Cisco Nexus 3000 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 5.0(3)U4(1)

初版：2012 年 08 月 26 日

最終更新：2012 年 08 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-26558-02-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、次の項目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。

Nexus 3000 シリーズ NX-OS ソフトウェアの関連資料

完全な Cisco NX-OS 3000 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/ps11541/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/ps11541/prod_release_notes_list.html

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

インストールおよびアップグレード ガイドは次の URL で入手できます。

http://www.cisco.com/en/US/products/ps11541/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。

- *Cisco Nexus 5000* シリーズ、*Cisco Nexus 3000* シリーズ、および *Cisco Nexus 2000* シリーズの安全に関する情報およびドキュメント
- 『*Regulatory, Compliance, and Safety Information for the Cisco Nexus 5000 Series, Cisco Nexus 3000 Series, and Cisco Nexus 2000 Series*』
- 『*Cisco Nexus 3000 Series Hardware Installation Guide*』

License Information

NX-OS の機能のライセンスに関する詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。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/nx-os/licensing/guide/b_Cisco_NX-OS_Licensing_Guide.html

NX-OS のエンド ユーザ契約書および著作権情報については、『*License and Copyright Information for Cisco NX-OS Software*』を参照してください。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

コンフィギュレーション ガイド

コンフィギュレーション ガイドは次の URL で入手できます。

http://www.cisco.com/en/US/products/ps11541/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。

- 『*Fundamentals Configuration Guide*』

- 『*Interfaces Configuration Guide*』
- 『*Layer 2 Switching Configuration Guide*』
- 『*Multicast Configuration Guide*』
- 『*Quality of Service Configuration Guide*』
- 『*Security Configuration Guide*』
- 『*System Management Configuration Guide*』
- 『*Unicast Routing Configuration Guide*』
- 『*Verified Scalability Guide for Cisco NX-OS*』

テクニカル リファレンス

テクニカル リファレンスは、次の URL で入手できます。

http://www.cisco.com/en/US/products/ps11541/prod_technical_reference_list.html

エラー メッセージおよびシステム メッセージ

エラー メッセージとシステム メッセージのリファレンス ガイドは次の URL で入手できます。

http://www.cisco.com/en/US/products/ps11541/products_system_message_guides_list.html

マニュアルに関するフィードバック

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

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

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。

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
sFLOW	データ ネットワークのリアルタイム トラフィックのモニタリングができます。	sFLOW の設定，（219 ページ）

このリリースの新規および変更情報

第 2 章

概要

この章は、次の内容で構成されています。

システム管理機能

このマニュアルに記載されているシステム管理機能について説明します。

機能	説明
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。
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。

機能	説明
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 ロールに複数の規則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。
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。

機能	説明
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 ポリシーを電子メールで通知します。 Cisco NX-OS では、ポケットベル サービス、標準的な電子メール、または XML ベースの自動化された解析アプリケーションとの最適な互換性のために、広範なメッセージ形式が提供されています。 この機能を使用して、ネットワーク サポート エンジニアや Network Operations Center を呼び出せます。また、Cisco Smart Call Home サービスを使用して、TAC でケースを自動的に生成することもできます。
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。

機能	説明
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

この章は、次の内容で構成されています。

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。 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。

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。

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。 インポートが完了した後で、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 を介した Cisco Fabric Services over IP（CFSoIP）の配信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。
- 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、設定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、設定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。
- 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。

接続の切断後の同期化の注意事項

- mgmt0 インターフェイスの接続切断後の設定同期化：mgmt0 インターフェイスの接続が切断され、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、両方のスイッチに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は、マージは mgmt0 インターフェイスが起動し、設定がもう一方のスイッチに適用されると、実行されます。

スイッチ プロファイルの設定

スイッチ プロファイルは作成および設定できます。 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

	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。

	コマンドまたはアクション	目的

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

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

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

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

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

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

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

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

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

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

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

スイッチ プロファイルへのスイッチの追加

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

スイッチを追加する場合は、次の注意事項に従ってください。

- スイッチは IP アドレスで識別されます。
- 宛先 IP は同期するスイッチの IP アドレスです。
- コミットされたスイッチ プロファイルは、ピア スイッチ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

	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	**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

	コマンドまたはアクション	目的

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

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

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

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

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

	コマンドまたはアクション	目的

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。設定端末モードの使用：

- 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

	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**：指定され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

	コマンドまたはアクション	目的
		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。
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)#
```

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** コマンドを入力することによって、スイッチ プロファイルに含まれているコマンドを確認できます。

手順

	コマンドまたはアクション	目的

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

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

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

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 スイッチのみでスイッチ プロファイルを削除します。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**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**：ローカルおよびピア スイッチでスイッチ 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。

	コマンドまたはアクション	目的
		• **local-config**：スイッチプロファイルおよびローカルコンフィギュレーションを削除します。

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

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

スイッチ プロファイルからのスイッチの削除

スイッチ プロファイルからスイッチを削除できます。

手順

	コマンドまたはアクション	目的

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

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

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

	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

	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 プロファイルのスイッチ 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のインターフェイス 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 バッファを表示する例を示します。

```
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)# 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設定の同期

新しい設定がスイッチ プロファイルを使用してピア スイッチ上でコミットされている間に Cisco Nexus シリーズ スイッチがリブートした場合は、リロード後にピア スイッチを同期するために、次の手順を実行します。

手順

ステップ 1 リブート中にピア スイッチ上で変更された設定を再適用します。

ステップ 2 **commit** コマンドを入力します。

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

スイッチ プロファイル設定の show コマンド

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

コマンド	目的
show switch-profile *name*	スイッチ プロファイル中のコマンドを表示します。
show switch-profile *name* **buffer**	スイッチ プロファイル中のコミットされていないコマンド、移動されたコマンド、削除されたコマンドを表示します。
show switch-profile *name* **peer** *IP-address*	ピア スイッチの同期ステータスが表示されます。
show switch-profile *name* **session-history**	最後の 20 のスイッチ プロファイル セッションのステータスを表示します。

コマンド	目的
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 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 3000 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。。

手順

	コマンドまたはアクション	目的

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

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

ステップ 3	スイッチ プロファイルが、ローカルおよびピア スイッチで同じであることを確認します。
	
	例：
	`switch(config-sync-sp)# show switch-profile abc status`
	
	`Start-time:  15801 usecs after Mon Aug 23 06:21:08 2010`
	`End-time:   6480 usecs after Mon Aug 23 06:21:13 2010`	

	コマンドまたはアクション	目的

	`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):`	

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`	

ステップ 5	スイッチ プロファイルのコマンドを検証します。
	
	例：
	`switch(config-sync-sp-if)# verify`
	`Verification Successful`	

ステップ 6	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

	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。	

	コマンドまたはアクション	目的

	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):`
	
	`switch(config-sync)#`	

実行コンフィギュレーションの表示

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

```
switch# configure sync
switch(config-sync)# show running-config switch-profile

switch(config-sync)#
```

ローカル スイッチとピア スイッチ間のスイッチ プロファイルの同期の表示

次に、2 台のピア スイッチの同期ステータスを表示する例を示します。

```
switch1# show switch-profile sp status

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

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

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

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

switch1#


switch2# show switch-profile sp status

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

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

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

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

同期の成功例と失敗例

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、ステータスが到達不能のピアによるピア 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、バッファ移動、およびバッファ削除の設定

次に、スイッチプロファイルバッファ、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)#
```

第 4 章

CFS の使用

この章は、次の内容で構成されています。

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する機能が備わっており、すべての CFS 対応スイッチの機能能力を検出できます。

Cisco Nexus シリーズ スイッチは、 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。

CFS には次の機能があります。

- CFS レイヤでクライアント/サーバ関係を持たないピアツーピア プロトコル。
- IPv4 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。

CFS 配信

CFS配信機能は、下位層の転送とは無関係です。 CiscoNexusシリーズスイッチは、IPおよび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適用します。 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。

CFS 配信ステータスの確認

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

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

アプリケーションの CFS サポート

CFS のアプリケーション要件

ネットワーク内のすべてのスイッチが CFS に対応している必要があります。 CFS に対応していないスイッチは配信を受信できません。これにより、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 に対応したアプリケーションに CFS タスクを初めて発行すると、設定変更プロセスが開始され、そのアプリケーションによってネットワークがロックされます。
- 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）、と配信範囲です。

```
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、この機能への設定変更は、スイッチ ソフトウェアにより、ロックを保持しているスイッチだけから行えます。 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。 ネットワークをロックしたユーザの名前は、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。

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。

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、物理的なプロキシミティに基づくスイッチ セット間での特定のプロファイルの配信を、（場合によって）ローカライズ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。

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 リージョンを実装することによって、このシナリオを実現できます。

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

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

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

CFS リージョンの管理

CFS リージョンの作成

CFS リージョンを作成できます。

手順

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

CFS リージョンへのアプリケーションの割り当て

スイッチでリージョンにアプリケーションを割り当てることができます。

手順

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

次に、リージョンにアプリケーションを割り当てる例を示します。

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

別の CFS リージョンへのアプリケーションの移動

あるリージョンから別のリージョンにアプリケーションを移動できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure**	コンフィギュレーション 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） アプリケーションを同じリージョンに複数回移動しようとすると、「Application already present in the same region」というエラー メッセージが表示されます。

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

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

リージョンからのアプリケーションの削除

リージョンからのアプリケーションの削除は、元のデフォルト リージョン（リージョン 0）へのアプリケーションの移動と同じです。これにより、ネットワーク全体がアプリケーションの配信の範囲になります。

手順

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

CFS リージョンの削除

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

手順

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

IP を介した CFS の設定

IPv4 を介した CFS のイネーブル化

IPv4 を介した CFS をイネーブルまたはディセーブルにできます。

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure**	コンフィギュレーションモードを開始します。
ステップ 2	switch(config)# **cfs ipv4 distribute**	スイッチのすべてのアプリケーションに対して IPv4 を介した CFS をグローバルでイネーブルにします。
ステップ 3	switch(config)# **no cfs ipv4 distribute**	（任意） スイッチの IPv4 を介した CFS をディセーブルにします（デフォルト）。

IPv6 を介した CFS のイネーブル化

IPv6 を介した CFS をイネーブルまたはディセーブルにできます。

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

手順

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

	コマンドまたはアクション	目的
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、**show cfs status** コマンドを使用して、IP を介した CFS の設定を確認する例を示します。

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

IP を介した CFS の IP マルチキャスト アドレスの設定

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

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

CFS の IPv4 マルチキャスト アドレスの設定

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure**	コンフィギュレーション 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

	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 アドレスの設定確認

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

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

CFS のデフォルト設定

次の表に、CFS のデフォルト設定を示します。

表 *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にされる
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 3000 Series 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/nexus3000/sw/mib/reference/n3k_mib_ref.html

第 5 章

PTP の設定

この章の内容は、次のとおりです。

PTP について

PTP は、ネットワーク全体にわたって分散したノードのため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。

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

PTP は、システム内のリアルタイム PTP クロックが互いに同期する方法を指定する分散プロトコルです。 これらのクロックはマスター スレーブの同期階層に構成され、その階層の一番上には、システム全体の基準時刻を決定するクロックであるグランドマスター クロックが含まれています。 同期は、タイミング情報を使用してメンバと PTP タイミング メッセージを交換し、階層内のマスターの時刻に合わせて各クロックを調整することによって実現されます。 PTP は、PTP ドメインと呼ばれる論理スコープ内で動作します。

PTP デバイス タイプ

次のクロックは、共通の PTP デバイスです。

オーディナリ クロック

エンド ホストと同様に 1 つの物理ポートに基づいてネットワークと通信します。 オーディナリ クロックは、グランドマスター クロックとして動作できます。

境界クロック

通常、各ポートがオーディナリ クロックのポートのように動作する複数の物理ポートです。ただし、各ポートはローカル クロックを共有し、クロック データ セットはすべてのポートに共通です。 各ポートは、境界クロックのその他すべてのポートを通じて、使用可能な最適なクロックに基づいて、個々の状態がマスターか（接続されている他のポートを同期する）またはスレーブか（ダウン ストリーム ポートに同期する）を決定します。 同期とマスター/スレーブ階層の確立に関するメッセージは、境界クロックのプロトコル エンジンで終端され、転送されません。

トランスペアレント クロック

通常のスイッチやルータのようにすべての PTP メッセージを転送しますが、スイッチ内でのパケットの滞留時間（パケットがトランスペアレント クロックを通過するのに要する時間）および場合によってはパケットの入力ポートのリンク遅延を測定します。 トランスペアレント クロックはグランドマスター クロックに同期する必要がないので、ポートには状態はありません。

次の 2 種類のトランスペアレント クロックがあります。

エンドツーエンド トランスペアレント クロック

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

ピアツーピア トランスペアレント クロック

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

（注） PTP は境界クロック モードだけで動作します。 シスコでは、スイッチに接続された同期化を必要とするクロックが含まれたサーバを使用したグランドマスター クロック（GMC）のアップストリームの配置を推奨します。

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

PTP プロセス

PTP プロセスは、マスター/スレーブ階層の確立およびクロックの同期の 2 段階で構成されます。

PTP ドメイン内では、オーディナリ クロックまたは境界クロックの各ポートは次のプロセスに従ってその状態を決定します。

- 受信したすべてのアナウンス メッセージ（マスター ステートのポートが発行する）の内容を検査します。
- 優先順位、クロック クラス、精度などに対して、（アナウンス メッセージ内の）外部マスターのデータ セットとローカル クロックを比較します。
- 自身の状態がマスターかスレーブかを決定します

マスター/スレーブ階層が確立されると、クロックは次のように同期されます。

- マスターはスレーブに同期メッセージを送信し、送信時刻を記録します。
- スレーブは同期メッセージを受信し、受信時刻を記録します。
- スレーブはマスターに遅延要求メッセージを送信し、送信時刻を記録します。
- マスターは遅延要求メッセージを受信し、受信時刻を記録します。
- マスターはスレーブに遅延応答メッセージを送信します。
- スレーブはこれらのタイムスタンプを使用して、クロックをマスターの時刻に合わせて調整します。

PTP のハイ アベイラビリティ

PTP では、ステートフル リスタートはサポートされていません。

PTP のライセンス要件

PTP にはライセンスは不要です。 ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。 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。

PTP の注意事項および制約事項

- PTP は境界クロック モードだけで動作します。 エンドツーエンド トランスペアレント クロック モードおよびピアツーピア トランスペアレント クロック モードはサポートされません。
- PTP はユーザ データグラム プロトコル（UDP）上の転送をサポートします。 イーサネット上の転送はサポートされません。
- PTP はマルチキャスト通信だけをサポートします。 ネゴシエートされたユニキャスト通信はサポートされません。
- PTP はネットワークごとに 1 つのドメインに制限されます。
- すべての管理メッセージは PTP がイネーブルのポートに転送されます。 管理メッセージの処理はサポートされていません。
- PTP 対応ポートは、ポート上で PTP をイネーブルにしない場合、PTP パケットを識別せず、これらのパケットにタイムスタンプを適用したり、パケットをリダイレクトしたりしません。
- Cisco Nexus 3000 シリーズ スイッチは、--2 ～ --5 の同期化ログ間隔を使用して、隣接するマスターから同期する必要があります。
- 同期化ログ間隔がこれらのポートすべてで -3 以下に設定されている場合、10 を超えるポート上で PTP をイネーブルにしないでください。

PTP のデフォルト設定

次の表に、PTP パラメータのデフォルト設定を示します。

表 *3*：デフォルトの *PTP* パラメータ

パラメータ	デフォルト
PTP	ディセーブル
PTP ドメイン	0

パラメータ	デフォルト
クロックをアドバタイズするときの priority 1 の値	255
クロックをアドバタイズするときの priority 2 の値	255
PTP アナウンス間隔	1 ログ秒
PTP 同期間隔	--2 ログ秒
PTP アナウンス タイムアウト	3 つのアナウンス間隔
PTP 最小遅延要求間隔	0 ログ秒
PTP VLAN	1

PTP の設定

PTP のグローバルな設定

デバイスで PTP をグローバルにイネーブルまたはディセーブルにできます。また、ネットワーク内のどのクロックにグランドマスターとして選択される最も高いプライオリティを与えるかを決定しやすくするために、さまざまな PTP クロック パラメータを設定することもできます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config) # [**no**] **feature ptp**	デバイス上で PTP をイネーブルまたはディセーブルにします。 （注） スイッチで PTP をイネーブルにしても、各インターフェイスで PTP はイネーブルになりません。
ステップ 3	switch(config) # [**no**] **ptp source** *ip-address* [**vrf** *vrf*]	すべての PTP パケットのソース IP アドレスを設定します。 *ip-address* には IPv4 または IPv6 形式を使用できます。

	コマンドまたはアクション	目的
ステップ 4	switch(config) # [**no**] **ptp domain** *number*	（任意） このクロックで使用するドメイン番号を設定します。PTP ドメインを使用すると、1 つのネットワーク上で、複数の独立した PTP クロッキング サブドメインを使用できます。 *number* の範囲は 0 ～ 128 です。
ステップ 5	switch(config) # [**no**] **ptp priority1** *value*	（任意） このクロックをアドバタイズするときに使用する priority1 の値を設定します。 この値によって、ベスト マスター クロック選択のデフォルト条件（クロック品質、クロック クラスなど）が上書きされます。 低い値が優先されます。 *value* の範囲は 0 ～ 255 です。
ステップ 6	switch(config) # [**no**] **ptp priority2** *value*	（任意） このクロックをアドバタイズするときに使用する priority2 の値を設定します。 この値は、デフォルト条件では同等と見なされる 2 つのデバイスのどちらかに決定するために使用されます。 たとえば、priority2 値を使用して、特定のスイッチが他の同等のスイッチよりも優先されるようにすることができます。 *value* の範囲は 0 ～ 255 です。
ステップ 7	switch(config) # **show ptp brief**	（任意） PTP のステータスを表示します。
ステップ 8	switch(config) # **show ptp clock**	（任意） ローカル クロックのプロパティを表示します。
ステップ 9	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

次に、デバイスで PTP をグローバルに設定し、PTP 通信の送信元 IP アドレスを指定して、クロックのプリファレンス レベルを設定する例を示します。

```
switch# configure terminal
switch(config)# feature ptp
switch(config)# ptp source 10.10.10.1
switch(config)# ptp priority1 1
switch(config)# ptp priority2 1
switch(config)# show ptp brief
```

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

インターフェイスでの PTP の設定

PTPをグローバルにイネーブルにしても、デフォルトでは、サポートされているすべてのインターフェイスでイネーブルにはなりません。 PTP インターフェイスを個別にイネーブルにする必要があります。

はじめる前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config) # **interface ethernet** *slot/port*	PTP をイネーブルにするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if) # [**no**] **feature ptp**	インターフェイスでPTPをイネーブルまたはディセーブルにします。
ステップ 4	switch(config-if) # [**no**] **ptp announce** {**interval** *log seconds* | **timeout** *count*}	（任意） インターフェイス上のPTPアナウンスメッセージ間の間隔またはタイムアウトがインターフェイスで発生する前の PTP 間隔の数を設定します。 PTP アナウンスの間隔の範囲は 0 ～ 4 秒であり、間隔のタイムアウトの範囲は 2 ～ 10 です。

	コマンドまたはアクション	目的
ステップ 5	switch(config-if) # [**no**] **ptp delay request minimum interval** *log seconds*	（任意） ポートがマスター ステートの場合に PTP 遅延要求メッセージ間で許可される最小間隔を設定します。 範囲は -1 ～ 6 秒です。
ステップ 6	switch(config-if) # [**no**] **ptp sync interval** *log seconds*	（任意） インターフェイス上の PTP 同期メッセージ間の間隔を設定します。 PTP アナウンスの間隔の範囲は -6 ～ 1 秒です。
ステップ 7	switch(config-if) # [**no**] **ptp vlan** *vlan-id*	（任意） PTP をイネーブルにするインターフェイスの VLAN を指定します。 インターフェイス上の 1 つの VLAN でのみ PTP をイネーブルにできます。 有効な範囲は 1 ～ 4094 です。
ステップ 8	switch(config-if) # **show ptp brief**	（任意） PTP のステータスを表示します。
ステップ 9	switch(config-if) # **show ptp port interface** *interface slot/port*	（任意） PTP ポートのステータスを表示します。
ステップ 10	switch(config-if)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

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

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

```
Announce receipt time out: 2
Peer mean path delay: 0
Announce interval(log mean): 3
Sync interval(log mean): -1
Delay Mechanism: End to End
Peer delay request interval(log mean): 0
switch(config-if)#
```

PTP 設定の確認

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。

表 *4*：*PTP Show* コマンド

コマンド	目的
show ptp brief	PTP のステータスを表示します。
show ptp clock	ローカル クロックのプロパティ（クロック ID を含む）を表示します。
show ptp clocks foreign-masters-record	PTP プロセスが認識している外部マスターの状態を表示します。この出力には外部マスターごとに、クロック ID、基本的なクロック プロパティ、およびそのクロックがグランドマスターとして使用されているかどうかが表示されます。
show ptp corrections	最後の数個の PTP 修正を表示します。
show ptp parent	PTP の親のプロパティを表示します。
show ptp port interface ethernet *slot/port*	スイッチ上の PTP ポートのステータスを表示します。

第 6 章

ユーザ アカウントと RBAC の設定

この章は、次の内容で構成されています。

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、各ユーザがスイッチにログインしたときに取得するアクセスの量を定義します。

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規則が含まれています。各ユーザ ロールに複数の規則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、ロール 1 では設定操作の実行だけが許可されており、ロール 2 ではデバッグ操作の実行だけが許可されている場合、ロール 1 とロール 2 の両方に属するユーザは、設定操作とデバッグ操作を実行できます。 特定の 、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。

（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。

ルール

規則は、ロールの基本要素です。 規則は、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。 規則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 3000 シリーズ 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、その機能に関連付けら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。 規則が適用される順序は、ユーザ指定の規則番号で決まります。 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 つの規則を持っている場合、規則 3 が規則 2 よりも前に適用され、規則 2 は規則 1 よりも前に適用されます。

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か、またはインターフェイスおよび VLAN へのアクセスを制限するユーザ ロール ポリシーを定義できます。

ユーザ ロール ポリシーは、ロールに定義されている規則で制約されます。 たとえば、特定のインターフェイスへのアクセスを許可するインターフェイス ポリシーを定義した場合は、ロールで **インターフェイス** コマンドを許可するためのコマンドルールを設定しない限り、ユーザはそのインターフェイスにアクセスできません。

コマンド ルールで特定のリソース（インターフェイス、VLAN）へのアクセスが許可されている場合は、ユーザがそのユーザに関連付けられたユーザ ロール ポリシーにリストされていなくても、ユーザはこれらのリソースへのアクセスが許可されます。

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
- shutdown
- sync
- sys
- uucp

- xfs

注意 Cisco Nexus 3000 シリーズ スイッチでは、すべて数字のユーザ名が TACACS+ または RADIUS で作成されている場合でも、すべて数字のユーザ名はサポートされません。 AAA サーバに数字だけのユーザ名が登録されていて、ログイン時に入力しても、スイッチはログイン要求を拒否します。

ユーザ パスワードの要件

Cisco Nexus 3000 シリーズ 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 3000 シリーズ スイッチはその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 アカウントと RBAC 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。

- ユーザ ロールには最大 256 のルールを追加できます。
- ユーザ アカウントには最大 64 のユーザ ロールを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 などの定義済みのロールは編集できません。
- SAN admin ユーザ ロールの場合、ルールの追加、削除、および編集はサポートされません。
- SAN admin ユーザ ロールの場合、インターフェイス、VLAN、または VSAN の範囲は変更できません。

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

ユーザ アカウントの設定

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **show role**	（任意） 使用可能なユーザ ロールを表示します。 必要に応じて、他のユーザ ロールを設定できます。
ステップ 3	switch(config) # **username** *user-id* [**password** *password*] [**expire** *date*] [**role** *role-name*]	ユーザ アカウントを設定します。 *user-id* は、最大 28 文字の英数字で、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い場合は、ユーザがスイッチにログインできない可能性があります。 **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。

	コマンドまたはアクション	目的
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
```

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 つの規則を持っている場合、規則 3 が規則 2 よりも前に適用され、規則 2 は規則 1 よりも前に適用されます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config) # **role name** *role-name*	ユーザ ロールを指定し、ロール コンフィギュレーション モードを開始します。 *role-name* 引数は、最大 16 文字の英数字で、大文字と小文字が区別されます。
ステップ 3	switch(config-role) # **rule** *number* {**deny** | **permit**} **command** *command-string*	コマンド規則を設定します。 *command-string* には、スペースおよび正規表現を含めることができます。 たとえば、interface ethernet * には、すべてのイーサネット インターフェイスが含まれます。

	コマンドまたはアクション	目的
		必要な規則の数だけこのコマンドを繰り返します。
ステップ 4	switch(config-role)# **rule** *number* {**deny** | **permit**} {**read** | **read-write**}	すべての操作の読み取り専用ルールまたは読み取り/書き込みルールを設定します。
ステップ 5	switch(config-role)# **rule** *number* {**deny** | **permit**} {**read** | **read-write**} **feature** *feature-name*	機能に対して、読み取り専用規則か読み取りと書き込みの規則かを設定します。 **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。 必要な規則の数だけこのコマンドを繰り返します。
ステップ 6	switch(config-role)# **rule** *number* {**deny** | **permit**} {**read** | **read-write**} **feature-group** *group-name*	機能グループに対して、読み取り専用規則か読み取りと書き込みの規則かを設定します。 **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。 必要な規則の数だけこのコマンドを繰り返します。
ステップ 7	switch(config-role)# **description** *text*	（任意） ロールの説明を設定します。 説明にはスペースも含めることができます。
ステップ 8	switch(config-role)# **end**	ロール コンフィギュレーション モードを終了します。
ステップ 9	switch# **show role**	（任意） ユーザ ロールの設定を表示します。
ステップ 10	switch# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を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

	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

	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、を指定できます。
ステップ 5	switch(config-role-interface) # **exit**	ロール インターフェイス ポリシー コンフィギュレーション モードを終了します。
ステップ 6	switch(config-role) # **show role**	（任意） ロール設定を表示します。
ステップ 7	switch(config-role) # **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

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

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

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

ユーザ アカウントおよび RBAC 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。

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

ユーザ アカウントおよび RBAC のユーザ アカウント デフォルト設定

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

表 *5*：デフォルトのユーザ アカウントと *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

この章は、次の内容で構成されています。

Session Manager の概要

Session Manager を使用すると、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

	コマンドまたはアクション	目的
ステップ 1	switch# **configure session** *name*	コンフィギュレーション セッションを作成し、セッション コンフィギュレーション モードを開始します。名前は任意の英数字ストリングです。 セッションの内容を表示します。
ステップ 2	switch(config-s)# **show configuration session** [*name*]	（任意） セッションの内容を表示します。
ステップ 3	switch(config-s)# **save** *location*	（任意） セッションをファイルに保存します。保存場所には、bootflash または volatile を指定できます。

セッションでの ACL の設定

コンフィギュレーション セッションで ACL を設定できます。

手順

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

セッションの確認

セッションを確認するには、セッション モードで次のコマンドを使用します。

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

セッションのコミット

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

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

セッションの保存

セッションを保存するには、セッション モードで次のコマンドを使用します。

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

セッションの廃棄

セッションを廃棄するには、セッション モードで次のコマンドを使用します。

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

Session Manager のコンフィギュレーション例

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 コンフィギュレーションの確認

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

コマンド	目的
show configuration session [*name*]	コンフィギュレーション ファイルの内容を表示します。

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

第 8 章

スケジューラの設定

この章は、次の内容で構成されています。

スケジューラの概要

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

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

ジョブは、定期的な作業を定義する単一または複数のコマンドで構成されています。 ジョブは、1 回だけ、または定期的な間隔でスケジューリングすることができます。

スケジューラでは、ジョブと、そのタイムテーブルを次のように定義できます。

ジョブ

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

スケジュール

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

1 つのスケジュールは、定期的、または 1 回だけ実行するように定義されます。

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

リモート ユーザ認証

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

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

スケジューラ ログ ファイル

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

スケジューラのライセンス要件

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。

スケジューラの注意事項および制約事項

- ジョブの実行中に次のいずれかの状況が発生した場合、スケジューラは失敗する可能性があります。
  - 機能ライセンスが、その機能のジョブがスケジュールされている時間に期限切れになった場合。
  - 機能が、その機能を使用するジョブがスケジューリングされている時間にディセーブルになっている場合。
- 時刻が設定されていることを確認します。スケジューラはデフォルトのタイムテーブルを適用しません。スケジュールを作成し、ジョブを割り当てても、時刻を設定しなければ、ジョブは開始されません。
- ジョブは開始されると非インタラクティブ方式で実行されるため、ジョブの定義中、インタラクティブなコマンドや中断を伴うコマンド（例：**copy bootflash:** *file* **ftp:***URI*、**write erase**、その他類似のコマンド）が指定されていないことを確認してください。

スケジューラのデフォルト設定

表 *6*：コマンド スケジューラのパラメータのデフォルト

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

スケジューラの設定

スケジューラのイネーブル化

手順

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

次に、スケジューラをイネーブルにする例を示します。

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

スケジューラ ログ ファイル サイズの定義

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config) # **scheduler logfile size** *value*	スケジューラ ログ ファイル サイズをキロバイト（KB）で定義します。

	コマンドまたはアクション	目的
		範囲は 16 ～ 1024 です。 デフォルトのログ ファイル サイズは 16 です。 （注） ジョブ出力のサイズがログ ファイルのサイズより大きい場合、出力内容は切り捨てられます。
ステップ 3	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、スケジューラ ログ ファイルのサイズを定義する例を示します。

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

リモート ユーザ認証の設定

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

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config) # **scheduler aaa-authentication password** [**0** | **7**] *password*	現在ログインしているユーザのパスワードを設定します。 クリアテキストパスワードを設定するには、**0** を入力します。 暗号化パスワードを設定するには、**7** を入力します。
ステップ 3	switch(config) # **scheduler aaa-authentication username** *name* **password** [**0** | **7**] *password*	リモート ユーザのクリア テキスト パスワードを設定します。

	コマンドまたはアクション	目的
ステップ 4	switch(config) # **show running-config | include "scheduler aaa-authentication"**	（任意） スケジューラのパスワード情報を表示します。
ステップ 5	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、NewUser という名前のリモート ユーザのクリア テキスト パスワードを設定する例を示します。

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

ジョブの定義

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

手順

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

	コマンドまたはアクション	目的
ステップ 5	switch(config-job) # **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、backup-cfg という名前のスケジューラ ジョブを作成し、実行コンフィギュレーションをブートフラッシュ内のファイルに保存し、そのファイルをブートフラッシュから TFTP サーバにコピーし、変更をスタートアップ コンフィギュレーションに保存する例を示します。

```
switch# configure terminal
switch(config) # scheduler job name backup-cfg
switch(config-job) # cli var name timestamp
$(timestamp) ;copy running-config
bootflash:/$(SWITCHNAME)-cfg.$(timestamp) ;copy
bootflash:/$(SWITCHNAME)-cfg.$(timestamp)
tftp://1.2.3.4/ vrf management
switch(config-job) # copy running-config startup-config
```

ジョブの削除

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config) # **no scheduler job name** *name*	特定のジョブおよびそこで定義されたすべてのコマンドを削除します。 *name* は 31 文字までに制限されています。
ステップ 3	switch(config-job) # **show scheduler job** [*name*]	（任意） ジョブ情報を表示します。
ステップ 4	switch(config-job) # **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、configsave という名前のジョブを削除する例を示します。

```
switch# configure terminal
switch(config)# no scheduler job name configsave
```

```
switch(config-job)# copy running-config startup-config
switch(config-job)#
```

タイムテーブルの定義

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

time コマンドで時刻を設定しない場合は、スケジューラは現在の時刻を使用します。 たとえば、現在の時刻が 2008 年 3 月 24 日の 22 時 00 分である場合、ジョブは次のように開始されます。

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

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config) # **scheduler schedule name** *name*	新しいスケジューラを作成し、そのスケジュールのスケジュール コンフィギュレーション モードを開始します。 *name* は 31 文字までに制限されています。
ステップ 3	switch(config-schedule) # **job name** *name*	このスケジュールにジョブを関連付けます。 1つのスケジュールに複数のジョブを追加できます。 *name* は 31 文字までに制限されています。

	コマンドまたはアクション	目的
ステップ 4	switch(config-schedule) # **time daily** *time*	ジョブが毎日 HH:MM の形式で指定された時刻に開始することを意味します。
ステップ 5	switch(config-schedule) # **time weekly** [[*day-of-week*:] *HH*:] *MM*	ジョブが週の指定された曜日に開始することを意味します。 曜日は整数（たとえば、日曜日は **1**、月曜日は **2**）または略語（たとえば、**sun**、 **mon**）で表します。 引数全体の最大長は 10 文字です。
ステップ 6	switch(config-schedule) # **time monthly** [[*day-of-month*:] *HH*:] *MM*	ジョブが月の特定の日に開始することを意味します。 29、30 または 31 のいずれかを指定した場合、そのジョブは各月の最終日に開始されます。
ステップ 7	switch(config-schedule) # **time start** {**now repeat** *repeat-interval* | *delta-time* [**repeat** *repeat-interval*]}	ジョブが定期的に開始することを意味します。 start-time の形式は [[[[yyyy:]mmm:]dd:]HH]:MM です。 • *delta-time*：スケジュールの設定後、ジョブの開始までの待機時間を指定します。 • **now**：ジョブが今から 2 分後に開始することを指定します。 • **repeat** *repeat-interval*：ジョブを反復する回数を指定します。
ステップ 8	switch(config-schedule) # **show scheduler config**	（任意） スケジューラの情報を表示します。
ステップ 9	switch(config-schedule) # **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、ジョブが毎月 28 日の 23 時 00 分に開始するタイムテーブルを定義する例を示します。

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

スケジューラ ログ ファイルの消去

手順

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

次に、スケジューラ ログ ファイルを消去する例を示します。

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

スケジューラのディセーブル化

手順

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

次に、スケジューラをディセーブルにする例を示します。

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

スケジューラの設定確認

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。

表 *7* : スケジューラの ***show*** コマンド

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

スケジューラの設定例

スケジューラ ジョブの作成

次に、実行中のコンフィギュレーションを bootflash 内のファイルに保存し、ファイルを bootflash から TFTP サーバにコピーするスケジューラ ジョブを作成する例を示します（ファイル名は、現在のタイム スタンプとスイッチ名を使用して作成されます）。

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

スケジューラ ジョブのスケジューリング

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

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

ジョブ スケジュールの表示

次に、ジョブ スケジュールを表示する例を示します。

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

スケジューラ ジョブの実行結果の表示

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

```
switch# show scheduler logfile
Job Name       : back-cfg                           Job Status: Failed (1)
Schedule Name  : daily                              User Name : admin
Completion time: Fri Jan 1  1:00:01 2009
-------------------------------- Job Output --------------------------------
`cli var name timestamp 2009-01-01-01.00.00`
`copy running-config bootflash:/$(HOSTNAME)-cfg.$(timestamp)`
`copy bootflash:/switch-cfg.2009-01-01-01.00.00 tftp://1.2.3.4/ vrf management `
copy: cannot access file '/bootflash/switch-cfg.2009-01-01-01.00.00'
==============================================================================
Job Name       : back-cfg                           Job Status: Success (0)
Schedule Name  : daily                              User Name : admin
Completion time: Fri Jan 2  1:00:01 2009
-------------------------------- Job Output --------------------------------
`cli var name timestamp 2009-01-02-01.00.00`
`copy running-config bootflash:/switch-cfg.2009-01-02-01.00.00`
`copy bootflash:/switch-cfg.2009--01-02-01.00.00 tftp://1.2.3.4/ vrf management `
Connection to Server Established.
[                       ]         0.50KBTrying to connect to tftp server......
[######                 ]        24.50KB
TFTP put operation was successful
==============================================================================
switch#
```

スケジューラの標準

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

第 9 章

オンライン診断の設定

この章は、次の内容で構成されています。

オンライン診断について

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

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 *8*：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、または起動時診断の完全なセットを実行するように Cisco Nexus 3000 シリーズ 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 *9*：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 *10*：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 *11*：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 *12*：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

	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。 • 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。

	コマンドまたはアクション	目的
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 *13*：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 10 章

Embedded Event Manager の設定

この章は、次の内容で構成されています。

Embedded Event Manager について

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

EEM は次の 3 種類の主要コンポーネントからなります。

イベント文

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

アクション文

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

ポリシー

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

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

Embedded Event Manager ポリシー

EEMポリシーは、イベント文および1つまたは複数のアクション文からなります。 イベント文では、探すイベントとともに、イベントのフィルタリング特性を定義します。 アクション文では、イベントの発生時に EEM が実行するアクションを定義します。

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

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

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

設定済みのシステム ポリシー

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

一部のシステムポリシーは上書きできます。 このような場合、イベントまたはアクションに対する上書きを設定できます。 設定した上書き変更がシステム ポリシーの代わりになります。

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

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

ユーザ作成ポリシー

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

ログ ファイル

EEM ポリシーの一致に関連するデータが格納されたログ ファイルは、/log/event_archive_1 ディレクトリにある event_archive_1 ログ ファイルで維持されます。

イベント文

対応策、通知など、一部のアクションが実行されるデバイス アクティビティは、EEMによってイベントと見なされます。 イベントは通常、インターフェイスやファンの誤動作といったデバイスの障害に関連します。

イベント文は、どのイベントがポリシー実行のトリガーになるかを指定します。

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

EEM ではイベント フィルタを定義して、クリティカル イベントまたは指定された時間内で繰り返し発生したイベントだけが関連付けられたアクションのトリガーになるようにします。

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

サポートされるイベント

EEM はイベント文で次のイベントをサポートします。

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

アクション文

アクション文は、イベントが発生したときに、ポリシーによってトリガーされるアクションを説明します。各ポリシーに複数のアクション文を設定できます。ポリシーにアクションを関連付けなかった場合、EEM はイベント観察を続けますが、アクションは実行されません。

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

（注） ユーザ ポリシーまたは上書きポリシー内のアクション文を設定する場合、アクション文が、相互に否定したり、関連付けられたシステム ポリシーに悪影響を与えるようなことがないように確認することが重要です。

サポートされるアクション

EEM がアクション文でサポートするアクションは、次のとおりです。

- CLI コマンドの実行
- カウンタのアップデート
- デバイスをリロードします。
- syslog メッセージの生成
- SNMP 通知の生成
- システム ポリシー用デフォルト アクションの使用

VSH スクリプト ポリシー

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

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

Embedded Event Manager のライセンス要件

この機能にはライセンスは不要です。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。

Embedded Event Manager の前提条件

EEM を設定するには、network-admin の権限が必要です。

Embedded Event Manager の注意事項および制約事項

EEM の設定を計画するときは、次の点を考慮します。

- 設定可能な EEM ポリシーの最大数は 500 です。
- ユーザ ポリシーまたは上書きポリシー内のアクション文が、相互に否定したり、関連付けられたシステム ポリシーに悪影響を与えるようなことがないようにする必要があります。
- 発生したイベントでデフォルトのアクションを処理できるようにする場合は、デフォルトのアクションを許可する EEM ポリシーを設定する必要があります。 たとえば、一致文でコマンドを照合する場合、EEM ポリシーに event-default アクション文を追加する必要があります。この文がないと、EEM ではコマンドを実行できません。
- イベント文が指定されていて、アクション文が指定されていない上書きポリシーを設定した場合、アクションは開始されません。また、障害も通知されません。
- 上書きポリシーにイベント文が含まれていないと、システム ポリシーで可能性のあるイベントがすべて上書きされます。
- 通常コマンドの表現の場合：すべてのキーワードを拡張する必要があり、アスタリスク（*）記号のみが引数の置換に使用できます。
- EEM イベント相関は 1 つのポリシーに最大 4 つのイベント文をサポートします。 イベント タイプは同じでも別でもかまいませんが、サポートされるイベント タイプは、cli、カウンタ、snmp、syslog、追跡だけです。
- 複数のイベント文が EEM ポリシーに存在する場合は、各イベント文に **tag** キーワードと一意な tag 引数が必要です。
- EEM イベント相関はシステムのデフォルト ポリシーを上書きしません。
- デフォルト アクション実行は、タグ付きのイベントで設定されているポリシーではサポートされません。
- イベント指定が CLI のパターンと一致する場合、SSH 形式のワイルドカード文字を使用できます。

  たとえば、すべての show コマンドを照合する場合は、**show *** コマンドを入力します。 **show .*** コマンドを入力すると、機能しません。
- イベント指定が一致する syslog メッセージの正規表現の場合、適切な正規表現を使用できます。

  たとえば、syslog が生成されているポート上で ADMIN_DOWN イベントを検出するには、**.ADMIN_DOWN** を使用します。 **ADMIN_DOWN** コマンドを入力すると、機能しません。

- syslog のイベント指定では、regex は、EEM ポリシーのアクションとして生成される syslog メッセージと一致しません。
- EEM イベントが CLI の **show** コマンドと一致し、画面に表示するために（および EEM ポリシーによってブロックされないために）**show** コマンドの出力が必要な場合は、EEM ポリシーの最初のアクションに対して、**event-default** コマンドを指定する必要があります。

Embedded Event Manager のデフォルト設定

表 *14*：デフォルトの *EEM* パラメータ

パラメータ	デフォルト
システム ポリシー	アクティブ

Embedded Event Manager の設定

環境変数の定義

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

手順

	コマンドまたはアクション	目的

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

ステップ 2	**event manager environment** *variable-name variable-value* 例： `switch(config) # event manager environment emailto "admin@anyplace.com"`	EEM 用の環境変数を作成します。 *variable-name* は大文字と小文字を区別し、最大 29 文字の英数字を使用できます。 *variable-value* は大文字と小文字が区別され、引用符で囲んだ最大 39 文字の英数字を使用できます。

	コマンドまたはアクション	目的
ステップ 3	**show event manager environment** {*variable-name* | **all**} 例： `switch(config) # show event manager environment all`	（任意） 設定した環境変数に関する情報を表示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次の作業

ユーザ ポリシーを設定します。

CLI によるユーザ ポリシーの定義

手順

	コマンドまたはアクション	目的

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

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

ステップ 3	**description** *policy-description* 例： `switch(config-applet)# description "Monitors interface shutdown."`	（任意） ポリシーの説明になるストリングを設定します。 string には最大 80 文字の英数字を使用できます。 ストリングは引用符で囲みます。

	コマンドまたはアクション	目的
ステップ 4	**event** *event-statement* 例： `switch(config-applet)# event cli match "shutdown"`	ポリシーのイベント文を設定します。
ステップ 5	**tag** *tag* {**and** | **andnot** | **or**} *tag* [**and** | **andnot** | **or** {*tag*}] {**happens** *occurs* **in** *seconds*} 例： `switch(config-applet)# tag one or two happens 1 in 10000`	（任意） ポリシー内の複数のイベントを相互に関連付けます。 *occurs* 引数の範囲は 1 ～ 4294967295 です。 *seconds* 引数の範囲は 0～4294967295 秒です。
ステップ 6	**action** *number*[.*number2*] *action-statement* 例： `switch(config-applet)# action 1.0 cli show interface e 3/1`	ポリシーのアクション文を設定します。 アクション文が複数ある場合、このステップを繰り返します。
ステップ 7	**show event manager policy-state** *name* [**module** *module-id*] 例： `switch(config-applet)# show event manager policy-state monitorShutdown`	（任意） 設定したポリシーの状態に関する情報を表示します。
ステップ 8	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次の作業

イベント文およびアクション文を設定します。

イベント文の設定

イベント文を設定するには、EEM コンフィギュレーション モード（config-applet）で次のいずれかのコマンドを使用します。

はじめる前に

ユーザ ポリシーを定義します。

手順

	コマンドまたはアクション	目的
ステップ 1	**event cli** [**tag** *tag*] **match** *expression* [**count** *repeats* | **time** *seconds* 例： `switch(config-applet) # event cli match "shutdown"`	正規表現と一致するコマンドが入力された場合に、イベントを発生させます。 **tag** *tag* キーワードと引数のペアは、複数のイベントがポリシーに含まれている場合、この特定のイベントを識別します。 *repeats* の範囲は 1 ～ 65000 です。 *time* の範囲は 0 ～ 4294967295 です。0 は無制限を示します。
ステップ 2	**event counter** [**tag** *tag*] **name** *counter* **entry-val** *entry* **entry-op** {**eq** | **ge** | **gt** | **le** | **lt** | **ne**} {**exit-val** *exit* **exit-op** {**eq** | **ge** | **gt** | **le** | **lt** | **ne**} 例： `switch(config-applet) # event counter name mycounter entry-val 20 gt`	カウンタが、開始演算子に基づいて開始のしきい値を超えた場合にイベントを発生させます。イベントはただちにリセットされます。任意で、カウンタが終了のしきい値を超えたあとでリセットされるように、イベントを設定できます。 **tag** *tag* キーワードと引数のペアは、複数のイベントがポリシーに含まれている場合、この特定のイベントを識別します。 *counter* name は大文字と小文字を区別し、最大 28 の英数字を使用できます。 *entry* および *exit* の値の範囲は 0 ～ 2147483647 です。
ステップ 3	**event fanabsent** [**fan** *number*] **time** *seconds* 例： `switch(config-applet) # event fanabsent time 300`	秒数で設定された時間を超えて、ファンがデバイスから取り外されている場合に、イベントを発生させます。 *number* の範囲はモジュールに依存します。 *seconds* の範囲は 10 ～ 64000 です。
ステップ 4	**event fanbad** [**fan** *number*] **time** *seconds* 例： `switch(config-applet) # event fanbad time 3000`	秒数で設定された時間を超えて、ファンが故障状態の場合に、イベントを発生させます。 *number* の範囲はモジュールに依存します。 *seconds* の範囲は 10 ～ 64000 です。
ステップ 5	**event memory** {**critical** | **minor** | **severe**} 例： `switch(config-applet) # event memory critical`	メモリのしきい値を超えた場合にイベントを発生させます。

	コマンドまたはアクション	目的
ステップ 6	**event policy-default count** *repeats* [**time** *seconds*] 例： `switch(config-applet) # event policy-default count 3`	システムポリシーで設定されているイベントを使用します。このオプションは、ポリシーを上書きする場合に使用します。 *repeats* の範囲は 1 ～ 65000 です。 *seconds* の範囲は 0 ～ 4294967295 秒です。0 は無制限を示します。
ステップ 7	**event snmp** [**tag** *tag*] **oid** *oid* **get-type** {**exact** | **next**} **entry-op** {**eq** | **ge** | **gt** | **le** | **lt** | **ne**} **entry-val** *entry* [**exit-comb** {**and** | **or**}]**exit-op** {**eq** | **ge** | **gt** | **le** | **lt** | **ne**} **exit-val** *exit* **exit-time** *time* **polling-interval** *interval* 例： `switch(config-applet) # event snmp oid 1.3.6.1.2.1.31.1.1.1.6 get-type next entry-op lt 300 entry-val 0 exit-op eq 400 exit-time 30 polling-interval 300`	SNMP OID が、開始演算子に基づいて開始のしきい値を超えた場合にイベントを発生させます。イベントはただちにリセットされます。または任意で、カウンタが終了のしきい値を超えたあとでリセットされるように、イベントを設定できます。OID はドット付き 10 進表記です。 **tag** *tag* キーワードと引数のペアは、複数のイベントがポリシーに含まれている場合、この特定のイベントを識別します。 *entry* および *exit* の値の範囲は 0 ～ 18446744073709551615 です。 *time* の範囲は 0 ～ 2147483647 秒です。 *interval* の範囲は 0 ～ 2147483647 秒です。
ステップ 8	**event sysmgr memory** [**module** *module-num*] **major** *major-percent* **minor** *minor-percent* **clear** *clear-percent* 例： `switch(config-applet) # event sysmgr memory minor 80`	指定したシステムマネージャのメモリのしきい値を超えた場合にイベントを発生させます。 *percent* の範囲は 1 ～ 99 です。
ステップ 9	**event temperature** [**module** *slot*] [**sensor** *number*] **threshold** {**any** | **down** | **up**} 例： `switch(config-applet) # event temperature module 2 threshold any`	温度センサーが設定されたしきい値を超えた場合に、イベントを発生させます。 *sensor* の範囲は 1 ～ 18 です。
ステップ 10	**event track** [**tag** *tag*] *object-number* **state** {**any** | **down** | **up** 例： `switch(config-applet) # event track 1 state down`	トラッキング対象オブジェクトが設定された状態になった場合に、イベントを発生させます。 **tag** *tag* キーワードと引数のペアは、複数のイベントがポリシーに含まれている場合、この特定のイベントを識別します。

	コマンドまたはアクション	目的
		指定できる *object-number* の範囲は 1 ～ 500 です。

次の作業

アクション文を設定します。

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

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

アクション文の設定

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

（注） 発生したイベントでデフォルトのアクションを処理できるようにする場合は、デフォルトのアクションを許可する EEM ポリシーを設定する必要があります。

たとえば、一致文でコマンドを照合する場合、EEM ポリシーに event-default アクション文を追加する必要があります。この文がないと、EEM ではコマンドを実行できません。 **terminal event-manager bypass** コマンドを使用すると、一致するすべての EEM ポリシーでコマンドを実行できます。

はじめる前に

ユーザ ポリシーを定義します。

手順

	コマンドまたはアクション	目的
ステップ 1	**action** *number*[.*number2*] **cli** *command1*[*command2.*] [**local**] 例： `switch(config-applet) # action 1.0 cli "show interface e 3/1"`	設定済みコマンドを実行します。任意で、イベントが発生したモジュール上でコマンドを実行できます。 アクション ラベルのフォーマットは number1.number2 です。 *number* には 1 ～ 16 桁の任意の番号を指定できます。 *number2* の範囲は 0 ～ 9 です。
ステップ 2	**action** *number*[.*number2*] **counter name** *counter* **value** *val* **op** {**dec** | **inc** | **nop** | **set**} 例： `switch(config-applet) # action 2.0 counter name mycounter value 20 op inc`	設定された値および操作でカウンタを変更します。 アクション ラベルのフォーマットは number1.number2 です。 *number* には 1 ～ 16 桁の任意の番号を指定できます。 *number2* の範囲は 0 ～ 9 です。 *counter* は大文字と小文字を区別し、最大 28 文字の英数字を使用できます。 *val* には 0 ～ 2147483647 の整数または置換パラメータを指定できます。
ステップ 3	**action** *number*[.*number2*] **event-default** 例： `switch(config-applet) # action 1.0 event-default`	関連付けられたイベントのデフォルト アクションを実行します。 アクション ラベルのフォーマットは number1.number2 です。 *number* には 1 ～ 16 桁の任意の番号を指定できます。 *number2* の範囲は 0 ～ 9 です。
ステップ 4	**action** *number*[.*number2*] **policy-default** 例： `switch(config-applet) # action 1.0 policy-default`	上書きしているポリシーのデフォルト アクションを実行します。 アクション ラベルのフォーマットは number1.number2 です。 *number* には 1 ～ 16 桁の任意の番号を指定できます。 *number2* の範囲は 0 ～ 9 です。
ステップ 5	**action** *number*[.*number2*] **reload** [**module** *slot* [**-** *slot*]] 例： `switch(config-applet) # action 1.0 reload module 3-5`	システム全体に 1 つ以上のモジュールをリロードします。 アクション ラベルのフォーマットは number1.number2 です。

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

次の作業

イベント文を設定します。

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

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

VSH スクリプトによるポリシーの定義

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

手順

ステップ 1　テキスト エディタで、ポリシーを定義するコマンド リストを指定します。
ステップ 2　テキスト ファイルに名前をつけて保存します。
ステップ 3　次のシステム ディレクトリにファイルをコピーします。bootflash://eem/user_script_policies

次の作業

VSH スクリプト ポリシーを登録してアクティブにします。

VSH スクリプト ポリシーの登録およびアクティブ化

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

はじめる前に

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

手順

	コマンドまたはアクション	目的

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

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

	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、変更を継続的に保存します。

次の作業

システム要件に応じて、次のいずれかを実行します。

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

システム ポリシーの上書き

手順

	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	**show event manager policy-state** *system-policy*
	
	例：
	`switch(config-applet)# show event manager policy-state __ethpm_link_flap`
	`Policy __ethpm_link_flap`
	`  Cfg count : 5`
	`  Cfg time interval : 10.000000 (seconds)`
	`  Hash default, Count 0`
		（任意）
		上書きするシステム ポリシーの情報をしきい値を含めて表示します。 システム ポリシー名を突き止めるには、**show event manager system-policy** コマンドを使用します。

ステップ 3	**event manager applet** *applet-name* **override** *system-policy* 例： `switch(config-applet)# event manager applet`	システム ポリシーを上書きし、アプレット コンフィギュレーション モードを開始します。 *applet-name* は大文字と小文字を区別し、最大 80 文字の英数字を使用できます。

	コマンドまたはアクション	目的
	`ethport override __ethpm_link_flap` `switch(config-applet)#`	*system-policy* は、システム ポリシーの 1 つにする必要があります。
ステップ 4	**description** *policy-description* 例： `switch(config-applet)# description "Overrides link flap policy"`	ポリシーの説明になるストリングを設定します。 *policy-description* は大文字と小文字を区別し、最大 80 文字の英数字を使用できますが、引用符で囲む必要があります。
ステップ 5	**event** *event-statement* 例： `switch(config-applet)# event policy-default count 2 time 1000`	ポリシーのイベント文を設定します。
ステップ 6	**section** *number action-statement* 例： `switch(config-applet)# action 1.0 syslog priority warnings msg "Link is flapping."`	ポリシーのアクション文を設定します。 複数のアクション文では、この手順を繰り返します。
ステップ 7	**show event manager policy-state** *name* 例： `switch(config-applet)# show event manager policy-state ethport`	（任意） 設定したポリシーに関する情報を表示します。
ステップ 8	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

メモリのしきい値の設定

メモリのしきい値は、イベントをトリガーし、メモリを割り当てることができない場合にオペレーティング システムがプロセスを停止するかどうかを設定するために使用されます。

手順

	コマンドまたはアクション	目的

ステップ 1	**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	**system memory-thresholds minor** *minor* **severe** *severe* **critical** *critical* 例： `switch(config)# system memory-thresholds minor 60 severe 70 critical 80`	EEM メモリ イベントを生成するシステム メモリしきい値を設定します。 デフォルト値は次のとおりです。 • minor：85 • severe：90 • critical：95 これらのメモリのしきい値を超えた場合、システムは次の syslog を生成します。 • 2009 May 7 17:06:30 switch %$ VDC-1 %$ %PLATFORM-2-MEMORY_ALERT: Memory Status Alert : MINOR • 2009 May 7 17:06:30 switch %$ VDC-1 %$ %PLATFORM-2-MEMORY_ALERT: Memory Status Alert : SEVERE • 2009 May 7 17:06:30 switch %$ VDC-1 %$ %PLATFORM-2-MEMORY_ALERT: Memory Status Alert : CRITICAL • 2009 May 7 17:06:35 switch %$ VDC-1 %$ %PLATFORM-2-MEMORY_ALERT: Memory Status Alert : MINOR ALERT RECOVERED • 2009 May 7 17:06:35 switch %$ VDC-1 %$ %PLATFORM-2-MEMORY_ALERT: Memory Status Alert : SEVERE ALERT RECOVERED • 2009 May 7 17:06:35 switch %$ VDC-1 %$ %PLATFORM-2-MEMORY_ALERT: Memory Status Alert : CRITICAL ALERT RECOVERED
ステップ 3	**system memory-thresholds threshold critical no-process-kill** 例： `switch(config)# system memory-thresholds threshold critical no-process-kill`	（任意） メモリを割り当てることができない場合にプロセスを停止しないようにシステムを設定します。 デフォルト値では、最もメモリを消費するプロセスから終了できます。

	コマンドまたはアクション	目的
ステップ 4	**show running-config | include "system memory"** 例： `switch(config)# show running-config | include "system memory"`	（任意） システム メモリ設定に関する情報を表示します。
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、変更を継続的に保存します。

次の作業

システム要件に応じて、次のいずれかを実行します。

- EEM パブリッシャとして syslog を設定します。
- EEM 設定を確認します。

EEM パブリッシャとしての syslog の設定

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

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

はじめる前に

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

手順

	コマンドまたはアクション	目的

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

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

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

次の作業

EEM 設定を確認します。

Embedded Event Manager の設定確認

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 event manager environment [*variable-name* | **all**]	イベント マネージャの環境変数に関する情報を表示します。
show event manager event-types [*event* | **all** | **module** *slot*]	イベント マネージャのイベント タイプに関する情報を表示します。

コマンド	目的
show event manager history events [**detail**] [**maximum** *num-events*] [**severity** {**catastrophic** | **minor** | **moderate** | **severe**}]	すべてのポリシーについて、イベント履歴を表示します。
show event manager policy internal [*policy-name*] [**inactive**]	設定したポリシーに関する情報を表示します。
show event manager policy-state *policy-name*	しきい値を含め、ポリシーの状態に関する情報を表示します。
show event manager script system [*policy-name* | **all**]	スクリプト ポリシーに関する情報を表示します。
show event manager system-policy [**all**]	定義済みシステム ポリシーに関する情報を表示します。
show running-config eem	EEM の実行コンフィギュレーションに関する情報を表示します。
show startup-config eem	EEM のスタートアップ コンフィギュレーションに関する情報を表示します。

Embedded Event Manager の設定例

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

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

次に、__ethpm_link_flap システム ポリシーを上書きし、インターフェイスをシャット ダウンする例を示します。

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

次に、ユーザがデバイスでコンフィギュレーション モードを開始すると、コマンドを実行できるが、SNMP 通知をトリガーする EEM ポリシーを作成する例を示します。

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

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

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

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

その他の参考資料

関連資料

関連項目	マニュアル タイトル
EEM コマンド	『*Cisco Nexus 3000 Series NX-OS System Management Command Reference*』

標準

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

EEM 機能の履歴

表 *15*：*EEM* 機能の履歴

機能名	リリース	機能情報
Embedded Event Manager（EEM）	5.0(3)U3(1)	機能が追加されました。

第 11 章

システム メッセージ ロギングの設定

この章は、次の内容で構成されています。

システム メッセージ ロギングの概要

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

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

デフォルトでは、Cisco Nexus 3000 シリーズ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 *16*：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、シスコ ファブリック サービス（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 *17*：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にスイッチを設定できます。

デフォルトでは、ターミナル セッションでロギングはイネーブルです。

手順

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

	コマンドまたはアクション	目的
		小さいほうが大きい重大度を示します）。 重大度は 0 ～ 7 の範囲です。 • 0：緊急 • 1：アラート • 2：クリティカル • 3：エラー • 4：警告 • 5：通知 • 6：情報 • 7：デバッグ 重大度が指定されていない場合、デフォルトの2が使用されます。 設定はTelnetおよびSSHセッションに適用されます。
ステップ 6	switch(config)# **no logging monitor** [*severity-level*]	（任意） Telnet および SSH セッションへのメッセージ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

	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。 重大度は 0 ～ 7 の範囲です。 • 0：緊急 • 1：アラート • 2：クリティカル • 3：エラー • 4：警告 • 5：通知 • 6：情報 • 7：デバッグ

	コマンドまたはアクション	目的
		ファイル サイズは 4096 ～ 10485760 バイトです。
ステップ 3	switch(config)# **no logging logfile** [*logfile-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 timestamp:               Seconds
Logging server:                  disabled
Logging logfile:                 enabled
        Name - my_log: Severity - informational Size - 4194304
Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
aaa                     3                       3
aclmgr                  3                       3
afm                     3                       3
altos                   3                       3
auth                    0                       0
authpriv                3                       3
bootvar                 5                       5
callhome                2                       2
capability              2                       2
cdp                     2                       2
cert_enroll             2                       2
...
```

モジュールおよびファシリティ メッセージのロギングの設定

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

手順

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

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

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

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

ロギング タイムスタンプの設定

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーション 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。

	コマンドまたはアクション	目的
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

	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されるログ エントリの最大数を設定します。 範囲は 0 ～ 1000000 エントリです。 デフォルト値は 8000 エントリです。
ステップ 3	switch(config)# **logging ip access-list cache interval** *seconds*	ログ更新間の秒数を設定します。 また、この期間中に非アクティブのエントリは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、一致するパケットの数によってロギングがトリガーされることはありません。

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

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

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

インターフェイスへの ACL ロギングの適用

mgmt0 インターフェイスだけに ACL ロギングを適用できます。

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

	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の 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 mgmt0 インターフェイスに適用する例を示します。

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

ACL ログの一致レベルの設定

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **acllog match-log-level** *number*	ACL ログ（acllog）に記録されるエントリに一致するログ レベルを指定します。 *number* は 0 ～ 7 の値です。 デフォルト値は 6 です。 （注） ログ メッセージがログに入力されるには、ACL ログ ファシリティ（acllog）のログ レベルおよびログ ファイルのロギング重大度が ACL ログの一致ログ レベルの設定以上である必要があります。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, （121 ページ）およびファイルへのシステム メッセージ ロギングの設定, （120 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

	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 ホストのホスト名あるいは IPv4 または IPv6 アドレスを識別します。 • *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 16： システム メッセージの重大度，（116 ページ） を参照してください。 • **use vrf** *vrf-name* キーワードおよび引数は、仮想ルーティングおよび転送（VRF）名の *default* または *management* 値を識別します。 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 3000 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/ps11541/prod_command_reference_list.html にあります。 （注） デバッグは CLI 機能ですが、デバッグの syslog はサーバに送信されません。

	コマンドまたはアクション	目的
ステップ 3	**no logging server** *host* 例： `switch(config)# no logging server 172.28.254.254 5`	（任意） 指定されたホストのロギング サーバを削除します。
ステップ 4	**show logging server** 例： `switch# show logging server`	（任意） Syslog サーバ設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、syslog サーバを設定する例を示します。

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

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

UNIX または Linux システムでの syslog の設定

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

facility.level <five tab characters> *action*

次の表に、設定可能な syslog フィールドを示します。

表 *18* : *syslog.conf* の *Syslog* フィールド

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

手順

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

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

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

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

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

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

Syslog サーバ設定の配布の設定

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

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

（注） スイッチを再起動すると、揮発性メモリに保持されている syslog サーバ設定の変更は失われる可能性があります。

はじめる前に

1 つまたは複数の syslog サーバを設定しておく必要があります。

手順

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

	コマンドまたはアクション	目的
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

	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。
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 ip access-list cache	IP アクセス リスト キャッシュを表示します。
show logging ip access-list cache detail	IP アクセス リスト キャッシュに関する詳細情報を表示します。
show logging ip access-list status	IP アクセス リスト キャッシュのステータスを表示します。
show logging last *number-lines*	ログ ファイルの末尾から指定行数を表示します。
show logging level [*facility*]	ファシリティ ロギング重大度設定を表示します。
show logging logfile [**start-time** *yyyy mmm dd hh:mm:ss*] [**end-time** *yyyy mmm dd hh:mm:ss*]	ログ ファイルのメッセージを表示します。
show logging module	モジュール ロギング設定を表示します。
show logging monitor	モニタ ロギング設定を表示します。
show logging nvram [**last** *number-lines*]	NVRAM ログのメッセージを表示します。
show logging pending	syslog サーバの保留中の配布設定を表示します。

コマンド	目的
show logging pending-diff	syslog サーバの保留中の配布設定の違いを表示します。
show logging server	syslog サーバ設定を表示します。
show logging session	ロギング セッションのステータスを表示します。
show logging status	ロギング ステータスを表示します。
show logging timestamp	ロギング タイムスタンプ単位設定を表示します。
show running-config acllog	ACL ログ ファイルの実行コンフィギュレーションを表示します。

第 12 章

Smart Call Home の設定

この章は、次の内容で構成されています。

Smart Call Home に関する情報

Smart Call Home は電子メールを使用して、重要なシステム イベントを通知します。 Cisco Nexus シリーズ スイッチは、幅広いメッセージ フォーマットを提供し、ポケットベル サービス、標準電子メール、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 サービス用にデバイスを登録できます。 Smart Call Home では、お使いのデバイスから送信された Smart Call Home メッセージを分析し、背景説明と推奨事項を提供することによって、システムの問題をすばやく解決できます。既知と特定できる問題、特に GOLD 診断エラーについては、シスコ TAC（Technical Assistance Center）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。
- お使いのデバイスから直接、またはダウンロード可能な Transport Gateway（TG; 転送ゲートウェイ）集約ポイントを介して転送されたメッセージのセキュリティ保護。 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。
- すべての Smart Call Home デバイスの Smart Call Home メッセージおよび推奨事項、インベントリおよび設定情報への Web ベースのアクセス、および現場の注意事項、セキュリティ勧告、および廃止情報。

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 機能は、次のとおりです。

- 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、シスコ TAC と通信できます。
- 複数の同時メッセージの宛先 それぞれの宛先プロファイルには、最大 50 個の電子メール宛先アドレスを設定できます。

Smart Call Home の宛先プロファイル

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

- 1 つまたは複数のアラート 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 つまたは複数の電子メール宛先：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、月別で送信するインベントリ アラート グループを使用して、定期的なインベントリ 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 のアラート グループ

アラート グループは、すべての Cisco Nexus 3000 シリーズ 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 グループ機能を使用すると、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関連付けら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、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 *19*：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
Diagnostic	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**
Supervisor hardware	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**
Linecard hardware	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**
Configuration	設定に関連した定期的なイベント	**show version** **show module** **show running-config all** **show startup-config**
System	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**
Environmental	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**
Inventory	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インベントリ 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 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 syslog の重大度をマッピングします。

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 レベルしきい値に関連付けることができます。 宛先プロファイルのこのしきい値よりも小さな値を持つ Smart Call Home メッセージは、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 *20*：重大度と *Syslog* レベルのマッピング

Smart Call Home レベル	Keyword	Syslog レベル	説明
9	Catastrophic	該当なし	ネットワーク全体に壊滅的な障害が発生しています。
8	Disaster	該当なし	ネットワークに重大な影響が及びます。
7	Fatal	緊急（0）	システムを使用できません。
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）	重大な状態。

Smart Call Home レベル	Keyword	Syslog レベル	説明
4	Minor	エラー（3）	軽微な状態。
3	Warning	警告（4）	警告状態です。
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 メッセージです。

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
- インベントリ 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 *21*：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
Device identification	設定されたデバイス名
Date/time stamp	起動イベントのタイム スタンプ
Error isolation message	起動イベントの簡単な説明（英語）
Alarm urgency level	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 *22*：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）
Time stamp	ISO 時刻通知でのイベントの日付/タイム スタンプ *YYYY-MM-DD HH:MM:SS GMT+HH:MM*	/aml/header/time
Message name	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
Message type	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
Message group	Syslog などのアラート グループの名前	/aml/header/group
Severity level	メッセージの重大度。	/aml/header/level
Source ID	ルーティングのための製品タイプ。	/aml/header/source
Device 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）
Customer 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
Contract 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
Site 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
Server 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
Message description	エラーを説明するショート テキスト	/aml/body/msgDesc
Device name	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）
Contact name	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
Contact e-mail	この装置の担当者の電子メール アドレス	/aml/body/sysContactEmail
Contact phone number	このユニットの連絡先である人物の電話番号。	/aml/body/sysContactPhoneNumber
Street address	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
Model name	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
Serial number	ユニットのシャーシのシリアル番号。	/aml/body/chassis/serialNo
Chassis part number	シャーシの最上アセンブリ番号。	/aml/body/chassis/partNo
特定のアラート グループ メッセージの固有のフィールドは、ここに挿入されます。		
このアラート グループに対して複数の CLI コマンドが実行されると、次のフィールドが繰り返される場合があります。		
Command output name	実行された CLI コマンドの正確な名前	/aml/attachments/attachment/name
Attachment type	特定のコマンド出力	/aml/attachments/attachment/type
MIME type	プレーン テキストまたは符号化タイプ	/aml/attachments/attachment/mime
Command output text	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 *23*：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）
Chassis hardware version	シャーシのハードウェア バージョン。	/aml/body/chassis/hwVersion
Supervisor module software version	最上レベルのソフトウェア バージョン。	/aml/body/chassis/swVersion
Affected FRU name	イベント メッセージを生成する関連 FRU の名前	/aml/body/fru/name
Affected FRU serial number	関連 FRU のシリアル番号	/aml/body/fru/serialNo
Affected FRU part number	関連 FRU の部品番号	/aml/body/fru/partNo
FRU slot	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 hardware version	関連 FRU のハードウェア バージョン	/aml/body/fru/hwVersion
FRU software version	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 *24*：インベントリ 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）
Chassis hardware version	シャーシのハードウェア バージョン	/aml/body/chassis/hwVersion
Supervisor module software version	最上レベルのソフトウェア バージョン。	/aml/body/chassis/swVersion
FRU name	イベント メッセージを生成する関連 FRU の名前	/aml/body/fru/name

データ項目（プレーン テキストおよび XML）	説明（プレーン テキストおよび XML）	XML タグ（XML のみ）
FRU s/n	FRU のシリアル番号	/aml/body/fru/serialNo
FRU part number	FRU の部品番号	/aml/body/fru/partNo
FRU slot	FRU のスロット番号	/aml/body/fru/slot
FRU hardware version	FRU のハードウェア バージョン	/aml/body/fru/hwVersion
FRU software version	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 メッセージ形式を示します。

表 *25*：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）
Process ID	固有のプロセス ID。	/aml/body/process/id
Process state	プロセスの状態（実行中、中止など）。	/aml/body/process/processState
Process exception	原因コードの例外。	/aml/body/process/exception

Smart Call Home の注意事項および制約事項

- IP 接続がない場合、またはプロファイル宛先への仮想ルーティングおよび転送（VRF）インスタンスのインターフェイスがダウン状態である場合、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。
- 担当者名（SNMP サーバの担当者）、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 *26*：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 のための登録

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

ステップ 1 ブラウザで、Smart Call Home の 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 を登録するための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

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **snmp-server contact** *sys-contact*	SNMP sysContact を設定します。
ステップ 3	switch(config)# **callhome**	Smart Call Home コンフィギュレーション モードを開始します。
ステップ 4	switch(config-callhome)# **email-contact** *email-address*	スイッチの担当者の電子メールアドレスを設定します。 *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） 任意の有効な電子メール 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、国際電話番号の形式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（+）記号を使用します。

	コマンドまたはアクション	目的
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 255 文字以内の英数字を使用できます。スペースを使用できます。
ステップ 7	switch(config-callhome)# **contract-id** *contract-number*	（任意） サービス契約からこのスイッチの契約番号を設定します。 *contract-number* には最大 255 文字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 文字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

	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 3000 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/ps11541/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電子メール アドレスに送信された Call Home メッセージの長さ。

（注） CiscoTAC-1 宛先プロファイルは変更または削除できません。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **callhome**	Smart Call Home コンフィギュレーション モードを開始します。
ステップ 3	switch(config-callhome)# **destination-profile** {*name* | **full-txt-destination** | **short-txt-destination**} **email-addr** *address*	ユーザ定義または定義済みの宛先プロファイルに電子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 個の電子メール 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* の範囲は 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** |	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 の範囲は 0 ～ 5000000 であり、デフォルトは 2500000 です。

	コマンドまたはアクション	目的
	short-txt-destination} **message-size** *number*	short-txt-destination の範囲は 0 ～ 100000 であり、デフォルトは 4000 です。 CiscoTAC-1 での値は 5000000 であり、変更できません。
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 グループを宛先プロファイルに関連付けます。

アラート グループと宛先プロファイルの関連付け

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **callhome**	Smart Call Home コンフィギュレーション モードを開始します。
ステップ 3	switch(config-callhome)# **destination-profile** *name* **alert-group** {**All** | **Cisco-TAC** | **Configuration** | **Diagnostic** | **Environmental** | **Inventory** | **License** | **Linecard-Hardware** |	アラート グループをこの宛先プロファイルに関連付けます。 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関連付けます。

	コマンドまたはアクション	目的
	Supervisor-Hardware | **Syslog-group-port** | **System** | **Test**}	
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

	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** |	**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。

	コマンドまたはアクション	目的
	Syslog-group-port | **System** | **Test**} **user-def-cmd** *show-cmd*	
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電子メール アドレスも設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **callhome**	Smart Call Home コンフィギュレーション モードを開始します。
ステップ 3	switch(config-callhome)# **transport email smtp-server** *ip-address* [**port** *number*] [**use-vrf** *vrf-name*]	SMTP サーバを、ドメイン ネーム サーバ（DNS）名、IPv4 アドレス、または IPv6 アドレスのいずれかとして設定します。 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。

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

デバイス上で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とハードウェアのインベントリ情報を定期的に送信するようにスイッチを設定できます。 スイッチは 2 つの Smart Call Home 通知（定期的な設定メッセージと定期的なインベントリ メッセージ）を生成します。

手順

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

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

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

次の作業

重複メッセージ抑制をディセーブルにします。

重複メッセージの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、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

	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 に対する重複メッセージの抑制をディセーブルにします。 重複メッセージの抑制は、デフォルトでイネーブルになっています。
ステップ 4	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

次に、重複メッセージの抑制をディセーブルにする例を示します。

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

次の作業

Smart Call Home をイネーブルにします。

Smart Call Home のイネーブル化またはディセーブル化

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **callhome**	Smart Call Home コンフィギュレーション モードを開始します。
ステップ 3	switch(config-callhome) # [**no**] **enable**	Smart Call Home をイネーブルまたはディセーブルにします。

	コマンドまたはアクション	目的
		Smart Call Home は、デフォルトではディセーブルになっています。
ステップ 4	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を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　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と、Smart Call Home のテストが失敗します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **callhome**	Smart Call Home コンフィギュレーション モードを開始します。
ステップ 3	switch(config-callhome) # **callhome send diagnostic**	指定された Smart Call Home メッセージを設定されたすべての宛先に送信します。

	コマンドまたはアクション	目的
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。
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。

コマンド	目的
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 13 章

DNS の設定

この章は、次の内容で構成されています。

DNS クライアントの概要

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

- 権限ネーム サーバは、その権限ゾーン内のドメイン名を求める DNS ユーザ照会に、自身のホスト テーブル内にキャッシュされた永久的なエントリを使用して応答します。 照会で求められているのが、自身の権限ゾーン内であるが、設定情報が登録されていないドメイン名の場合、権限ネーム サーバは単に、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

	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。

	コマンドまたはアクション	目的

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*] 例： `switch(config)# ip name-server 192.0.2.22`	（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。 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。

	コマンドまたはアクション	目的
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 14 章

SNMP の設定

この章は、次の内容で構成されています。

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 3000 シリーズ 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 3000 シリーズ 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。

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 3000 シリーズ 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 *27*：*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 *28*： 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

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

次の例は、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 ロールを関連付けます。

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 3000 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/ps11541/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 3000 シリーズ 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
```

VRF を使用する SNMP 通知レシーバの設定

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

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

手順

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

	コマンドまたはアクション	目的
		0 ～ 65535 です。 このコマンドによって、CISCO-SNMP-TARGET-EXT-MB の ExtSnmpTargetVrfTable にエントリが追加されます。
ステップ 3	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

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

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

VRF に基づいた SNMP 通知のフィルタリング

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **snmp-server host** *ip-address* **filter-vrf** *vrf_name* [**udp_port** *number*]	設定された VRF に基づいて、通知ホスト レシーバへの通知をフィルタリングします。 ip-address は IPv4 または IPv6 アドレスを使用できます。 VRF 名には最大 255 の英数字を使用できます。 UDP ポート番号の範囲は 0 ～ 65535 です。 このコマンドによって、CISCO-SNMP-TARGET-EXT-MB の ExtSnmpTargetVrfTable にエントリが追加されます。
ステップ 3	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

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

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

インバンド アクセスのための SNMP の設定

次のものを使用して、インバンド アクセス用に SNMP を設定できます。

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **snmp-server context** *context-name* **vrf** *vrf-name*	管理 VRF またはデフォルト VRF に SNMP コンテキストをマッピングします。 カスタム VRF はサポートされません。 名前には最大 32 の英数字を使用できます。
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 *29* : *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**

MIB	関連コマンド
CISCO-FCC-MIB	**snmp-server enable traps fcc**
CISCO-DM-MIB	**snmp-server enable traps fcdomain**
CISCO-NS-MIB	**snmp-server enable traps fcns**
CISCO-FCS-MIB	**snmp-server enable traps fcs discovery-complete** **snmp-server enable traps fcs request-reject**
CISCO-FDMI-MIB	**snmp-server enable traps fdmi**
CISCO-FSPF-MIB	**snmp-server enable traps fspf**
CISCO-PSM-MIB	**snmp-server enable traps port-security**
CISCO-RSCN-MIB	**snmp-server enable traps rscn** **snmp-server enable traps rscn els** **snmp-server enable traps rscn ils**
CISCO-ZS-MIB	**snmp-server enable traps zone** **snmp-server enable traps zone default-zone-behavior-change** **snmp-server enable traps zone enhanced-zone-db-change** **snmp-server enable traps zone merge-failure** **snmp-server enable traps zone merge-success** **snmp-server enable traps zone request-reject** **snmp-server enable traps zone unsupp-mem**

（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。

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

リンクの通知の設定

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

- 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

	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

	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

	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

	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。

	コマンドまたはアクション	目的
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

	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。

第 15 章

RMON の設定

この章は、次の内容で構成されています。

RMON について

RMON は、各種のネットワーク エージェントおよびコンソール システムがネットワーク モニタリング データを交換できるようにするための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 3000 シリーズ 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 3000 シリーズでは 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 3000 シリーズ 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 3000 シリーズ 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 3000 シリーズ 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 3000 シリーズ 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 アラームに関連付けることができます。 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

	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*	RMON 高容量アラームを作成します。 値の範囲は、–2147483647 ～ 2147483647 です。 オーナー名は任意の英数字ストリングです。 ストレージタイプの範囲は 1 ～ 5 です。

	コマンドまたはアクション	目的
	falling-threshold-low *value* [*event-index*] [**owner** *name*] [**storagetype** *type*]	
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 アラームと関連付けるよう 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

	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。

	コマンドまたはアクション	目的
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 *30*：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 16 章

SPAN の設定

この章は、次の内容で構成されています。

SPAN について

スイッチド ポート アナライザ（SPAN）機能（ポート ミラーリングまたはポート モニタリングとも呼ばれる）は、ネットワーク アナライザによる分析のためのネットワーク トラフィックを選択します。 ネットワーク アナライザには、Cisco SwitchProbeまたはその他のリモート モニタリング（RMON）プローブを使用できます。

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、ポート チャネル、、および VLAN をサポートします。 VLAN では、指定された VLAN でサポートされているすべてのインターフェイスが SPAN 送信元として含まれます。 イーサネット、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。

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 をサポートします。

送信元ポートの特性は、次のとおりです。

- イーサネット、ポートチャネル、またはVLANのいずれのポートタイプでもかまいません。
- 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 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/TX オプションは、VLAN の SPAN セッションでは使用できません。
- 送信元ポートは、同じか、あるいは異なる VLAN 内に存在できます。

SPAN 宛先

SPAN 宛先とは、送信元ポートをモニタリングするインターフェイスを表します。 Cisco Nexus 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 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

宛先ポートの特性

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

- どの物理ポートであってもかまいません。送信元イーサネットのポートを宛先ポートにすることはできません。
- 送信元ポートにはなれません。
- ポート チャネルにはできません。
- SPAN セッションがアクティブなときは、スパニングツリーに参加しません。
- 任意の SPAN セッションのソース 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 には、次の注意事項と制限事項があります。

- NX-OS 5.0(3) U 2(2) をインストールし、その後でソフトウェアを以前のバージョンにダウングレードした場合、SPAN の設定は失われます。

  これを回避するには、NX-OS 5.0(3)U2(2) にアップグレードする前に設定を保存し、ダウングレード後にローカル SPAN の設定を再適用する必要があります。

  同様の ERSPAN の制約事項については、ERSPAN についてERSPAN の注意事項および制約事項, （206 ページ）を参照してください。

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。そのセッションがすでに存在する場合は、追加の設定情報がすべて既存のセッションに追加されます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **monitor session** *session-number*	モニタ コンフィギュレーション モードを開始します。 既存のセッション設定に新しいセッション設定が追加されます。

次に、SPAN モニタ セッションを設定する例を示します。

```
switch# configure terminal
switch(config) # monitor session 2
switch(config) #
```

イーサネット宛先ポートの設定

SPAN 宛先ポートとしてイーサネット インターフェイスを設定できます。

（注） SPAN 宛先ポートは、スイッチ上の物理ポートにのみ設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバルコンフィギュレーションモードを開始します。
ステップ 2	switch(config)# **interface ethernet** *slot*/*port*	指定されたスロットとポートでイーサネット インターフェイスのインターフェイス コンフィギュレーション モードを開始します。
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*	指定された SPAN セッションのモニタ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 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)#
```

送信元ポートの設定

送信元ポートは、イーサネット ポートにのみ設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config) # **monitor session** *session-number*	指定されたモニタリング 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。 イーサネットのポートの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)#
```

送信元ポート チャネルまたは VLAN の設定

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

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config) # **monitor session** *session-number*	指定された 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**} *channel-number* [**rx** | **tx** | **both**] | **vlan** *vlan-range*}	ポート チャネルまたは VLAN 送信元を設定します。 VLAN 送信元の場合、モニタリング方向は暗黙的です。

次に、ポート チャネル SPAN 送信元を設定する例を示します。

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

次に、VLAN 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)#
```

SPAN セッションの説明の設定

参照を容易にするために、SPAN セッションの説明的な名前を指定できます。

手順

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

	コマンドまたはアクション	目的
ステップ 2	switch(config) # **monitor session** *session-number*	指定された 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 セッションの説明的な名前を作成します。

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

	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。

手順

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

	コマンドまたはアクション	目的
ステップ 1	switch# **show monitor** [**session** {**all** | *session-number* | **range** *session-range*} [**brief**]]	SPAN 設定を表示します。

次に、SPAN セッションの情報を表示する例を示します。

```
switch# show monitor
SESSION  STATE        REASON                   DESCRIPTION
-------  -----------  -----------------------  --------------------------------
2        up           The session is up
3        down         Session suspended
4        down         No hardware resource
```

次に、SPAN セッションの詳細を表示する例を示します。

```
switch# show monitor session 2
   session 2
---------------
type              : local
state             : up
source intf       :

source VLANs      :
    rx            :

destination ports : Eth3/1
```

第 17 章

ERSPAN の設定

この章は、次の内容で構成されています。

ERSPAN について

Cisco NX-OS システムは、送信元ポートと宛先ポートの両方で ERSPAN（Encapsulated Remote Switching Port Analyser）機能をサポートします。 ERSPAN は、ミラーリングされたトラフィックを IP ネットワーク経由で転送します。 トラフィックは送信元ルータでカプセル化され、ネットワーク全体にわたって転送されます。 パケットは宛先ルータでカプセル化解除されてから、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 GRE（Generic Routing Encapsulation）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

トラフィックをモニタできるモニタ元インターフェイスのことを ERSPAN 送信元と呼びます。 送信元では、監視するトラフィックを指定し、さらに入力、出力、または両方向のトラフィックをコピーするかどうかを指定します。 ERSPAN 送信元には次のものが含まれます。

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

ERSPAN 送信元ポートには、次の特性があります。

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

ERSPAN 宛先

宛先ポートは ERSPAN 送信元からコピーされたトラフィックを受信します。

ERSPAN 宛先ポートには、次の特性があります。

- ERSPANセッションの宛先には、アクセス モードまたはトランク モードのイーサネット ポートまたはポートチャネル インターフェイスが含まれます。
- 宛先ポートとして設定されたポートを送信元ポートとしても設定することはできません。
- 宛先ポートは、一度に 1 つの ERSPAN セッションだけで設定できます。
- 宛先ポートは、どのスパニングツリー インスタンスにも、どのレイヤ 3 プロトコルにも参加しません。
- モニタ宛先ポートでは、入力オプションおよび入力ラーニング オプションはサポートされていません。
- HIF ポート チャネルおよびファブリック ポート チャネルのポートは、SPAN 宛先ポートとしてサポートされていません。

ERSPAN セッション

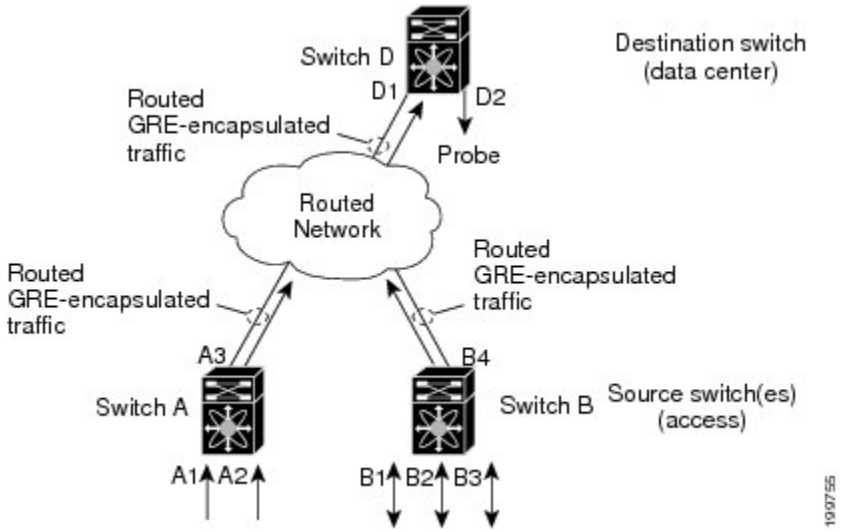
モニタする送信元と宛先を指定する ERSPAN セッションを作成できます。

ERSPAN 送信元セッションを設定する場合は、宛先 IP アドレスを設定する必要があります。 ERSPAN 宛先セッションを設定する場合は、送信元 IP アドレスを設定する必要があります。 送信元セッションのプロパティについてはERSPAN 送信元, （204 ページ）を、宛先セッションのプロパティについてはERSPAN 宛先, （204 ページ）を参照してください。

（注） すべてのスイッチにわたって同時に実行できるのは 2 つの ERSPAN または SPAN 送信元セッションだけです。 すべてのスイッチにわたって同時に実行できるのは 23 の ERSPAN 宛先セッションだけです。

次の図は、ERSPAN の設定を示しています。

図 *1* : ***ERSPAN*** の設定



マルチ ERSPAN セッション

最大 48 個の ERSPAN セッションを定義できますが、同時に実行できる ERSPAN または SPAN セッションは 2 個だけです。 未使用の ERSPAN セッションはシャット ダウンできます。

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, （213 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 リスタートおよびステートフル リスタートをサポートします。 リブートまたはスーパーバイザ スイッチオーバー後に、実行コンフィギュレーションを適用します。

ERSPAN のライセンス要件

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 のライセンス方式の詳細については、『*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。

•各デバイス上で、まず所定の ERSPAN 設定をサポートする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。

ERSPAN の注意事項および制約事項

ERSPAN 設定時の注意事項と制限事項は次のとおりです。

- ERSPAN は次をサポートしています。
  - 4 ～ 6 トンネルから
  - 非トンネル パケット
  - IP-in-IP トンネル
  - IPv4 トンネル（制限あり）
  - ERSPAN 送信元セッション タイプ（パケットは GRE トンネル パケットとしてカプセル化され、IP ネットワーク上で送信されます。 ただし、他のシスコ デバイスとは異なり、ERSPAN ヘッダーはパケットに追加されません。）
  - ERSPAN 宛先セッション タイプ（ただし、ERSPAN パケットをカプセル化解除するためのサポートは使用できません。 カプセル化されたパケット全体が、ERSPAN 終端ポイントにある前面パネル ポートにスパンされます。）
- カプセル化されたミラー パケットがレイヤ 2 の MTU チェックに失敗すると、ERSPAN パケットはドロップされます。

- 出力カプセル化には、112 バイトの制限があります。 この制限を超えるパケットはドロップされます。 このシナリオは、トンネルとミラーリングが混在しているときに発生することがあります。
- ERSPAN セッションは複数のローカル セッションで共有されます。 最大 18 セッションが設定できます。ただし、同時に動作できるのは最大4セッションのみです。 受信ソースと送信ソースの両方が同じセッションで設定されている場合、2 セッションのみが動作できます。
- NX-OS 5.0(3) U 2(2) をインストールし、ERSPAN を設定し、その後でソフトウェアを以前のバージョンにダウングレードすると、ERSPAN の設定は失われます。 この状況は、ERSPAN が NX-OS 5.0(3) U 2(2) よりも前のバージョンでサポートされていないため発生します。

  同様の SPAN の制約事項については、SPAN について SPAN の注意事項および制約事項, （197 ページ）を参照してください。
- ERSPAN、およびERSPAN ACLは、スーパーバイザが生成したパケットではサポートされません。
- ERSPAN と ERSPAN ACL セッションは、宛先ルータで同様に終了します。
- ERSPAN は、管理ポートではサポートされません。
- 宛先ポートは、一度に 1 つの ERSPAN セッションだけで設定できます。
- ポートをソース ポートと宛先ポートの両方として設定することはできません。
- 1 つの ERSPAN セッションに、次の送信元を組み合わせて使用できます。
  - イーサネット ポートまたはポート チャネル（サブ インターフェイスを除く）。
  - ポート チャネル サブインターフェイスに割り当てることのできる VLAN またはポート チャネル。
  - コントロール プレーン CPU へのポート チャネル。

  （注） ERSPAN は送信元に関係なく、スーパーバイザによって生成されるパケットをモニタしません。
- 宛先ポートはスパニングツリー インスタンスまたはレイヤ 3 プロトコルに参加しません。
- ERSPAN セッションに、送信方向または送信および受信方向でモニタされている送信元ポートが含まれている場合、パケットが実際にはその送信元ポートで送信されなくても、これらのポートを受け取るパケットが ERSPAN の宛先ポートに複製される可能性があります。 送信元ポートでこの動作が生じる例の一部を示します。
  - フラッディングから発生するトラフィック
  - ブロードキャストおよびマルチキャスト トラフィック

- 入力と出力の両方が設定されている VLAN ERSPAN セッションでは、パケットが同じ VLAN 上でスイッチングされる場合に、宛先ポートから 2 つのパケット（入力側から 1 つ、出力側から 1 つ）が転送されます。
- VLAN ERSPAN がモニタするのは、VLAN のレイヤ 2 ポートを出入りするトラフィックだけです。
- パケットがミラーリングされ、ERSPAN宛先ポートに送信された場合、GREヘッダーは削除されません。 パケットは、GRE ペイロードとして元のパケットを含む GRE パケットとして GRE ヘッダーとともに送信されます。

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 *31*：デフォルトの *ERSPAN* パラメータ

パラメータ	デフォルト
ERSPAN セッション	シャット ステートで作成されます。

ERSPAN の設定

ERSPAN 送信元セッションの設定

ERSPAN セッションを設定できるのはローカル デバイス上だけです。 デフォルトでは、ERSPAN セッションはシャット ステートで作成されます。

送信元には、イーサネット ポート、ポート チャネル、および VLAN を指定できます。 1 つの ERSPAN セッションに、イーサネット ポートまたは VLAN を組み合わせた送信元を使用できます。

（注） ERSPAN は送信元に関係なく、スーパーバイザによって生成されるパケットをモニタしません。

手順

	コマンドまたはアクション	目的

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

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

ステップ 3	**no monitor session** {*session-number* | **all**} 例： `switch(config)# no monitor session 3`	指定した ERSPAN セッションのコンフィギュレーションを消去します。新しいセッション コンフィギュレーションは、既存のセッション コンフィギュレーションに追加されます。

ステップ 4	**monitor session** {*session-number* | **all**} **type erspan-source**
	
	例：
	`switch(config)# monitor session 3 type erspan-source`
	`switch(config-erspan-src)#`
		ERSPAN 送信元セッションを設定します。

ステップ 5	**description** *description* 例： `switch(config-erspan-src)# description erspan_src_session_3`	セッションの説明を設定します。デフォルトでは、説明は定義されません。説明には最大 32 の英数字を使用できます。

ステップ 6	**source** {[**interface** [*type slot/port*[*-port*][*, type slot/port[-port*]]] [**port-channel** *channel-number*]] | [**vlan** {*number* | *range*}]} [**rx** | **tx** | **both**]
	
	例：
	`switch(config-erspan-src)# source interface ethernet 2/1-3, ethernet 3/1 rx`
	
	例：
	`switch(config-erspan-src)# source interface port-channel 2`
	
	例：
	`switch(config-erspan-src)# source interface sup-eth 0 both`
		送信元およびパケットをコピーするトラフィックの方向を設定します。イーサネット ポート範囲、ポート チャネル、または VLAN 範囲を入力できます。
		
		送信元は 1 つ設定することも、またはカンマで区切った一連のエントリとして、または番号の範囲として、複数設定することもできます。最大 128 のインターフェイスを指定できます。VLAN 範囲の詳細については、『*Cisco Nexus 3000 Series NX-OS Layer 2 Switching Configuration Guide, Release 5.x*』を参照してください。

	コマンドまたはアクション	目的

	例：
	`switch(config-erspan-src)# source vlan 3, 6-8 tx`
	
	例：
	`switch(config-monitor)# source interface ethernet 101/1/1-3`
		入力、出力、またはその両方としてコピーするトラフィックの方向を指定できます。 デフォルトは both です。

ステップ 7	ステップ 6 を繰り返して、すべての ERSPAN 送信元を設定します。	（任意） —
ステップ 8	**destination ip** *ip-address* 例： `switch(config-erspan-src)# destination ip 10.1.1.1`	ERSPAN セッションの宛先 IP アドレスを設定します。 ERSPAN 送信元セッションごとに宛先 IP アドレスが 1 つだけサポートされます。
ステップ 9	**vrf** *vrf-name* 例： `switch(config-erspan-src)# vrf default`	ERSPAN 送信元セッションがトラフィックの転送に使用する VRF を設定します。
ステップ 10	**ip ttl** *ttl-number* 例： `switch(config-erspan-src)# ip ttl 25`	（任意） ERSPAN トラフィックの IP 存続可能時間（TTL）値を設定します。 指定できる範囲は 1 ～ 255 です。
ステップ 11	**ip dscp** *dscp-number* 例： `switch(config-erspan-src)# ip dscp 42`	（任意） ERSPAN トラフィックのパケットの DiffServ コード ポイント（DSCP）値を設定します。 指定できる範囲は 0 ～ 63 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） 同時に実行できる ERSPAN 送信元セッションは 2 つだけです。
ステップ 13	**show monitor session** {**all** | *session-number* | **range** *session-range*} 例： `switch(config-erspan-src)# show monitor session 3`	（任意） ERSPAN セッション設定を表示します。

	コマンドまたはアクション	目的
ステップ 14	**show running-config monitor** 例： `switch(config-erspan-src)# show running-config monitor`	（任意） 実行 ERSPAN コンフィギュレーションを表示します。
ステップ 15	**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 16	**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 宛先セッションの設定

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

はじめる前に

すでにモニタ モードで宛先ポートが設定されていることを確認します。

手順

	コマンドまたはアクション	目的

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

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

	コマンドまたはアクション	目的
ステップ 3	**switchport** 例： `switch(config-if)# switchport`	選択したスロットおよびポートまたはポート範囲でスイッチポートパラメータを設定します。
ステップ 4	**switchport mode** [**access** | **trunk**] 例： `switch(config-if)# switchport mode trunk`	選択したスロットおよびポートまたはポート範囲で次のスイッチポートモードを設定します。 • access • trunk
ステップ 5	**switchport monitor** 例： `switch(config-if)# switchport monitor`	ERSPAN 宛先としてスイッチポート インターフェイスを設定します。
ステップ 6	ステップ 2 ～ 5 を繰り返して、追加の ERSPAN 宛先でモニタリングを設定します。	—
ステップ 7	**no monitor session** {*session-number* | **all**} 例： `switch(config-if)# no monitor session 3`	指定した ERSPAN セッションのコンフィギュレーションを消去します。新しいセッション コンフィギュレーションは、既存のセッション コンフィギュレーションに追加されます。

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

ステップ 9	**description** *description* 例： `switch(config-erspan-dst)# description erspan_dst_session_3`	セッションの説明を設定します。デフォルトでは、説明は定義されません。説明には最大 32 の英数字を使用できます。
ステップ 10	**source ip** *ip-address* 例： `switch(config-erspan-dst)# source ip 10.1.1.1`	ERSPAN セッションの送信元 IP アドレスを設定します。ERSPAN 宛先セッションごとに送信元 IP アドレスが 1 つだけサポートされます。
ステップ 11	**destination** {[**interface** [*type slot/port*[*-port*][, *type slot/port[-port*]]] [**port-channel** *channel-number*]]}	コピーされた送信元パケットの宛先を設定します。1 つ以上のインターフェイスをカ

	コマンドまたはアクション	目的
	例： `switch(config-erspan-dst)# destination interface ethernet 2/5, ethernet 3/7`	ンマで区切った一連のエントリとして設定できます。 （注） トランク ポートとして宛先ポートを設定できます。
ステップ 12	ステップ 11 を繰り返して、すべての ERSPAN 宛先を設定します。	（任意） —
ステップ 13	**no shut** 例： `switch(config)# no shut`	ERSPAN 宛先セッションをイネーブルにします。 デフォルトでは、セッションはシャット ステートで作成されます。 （注） 同時に実行できる ERSPAN 宛先セッションは 23 個だけです。
ステップ 14	**show monitor session** {**all** | *session-number* | **range** *session-range*} 例： `switch(config)# show monitor session 3`	（任意） ERSPAN セッション設定を表示します。
ステップ 15	**show running-config monitor** 例： `switch(config-erspan-src)# show running-config monitor`	（任意） 実行 ERSPAN コンフィギュレーションを表示します。
ステップ 16	**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 17	**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 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することができます。 同時に実行できる ERSPAN セッションは、Cisco Nexus 5000 シリーズ スイッチでは 2 つだけであるため、セッションをシャットダウンすることにより、ハードウェア リソースを解放して別のセッションをイネーブルにすることができます。 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。

送信元から宛先へのパケットのコピーをアクティブにするために、ERSPAN セッションをイネーブルにすることができます。 すでにイネーブルになっているが、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して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 モードのどちらのコマンドでも使用できます。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**monitor session** {*session-range* | **all**} **shut** 例： `switch(config)# monitor session 3 shut`	指定された 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`	指定された 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になっているが、その動作状況がダウンの場合に、そのセッションをイネーブルにするには、最初に **monitor session shut** コマンドを指定してから、**no monitor session shut** コマンドを続ける必要があります。

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

ステップ 5	**monitor session** *session-number* **type erspan-destination** 例： `switch(config-erspan-src)# monitor session 3 type erspan-destination`	ERSPAN 宛先タイプのモニタ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 6	**shut** 例： `switch(config-erspan-src)# shut`	ERSPAN セッションをシャットダウンします。デフォルトでは、セッションはシャット ステートで作成されます。
ステップ 7	**no shut** 例： `switch(config-erspan-src)# no shut`	ERSPAN セッションをイネーブルにします。 デフォルトでは、セッションはシャット ステートで作成されます。
ステップ 8	**show monitor session all** 例： `switch(config-erspan-src)# show monitor session all`	（任意） ERSPANセッションのステータスを表示します。
ステップ 9	**show running-config monitor** 例： `switch(config-erspan-src)# show running-config monitor`	（任意） 実行 ERSPAN 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	実行 ERSPAN コンフィギュレーションを表示します。
show startup-config monitor	ERSPAN のスタートアップ コンフィギュレーションを表示します。

ERSPAN の設定例

ERSPAN 送信元セッションの設定例

次に、ERSPAN 送信元セッションを設定する例を示します。

```
switch# config t
switch(config)# interface e14/30
switch(config-if)# no shut
switch(config-if)# exit
switch(config)# monitor erspan origin ip-address 3.3.3.3 global
switch(config)# monitor session 1 type erspan-source
switch(config-erspan-src)# source interface e14/30
switch(config-erspan-src)# ip ttl 16
switch(config-erspan-src)# ip dscp 5
switch(config-erspan-src)# vrf default
switch(config-erspan-src)# destination ip 9.1.1.2
switch(config-erspan-src)# no shut
switch(config-erspan-src)# exit
switch(config)# show monitor session 1
```

ERSPAN 宛先セッションの設定例

次に、ERSPAN 宛先セッションを設定する例を示します。

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

その他の参考資料

関連資料

関連項目	マニュアル タイトル
ERSPAN コマンド：コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト設定、使用に関する注意事項、および例	『*Cisco Nexus 3000 Series NX-OS System Management Command Reference*』『*Cisco Nexus 5000 Series NX-OS System Management Command Reference*』

第 18 章

sFLOW の設定

この章は、次の内容で構成されています。

sFlow について

sFlow を使用すると、スイッチやルータを含むデータ ネットワーク内のリアルタイム トラフィックをモニタできます。 sFlow では、トラフィックをモニタするためにスイッチやルータ上の sFlow エージェント ソフトウェアでサンプリング メカニズムを使用して、入力および出力ポート上のサンプル データを中央のデータ コレクタ（sFlow アナライザとも呼ばれる）に転送します。

sFlow の詳細については、RFC 3176 を参照してください。

sFlow エージェント

Cisco NX-OS ソフトウェアに組み込まれている sFlow エージェントは、サンプリングされるパケットのデータ ソースに関連付けられたインターフェイス カウンタを定期的にサンプリングまたは

ポーリングします。 このデータ ソースは、イーサネット インターフェイス、EtherChannel インターフェイス、ある範囲に属するイーサネットインターフェイスのいずれかです。 sFlowエージェントは、イーサネット ポート マネージャにクエリーを送信して対応する EtherChannel メンバーシップ情報を確認するほか、イーサネットポートマネージャからもメンバーシップの変更の通知を受信します。

Cisco NX-OS ソフトウェアで sFlow サンプリングをイネーブルにすると、サンプリング レートとハードウェア内部の乱数に基づいて、入力パケットと出力パケットが sFlow でサンプリングされたパケットとして CPU に送信されます。 sFlow エージェントはサンプリングされたパケットを処理し、sFlow アナライザに sFlow データグラムを送信します。 sFlow データグラムには、元のサンプリングされたパケットに加えて、入力ポート、出力ポート、および元のパケット長に関する情報が含まれます。 sFlow データグラムには、複数の sFlow サンプルを含めることができます。

ライセンスの要件

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。

前提条件

sFlow を設定するには、**feature sflow** コマンドを使用して sFlow 機能をイネーブルにする必要があります。

sFlow の注意事項および制約事項

sFlow の設定を計画する場合、次の点を考慮します。

- インターフェイスの sFlow をイネーブルにすると、入力と出力の両方に対してイネーブルになります。 入力だけまたは出力だけの sFlow をイネーブルにできません。
- マルチキャスト、ブロードキャスト、または未知のユニキャスト パケットの sFlow の出力のサンプリングはサポートされません。
- システムの sFlow の設定およびトラフィックに基づいてサンプリング レートを設定する必要があります。
- Cisco Nexus 3000 シリーズは、1 つの sFlow コレクタだけをサポートします。

sFlow のデフォルト設定

表 *32* : デフォルトの *sFlow* パラメータ

パラメータ	デフォルト
sFlow sampling-rate	4096
sFlow sampling-size	128
sFlow max datagram-size	1400
sFlow collector-port	6343
sFlow counter-poll-interval	20

sFLow の設定

sFlow 機能のイネーブル化

スイッチの sFlow を設定する前に sFlow 機能をイネーブルにする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	[**no**] **feature sflow**	sFlow 機能をイネーブルにします。
ステップ 3	**show feature**	（任意） イネーブルおよびディセーブルにされた機能を表示します。
ステップ 4	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、sFlow 機能をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# feature sflow
switch(config)# copy running-config startup-config
```

サンプリング レートの設定

はじめる前に

sFlow 機能がイネーブルになっていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	[**no**] **sflow sampling-rate** *sampling-rate*	パケットの sFlow のサンプリング レートを設定します。 *sampling-rate* には 4096 ～ 1000000000 間の整数を指定できます。 デフォルト値は 4096 です。 （注） *sampling-rate* を 0 にすると、サンプリングがディセーブルになります。
ステップ 3	**show sflow**	（任意） sFlow 情報を表示します。
ステップ 4	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

次に、サンプリング レートを 50,000 に設定する例を示します。

```
switch# configure terminal
switch(config)# sflow sampling-rate 50000
switch(config)# copy running-config startup-config
```

最大サンプリング サイズの設定

サンプリングされたパケットからコピーする最大バイト数を設定できます。

はじめる前に

sFlow 機能がイネーブルになっていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	[**no**] **sflow max-sampled-size** *sampling-size*	sFlow の最大サンプリング サイズ パケットを設定します。 *sampling-size* の範囲は 64～256 バイトです。 デフォルト値は 128 です。
ステップ 3	**show sflow**	（任意） sFlow 情報を表示します。
ステップ 4	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

次に、sFlow エージェントの最大サンプリング サイズを設定する例を示します。

```
switch# configure terminal
switch(config)# sflow max-sampled-size 200
switch(config)# copy running-config startup-config
```

カウンタのポーリング間隔の設定

データ ソースに関連するカウンタの継続的なサンプル間の最大秒数を設定できます。サンプリング間隔 0 は、カウンタのサンプリングをディセーブルにします。

はじめる前に

sFlow 機能がイネーブルになっていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	[**no**] **sflow counter-poll-interval** *poll-interval*	インターフェイスの sFlow のポーリング間隔を設定します。 *poll-interval* の範囲は 0～2147483647 秒です。 デフォルト値は 20 です。

	コマンドまたはアクション	目的
ステップ 3	**show sflow**	（任意） sFlow 情報を表示します。
ステップ 4	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

次に、インターフェイスの sFlow のポーリング間隔を設定する例を示します。

```
switch# configure terminal
switch(config)# sflow counter-poll-interval 100
switch(config)# copy running-config startup-config
```

最大データグラム サイズの設定

1 つのサンプル データグラムで送信できるデータの最大バイト数を設定できます。

はじめる前に

sFlow 機能がイネーブルになっていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	[**no**] **sflow max-datagram-size** *datagram-size*	sFlow の最大データグラム サイズを設定します。 *datagram-size* の範囲は 200～9000 バイトです。デフォルト値は 1400 です。
ステップ 3	**show sflow**	（任意） sFlow 情報を表示します。
ステップ 4	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

次に、sFlow の最大データグラム サイズを設定する例を示します。

```
switch# configure terminal
switch(config)# sflow max-datagram-size 2000
switch(config)# copy running-config startup-config
[########################################] 100%
```

sFlow アナライザのアドレスの設定

はじめる前に

sFlow 機能がイネーブルになっていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	[**no**] **sflow collector-ip** *IP-address vrf-instance*	sFlow アナライザの IPv4 アドレスを設定します。 *vrf-instance* には次のいずれかを指定できます。 • ユーザ定義の VRF 名。 最大 32 文字の英数字を指定できます。 • **vrf management**。 sFlow データ コレクタが管理ポートに接続されたネットワークに存在する場合は、このオプションを使用する必要があります。 • **vrf default**。 sFlow データ コレクタが前面パネルのポートに接続されたネットワークに存在する場合は、このオプションを使用する必要があります。
ステップ 3	**show sflow**	（任意） sFlow 情報を表示します。
ステップ 4	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

次に、管理ポートに接続されている sFlow データ コレクタの IPv4 アドレスを設定する例を示します。

```
switch# configure terminal
switch(config)# sflow collector-ip 192.0.2.5 vrf management
switch(config)# copy running-config startup-config
```

sFlow アナライザ ポートの設定

sFlow データグラムの宛先ポートを設定できます。

はじめる前に

sFlow 機能がイネーブルになっていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	[**no**] **sflow collector-port** *collector-port*	sFlow アナライザの UDP ポートを設定します。 *collector-port* の範囲は 0～65535 です。 デフォルト値は 6343 です。
ステップ 3	**show sflow**	（任意） sFlow 情報を表示します。
ステップ 4	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

次に、sFlow データグラムの宛先ポートを設定する例を示します。

```
switch# configure terminal
switch(config)# sflow collector-port 7000
switch(config)# copy running-config startup-config
[########################################] 100%
switch(config)#
```

sFlow エージェント アドレスの設定

はじめる前に

sFlow 機能がイネーブルになっていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	[**no**] **sflow agent-ip** *ip-address*	sFlow エージェントの IPv4 アドレスを設定します。 デフォルトの *ip-address* は 0.0.0.0 です。つまり、すべてのサンプリングがスイッチでディセーブルであることを示します。 sFlow 機能をイネーブルにするには、有効な IP アドレスを指定する必要があります。
ステップ 3	**show sflow**	（任意） sFlow 情報を表示します。
ステップ 4	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

次に、sFlow エージェントの IPv4 アドレスを設定する例を示します。

```
switch# configure terminal
switch(config)# sflow agent-ip 192.0.2.3
switch(config)# copy running-config startup-config
```

sFlow サンプリング データ ソースの設定

sFlow のサンプリング データ ソースには、イーサネット ポート、イーサネット ポートの範囲、またはポート チャネルを指定できます。

はじめる前に

- sFlow 機能がイネーブルになっていることを確認します。
- データ ソースとしてポート チャネルを使用する場合は、すでにポート チャネルを設定して、ポート チャネル番号がわかっていることを確認してください。

手順

	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**] **sflow data-source interface** [**ethernet** *slot*/*port*[*-port*] |**port-channel** *channel-number*]	sFlow のサンプリング データ ソースを設定します。 イーサネットのデータ ソースの場合、*slot* はスロット番号、*port* は 1 つのポート番号または *port-port* で指定されたポートの範囲です。
ステップ 3	switch(config)# **show sflow**	（任意） sFlow 情報を表示します。
ステップ 4	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

次に、sFlow のサンプラのイーサネット ポート 5～12 を設定する例を示します。

```
switch# configure terminal
switch(config)# sflow data-source interface ethernet 1/5-12
switch(config)# copy running-config startup-config
[########################################] 100%
switch(config)#
```

次に、sFlow のサンプラのポート チャネル 100 を設定する例を示します。

```
switch# configure terminal
switch(config)# sflow data-source interface port-channel 100
switch(config)# copy running-config startup-config
[########################################] 100%
switch(config)#
```

sFLOW Show コマンド

sFlow の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
show sflow	sFlow のグローバル コンフィギュレーションを表示します。
show sflow statistics	sFlow の統計情報を表示します。

コマンド	目的
clear sflow statistics	sFlow 統計情報をクリアします。
show running-config sflow [all]	現在実行中の sFlow コンフィギュレーションを表示します。

sFlow の設定例

次に sFlow を設定する例を示します。

```
feature sflow
sflow sampling-rate 5000
sflow max-sampled-size 200
sflow counter-poll-interval 100
sflow max-datagram-size 2000
sflow collector-ip 192.0.2.5 vrf management
sflow collector-port 7000
sflow agent-ip 192.0.2.3
sflow data-source interface ethernet 1/5
```

sFlow に関する追加情報

表 *33*：*sFlow* の関連資料

関連項目	マニュアル タイトル
sFlow CLI コマンド	『*Cisco Nexus 3000 Series NX-OS System Management Command Reference*』。
RFC 3176	sFlow のパケット形式と SNMP MIB を定義します。 http://www.sflow.org/rfc3176.txt

sFlow の機能の履歴

この表は、機能の追加または変更が行われたリリースの更新のみを示します。

機能名	リリース	機能情報
sFlow	5.0(3)U4(1)	この機能が導入されました。

索 引

V

あ

い

え

か

き

さ

し

す

せ

そ

た

ち

つ

て

と

は

ひ

ふ

へ

ほ

め

も

ゆ

よ

ら

り

る

れ

ろ