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

宛先プロファイルの変更

定義済みまたはユーザ定義の宛先プロファイルの次の属性を変更できます。

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

（注） CiscoTAC-1 宛先プロファイルは変更または削除できません。

手順の概要

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. （任意） switch# **show callhome destination-profile** [**profile** *name*]
7. （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。

	コマンドまたはアクション	目的
ステップ 3	switch(config-callhome)# **destination-profile** {*name* | **full-txt-destination** | **short-txt-destination**} **email-addr** *address*	ユーザ定義または定義済みの宛先プロファイルに E メール アドレスを設定します。 宛先プロファイルには、最大 50 個の E メール アドレスを設定できます。
ステップ 4	**destination-profile** {*name* | **full-txt-destination** | **short-txt-destination**} **message-level** *number*	この宛先プロファイルの Call Home メッセージの重大度を設定します。 Call Home 重大度が一致する、またはそれ以上であるアラートのみが、このプロファイルの宛先に送信されます。 *number* に指定できる範囲は 0 ～ 9 です。9 は最大の重大度を示します。
ステップ 5	switch(config-callhome)# **destination-profile** {*name* | **full-txt-destination** | **short-txt-destination**} **message-size** *number*	この宛先プロファイルの最大メッセージ サイズを設定します。 full-txt-destination の値の範囲は 0 ～ 5000000 で、デフォルトは 2500000 です。 short-txt-destination の値の範囲は 0 ～ 100000 で、デフォルトは 4000 です。 CiscoTAC-1 では、値は 5000000 で、これは変更不可能です。
ステップ 6	switch# **show callhome destination-profile** [**profile** *name*]	（任意） 1 つまたは複数の宛先プロファイルに関する情報を表示します。
ステップ 7	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

次に、Call Home の宛先プロファイルを変更する例を示します。

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

次の作業

アラート グループと宛先プロファイルをアソシエートします。

アラート グループと宛先プロファイルのアソシエーション

手順の概要

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

次に、すべてのアラート グループを宛先プロファイル Noc101 に関連付ける例を示します。

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

次の作業

任意で show コマンドをアラート グループに追加し、SMTP 電子メール サーバを設定します。

アラート グループへの show コマンドの追加

1 つのアラート グループにユーザ定義の CLI **show** コマンドを 5 つまで割り当てることができます。

手順の概要

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. （任意） switch# **show callhome user-def-cmds**
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)# **alert-group** {**Configuration** | **Diagnostic** | **Environmental** | **Inventory** | **License** | **Linecard-Hardware** | **Supervisor-Hardware** | **Syslog-group-port** | **System** | **Test**} **user-def-cmd** *show-cmd*	**show** コマンド出力を、このアラート グループに送信された Call Home メッセージに追加します。 有効な **show** コマンドだけが受け入れられます。 （注） CiscoTAC-1 宛先プロファイルには、ユーザ定義の CLI **show** コマンドを追加できません。
ステップ 4	switch# **show callhome user-def-cmds**	（任意） アラート グループに追加されたすべてのユーザ定義 **show** コマンドに関する情報を表示します。
ステップ 5	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

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

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

次の作業

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

電子メール サーバの詳細の設定

Call Home 機能が動作するよう SMTP サーバ アドレスを設定します。 送信元および返信先 E メール アドレスも設定できます。

手順の概要

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. （任意） switch(config-callhome)# **transport email from** *email-address*
5. （任意） switch(config-callhome)# **transport email reply-to** *email-address*
6. （任意） switch# **show callhome transport-email**
7. （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)# **transport email smtp-server** *ip-address* [**port** *number*] [**use-vrf** *vrf-name*]	SMTP サーバを、ドメイン ネーム サーバ（DNS）名、IPv4 アドレス、または IPv6 アドレスのいずれかとして設定します。 port*number* の範囲は 1 ～ 65535 です。 デフォルトのポート番号は 25 です。 この SMTP サーバと通信する際に使用するよう任意で VRF を設定できます。

	コマンドまたはアクション	目的
ステップ 4	switch(config-callhome)# **transport email from** *email-address*	（任意） Smart Call Home メッセージの送信元電子メール フィールドを設定します。
ステップ 5	switch(config-callhome)# **transport email reply-to** *email-address*	（任意） Smart Call Home メッセージの返信先電子メール フィールドを設定します。
ステップ 6	switch# **show callhome transport-email**	（任意） Smart Call Home の電子メール設定に関する情報を表示します。
ステップ 7	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

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

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

次の作業

定期的なインベントリ通知を設定します。

定期的なインベントリ通知の設定

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

手順の概要

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

次に、定期的なコンポーネント メッセージを 20 日ごとに生成するよう設定する例を示します。

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

次の作業

重複メッセージ抑制をディセーブルにします。

重複メッセージ抑制のディセーブル化

同じイベントについて受信する重複メッセージの数を制限できます。 デフォルトでは、スイッチは同じイベントについて受信する重複メッセージの数を制限します。 2 時間の時間枠内で送信された重複メッセージの数が 30 メッセージを超えると、スイッチは同じアラート タイプの以降のメッセージは廃棄されます。

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	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

次に、重複メッセージ抑制をディセーブルにする例を示します。

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

次の作業

Smart Call Home をイネーブルにします。

Smart Call Home のイネーブル化またはディセーブル化

手順の概要

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	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

次に、Smart Call Home をイネーブルにする例を示します。

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

次の作業

任意でテスト メッセージを生成します。

Smart Call Home 設定のテスト

はじめる前に

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

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

手順の概要

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	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

次に、Smart Call Home をイネーブルにする例を示します。

```
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

設定を確認するには、次のいずれかのコマンドを使用します。

コマンド	目的
switch# **show callhome**	Call Home のステータスを表示します。
switch# **show callhome destination-profile** *name*	1 つまたは複数の Call Home 宛先プロファイルを表示します。
switch# **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。
switch# **show callhome status**	Smart Call Home ステータスを表示します。
switch# **show callhome transport-email**	Smart Call Home の電子メール設定を表示します。

コマンド	目的
switch# **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。
switch# **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。
switch# **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。
switch# **show tech-support callhome**	Smart Call Home のテクニカル サポート出力を表示します。

フル テキスト形式での syslog アラート通知の例

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

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

XML 形式での Syslog アラート通知の例

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

```
From: example
Sent: Wednesday, April 25, 2007 7:20 AM
To: User (user)
Subject: System Notification From Router - syslog - 2007-04-25 14:19:55
GMT+00:00
<?xml version="1.0" encoding="UTF-8"?>
<soap-env:Envelope xmlns:soap-env="http://www.w3.org/2003/05/soap-envelope">
```

```
<soap-env:Header>
<aml-session:Session xmlns:aml-session="http://www.example.com/2004/01/aml-session"
soap-env:mustUnderstand="true" soap-env:role=
"http://www.w3.org/2003/05/soap-envelope/role/next">
<aml-session:To>http://tools.example.com/services/DDCEService</aml-session:To>
<aml-session:Path>
<aml-session:Via>http://www.example.com/appliance/uri</aml-session:Via>
</aml-session:Path>
<aml-session:From>http://www.example.com/appliance/uri</aml-session:From>
<aml-session:MessageId>M2:69000101:C9D9E20B</aml-session:MessageId>
</aml-session:Session>
</soap-env:Header>
<soap-env:Body>
<aml-block:Block xmlns:aml-block="http://www.example.com/2004/01/aml-block">
<aml-block:Header>
<aml-block:Type>http://www.example.com/2005/05/callhome/syslog</aml-block:Type>
<aml-block:CreationDate>2007-04-25 14:19:55 GMT+00:00</aml-block:CreationDate>
<aml-block:Builder>
<aml-block:Name>Cat6500</aml-block:Name>
<aml-block:Version>2.0</aml-block:Version>
</aml-block:Builder>
<aml-block:BlockGroup>
<aml-block:GroupId>G3:69000101:C9F9E20C</aml-block:GroupId>
<aml-block:Number>0</aml-block:Number>
<aml-block:IsLast>true</aml-block:IsLast>
<aml-block:IsPrimary>true</aml-block:IsPrimary>
<aml-block:WaitForPrimary>false</aml-block:WaitForPrimary>
</aml-block:BlockGroup>
<aml-block:Severity>2</aml-block:Severity>
</aml-block:Header>
<aml-block:Content>
<ch:Call Home xmlns:ch="http://www.example.com/2005/05/callhome" version="1.0">
<ch:EventTime>2007-04-25 14:19:55 GMT+00:00</ch:EventTime>
<ch:MessageDescription>03:29:29: %CLEAR-5-COUNTERS: Clear counter on all
interfaces by console</ch:MessageDescription>
<ch:Event>
<ch:Type>syslog</ch:Type>
<ch:SubType>
</ch:SubType>
<ch:Brand>Cisco Systems</ch:Brand>
<ch:Series>Catalyst 6500 Series Switches</ch:Series>
</ch:Event>
<ch:CustomerData>
<ch:UserData>
<ch:Email>person@example.com</ch:Email>
</ch:UserData>
<ch:ContractData>
<ch:CustomerId>12345</ch:CustomerId>
<ch:SiteId>building 1</ch:SiteId>
<ch:ContractId>abcdefg12345</ch:ContractId>
<ch:DeviceId>WS-C6509@C@69000101</ch:DeviceId>
</ch:ContractData>
<ch:SystemInfo>
<ch:Name>Router</ch:Name>
<ch:Contact>
</ch:Contact>
<ch:ContactEmail>user@example.com</ch:ContactEmail>
<ch:ContactPhoneNumber>+1-408-555-1212</ch:ContactPhoneNumber>
<ch:StreetAddress>#1234 Any Street, Any City, Any State, 12345
</ch:StreetAddress>
</ch:SystemInfo>
</ch:CustomerData>
<ch:Device>
<rme:Chassis xmlns:rme="http://www.example.com/rme/4.0">
<rme:Model>WS-C6509</rme:Model>
<rme:HardwareVersion>1.0</rme:HardwareVersion>
<rme:SerialNumber>69000101</rme:SerialNumber>
<rme:AdditionalInformation>
<rme:AD name="PartNumber" value="73-3438-03 01" />
<rme:AD name="SoftwareVersion" value="4.0(20080421:012711)" />
</rme:AdditionalInformation>
</rme:Chassis>
</ch:Device>
```

```
</ch:Call Home>
</aml-block:Content>
<aml-block:Attachments>
<aml-block:Attachment type="inline">
<aml-block:Name>show logging</aml-block:Name>
<aml-block:Data encoding="plain">
<![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-Apr-07 15:54 by xxx
Firmware compiled 11-Apr-07 03:34 by integ Build [100]00:01:01: %PFREDUN-6-ACTIVE:
 Initializing as ACTIVE processor for this switch00:01:01: %SYS-3-LOGGER_FLUSHED:
System was paused for 00:00:00 to ensure console debugging output.00:03:00: SP: SP:
 Currently running ROMMON from F1 region00:03:07: %C6K_PLATFORM-SP-4-CONFREG_BREAK
_ENABLED: The default factory setting for config register is 0x2102.It is advisable
 to retain 1 in 0x2102 as it prevents returning to ROMMON when break is issued.00:03:18:
 %SYS-SP-5-RESTART: System restarted --Cisco IOS Software, s72033_sp Software
 (s72033_sp-ADVENTERPRISEK9_DBG-VM), Experimental Version 12.2(20070421:012711)Copyright
 (c) 1986-2007 by Cisco Systems, Inc.
Compiled Thu 26-Apr-07 18:00 by xxx
00:03:18: %SYS-SP-6-BOOTTIME: Time taken to reboot after reload =  339 seconds
00:03:18: %OIR-SP-6-INSPS: Power supply inserted in slot 1
00:03:18: %C6KPWR-SP-4-PSOK: power supply 1 turned on.
00:03:18: %OIR-SP-6-INSPS: Power supply inserted in slot00:01:09: %SSH-5-ENABLED:
 SSH 1.99 has been enabled
00:03:18: %C6KPWR-SP-4-PSOK: power supply 2 turned on.
00:03:18: %C6KPWR-SP-4-PSREDUNDANTMISMATCH: power supplies rated outputs do not match.
00:03:18: %C6KPWR-SP-4-PSREDUNDANTBOTHSUPPLY: in power-redundancy mode, system is
 operating on both power supplies.
00:01:10: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
00:01:10: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
00:03:20: %C6KENV-SP-4-FANHIOUTPUT: Version 2 high-output fan-tray is in effect
00:03:22: %C6KPWR-SP-4-PSNOREDUNDANCY: Power supplies are not in full redundancy,
 power usage exceeds lower capacity supply
00:03:26: %FABRIC-SP-5-FABRIC_MODULE_ACTIVE: The Switch Fabric Module in slot 6
 became active.
00:03:28: %DIAG-SP-6-RUN_MINIMUM: Module 6: Running Minimal Diagnostics...
00:03:50: %DIAG-SP-6-DIAG_OK: Module 6: Passed Online Diagnostics
00:03:50: %OIR-SP-6-INSCARD: Card inserted in slot 6, interfaces are now online
00:03:51: %DIAG-SP-6-RUN_MINIMUM: Module 3: Running Minimal Diagnostics...
00:03:51: %DIAG-SP-6-RUN_MINIMUM: Module 7: Running Minimal Diagnostics...
00:03:51: %DIAG-SP-6-RUN_MINIMUM: Module 9: Running Minimal Diagnostics...
00:01:51: %MFIB_CONST_RP-6-REPLICATION_MODE_CHANGE: Replication Mode Change Detected.
 Current system replication mode is Ingress
00:04:01: %DIAG-SP-6-DIAG_OK: Module 3: Passed Online Diagnostics
00:04:01: %OIR-SP-6-DOWNGRADE: Fabric capable module 3 not at an appropriate hardware
 revision level, and can only run in flowthrough mode
00:04:02: %OIR-SP-6-INSCARD: Card inserted in slot 3, interfaces are now online
00:04:11: %DIAG-SP-6-DIAG_OK: Module 7: Passed Online Diagnostics
00:04:14: %OIR-SP-6-INSCARD: Card inserted in slot 7, interfaces are now online
00:04:35: %DIAG-SP-6-DIAG_OK: Module 9: Passed Online Diagnostics
00:04:37: %OIR-SP-6-INSCARD: Card inserted in slot 9, interfaces are now online
00:00:09: DaughterBoard (Distributed Forwarding Card 3)
Firmware compiled 11-Apr-07 03:34 by integ Build [100]
00:00:22: %SYS-DFC4-5-RESTART: System restarted --
Cisco DCOS Software, c6lc2 Software (c6lc2-SPDBG-VM), Experimental Version 4.0
(20080421:012711)Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 26-Apr-08 17:20 by xxx
00:00:23: DFC4: Currently running ROMMON from F2 region
00:00:25: %SYS-DFC2-5-RESTART: System restarted --
Cisco IOS Software, c6slc Software (c6slc-SPDBG-VM), Experimental Version 12.2
```

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

第 11 章

ロールバックの設定

この章の内容は、次のとおりです。

ロールバックの概要

ロールバック機能を使用すると、Cisco NX-OS のコンフィギュレーションのスナップショットまたはユーザ チェックポイントを使用して、スイッチをリロードしなくても、いつでもそのコンフィギュレーションをスイッチに再適用できます。 権限のある管理者であれば、チェックポイントで設定されている機能について専門的な知識がなくても、ロールバック機能を使用して、そのチェックポイント コンフィギュレーションを適用できます。

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

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

注意事項および制約事項

ロールバックに関する設定時の注意事項および制約事項は、次のとおりです。

- 作成できるチェックポイント コピーの最大数は 10 です。
- あるスイッチのチェックポイント ファイルを別のスイッチに適用することはできません。
- チェックポイント ファイル名の長さは、最大 75 文字です。
- チェックポイントのファイル名の先頭を system にすることはできません。
- Cisco NX-OS Release 5.0(2)N1(1) 以降は、チェックポイントのファイル名の先頭を auto にできます。
- Cisco NX-OS Release 5.0(2)N1(1) 以降は、チェックポイントのファイル名を summary、または summary の何らかの省略形にすることもできます。
- FCoE をイネーブルにすると、チェック ポイントおよび設定のロール バックの機能はディセーブルになります。
- チェックポイント、ロールバック、または実行コンフィギュレーションからスタートアップ コンフィギュレーションへのコピーを同時に実行できるのは、1 ユーザだけです。
- **write erase** および **reload** コマンドを入力すると、チェック ポイントが削除されます。 clear checkpoint database コマンドを使用すると、すべてのチェックポイント ファイルを削除できます。
- ブートフラッシュでチェックポイントを作成した場合、ロールバックの実行前は実行システム コンフィギュレーションとの違いは実行できず、「変更なし」と報告されます。
- チェック ポイントはスイッチに対してローカルです。
- **checkpoint** および **checkpoint** *checkpoint_name* コマンドを使用して作成されたチェックポイントは、すべてのスイッチの 1 つのスイッチオーバーに対して存在します。
- ブートフラッシュ時のファイルへのロールバックは、**checkpoint** *checkpoint_name* コマンドを使用して作成されたファイルでのみサポートされます。他の ASCII タイプのファイルではサポートされません。
- チェックポイントの名前は一意にする必要があります。 以前に保存したチェックポイントを同じ名前で上書きすることはできません。
- 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* [**all**]

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	switch# **no checkpoint***cp-name* 例： `switch# no checkpoint stable`	（任意） **checkpoint** コマンドの **no** 形式を使用すると、チェックポイント名を削除できます。 **delete** コマンドを使用して、チェックポイント ファイルを削除できます。
ステップ 3	switch# **show checkpoint***cp-name* [**all**] 例： `switch# show checkpoint stable`	（任意） チェックポイント名の内容を表示します。

ロールバックの実装

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

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

手順の概要

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。

次に、チェックポイント ファイルを作成し、次に、ユーザ チェックポイント名への atomic ロール バックを実行する例を示します。

```
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表示するには、次のいずれかの作業を行います。

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

DNS の設定

この章の内容は、次のとおりです。

DNS クライアントの概要

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

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

ネーム サーバ

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

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

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

DNS の動作

ネーム サーバは、クライアントが DNS サーバに発行した、特定のゾーン内でローカルに定義されたホストの照会を次のように処理します。

- 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 サーバは単に、その情報が存在しないと返信します。
- 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、正規の返信は送信されません。

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

ハイ アベイラビリティ

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

DNS クライアントの前提条件

DNS クライアントには次の前提条件があります。

- ネットワーク上に DNS ネーム サーバが必要です。

DNS クライアントのライセンス要件

次の表に、この機能のライセンス要件を示します。

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

デフォルト設定値

次の表に、DNS クライアント パラメータのデフォルト設定を示します。

パラメータ	デフォルト
DNS クライアント	イネーブル

DNS クライアントの設定

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

はじめる前に

- ネットワーク上にドメイン ネーム サーバがあることを確認します。

手順の概要

1. configuration terminal
2. vrf context managment
3. ip host *name address1 [address2... address6]*
4. ip domain name *name* [**use-vrf** *vrf-name*]
5. ip domain-list *name* [**use-vrf** *vrf-name*]
6. ip name-server *server-address1* [*server-address2... server-address6*] [**use-vrf** *vrf-name*]
7. ip domain-lookup
8. show hosts
9. exit
10. 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)#`
		コンフィギュレーション端末モードを開始します。

ステップ 2	vrf context managment
	
	例：
	`switch(config)# vrf context management`
	`switch(config)#`
		設定可能な VRF 名を指定します。

ステップ 3	ip host *name address1 [address2... address6]*
	
	例：
	`switch# ip host cisco-rtp 192.0.2.1`
	`switch(config)#`
		ホスト名キャッシュに、6つまでのスタティック ホスト名前/アドレス マッピングを定義します。

ステップ 4	ip domain name *name* [**use-vrf** *vrf-name*]
	
	例：
	`switch(config)# ip domain-name myserver.com`
	`switch(config)#`
		（任意）Cisco NX-OS が無条件ホスト名を完成するために使用するデフォルト ドメイン ネーム サーバを定義します。 このドメイン名を設定した VRF でこのドメイン ネーム サーバを解決できない場合は、任意で、Cisco NX-OS がこのドメイン ネーム サーバを解決するために使用する VRF を定義することもできます。
		
		Cisco NX-OS は、ドメイン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	ip domain-list *name* [**use-vrf** *vrf-name*]
	
	例：
	`switch(config)# ip domain-list mycompany.com`
	`switch(config)#`
		（任意）Cisco NX-OS が無条件ホスト名を完成するために使用できる追加のドメイン ネーム サーバを定義します。 このドメイン名を設定した VRF でこのドメイン ネーム サーバを解決できない場合は、任意で、Cisco NX-OS がこのドメイン ネーム サーバを解決するために使用する VRF を定義することもできます。
		
		Cisco NX-OS はドメイン リスト内の各エントリを使用して、ドメイン名ルックアップを開始する前に、完全なドメイン名を含まないあらゆるホスト名にこのドメイン名を追加します。 Cisco NX-OS は、一致するものが見つかるまで、ドメイン リストの各エントリにこれを実行します。

ステップ 6	ip name-server *server-address1* [*server-address2... server-address6*] [**use-vrf** *vrf-name*]	（任意）最大6つのネーム 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。

	コマンドまたはアクション	目的
	例： `switch(config)# ip name-server 192.0.2.22`	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	ip domain-lookup 例： `switch(config)# ip domain-lookup`	（任意）DNS ベースのアドレス変換をイネーブルにします。デフォルトでは、イネーブルです。
ステップ 8	show hosts 例： `switch(config)# show hosts`	（任意）DNS に関する情報を表示します。

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

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

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

第 13 章

SNMP の設定

この章の内容は、次のとおりです。

SNMP について

簡易ネットワーク管理プロトコル（SNMP）は、SNMP マネージャとエージェントの間の通信のメッセージフォーマットを提供するアプリケーション層プロトコルです。 SNMP は、ネットワーク内のデバイスのモニタリングおよび管理に使用する標準フレームワークと共通言語を提供します。

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 5000

Series スイッチ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

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

Cisco Nexus 5000 Series スイッチは、SNMPv1、SNMPv2c、および SNMPv3 をサポートします。 SNMPv1 と SNMPv2c は、ともにコミュニティベース形式のセキュリティを使用します。

Cisco NX-OS は IPv6 による SNMP をサポートしています。

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

SNMP 通知

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

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

トラップの信頼性はインフォームより低くなります。SNMP マネージャはトラップを受信しても Acknowledgment（ACK; 確認応答）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 Protocol Data Unit（PDU; プロトコル データ ユニット）でメッセージの受信を確認します。 Cisco Nexus 5000 Series スイッチが応答を受信しない場合、インフォーム要求を再度送信できます。

複数のホスト レシーバ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。
- authNoPriv：認証は実行するが、暗号化を実行しないセキュリティ レベル。
- authPriv：認証と暗号化両方を実行するセキュリティ レベル。

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

表 *22*：***SNMP*** セキュリティ モデルおよびセキュリティ レベル

モデル	レベル	認証	暗号化	結果
v1	noAuthNoPriv	コミュニティ ストリング	No	コミュニティ ストリングの照合を使用して認証します。
v2c	noAuthNoPriv	コミュニティ ストリング	No	コミュニティ ストリングの照合を使用して認証します。
v3	noAuthNoPriv	ユーザ名	No	ユーザ名の照合を使用して認証します。

モデル	レベル	認証	暗号化	結果
v3	authNoPriv	HMAC-MD5 または HMAC-SHA	No	Hash-Based Message Authentication Code（HMAC）Message Digest 5（MD5; メッセージ ダイジェスト 5）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 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 User-Based Security Model（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ていないことを保証します。また、データ シーケンスが、通常発生するものよりも高い頻度で変更されていないことを保証します。
- メッセージ発信元の認証：受信データを発信したユーザのアイデンティティが確認されたことを保証します。
- メッセージの機密性：情報が使用不可であること、または不正なユーザ、エンティティ、またはプロセスに開示されないことを保証します。

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

Cisco NX-OSは、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 を選択できます。 **priv** オプションを **aes-128** トークンと併用すると、プライバシー パスワードは 128 ビット AES キーの生成に使用されます。AES のプライバシー パスワードは最小で 8 文字です。 パスフレーズをクリア テキストで指定する場合、最大 64 文字を指定できます。 ローカライズド キーを使用する場合は、最大 130 文字を指定できます。

（注） 外部の Authentication, Authorization, Accounting（AAA; 認証、許可、アカウンティング）サーバを使用して SNMPv3 を使う場合、外部 AAA サーバのユーザ設定でプライバシー プロトコルに AES を指定する必要があります。

コマンドライン インターフェイス（CLI）および SNMP ユーザの同期

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

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

Cisco NX-OSは、次のようにユーザ設定を同期化します。

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

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

グループベースの SNMP アクセス

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

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

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

SNMP のライセンス要件

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

SNMP の注意事項および制約事項

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

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

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

SNMP のデフォルト設定

表 *23*： 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

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

手順の概要

1. **configure terminal**
2. switch(config)# **snmp-server user** *name* [**auth** {**md5** | **sha**} *passphrase* [**auto**] [**priv** [**aes-128**] *passphrase*] [**engineID** *id*] [**localizedkey**]]
3. （任意） switch# **show snmp user**
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	switch(config)# **snmp-server user** *name* [**auth** {**md5** | **sha**} *passphrase* [**auto**] [**priv** [**aes-128**] *passphrase*] [**engineID** *id*] [**localizedkey**]] 例： `switch(config)# snmp-server user Admin auth sha abcd1234 priv abcdefgh`	認証およびプライバシー パラメータのある SNMP ユーザを設定します。 パスフレーズには最大 64 文字の英数字を使用できます。大文字と小文字を区別します。 **localizedkey** キーワードを使用する場合は、パスフレーズに大文字と小文字を区別した英数字を 130 文字まで使用できます。 engineID の形式は、12 桁のコロンで区切った 10 進数字です。
ステップ 3	switch# **show snmp user** 例： `switch(config) # show snmp user`	（任意） 1 人または複数の SNMP ユーザに関する情報を表示します。

	コマンドまたはアクション	目的
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

次の例は、SNMP ユーザを設定します。

```
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、認証と暗号化なしで SNMPv3 メッセージを受け入れます。 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 パラメータを使用しているすべての 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に強制するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

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

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

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

SNMPv3 ユーザに対する複数のロールの割り当て

SNMP ユーザを作成した後で、そのユーザに複数のロールを割り当てることができます。

（注） 他のユーザにロールを割り当てることができるのは、network-admin ロールに属するユーザだけです。

コマンド	目的
switch(config)# **snmp-server user** *name group*	この SNMP ユーザと設定されたユーザ ロールをアソシエートします。

SNMP コミュニティの作成

SNMPv1 または SNMPv2c の SNMP コミュニティを作成できます。

グローバル コンフィギュレーション モードで SNMP コミュニティ ストリングを作成する手順は、次のとおりです。

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 Security Configuration Guide*』を参照してください。 Nexus 5000 用の入手可能なセキュリティ設定ガイドラインは http://www.cisco.com/en/US/products/ps9670/products_installation_and_configuration_guides_list.html にあります。

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

コマンド	目的
switch(config)# **snmp-server community** *community name* **use-acl** *acl-name* **Example:** `switch(config)# snmp-server community public use-acl my_acl_for_public`	ACL を SNMP コミュニティに割り当てて SNMP 要求をフィルタします。

はじめる前に

SNMP コミュニティに割り当てる ACL を作成します。

ACL を SNMP コミュニティに割り当てます。

SNMP 通知レシーバの設定

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

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。 community 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。

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。 community 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。

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。 username 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。

（注） SNMP マネージャは、SNMPv3 メッセージを認証し暗号解除するために、Cisco Nexus 5000 Series スイッチの SNMP engineID に基づくユーザ クレデンシャル（authKey/PrivKey）を認識する必要があります。

次に、SNMPv1 トラップのホスト レシーバを設定する例を示します。

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

次に、SNMPv2 インフォームのホスト レシーバを設定する例を示します。

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

次に、SNMPv3 インフォームのホスト レシーバを設定する例を示します。

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

すべての SNMP 通知を送信するための送信元インターフェイスの設定

通知の送信元 IP アドレスとしてインターフェイスの IP アドレスを使用するよう、SNMP を設定できます。 通知が生成される場合、送信元 IP アドレスは、この設定済みインターフェイスの IP アドレスに基づいています。

（注） 発信トラップパケットの送信元インターフェイス IP アドレスを設定すると、デバイスがトラップの送信に同じインターフェイスを使用することが保証されません。 送信元インターフェイス IP アドレスは、SNMP トラップの内部で送信元アドレスを定義し、出力インターフェイスアドレスを送信元として接続が開きます。

すべての SNMP 通知を送信するよう送信元インターフェイスを設定するには、次の手順を実行します。

手順の概要

1. **configure terminal**
2. switch(config) # **snmp-server source-interface** {**traps** | **informs**} *if-type if-number*

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

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

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

次の作業

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

SNMP 通知のホスト レシーバの設定

（注） このコンフィギュレーションは、グローバル発信元インターフェイスのコンフィギュレーションよりも優先されます。

すべての SNMP 通知を受信する、送信元インターフェイス上のホスト レシーバを設定するには、次の手順を実行します。

手順の概要

1. **configure terminal**
2. switch(config) # **snmp-server host** *ip-address* **source-interface** *if-type if-number* [**udp_port** *number*]

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

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

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

次の作業

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

インバンド アクセスのための SNMP の設定

次のものを使用して、インバンド アクセス用に SNMP を設定できます。

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

手順の概要

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

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

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

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

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

```
switch(config)# snmp-server community comm group network-admin
switch(config)#
```

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

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

SNMP 通知のイネーブル化

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

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

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

表 *24*： ***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**

MIB	関連コマンド
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**
CISCO-ZS-MIB	**snmp-server enable traps zone** **snmp-server enable traps zone default-zone-behavior-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**

（注） ライセンス通知は、デフォルトではイネーブルです。

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

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

コマンド	目的
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。

- Cisco：Cisco NX-OS は、インターフェイスに対して ifLinkUpDownTrapEnable（IF-MIB で定義）がイネーブルの場合は、シスコ定義の通知（CISCO-IF-EXTENSION-MIB.my の cieLinkUp、cieLinkDown）だけを送信します。
- IETF：Cisco NX-OS は、インターフェイスに対して ifLinkUpDownTrapEnable（IF-MIB で定義）がイネーブルの場合は、定義されている変数バインドだけを IETF 定義の通知（IF-MIB の linkUp、linkDown）と一緒に送信します。
- IEFT extended：Cisco NX-OS は、インターフェイスに対して ifLinkUpDownTrapEnable（IF-MIB で定義）がイネーブルの場合は、IETF 定義の通知（IF-MIB の linkUp、linkDown）だけを送信します。 Cisco NX-OS は、IF-MIB に定義されている変数バインドに加え、シスコに固有の変数バインドも送信します。 これがデフォルトの設定です。
- IEFT Cisco：Cisco NX-OS は、インターフェイスに対して ifLinkUpDownTrapEnable（IF-MIB で定義）がイネーブルの場合は、IF-MIB に定義された通知（linkUp、linkDown）および CISCO-IF-EXTENSION-MIB.my に定義された通知（cieLinkUp、cieLinkDown）を送信します。 Cisco NX-OS は、linkUp および linkDown 通知に定義された変数バインドだけを送信します。
- IEFT extended Cisco：Cisco NX-OS は、インターフェイスに対して ifLinkUpDownTrapEnable（IF-MIB で定義）がイネーブルの場合は、IF-MIB に定義された通知（linkUp、linkDown）および CISCO-IF-EXTENSION-MIB.my に定義された通知（cieLinkUp、cieLinkDown）を送信します。 Cisco NX-OS は、linkUp および linkDown 通知の IF-MIB に定義されている変数バインドに加え、シスコ固有の変数バインドも送信します。

手順の概要

1. **configure terminal**
2. **snmp-server enable traps link** [**cisco**] [**ietf** | **ietf-extended**]

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** [**cisco**] [**ietf** | **ietf-extended**] 例： `switch(config)# snmp-server enable traps link cisco`	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。 フラッピング インターフェイス（Up と Down の間を頻繁に切り替わるインターフェイス）で、この制限通知を使用できます。

手順の概要

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**	コン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。 デフォルトでは、イネーブルです。

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。デフォルトはディセーブルです。

SNMP スイッチの連絡先および場所の情報の割り当て

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

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **snmp-server contact** *name*
3. switch(config)# **snmp-server location** *name*
4. （任意） switch# **show snmp**
5. （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**	コン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	switch# **show snmp**	（任意） 1 つまたは複数の宛先プロファイルに関する情報を表示します。
ステップ 5	switch# **copy running-config startup-config**	（任意） この設定変更を保存します。

コンテキストとネットワーク エンティティ間のマッピング設定

プロトコル インスタンス、VRF などの論理ネットワーク エンティティに対する SNMP コンテキストのマッピングを設定できます。

手順の概要

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. （任意） switch(config)# **no snmp-server context** *context-name* [**instance** *instance-name*] [**vrf** *vrf-name*] [**topology** *topology-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**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **snmp-server context** *context-name* [**instance** *instance-name*] [**vrf** *vrf-name*] [**topology** *topology-name*]	SNMP コンテキストをプロトコル インスタンス、VRF、またはトポロジにマッピングします。 名前には最大 32 の英数字を使用できます。
ステップ 3	switch(config)# **snmp-server mib community-map** *community-name* **context** *context-name*	SNMPv2c コミュニティを SNMP コンテキストにマッピングします。 名前には最大 32 の英数字を使用できます。
ステップ 4	switch(config)# **no snmp-server context** *context-name* [**instance** *instance-name*] [**vrf** *vrf-name*] [**topology** *topology-name*]	（任意） SNMP コンテキストとプロトコル インスタンス、VRF、またはトポロジ間のマッピングを削除します。 名前には最大 32 の英数字を使用できます。 （注） コンテキスト マッピングを削除する目的で、インスタンス、VRF、またはトポロジを入力しないでください。 **instance**、**vrf**、または **topology** キーワードを使用すると、コンテキストとゼロ長ストリング間のマッピングが設定されます。

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 の設定の確認

SNMP 設定情報を表示するには、次の作業を行います。

コマンド	目的
switch# **show snmp**	SNMP のステータスを表示します。
switch# **show snmp community**	SNMP コミュニティ ストリングを表示します。
switch# **show snmp engineID**	SNMP engineID を表示します。
switch# **show snmp group**	SNMP ロールを表示します。
switch# **show snmp sessions**	SNMP セッションを表示します。
switch# **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。
switch# **show snmp user**	SNMPv3 ユーザを表示します。

SNMP の機能の履歴

表 *25* : ***SNMP*** の機能の履歴

機能名	リリース	情報
IPv6 のサポート	5.2(1)N1(1)	この機能が導入されました。

第 14 章

RMON の設定

この章の内容は、次のとおりです。

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インターネット技術特別調査委員会（IETF）標準モニタリング仕様です。 Cisco NX-OS は、Cisco Nexus 5000 Series スイッチをモニタするための RMON アラーム、イベント、およびログをサポートします。

RMON アラームは、指定された期間、特定の MIB（Management Information Base; 管理情報ベース）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 Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）通知を生成できます。

Cisco Nexus 5000 Series 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 のアラームおよびイベントを設定するには、CLI または SNMP 準拠の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 5000 Series スイッチが使用する間隔。
- サンプル タイプ：絶対サンプルは 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 5000 Series スイッチ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場合の値。
- 下限しきい値：Cisco Nexus 5000 Series スイッチ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場合の値。
- イベント：アラーム（上限または下限）の発生時に Cisco Nexus 5000 Series スイッチが実行するアクション。

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

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

（注） 下限しきい値には、上限しきい値よりも小さな値を指定してください。

RMON イベント

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

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

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

下限アラームおよび上限アラームに異なるイベントを指定できます。

RMON の設定時の注意事項および制約事項

RMON には、次の注意事項および制限事項があります。

- SNMP 通知イベントタイプを使用するよう、SNMP ユーザを通知レシーバに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。

手順の概要

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. （任意） switch# **show rmon** {**alarms** | **hcalarms**}
5. （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# **configure terminal**	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **rmon alarm** *index mib-object sample-interval* {**absolute** | **delta**} **rising-threshold** *value* [*event-index*] **falling-threshold** *value* [*event-index*] [**owner** *name*]	RMON アラームを作成します。 値の範囲は、–2147483647 ～ 2147483647 です。 オーナー名は任意の英数字ストリングです。
ステップ 3	switch(config)# **rmon hcalarm** *index mib-object sample-interval* {**absolute** | **delta**} **rising-threshold-high** *value* **rising-threshold-low** *value* [*event-index*] **falling-threshold-high** *value* **falling-threshold-low** *value* [*event-index*] [**owner** *name*] [**storagetype** *type*]	RMON 高容量アラームを作成します。 値の範囲は、–2147483647 ～ 2147483647 です。 オーナー名は任意の英数字ストリングです。 ストレージ タイプの範囲は 1 ～ 5 です。
ステップ 4	switch# **show rmon** {**alarms** | **hcalarms**}	（任意） RMONアラームまたは高容量アラームに関する情報を表示します。
ステップ 5	switch# **copy running-config startup-config**	（任意） この設定変更を保存します。

次に、RMON アラームを設定する例を示します。

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

RMON イベントの設定

RMON アラームとアソシエートするよう RMON イベントを設定できます。 複数の RMON アラームで同じイベントを再利用できます。

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

手順の概要

1. switch# **configure terminal**
2. switch(config)# **rmon event** *index* [**description** *string*] [**log**] [**trap**] [**owner** *name*]
3. （任意） switch(config)# **show rmon** {**alarms** | **hcalarms**}
4. （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# **configure terminal**	コン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	switch(config)# **show rmon** {**alarms** | **hcalarms**}	（任意） RMONアラームまたは高容量アラームに関する情報を表示します。
ステップ 4	switch# **copy running-config startup-config**	（任意） この設定変更を保存します。

RMON の設定の確認

RMON 設定情報を表示するには、次のいずれかの作業を行います。

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

デフォルトの RMON 設定

次の表に、RMON パラメータのデフォルト設定を示します。

表 *26*： デフォルトの *RMON* パラメータ

パラメータ	デフォルト
アラーム	未設定。
イベント	未設定。

第 15 章

SPAN の設定

この章の内容は、次のとおりです。

SPAN に関する情報

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のネットワーク 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。

SPAN 送信元

SPAN 送信元とは、トラフィックをモニタリングできるインターフェイスを表します。 Cisco Nexus シリーズ デバイスは、SPAN 送信元として、イーサネット、ファイバ チャネル、仮想ファイバ チャネル、ポート チャネル、SAN ポート チャネル、VSAN、および VLAN をサポートします。 VLAN または VSAN では、指定された VLAN または VSAN でサポートされているすべてのインターフェイスが SPAN 送信元として含まれます。 イーサネット、ファイバ チャネル、および仮想ファイバ チャネルの送信元インターフェイスで、入力方向、出力方向、または両方向の SPAN トラフィックを選択できます。

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

SPAN 送信元インターフェイスが 6 Gbps よりも大きいトラフィックを送信した場合、またはトラフィックがあまりにも急増した場合、デバイスは送信元インターフェイスでトラフィックをドロップします。 送信元インターフェイスの実際のトラフィックのドロップを減らすために、SPAN 宛先に対して **switchport monitor rate-limit 1G** コマンドを使用できます。ただし、SPAN トラフィックは 1 Gbps に制限されます。 詳細は、SPAN トラフィックのレート制限の設定, （197 ページ）を参照してください。

（注） トラフィックはデフォルトで 1 Gbps にレート制限されているため、**switchport monitor rate-limit 1G** コマンドは、Nexus 5500 プラットフォームではサポートされません。

（注） Cisco Nexus 5548 デバイスでは、ファイバ チャネル ポートと VSAN のポートを、SPAN セッションの入力送信元ポートとして設定できません。

送信元ポートの特性

送信元ポート（モニタリング対象ポートとも呼ばれる）は、ネットワーク トラフィック分析のためにモニタリングするスイッチド インターフェイスです。 スイッチは、任意の数の入力送信元ポート（スイッチで使用できる最大数のポート）と任意の数の送信元 VLAN または VSAN をサポートします。

送信元ポートの特性は、次のとおりです。

- イーサネット、ファイバ チャネル、仮想ファイバ チャネル、ポート チャネル、SAN ポート チャネル、VSAN または VLAN ポート タイプにできます。
- 複数の SPAN セッションではモニタリングできません。
- 宛先ポートには設定できません。
- モニタする方向（入力、出力、または両方）を指定して、各送信元ポートを設定できます。 VLAN および VSAN 送信元の場合、モニタリング方向は入力のみであり、グループ内のすべての物理ポートに適用されます。 RX と TX のオプションは、VLAN または VSAN の SPAN セッションでは使用できません。
- 出力 SPAN ポート数の制限はありませんが、モニタ セッションの送信元ポートには 128 の上限があります。
- ポート チャネルおよび SAN ポート チャネル インターフェイスは入力または出力送信元ポートとして設定できます。
- 送信元ポートは、同じ VLAN または VSAN か、別の VLAN または VSAN に設定できます。
- VLAN または VSAN の SPAN 送信元では、ソース VLAN または VSAN のすべてのアクティブ ポートが送信元ポートとして含まれます。

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 インターフェイスとファイバ チャネル インターフェイスをサポートします。

送信元 SPAN	宛先 SPAN
イーサネット	イーサネット
ファイバ チャネル	ファイバ チャネル
ファイバ チャネル	イーサネット（FCoE）
仮想ファイバ チャネル	ファイバ チャネル

送信元 SPAN	宛先 SPAN
仮想ファイバ チャネル	イーサネット（FCoE）

宛先ポートの特性

各ローカル SPAN セッションには、送信元ポート、VSAN、または VLAN からトラフィックのコピーを受信する宛先ポート（モニタリング ポートとも呼ばれる）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。 イーサネット、イーサネット（FCoE）、またはファイバ チャネル、および仮想ファイバ チャネル 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 チャネルまたは SAN ポート チャネル グループにはできません。
- SPAN セッションがアクティブなときは、スパニングツリーに参加しません。
- 任意の SPAN セッションのソース VLAN に属する場合、送信元リストから除外され、モニタリングされません。
- すべてのモニタリング対象送信元ポートの送受信トラフィックのコピーを受信します。 宛先ポートがオーバーサブスクライブ型の場合、輻輳が発生する可能性があります。 輻輳が発生すると、1 つまたは複数の送信元ポートでのトラフィック転送に影響を及ぼす可能性があります。

SPAN の注意事項および制約事項

SPAN トラフィックは、実稼働トラフィックに悪影響を及ぼさないように、次のように Nexus 5500 シリーズのスイッチでレート制限されます。

- SPAN は 8 ポート（1 ASIC）ごとに 5 Gbps にレート制限されます。
- RX-SPAN は、ポートの RX トラフィックが 5 Gbps を超える場合は、ポートごとに 0.71 Gbps にレート制限されます。

SPAN セッションの作成または削除

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

手順の概要

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

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*	モニタ コンフィギュレーション モードを開始します。既存のセッション設定に新しいセッション設定が追加されます。

次に、SPAN モニタ セッションを設定する例を示します。

```
switch# configure terminal
switch(config) # monitor session 2
switch(config) #
```

イーサネット宛先ポートの設定

SPAN 宛先ポートとしてイーサネット インターフェイスを設定できます。

（注） SPAN 宛先ポートは、スイッチ上の物理ポートにのみ設定できます。

手順の概要

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*

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*	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。
ステップ 3	switch(config-if)# **switchport monitor**	指定されたイーサネット インターフェイスのモニタ モードを開始します。 ポートがSPAN宛先として設定されている場合、プライオリティ フロー制御はディセーブルです。
ステップ 4	switch(config-if)# **exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	switch(config)# **monitor session** *session-number*	指定したSPANセッションのモニタ コンフィギュレーション モードを開始します。
ステップ 6	switch(config-monitor)# **destination interface ethernet** *slot/port*	イーサネット SPAN 宛先ポートを設定します。

次に、イーサネット SPAN 宛先ポートを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/3
switch(config-if)# switchport monitor
switch(config-if)# exit
switch(config)# monitor session 2
switch(config-monitor)# destination interface ethernet 1/3
switch(config-monitor)#
```

SPAN セッションごとの MTU の切り捨ての設定

SPAN トラフィック帯域幅を減らすには、SPANセッションの各複製パケットで許可される最大バイト数を設定できます。 この値は、最大伝送単位（MTU）の切り捨てサイズと呼ばれます。 設定されたサイズよりも大きい SPAN パケットはすべて、設定されたサイズに切り捨てられます。

手順の概要

1. switch# **configure terminal**
2. switch(config) # **monitor session** *session-number*
3. switch(config-monitor) # [**no**] **mtu**
4. （任意） switch(config-monitor) # **show monitor session** *session-number*
5. （任意） switch(config-monitor) # **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 session** *session-number*	モニタ コンフィギュレーション モードを開始し、MTU 切り捨てサイズが設定された SPAN セッションを指定します。
ステップ 3	switch(config-monitor) # [**no**] **mtu**	指定した SPAN セッションのパケットの MTU 切り捨てサイズを設定します。 指定できる範囲は 64 ～ 1518 バイトです。
ステップ 4	switch(config-monitor) # **show monitor session** *session-number*	（任意） MTU切り捨ての設定ステータス、セッションごとに各パケットで許可される最大バイト数、MTU切り捨てがサポートされるモジュールとサポートされないモジュールを含む、SPAN セッションのステータスを表示します。
ステップ 5	switch(config-monitor) # **copy running-config** startup-config	（任意） 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

次に、SPAN セッションの MTU 切り捨てを設定する例を示します。

```
switch# configure terminal
switch(config) # monitor session 3
switch(config-monitor) # mtu
switch(config-monitor) # copy running-config startup-config
switch(config-monitor) #
```

SPAN トラフィックのレート制限の設定

モニタ セッション全体で SPAN トラフィックのレート制限を 1Gbps に設定することで、モニタされた実稼働トラフィックへの影響を回避できます。 Nexus 5000 シリーズ スイッチの場合：

- 1 Gbps を超えるトラフィックを 1 Gb の SPAN 宛先インターフェイスに分散させる場合、SPAN 送信元トラフィックはドロップされません。
- 6 Gbps を超える（ただし 10 Gbps 未満）のトラフィックを 10 Gb の SPAN 宛先インターフェイスに分散させる場合、SPAN トラフィックは、宛先またはスニファで 10 Gbps が可能な場合でも、1 Gbps に制限されます。

Nexus 5500 シリーズで、SPAN トラフィックはデフォルトで 1Gbps にレート制限されるため、**switchport monitor rate-limit 1G** インターフェイス コマンドはサポートされません。 また、モニタ対象実稼働トラフィックへの影響を回避するには、次のようにします。

- SPAN は 8 ポート（1 ASIC）ごとに 5 Gbps にレート制限されます。

- RX-SPAN は、ポートの RX トラフィックが 5 Gbps を超える場合は、ポートごとに 0.71 Gbps にレート制限されます。

手順の概要

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

手順の詳細

	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*	スロット値およびポート値による選択で指定されたイーサネット インターフェイスで、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# **switchport monitor rate-limit 1G**	レート制限が 1 Gbps であることを指定します。 （注） トラフィックはデフォルトで 1 Gbps にレート制限されているため、このコマンドは Nexus 5500 プラットフォームではサポートされません。
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。

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

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

ファイバ チャネル宛先ポートの設定

（注） SPAN 宛先ポートは、スイッチ上の物理ポートにのみ設定できます。

ファイバ チャネル ポートを SPAN 宛先ポートとして設定できます。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface fc** *slot*/*port*
3. switch(config-if)# **switchport mode SD**
4. switch(config-if)# **switchport speed 1000**
5. switch(config-if)# **exit**
6. switch(config)# **monitor session** *session-number*
7. switch(config-monitor)# **destination interface fc** *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)# **interface fc** *slot*/*port*	スロット値およびポート値による選択で指定されたファイバ チャネル インターフェイスで、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# **switchport mode SD**	インターフェイスを SPAN 宛先（SD）モードに設定します。
ステップ 4	switch(config-if)# **switchport speed 1000**	インターフェイス速度を 1000 に設定します。 自動速度オプションは使用できません。
ステップ 5	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 6	switch(config)# **monitor session** *session-number*	モニタ コンフィギュレーション モードを開始します。
ステップ 7	switch(config-monitor)# **destination interface fc** *slot*/*port*	ファイバ チャネル宛先ポートを設定します。

次に、イーサネット SPAN 宛先ポートを設定する例を示します。

```
switch# configure terminal
switch(config)# interface fc 2/4
switch(config-if)# switchport mode SD
switch(config-if)# switchport speed 1000
switch(config-if)# exit
switch(config)# monitor session 2
switch(config-monitor)# destination interface fc 2/4
```

送信元ポートの設定

送信元ポートは、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に設定できます。

手順の概要

1. switch# **configure terminal**
2. switch(config) # **monitor session** *session-number*
3. switch(config-monitor) # **source interface** *type slot/port* [**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*	指定したモニタリング セッションのモニタ コンフィギュレーション モードを開始します。
ステップ 3	switch(config-monitor) # **source interface** *type slot/port* [**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方向を設定します。 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。 コピー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。

次に、イーサネット SPAN 送信元ポートを設定する例を示します。

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

次に、ファイバ チャネル SPAN 送信元ポートを設定する例を示します。

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

次に、仮想ファイバ チャネル SPAN 送信元ポートを設定する例を示します。

```
switch# configure terminal
switch(config)# monitor session 2
switch(config-monitor)# source interface vfc 129
switch(config-monitor)#
```

送信元ポート チャネル、VSAN、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、SAN ポート チャネル、VSAN、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。

（注） Cisco Nexus 5000 シリーズ スイッチは、2 つのアクティブな SPAN セッションをサポートします。 Cisco Nexus 5548 スイッチは、4 つのアクティブな SPAN セッションをサポートします。 2 つを超える SPAN セッションを設定すると、最初の 2 つのセッションがアクティブになります。 起動中にアクティブなセッションの順序が逆になり、最後の 2 つのセッションがアクティブになります。 たとえば、セッション 1 ～ 10 を設定して、1 と 2 がアクティブな場合、リブート後はセッション 9 と 10 がアクティブになります。 確定した動作を可能にするには、**monitor session** *session-number* **shut** コマンドを使用して、セッション 3 ～ 10 を明示的に一時停止します。

手順の概要

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

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 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、モニタ方向は暗黙的です。

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、SAN ポート チャネル SPAN 送信元を設定する例を示します。

```
switch(config-monitor)#switch# configure terminal
switch(config)# monitor session 2
switch(config-monitor)# source interface san-port-channel 3 rx
switch(config-monitor)#
```

次に、VLAN の 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)#
```

switch(config-monitor)# 次に、VSAN SPAN 送信元を設定する例を示します。

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

手順の概要

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

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 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) # **description** *description*	SPANセッションのわかりやすい名前を作成します。

次に、SPAN セッションの説明を設定する例を示します。

```
switch# configure terminal
switch(config) # monitor session 2
switch(config-monitor) # description monitoring ports eth2/2-eth2/4
switch(config-monitor) #
```

SPAN セッションのアクティブ化

デフォルトでは、セッション ステートは shut に保持されます。 送信元から宛先へパケットをコピーするセッションを開くことができます。

手順の概要

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

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 monitor session** {**all** | *session-number*} **shut**	指定された SPAN セッションまたはすべてのセッションを開始します。

次に、SPAN セッションをアクティブにする例を示します。

```
switch# configure terminal
switch(config) # no monitor session 3 shut
```

SPAN セッションの一時停止

デフォルトでは、セッション ステートは **shut** です。

（注） Cisco Nexus スイッチは、2 つのアクティブな SPAN セッションをサポートします。 Cisco Nexus 5548 スイッチは、4 つのアクティブな SPAN セッションをサポートします。 2 つを超える SPAN セッションを設定すると、最初の 2 つのセッションがアクティブになります。 起動中にアクティブなセッションの順序が逆になり、最後の 2 つのセッションがアクティブになります。 たとえば、セッション 1 ～ 10 を設定して、1 と 2 がアクティブな場合、リブート後はセッション 9 と 10 がアクティブになります。 確定した動作を可能にするには、**monitor session** *session-number* **shut** コマンドを使用して、セッション 3 ～ 10 を明示的に一時停止します。

手順の概要

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

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** {**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。

次に、SPAN セッションを一時停止する例を示します。

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

SPAN 情報の表示

手順の概要

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

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 monitor** [**session** {**all** | *session-number* | **range** *session-range*} [**brief**]]	SPAN 設定を表示します。

次に、SPAN セッションの情報を表示する例を示します。

```
switch# show monitor
SESSION  STATE        REASON                   DESCRIPTION
-------  -----------  ----------------------   --------------------------------
2        up           The session is up
3        down         Session suspended
4        down         No hardware resource
```

次に、SPAN セッションの詳細を表示する例を示します。

```
switch# show monitor session 2
   session 2
---------------
type              : local
state             : up
source intf       :
    rx            : fc3/1
    tx            : fc3/1
    both          : fc3/1
source VLANs      :
    rx            :
```

```
source VSANs      :
    rx            : 1
destination ports : Eth3/1
```

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

ERSPAN は、IP ネットワークでミラーリングされたトラフィックを転送して、ネットワーク内で複数のスイッチのリモートモニタリングを提供します。 トラフィックは、送信元ルータでカプセル化され、ネットワーク間を転送されます。 パケットは宛先ルータでカプセル化解除され、宛先インターフェイスに送信されます。

ERSPAN は、ERSPAN 送信元セッション、ルーティング可能な ERSPAN 総称ルーティング カプセル化（GRE）カプセル化トラフィック、および ERSPAN 宛先セッションで構成されています。 異なるスイッチで ERSPAN 送信元セッションおよび宛先セッションを個別に設定します。

Cisco Nexus 5000 シリーズ スイッチでの ERSPAN の実装は、送信元セッションではなく、宛先セッションのみをサポートします。 1 つ以上の送信元ポートでトラフィックをモニタできます。

ERSPAN 送信元セッション

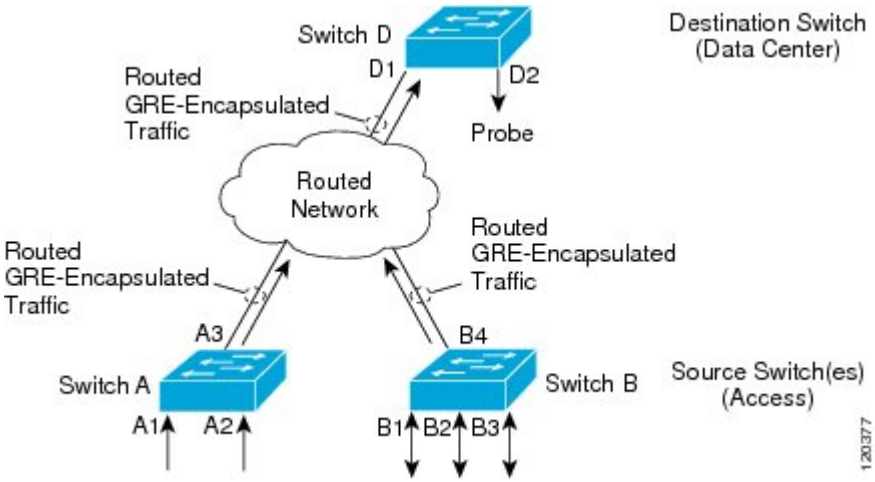
ERSPAN 送信元セッションは、次によって定義されます。

- セッション ID。
- セッションでモニタされる送信元ポート、送信元 VLAN、または送信元 VSAN のリスト。
- ERSPAN フロー ID。
- IP TOS や TTL など、GRE エンベロープに関連するオプション属性
- 宛先 IP アドレス。
- 仮想ルーティングおよび転送テーブル。

ERSPAN 送信元セッションは、ERSPAN GRE カプセル化されたトラフィックを送信元ポートからコピーしません。 ERSPAN送信元セッションごとに、送信元としてポート、VLAN、またはVSANを設定できます。 ただし、次のようないくつかの制限があります。 詳細については、ERSPAN の注意事項および制約事項, （210 ページ）を参照してください。

次の図は、ERSPAN 設定の例を示します。

図 4 : *ERSPAN* の設定



モニタ対象トラフィック

デフォルトでは、ERSPAN は、マルチキャストおよびブリッジ プロトコル データ ユニット（BPDU）フレームを含む、すべてのトラフィックをモニタします。

ERSPAN がモニタするトラフィックの方向は、次のように送信元によって決まります。

- 送信元ポートについては、ERSPAN は、入力トラフィック、出力トラフィック、または入出力トラフィックをモニタできます。
- 送信元 VLAN または送信元 VSAN については、ERSPAN は入力トラフィックのみをモニタできます。

ERSPAN 送信元

トラフィックをモニタできるモニタ元インターフェイスのことをERSPANソースと呼びます。 送信元では、モニタするトラフィックを指定し、さらに入力、出力、または両方向のトラフィックをコピーするかどうかを指定します。 ERSPAN 送信元には次のものが含まれます。

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

切り捨てられた ERSPAN

切り捨てられた ERSPAN を使用して、ERSPAN パケットの送信で使用されるファブリックまたはネットワーク帯域幅の量を減らすことができます。

デフォルトでは切り捨ては行われないため、大規模な ERSPAN パケットを受信するスイッチまたはルータは、これらの大きすぎるパケットをドロップする可能性があります。

（注） Cisco Catalyst 6000 シリーズ スイッチは、これらの切り捨てられたパケットをドロップするため、宛先 ERSPAN 宛先ルータが Cisco Catalyst 6000 シリーズ スイッチの場合、切り捨てられた ERSPAN 機能をイネーブルにしないでください。

マルチ ERSPAN セッション

最大 18 の ERSPAN セッションを作成できますが、Cisco Nexus 5000 シリーズ スイッチで同時に実行できるのは 2 つの ERSPAN または SPAN セッションのみで、Cisco Nexus 5500 シリーズ スイッチで同時に実行できるのは 4 つの ERSPAN または SPAN セッションのみです。 未使用の ERSPAN セッションはシャットダウンもできます。

ERSPAN セッションのシャットダウンについては、ERSPAN セッションのシャットダウンまたはアクティブ化, （217 ページ）を参照してください。

ハイ アベイラビリティ

ERSPAN 機能はステートレス リスタートリスタートをサポートします。 リブート後に、実行コンフィギュレーションが適用されます。

ERSPAN のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	ERSPAN にはライセンスは不要です。 ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。 Cisco NX-OS のライセンス スキームの詳細は、『*License and Copyright Information for Cisco NX-OS Software*』 を参照してください。次の URL で入手できます。http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_0/nx-os/license_agreement/nx-ossw_lisns.htmlを参照してください。

ERSPAN の前提条件

ERSPAN の前提条件は、次のとおりです。

•所定の ERSPAN 設定をサポートするには、まず各デバイス上でポートのイーサネット インターフェイスを設定する必要があります。 詳細については、『*Cisco Nexus 5000 Series NX-OS Layer 2 Switching Configuration Guide*』を参照してください。

ERSPAN の注意事項および制約事項

ERSPAN には、次の注意事項および制約事項があります。

- Cisco Nexus 5000 シリーズ スイッチは、ERSPAN 送信元セッションのみをサポートします。宛先セッションはサポートされません。
- Cisco Nexus 5000 シリーズ スイッチは、最大 2 個のセッションをサポートします。
- Cisco Nexus 5500 シリーズ スイッチは、最大 4 個のセッションをサポートします。
- 各 ERSPAN セッションの最大ポート数は 32 です。
- 1 つの ERSPAN セッションに送信元ポート、送信元 VLAN、および送信元 VSAN を設定できます。
- Cisco Nexus 5000 シリーズ スイッチでは、VLAN が VSAN にマップされていない限り、ERSPAN は、送信元ポートでは入力、出力、または入出力トラフィックをモニタでき、送信元 VLAN または送信元 VSAN では入力トラフィックのみをモニタできます。

- Cisco 5500 シリーズ スイッチでは、送信元ポートおよび送信元 VLAN は同じ ERSPAN セッション内に設定できます。
- ERSPAN トラフィックは、レイヤ 2 インターフェイス、レイヤ 3 インターフェイス、ポートチャネル、または FabricPath コア ポートからスイッチを終了できます。
- Cisco Nexus 5000 シリーズ スイッチは、仮想イーサネット ポートまたは FEX ポートを介してリモート スイッチの宛先 IP アドレスに到達できません。 この機能はサポートされません。
- ERSPAN トラフィックは、宛先 IP アドレスへの到達可能性がレイヤ 3 ECMP またはポートチャネルである場合、ロードバランシングされません。 ECMP の場合、ERSPAN トラフィックは、ポート チャネルの 1 つのネクスト ホップ ルータまたは 1 つのメンバーのみに送信されます。
- Cisco Nexus 5000 シリーズ スイッチの ERSPAN は、送信元セッションの送信元ポートとしてファストイーサネット、ギガビットイーサネット、TenGigabit イーサネット、およびポートチャネル インターフェイスをサポートします。
- ERSPAN コンフィギュレーション コマンドを使用してセッションを設定する場合、セッション ID とセッション タイプは変更できません。 これらを変更するには、まずコンフィギュレーション コマンドの no バージョンを使用してセッションを削除してから、セッションを再設定する必要があります。
- ERSPAN トラフィックは通常のデータ トラフィックと競合する場合があります。
- ERSPAN トラフィックは QoS class-default システム クラス（qos-group 0）に割り当てられます。
- データ トラフィックを ERSPAN トラフィックに優先させるには、ERSPAN 宛先ポートの class-default システム クラスよりも大きいプライオリティを設定して QoS システム クラスを作成できます。

  レイヤ 3 ネットワークでは、ERSPAN トラフィックは、ip dscp コマンドを使用して目的の DiffServ コード ポイント（DSCP）値でマークできます。 デフォルトでは、ERSPAN トラフィックは、DSCP 値 0 でマークされます。
- ERSPAN は、Cisco Nexus 5010 および 5020 スイッチの送信元 VSAN の入力トラフィックのみをモニタできます。
- ERSPAN は、Cisco Nexus 5000 シリーズ スイッチ上の送信元 VLAN と VSAN の出力トラフィックをモニタできません。
- ERSPAN は、送信元ポートの入力、出力、または入出力トラフィックをモニタできます。
- ERSPAN 送信元としての VSAN は、Cisco Nexus 5548 および 5596 スイッチでは許可されません。

デフォルト設定値

次の表に、ERSPAN パラメータのデフォルト設定を示します。

表 *27*：デフォルトの *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。
切り捨てられた ERSPAN	ディセーブル

ERSPAN の設定

ERSPAN 送信元セッションの設定

ERSPAN 送信元セッションは、モニタするセッション設定パラメータおよびポートまたは VLAN を定義します。 ここでは、ERSPAN 送信元セッションを設定する方法について説明します。

手順の概要

1. **configuration terminal**
2. **monitor session** *span-session-number* **type** {**erspan-source | local**}
3. （任意） **description** *erspan_session_description*
4. **source interface** { **ethernet** *slot/chassis number* | **portchannel** *number* }
5. **source vlan** *number*
6. **source vsan** *number*
7. **destination ip** *ip-address*
8. **erspan-id** *flow-id*
9. **vrf** {*vrf-name* | **default** }
10. （任意） **ip ttl** *ttl-number*
11. （任意） **ip dscp** *dscp_value*
12. **no shut**
13. **exit**
14. （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# 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	**monitor session** *span-session-number* **type** {**erspan-source** | **local**}
	
	例：
	`switch(config)# monitor session 1 type erspan-source`
	`switch(config-erspan-src)#`
		セッション ID とセッション タイプを使用して ERSPAN 送信元セッションを定義し、ERSPAN のモニタ送信元セッション コンフィギュレーション モードでコマンドを開始します。
		
		span-session-number 引数の範囲は 1 ～ 1024 です。 同じセッション番号は複数回使用できません。
		
		送信元セッションのセッション ID は同じグローバルな ID スペース内にあるため、各セッション ID は両方のセッション タイプに対してグローバルに一意です。
		
		セッション ID（*span-session-number* 引数によって設定）およびセッション タイプ（**erspan-source** キーワードによって設定）は、入力後は変更できません。 セッション ID またはセッション タイプを変更するには、コマンドの **no** バージョンを使用してセッションを削除してから、新しいセッション ID または新しいセッション タイプでコマンドを使用してセッションを再作成します。

ステップ 3	**description** *erspan_session_description* 例： `switch(config-erspan-src)# description source1`	（任意） ERSPAN 送信元セッションの説明を入力します。 *erspan_session_description* 引数には最大 240 文字を使用できます。ただし、特殊文字またはスペースは使用できません。
ステップ 4	**source interface** { **ethernet** *slot/chassis number* | **portchannel** *number* } 例： `switch(config-erspan-src)# source interface eth 1/1`	ERSPAN 送信元セッション番号を送信元ポート（1 ～ 255）にアソシエートします。
ステップ 5	**source vlan** *number* 例： `switch(config-erspan-src)# source vlan 1`	ERSPAN 送信元セッション番号を VLAN（1 ～ 4096）にアソシエートします。
ステップ 6	**source vsan** *number* 例： `switch(config-erspan-src)# source vsan 1`	Cisco Nexus 5000 シリーズ スイッチでは、VSAN ID 番号を指定します。 有効範囲は 1 ～ 4093 です。 Cisco Nexus 5500 シリーズ スイッチでは、送信元 VSAN を設定できません。
ステップ 7	**destination ip** *ip-address* 例： `switch(config-erspan-src)# destination ip 192.0.2.2`	ERSPAN セッションの宛先 IP アドレスを設定します。 ERSPAN 送信元セッションごとに 1 つの宛先 IP アドレスのみがサポートされます。

	コマンドまたはアクション	目的
ステップ 8	**erspan-id** *flow-id* 例： `switch(config-erspan-src)# erspan-id 5`	ERSPAN フローを識別するフロー ID を設定します。 指定できる範囲は 1 ～ 1023 です。
ステップ 9	**vrf** {*vrf-name* | **default** } 例： `switch(config-erspan-src)# vrf default`	グローバル ルーティング テーブルの代わりに使用する VRF を設定します。 特に設定した VRF、またはデフォルト VRF を使用できます。
ステップ 10	**ip ttl** *ttl-number* 例： `switch(config-erspan-src)# ip ttl 5`	（任意） ERSPAN トラフィック内のパケットの IP 存続可能時間（TTL）値を設定します。 有効な値は 1 ～ 255 です。 デフォルト値は 255 です。
ステップ 11	**ip dscp** *dscp_value* 例： `switch(config-erspan-src)# ip dscp 42`	（任意） ERSPAN トラフィックのパケットの IP DiffServ コード ポイント（DSCP）値を設定します。 有効値は、0 ～ 63 です。 デフォルト値は 0 です。
ステップ 12	**no shut** 例： `switch(config-erspan-src)# no shut`	ERSPAN 送信元セッションをイネーブルにします。 デフォルトでは、セッションはシャット ステートで作成されます。 （注） Cisco Nexus 5000 シリーズ スイッチでは、2 つの ERSPAN 送信元セッションのみを同時に実行できます。 Cisco Nexus 5500 シリーズ スイッチでは、最大 4 つの送信元セッションを同時に実行できます。

ステップ 13	**exit**
	
	例：
	`switch(config-erspan-src)# exit`
	`switch(config)# exit`
		設定を更新し、ERSPAN 送信元セッション コンフィギュレーション モードを終了します。

ステップ 14	**copy running-config startup-config** 例： `switch(config-erspan-src)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ERSPAN パケットの発信元の IP アドレスの設定

IP アドレスを ERSPAN トラフィックの送信元として使用するように設定する必要があります。

手順の概要

1. **configure terminal**
2. **monitor erspan origin ip-address** *ip_address*
3. **exit**
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	**monitor erspan origin ip-address** *ip_address* 例： `switch(config)# monitor erspan origin ip-address 192.0.2.1`	IP アドレスを ERSPAN トラフィックの送信元として使用するように設定します。
ステップ 3	**exit** 例： `switch(config-erspan-src)# exit`	設定を更新し、ERSPAN 送信元セッション コンフィギュレーション モードを終了します。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

切り捨てられた ERSPAN の設定

ERSPAN パケットの送信で使用されるファブリックのまたはネットワーク帯域幅の量を減らすには、ERSPAN トラフィックの MTU サイズを設定できます。

手順の概要

1. enable
2. **configure terminal**
3. **monitor session** *erspan_session_number* **type** {**erspan-source** | **local**}
4. **mtu** *mtu-value*
5. **exit**
6. （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	enable 例： `switch> enable`	特権EXECモードをイネーブルにします。 プロンプトが表示されたら、パスワードを入力します。

ステップ 2	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 3	**monitor session** *erspan_session_number* **type** {**erspan-source** | **local**}
	
	例：
	`switch(config)# monitor session 1 type erspan-source`
	`switch(config-erspan-src)#`
		セッション ID とセッション タイプを使用して ERSPAN 送信元セッションを定義し、ERSPAN のモニタ送信元セッション コンフィギュレーション モードでコマンドを開始します。
		
		span-session-number 引数の範囲は 1 ～ 1024 です。 同じセッション番号は複数回使用できません。
		
		送信元セッションのセッション ID は同じグローバルな ID スペース内にあるため、各セッション ID は両方のセッション タイプに対してグローバルに一意です。
		
		セッション ID（span-session number 引数によって設定）およびセッション タイプ（erspan-source キーワードによって設定）は、入力後は変更できません。 セッション ID またはセッション タイプを変更するには、コマンドの no バージョンを使用してセッションを削除してから、新しいセッション ID または新しいセッション タイプでコマンドを使用してセッションを再作成します。

ステップ 4	**mtu** *mtu-value* 例： `switch(config-erspan-src)# mtu 64`	ERSPAN パケットの最大伝送単位（MTU）の切り捨てサイズを定義します。 有効値は、64 ～ 1518 です。 デフォルトでは、切り捨てはイネーブルではありません。

	コマンドまたはアクション	目的
ステップ 5	**exit** 例： `switch(config-mon-erspan-src)# exit`	設定を更新し、ERSPAN送信元セッション コンフィギュレーション モードを終了します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

ERSPAN セッションのシャットダウンまたはアクティブ化

ERSPAN セッションをシャットダウンすると、送信元から宛先へのパケットのコピーを切断できます。 Cisco Nexus 5000 シリーズ スイッチの 2 つの ERSPAN セッション、および Cisco Nexus 5500 シリーズ スイッチの 4 つの ERSPAN セッションのみを同時に実行できるため、ハードウェア リソースを解放して、他のセッションをイネーブルにするために、1 つのセッションをシャット ダウンできます。 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。 同時に実行できるセッションは 2 つだけです。
ステップ 3	**no monitor session** {*session-range* | **all**} **shut** 例： `switch(config)# no monitor session 3 shut`	指定の ERSPAN セッションを再開（イネーブルに）します。 セッションの範囲は 1 ～ 48 です。 デフォルトでは、セッションはシャット ステートで作成されます。 同時に実行できるセッションは 2 つだけです。 （注） モニタ セッションがイネーブルで動作状況がダウンの場合、セッションをイネーブルにするには、最初に **monitor session shut** コマンドを指定してから、**no monitor session shut** コマンドを続ける必要があります。

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

ステップ 5	**monitor session** *session-number* **type erspan-destination** 例： `switch(config-erspan-src)# monitor session 3 type erspan-destination`	ERSPAN 宛先タイプのモニタ コンフィギュレーションモードを開始します。
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。

	コマンドまたはアクション	目的
ステップ 8	**show monitor session all** 例： `switch(config-erspan-src)# show monitor session all`	（任意） ERSPAN セッションのステータスを表示します。
ステップ 9	**show running-config monitor** 例： `switch(config-erspan-src)# show running-config monitor`	（任意） ERSPAN の実行コンフィギュレーションを表示します。
ステップ 10	**show startup-config monitor** 例： `switch(config-erspan-src)# show startup-config monitor`	（任意） ERSPAN のスタートアップ コンフィギュレーションを表示します。
ステップ 11	**copy running-config startup-config** 例： `switch(config-erspan-src)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

ERSPAN 設定の確認

ERSPAN の設定を表示するには、次のいずれかの作業を行います。

コマンド	目的
show monitor session {**all** | *session-number* | **range** *session-range*}	ERSPAN セッション設定を表示します。
show running-config monitor	ERSPAN の実行コンフィギュレーションを表示します。
show startup-config monitor	ERSPAN のスタートアップ コンフィギュレーションを表示します。

ERSPAN の設定例

ERSPAN 送信元セッションの設定例

次に、ERSPAN 送信元セッションを設定する例を示します。

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# monitor session 1 type erspan-source
switch(config-erspan-src)# description source1
switch(config-erspan-src)# source interface ethernet 1/1
switch(config-erspan-src)# source vlan 1
switch(config-erspan-src)# source vsan 1
switch(config-erspan-src)# destination ip 192.0.2.2
switch(config-erspan-src)# erspan-id 1
switch(config-erspan-src)# vrf default
switch(config-erspan-src)# ip ttl 5
switch(config-erspan-src)# ip dscp 5
switch(config-erspan-src)# no shut
switch(config-erspan-src)# exit
switch(config)# copy running-config startup config
```

ERSPAN セッションの送信元としての IP アドレスの設定例

次に、ERSPAN セッションの送信元として IP アドレスを設定する例を示します。

```
switch# configure terminal
switch(config)# monitor erspan origin ip-address 192.0.2.1
switch(config)#  exit
switch(config)# copy running-config startup config
```

切り捨てられた ERSPAN の設定例

次に、切り捨てられた ERSPAN を設定する例を示します。

```
switch# configure terminal
switch(config)# monitor session 1 type erspan-source
switch(config-erspan-src)# mtu 64
switch(config-mon-erspan-src)# exit
switch(config)# copy running-config startup config
```

その他の関連資料

関連資料

関連項目	参照先
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	

関連資料

索 引

R

S

あ

い

か

き

さ

し

す

せ

そ

た

ち

つ

て

と

は

ふ

へ

め

も

ゆ

よ

ら

り

る

れ

ろ