



Cisco Nexus 5000 シリーズ NX-OS システム管理コンフィギュレーションガイドリリース 5.0(3)N1(1)

初版：2011年10月14日

最終更新：2012年02月26日

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>

【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。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザー側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

このマニュアルで使用している IP アドレスは、実際のアドレスを示すものではありません。マニュアル内の例、コマンド出力、および図は、説明のみを目的として使用されています。説明の中に実際のアドレスが使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

© 2011-2012 Cisco Systems, Inc. All rights reserved.



目次

はじめに xi

対象読者 xi

表記法 xi

関連資料 xiii

マニュアルの入手方法およびテクニカル サポート xv

新機能および変更された機能に関する情報 1

このリリースの新規情報および変更情報 1

概要 3

システム管理機能 3

スイッチ プロファイルの設定 9

スイッチ プロファイルに関する情報 10

スイッチ プロファイル コンフィギュレーション モード 10

設定の確認 11

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 12

スイッチ プロファイルの前提条件 13

スイッチ プロファイルの注意事項および制約事項 13

スイッチ プロファイルの設定 14

スイッチ プロファイルへのスイッチの追加 16

スイッチ プロファイルのコマンドの追加または変更 18

スイッチ プロファイルのインポート 21

vPC トポロジでの設定のインポート 23

スイッチ プロファイルのコマンドの確認 23

ピア スイッチの分離 24

スイッチ プロファイルの削除 25

スイッチ プロファイルからのスイッチの削除 26

スイッチ プロファイル設定の show コマンド	27
スイッチ プロファイルの設定例	28
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	28
同期ステータスの確認例	30
実行コンフィギュレーションの表示	31
ローカルとピア スイッチ間のスイッチ プロファイルの同期の表示	32
ローカルおよびピア スイッチでの確認とコミットの表示	33
ローカルおよびピア スイッチ間の成功および失敗した同期の表示	34
スイッチ プロファイルバッファの表示	34
設定のインポート	35
import コマンドを使用したサンプル移行	37
ファブリック エクステンダ A-A トポロジでの Cisco NX-OS Release 5.0(2)N1(1) の移行例	37
ファブリック エクステンダのストレート型トポロジでの Cisco NX-OS Release 5.0(2)N1(1) の移行例	38
設定の同期	39
モジュールの事前プロビジョニングの設定	41
モジュールの事前プロビジョニングに関する情報	41
注意事項および制約事項	42
モジュールの事前プロビジョニングのイネーブル化	42
モジュールの事前プロビジョニングの削除	43
事前プロビジョニングした設定の確認	45
事前プロビジョニングの設定例	45
CFS の使用	47
CFS について	47
CFS 配信	48
CFS の配信モード	48
非協調型配信	49
協調型配信	49
無制限の非協調型配信	49
スイッチ上での CFS 配信のディセーブル化またはイネーブル化	49
CFS 配信ステータスの確認	50

IP を介した CFS 配信	50
ファイバ チャネルを介した CFS 配信	52
CFS 配信の範囲	52
CFS 結合のサポート	53
アプリケーションの CFS サポート	53
CFS のアプリケーション要件	53
アプリケーションに対する CFS のイネーブル化	54
アプリケーション登録ステータスの確認	54
ネットワークのロック	55
CFS ロック ステータスの確認	55
変更のコミット	56
変更の廃棄	56
設定の保存	56
ロック済みセッションのクリア	57
CFS リージョン	57
CFS リージョンの概要	57
シナリオ例	57
CFS リージョンの管理	58
CFS リージョンの作成	58
CFS リージョンへのアプリケーションの割り当て	58
別の CFS リージョンへのアプリケーションの移動	59
リージョンからのアプリケーションの削除	60
CFS リージョンの削除	60
IP を介した CFS の設定	61
IPv4 を介した CFS のイネーブル化	61
IPv6 を介した CFS のイネーブル化	62
IP を介した CFS 設定の確認	63
IP を介した CFS の IP マルチキャストアドレスの設定	63
CFS の IPv4 マルチキャストアドレスの設定	63
CFS の IPv6 マルチキャストアドレスの設定	64
IP を介した CFS の IP マルチキャストアドレス設定の確認	65
CFS 配信情報の表示	65

CFS のデフォルト設定	67
ユーザアカウントと RBAC の設定	69
ユーザアカウントと RBAC の概要	69
ユーザアカウントの設定の制限事項	69
ユーザパスワードの要件	70
ユーザロール	71
ルール	71
ユーザロールポリシー	72
ユーザアカウントの注意事項および制約事項	72
ユーザアカウントの設定	72
RBAC の設定	74
ユーザロールおよびルールの作成	74
機能グループの作成	75
ユーザロールインターフェイスポリシーの変更	76
ユーザロール VLAN ポリシーの変更	77
ユーザロール VSAN ポリシーの変更	78
ユーザアカウントと RBAC の設定の確認	79
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	80
Session Manager の設定	81
Session Manager の概要	81
Session Manager の注意事項および制約事項	82
Session Manager の設定	82
セッションの作成	82
セッションでの ACL の設定	83
セッションの確認	83
セッションのコミット	84
セッションの保存	84
セッションの廃棄	84
Session Manager のコンフィギュレーション例	85
Session Manager 設定の確認	85
オンライン診断の設定	87
オンライン診断について	87

起動時診断	87
ヘルス モニタリング診断	88
拡張モジュール診断	89
オンライン診断の設定	90
オンライン診断設定の確認	91
オンライン診断のデフォルト設定	91
システム メッセージ ログिंगの設定	93
システム メッセージ ログिंगの概要	93
syslog サーバ	94
システム メッセージ ログिंगのライセンス要件	95
システム メッセージ ログिंगの注意事項および制約事項	95
システム メッセージ ログिंगのデフォルト設定	95
システム メッセージ ログिंगの設定	96
ターミナルセッションへのシステム メッセージ ログिंगの設定	96
ファイルへのシステム メッセージ ログिंगの設定	98
モジュールおよびファシリティ メッセージのログिंगの設定	100
ログिंग タイムスタンプの設定	102
syslog サーバの設定	103
UNIX または Linux システムでの syslog の設定	104
syslog サーバ設定の配布の設定	106
ログ ファイルの表示およびクリア	107
システム メッセージ ログिंगの設定確認	108
Smart Call Home の設定	111
Smart Call Home に関する情報	111
Smart Call Home の概要	112
Smart Call Home 宛先プロファイル	112
Smart Call Home アラート グループ	113
Smart Call Home のメッセージ レベル	115
Call Home のメッセージ形式	116
Smart Call Home の注意事項および制約事項	121
Smart Call Home の前提条件	122
Call Home のデフォルト設定	122

Smart Call Home の設定	123
Smart Call Home の登録	123
担当者情報の設定	123
宛先プロファイルの作成	125
宛先プロファイルの変更	127
アラートグループと宛先プロファイルのアソシエーション	129
アラートグループへの show コマンドの追加	130
電子メールサーバの詳細の設定	131
定期的なインベントリ通知の設定	132
重複メッセージ抑制のディセーブル化	133
Smart Call Home のイネーブル化またはディセーブル化	134
Smart Call Home 設定のテスト	135
Smart Call Home 設定の確認	136
フルテキスト形式での syslog アラート通知の例	137
XML 形式での syslog アラート通知の例	137
ロールバックの設定	141
ロールバックの概要	141
注意事項および制約事項	141
チェックポイントの作成	142
ロールバックの実装	143
ロールバック コンフィギュレーションの確認	144
DNS の設定	147
DNS クライアントの概要	147
ネームサーバ	147
DNS の動作	148
ハイアベイラビリティ	148
DNS クライアントの前提条件	148
DNS クライアントのライセンス要件	148
デフォルト設定値	149
DNS クライアントの設定	149
SNMP の設定	153
SNMP について	153

SNMP 機能の概要	153
SNMP 通知	154
SNMPv3	154
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	155
ユーザベースのセキュリティ モデル	156
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	157
グループベースの SNMP アクセス	158
SNMP のライセンス要件	158
SNMP の注意事項および制約事項	158
SNMP のデフォルト設定	158
SNMP の設定	159
SNMP ユーザの設定	159
SNMP メッセージ暗号化の適用	160
SNMPv3 ユーザに対する複数のロールの割り当て	160
SNMP コミュニティの作成	161
SNMP 要求のフィルタリング	161
SNMP 通知レシーバの設定	162
すべての SNMP 通知を送信するための送信元インターフェイスの設定	163
SNMP 通知のホスト レシーバの設定	164
インバンド アクセスのための SNMP の設定	165
SNMP 通知のイネーブル化	166
リンクの通知の設定	168
インターフェイスでのリンク通知のディセーブル化	170
TCP での SNMP に対するワンタイム認証のイネーブル化	170
SNMP スイッチの連絡先および場所の情報の割り当て	170
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	171
SNMP のディセーブル化	172
SNMP の設定の確認	173
RMON の設定	175
RMON について	175
RMON アラーム	176

RMON イベント	176
RMON の設定時の注意事項および制約事項	177
RMON の設定	177
RMON アラームの設定	177
RMON イベントの設定	178
RMON の設定の確認	179
デフォルトの RMON 設定	180
SPAN の設定	181
SPAN に関する情報	182
SPAN 送信元	182
送信元ポートの特性	183
SPAN 宛先	183
宛先ポートの特性	184
SPAN の注意事項および制約事項	184
SPAN セッションの作成または削除	184
イーサネット宛先ポートの設定	185
SPAN セッションごとの MTU の切り捨ての設定	186
SPAN トラフィックのレート制限の設定	187
ファイバチャネル宛先ポートの設定	188
送信元ポートの設定	190
送信元ポートチャネル、VSAN、または VLAN の設定	191
SPAN セッションの説明の設定	192
SPAN セッションのアクティブ化	193
SPAN セッションの一時停止	193
SPAN 情報の表示	194



はじめに

ここでは、次の項について説明します。

- [対象読者](#), [xi ページ](#)
- [表記法](#), [xi ページ](#)
- [関連資料](#), [xiii ページ](#)
- [マニュアルの入手方法およびテクニカル サポート](#), [xv ページ](#)

対象読者

この出版物は Cisco Nexus シリーズ デバイスおよび Cisco Nexus 2000 シリーズ ファブリック エクステンダの設定と保守を行う経験豊富なネットワーク管理者を対象としています。

表記法

コマンドの説明には、次のような表記法が使用されます。

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

例では、次の表記法を使用しています。

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

このマニュアルでは、次の表記法を使用しています。



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

**注意**

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

関連資料

完全な Cisco NX-OS 5000 シリーズ マニュアル セットは、次の URL で入手できます。

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

リリースノート

リリースノートは、次の URL で入手できます。

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

コンフィギュレーションガイド

これらのマニュアルは、次の URL で入手できます。

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

このカテゴリのマニュアルは次のとおりです。

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

メンテナンスおよび操作ガイド

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

インストールガイドおよびアップグレードガイド

これらのマニュアルは、次の URL で入手できます。

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

このカテゴリのマニュアルは次のとおりです。

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

ライセンスガイド

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

コマンドリファレンス

これらのマニュアルは、次の URL で入手できます。

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

このカテゴリのマニュアルは次のとおりです。

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

テクニカル リファレンス

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

エラー メッセージおよびシステム メッセージ

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

トラブルシューティング ガイド

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

マニュアルの入手方法およびテクニカル サポート

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

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

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



第 1 章

新機能および変更された機能に関する情報

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

- [このリリースの新規情報および変更情報, 1 ページ](#)

このリリースの新規情報および変更情報

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

表 1: 新機能

機能	説明	参照先
設定同期	スイッチプロファイルで設定されたポートチャネルメンバーポートの設定の同期の改善。	スイッチプロファイルの設定, (9 ページ)
システムメッセージロギング	8 台の syslog サーバのサポート。	システムメッセージロギングの設定, (93 ページ)
ERSPAN	Encapsulated Remote Switched Port Analyzer (ERSPAN) 機能の設定のサポート。	ERSPAN の設定
IPv6 の SNMP サポート	IPv6 をサポートするための SNMP の機能拡張。	SNMP の設定, (153 ページ)



第 2 章

概要

この章の内容は、次のとおりです。

- [システム管理機能, 3 ページ](#)

システム管理機能

このマニュアルに記載されているシステム管理機能について説明します。

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

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

機能	説明
オンライン診断	<p>Cisco Generic Online Diagnostics (GOLD) では、複数のシスコプラットフォームにまたがる診断操作の共通フレームワークを定義しています。オンライン診断フレームワークでは、中央集中システムおよび分散システムに対応する、プラットフォームに依存しない障害検出アーキテクチャを規定しています。これには共通の診断 CLI とともに、起動時および実行時に診断するための、プラットフォームに依存しない障害検出手順が含まれます。</p> <p>プラットフォーム固有の診断機能は、ハードウェア固有の障害検出テストを行い、診断テストの結果に応じて適切な対策を実行できます。</p>
システム メッセージ ロギング	<p>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。</p> <p>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。</p>
Smart Call Home	<p>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。</p>

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

機能	説明
ERSPAN	<p>Encapsulated Remote Switched Port Analyzer</p> <p>(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。</p> <p>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。</p> <p>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。</p> <p>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。</p>



第 3 章

スイッチ プロファイルの設定

この章の内容は、次のとおりです。

- [スイッチ プロファイルに関する情報, 10 ページ](#)
- [スイッチ プロファイル コンフィギュレーション モード, 10 ページ](#)
- [設定の確認, 11 ページ](#)
- [スイッチ プロファイルを使用したソフトウェアのアップグレードおよびダウングレード, 12 ページ](#)
- [スイッチ プロファイルの前提条件, 13 ページ](#)
- [スイッチ プロファイルの注意事項および制約事項, 13 ページ](#)
- [スイッチ プロファイルの設定, 14 ページ](#)
- [スイッチ プロファイルへのスイッチの追加, 16 ページ](#)
- [スイッチ プロファイルのコマンドの追加または変更, 18 ページ](#)
- [スイッチ プロファイルのインポート, 21 ページ](#)
- [vPC トポロジでの設定のインポート, 23 ページ](#)
- [スイッチ プロファイルのコマンドの確認, 23 ページ](#)
- [ピア スイッチの分離, 24 ページ](#)
- [スイッチ プロファイルの削除, 25 ページ](#)
- [スイッチ プロファイルからのスイッチの削除, 26 ページ](#)
- [スイッチ プロファイル設定の show コマンド, 27 ページ](#)
- [スイッチ プロファイルの設定例, 28 ページ](#)

スイッチ プロファイルに関する情報

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

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

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

スイッチ プロファイル コンフィギュレーション モード

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

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

コンフィギュレーション同期モード

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

スイッチ プロファイル モード

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

スイッチ プロファイル インポート モード

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

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

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

設定の確認

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

- 相互排除チェック
- マージチェック

相互排除チェック

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

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

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

次の例外は相互排除ポリシーに適用されます。

- インターフェイス設定：リリース 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。リリース 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。

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

スイッチ プロファイルの注意事項および制約事項

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

- **mgmt0** インターフェイスを使用してのみ設定同期化をイネーブルにできます。
- 設定の同期は、**mgmt0** インターフェイスを使用して実行され、管理 SVI を使用して実行できません。
- 同じスイッチ プロファイル名で同期されたピアを設定する必要があります。
- スイッチ プロファイル設定で使用可能なコマンドを、設定スイッチ プロファイル (**config-sync-sp**) モードで設定できます。
- サポートされているスイッチ プロファイル コマンドは、**vPC** コマンドに関連します。FCoE コマンドはサポートされません。
- 1つのスイッチ プロファイル セッションを一度に進行できます。別のセッションの開始を試みると失敗します。
- スイッチ プロファイル セッションの進行中は、コンフィギュレーション 端末モードから実行されたサポートされているコマンドの変更はブロックされます。スイッチ プロファイル セッションが進行しているときは、コンフィギュレーション 端末モードからサポートされていないコマンドの変更を行わないでください。
- **commit** コマンドを入力し、ピア スイッチに到達可能である場合、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、コミットを再実行します。
- シスコでは、インターフェイス コンフィギュレーション が設定同期機能を使用して同期される、すべての Generic Expansion Module (GEM) モジュールおよび Cisco Nexus ファブリック エクステンダ モジュールで事前プロビジョニングをイネーブルにすることを推奨します。ファブリック エクステンダが1台のスイッチでオンラインでない可能性があり、その設定が変更され、他のスイッチで同期される、Cisco Nexus ファブリック エクステンダ アクティブ/アクティブ トポロジでは、次の注意事項に従ってください。このシナリオでは、事前プロ

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

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



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

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

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

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



(注) vPC トポロジの Cisco Nexus 5000 シリーズ スイッチまたは Cisco Nexus 2000 シリーズ ファブリック エクステンダをスイッチ プロファイルで置き換える方法については、『Cisco Nexus 5000 Series NX-OS Operations Guide』を参照してください。

スイッチ プロファイルの設定

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

はじめる前に

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	cfs ipv4 distribute 例： switch(config)# cfs ipv4 distribute switch(config)#	ピア スイッチ間の CFS 配信をイネーブルにします。
ステップ 3	config sync 例： switch# config sync switch(config-sync)#	コンフィギュレーション同期モードを開始します。
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。

	コマンドまたはアクション	目的
ステップ 7	exit 例： switch(config-sync-sp)# exit switch#	スイッチプロファイルコンフィギュレーションモードを終了し、EXEC モードに戻ります。
ステップ 8	copy running-config startup-config 例： switch(config)# copy running-config startup-config	(任意) リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を永続的に保存します。

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

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

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

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

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

スイッチ プロファイルへのスイッチの追加

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

スイッチを追加する場合は、次の注意事項に従ってください。

- スイッチは IP アドレスで識別されます。
- 宛先 IP は同期するスイッチの IP アドレスです。

- コミットされたスイッチ プロファイルは、ピア スイッチでも設定の同期が設定されている場合に、新しく追加されたピアと（オンラインの場合）同期されます。

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

はじめる前に

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	config sync 例： switch# config sync switch(config-sync)#	コンフィギュレーション同期モードを開始します。
ステップ 2	switch-profile name 例： switch(config-sync)# switch-profile abc switch(config-sync-sp)#	スイッチ プロファイルを設定し、スイッチ プロファイルの名前を設定し、スイッチ プロファイル同期コンフィギュレーションモードを開始します。
ステップ 3	sync-peers destination destination IP 例： switch(config-sync-sp)# sync-peers destination 10.1.1.1 switch(config-sync-sp)#	スイッチ プロファイルにスイッチを追加します。
ステップ 4	exit 例： switch(config-sync-sp)# exit switch#	スイッチ プロファイルコンフィギュレーションモードを終了します。

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

はじめる前に

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

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	config sync 例： <pre>switch# config sync switch(config-sync)#</pre>	コンフィギュレーション同期モードを開始します。
ステップ 2	switch-profile name 例： <pre>switch(config-sync)# switch-profile abc switch(config-sync-sp)#</pre>	スイッチプロファイルを設定し、スイッチプロファイルの名前を設定し、スイッチプロファイル同期コンフィギュレーションモードを開始します。
ステップ 3	command argument 例： <pre>switch(config-sync-sp)# interface Port-channel100 switch(config-sync-sp-if)# speed 1000 switch(config-sync-sp-if)# interface Ethernet1/1 switch(config-sync-sp-if)# speed 1000 switch(config-sync-sp-if)# channel-group 100</pre>	スイッチプロファイルにコマンドを追加します。
ステップ 4	show switch-profile name buffer 例： <pre>switch(config-sync-sp)# show switch-profile abc buffer switch(config-sync-sp)#</pre>	(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： <pre>switch(config-sync-sp)# verify</pre>	スイッチプロファイルバッファ内のコマンドを確認します。

	コマンドまたはアクション	目的
ステップ 6	commit 例： switch(config-sync-sp)# commit	スイッチ プロファイルにコマンドを保存し、ピアスイッチと設定を同期します。
ステップ 7	show switch-profile name status 例： switch(config-sync-sp)# show switch-profile abc status switch(config-sync-sp)#	(任意) ローカルスイッチのスイッチプロファイルのステータスとピアスイッチのステータスを表示します。
ステップ 8	exit 例： switch(config-sync-sp)# exit switch#	スイッチ プロファイル コンフィギュレーション モードを終了します。
ステップ 9	copy running-config startup-config 例： switch# copy running-config startup-config	(任意) 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

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

```
switch# configuration terminal
switch(config)# cfs ipv4 distribute
switch(config-sync)# switch-profile abc
switch(config-sync-sp)# sync-peers destination 10.1.1.1
switch(config-sync-sp)# interface port-channel100
switch(config-sync-sp-if)# speed 1000
switch(config-sync-sp-if)# interface Ethernet1/1
switch(config-sync-sp-if)# speed 1000
switch(config-sync-sp-if)# channel-group 100
switch(config-sync-sp)# verify
switch(config-sync-sp)# commit
switch(config-sync-sp)# exit
switch#
```

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

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

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

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

```
interface Ethernet1/1
  switchport mode trunk
  switchport trunk allowed vlan 5-10
```

スイッチ プロファイルのインポート

インポートするコマンドのセットに基づいてスイッチプロファイルをインポートできます。コンフィギュレーション端末モードを使用して、次の作業を行います。

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

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

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

手順の概要

1. **config sync**
2. **switch-profile name**
3. **import {interface port/slot | running-config [exclude interface ethernet]}**
4. **commit**
5. (任意) **abort**
6. **exit**
7. (任意) **show switch-profile**
8. (任意) **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	config sync 例： switch# config sync switch(config-sync)#	コンフィギュレーション同期モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	switch-profile name 例： <pre>switch(config-sync)# switch-profile abc switch(config-sync-sp)#</pre>	スイッチ プロファイルを設定し、スイッチ プロファイルの名前を設定し、スイッチプロファイル同期コンフィギュレーション モードを開始します。
ステップ 3	import {interface port/slot running-config [exclude interface ethernet]} 例： <pre>switch(config-sync-sp)# import ethernet 1/2 switch(config-sync-sp-import)#</pre>	インポートするコマンドを識別し、スイッチプロファイルインポート モードを開始します。 <ul style="list-style-type: none"> • <CR>：選択したコマンドを追加します。 • interface：指定したインターフェイスのサポートされるコマンドを追加します。 • running-config：サポートされるシステムレベル コマンドを追加します。 • running-config exclude interface ethernet：物理インターフェイス コマンドを除く、サポートされるシステムレベル コマンドを追加します。
ステップ 4	commit 例： <pre>switch(config-sync-sp-import)# commit</pre>	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： <pre>switch(config-sync-sp-import)# abort</pre>	(任意) インポート プロセスを中止します。
ステップ 6	exit 例： <pre>switch(config-sync-sp)# exit switch#</pre>	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： <pre>switch# show switch-profile</pre>	(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： <pre>switch# copy running-config startup-config</pre>	(任意) 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

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

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

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

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

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

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

vPC トポロジでの設定のインポート

2 スイッチ vPC トポロジで設定をインポートできます。



(注) 次の手順の詳細については、この章の該当する項を参照してください。

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



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

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

スイッチ プロファイルのコマンドの確認

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	config sync 例： switch# config sync switch(config-sync)#	コンフィギュレーション同期モードを開始します。
ステップ 2	switch-profile name 例： switch(config-sync)# switch-profile abc switch(config-sync-sp)#	スイッチプロファイルを設定し、スイッチプロファイルの名前を設定し、スイッチプロファイル同期コンフィギュレーションモードを開始します。
ステップ 3	verify 例： switch(config-sync-sp)# verify	スイッチプロファイルバッファ内のコマンドを確認します。
ステップ 4	exit 例： switch(config-sync-sp)# exit switch#	スイッチプロファイル コンフィギュレーション モードを終了します。
ステップ 5	copy running-config startup-config 例： switch# copy running-config startup-config	(任意) 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

ピア スイッチの分離

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

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



(注) 次の手順の詳細については、この章の該当する項を参照してください。

一時的にピア スイッチを分離するには、次の手順を実行します。

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

スイッチ プロファイルの削除

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

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	config sync 例： switch# config sync switch(config-sync)#	コンフィギュレーション同期モードを開始します。
ステップ 2	no switch-profile name {all-config local-config}	次の手順に従って、スイッチ プロファイルを削除します。 • all-config : ローカル スイッチおよびピア スイッチのスイッチ プロファイルを削除します。ピア スイッチ

	コマンドまたはアクション	目的
	例 : <pre>switch(config-sync)# no switch-profile abc local-config switch(config-sync-sp)#</pre>	が到達可能でない場合は、ローカルスイッチプロファイルだけが削除されます。 • local-config : スイッチ プロファイルおよびローカルコンフィギュレーションを削除します。
ステップ 3	exit 例 : <pre>switch(config-sync-sp)# exit switch#</pre>	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 : <pre>switch# copy running-config startup-config</pre>	(任意) 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

スイッチ プロファイルからのスイッチの削除

スイッチ プロファイルからスイッチを削除できます。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	config sync 例 : <pre>switch# config sync switch(config-sync)#</pre>	コンフィギュレーション同期モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	switch-profile name 例： switch(config-sync)# switch-profile abc switch(config-sync-sp)#	スイッチプロファイルを設定し、スイッチプロファイルの名前を設定し、スイッチプロファイル同期コンフィギュレーション モードを開始します。
ステップ 3	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。
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 expand-port-profile	ポート プロファイルについての詳細が表示されます。
show running-config exclude-provision	オフラインで事前プロビジョニングされた非表示のインターフェイスの設定を表示します。
show running-config switch-profile	ローカルスイッチのスイッチプロファイルの実行コンフィギュレーションを表示します。
show startup-config switch-profile	ローカルスイッチのスイッチプロファイルのスタートアップコンフィギュレーションを表示します。

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

スイッチ プロファイルの設定例

ローカルおよびピア スイッチでのスイッチ プロファイルの作成例

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
<p>ステップ 1</p>	<p>ローカルおよびピア スイッチで CFSoIP 配信をイネーブルにします。</p> <p>例： switch# configuration terminal switch(config)# cfs ipv4 distribute</p>	
<p>ステップ 2</p>	<p>ローカルおよびピア スイッチでスイッチ プロファイルを作成します。</p> <p>例： switch(config-sync)# switch-profile abc switch(config-sync-sp)# sync-peers destination 10.1.1.1</p>	
<p>ステップ 3</p>	<p>スイッチ プロファイルが、ローカルおよびピア スイッチで同じであることを確認します。</p> <p>例： switch(config-sync-sp)# show switch-profile abc status</p> <pre> 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) :</pre>	
<p>ステップ 4</p>	<p>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。</p> <p>例： switch(config-sync-sp)# class-map type qos c1 switch(config-sync-sp-cmap-qos)# match cos 2 switch(config-sync-sp-cmap-qos)# class-map type qos c2 switch(config-sync-sp-cmap-qos)# match cos 5 switch(config-sync-sp-cmap-qos)# policy-map type qos p1 switch(config-sync-sp-pmap-qos)# class c1 switch(config-sync-sp-pmap-c-qos)# set qos-group 2 switch(config-sync-sp-pmap-c-qos)# class c2 switch(config-sync-sp-pmap-c-qos)# set qos-group 3 switch(config-sync-sp-pmap-c-qos)# system qos switch(config-sync-sp-sys-qos)# service-policy type qos input p1 switch(config-sync-sp-sys-qos)# vlan 1-50</p>	

	コマンドまたはアクション	目的
	<pre>switch(config-sync-sp-vlan)# interface port-channel 100 switch(config-sync-sp-if)# vpc peer-link switch(config-sync-sp-if)# switchport mode trunk switch(config-sync-sp-if)# interface port-channel 10 switch(config-sync-sp-if)# vpc 1 switch(config-sync-sp-if)# switchport mode trunk switch(config-sync-sp-if)# switchport trunk allowed vlan 1, 10-50</pre>	
ステップ 5	<p>バッファ リングされたコマンドを表示します。</p> <p>例 :</p> <pre>switch(config-sync-sp-if)# show switch-profile switch-profile buffer</pre> <pre>----- Seq-no Command ----- 1 class-map type qos match-all c1 1.1 match cos 2 2 class-map type qos match-all c2 2.1 match cos 5 3 policy-map type qos p1 3.1 class c1 3.1.1 set qos-group 2 3.2 class c2 3.2.1 set qos-group 3 4 system qos 4.1 service-policy type qos input p1 5 vlan 2-50 6 interface port-channel100 6.1 vpc peer-link 6.2 switchport mode trunk 7 interface port-channel10 7.1 vpc 1 7.2 switchport mode trunk 7.3 switchport trunk allowed vlan 1, 10-50</pre>	
ステップ 6	<p>スイッチ プロファイルのコマンドを検証します。</p> <p>例 :</p> <pre>switch(config-sync-sp-if)# verify Verification Successful</pre>	
ステップ 7	<p>スイッチ プロファイルにコマンドを適用し、ローカルとピア スイッチ間の設定を同期させます。</p> <p>例 :</p> <pre>switch(config-sync-sp)# commit Commit Successful switch(config-sync)#</pre>	

同期ステータスの確認例

次に、ローカルとピア スイッチ間の同期ステータスを確認する例を示します。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<p>show switch-profile switch-profile status コマンドを入力します。</p> <p>例 :</p> <pre>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)#</pre>	

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設定する例を示します。

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

interface port-channel10
  switchport mode trunk
```

```
vpc 1
switchport trunk allowed vlan 1,10-50

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

ローカル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台のピア間の最初の正常な同期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#
```


ローカルおよびピアスイッチでの確認とコミットの表示

次に、ローカル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.
sw01(config-sync)# switch-profile sp
Switch-Profile started, Profile ID is 1
sw01(config-sync-sp)# interface Ethernet1/1
sw01(config-sync-sp-if)# description foo
sw01(config-sync-sp-if)# verify
Verification Successful
sw01(config-sync-sp)# commit
Commit Successful
sw01(config-sync)# show running-config switch-profile
switch-profile sp
  sync-peers destination 10.193.194.52
  interface Ethernet1/1
    description foo
sw01(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#
```

ローカルおよびピア スイッチ間の成功および失敗した同期の表示

次に、ピア スイッチでスイッチ プロファイルの同期ステータスを設定する例を示します。最初の例は正常な同期を示し、2 番目の例はピアの到達不能な状態を示します。

例 1 :

```
switch1# show switch-profile abc peer

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

例 2 :

```
switch1# 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)        :
switch1#
```

スイッチ プロファイル バッファの表示

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

```
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)# vlan 101
switch1(config-sync-sp-vlan)# ip igmp snooping querier 10.101.1.1
switch1(config-sync-sp-vlan)# exit
switch1(config-sync-sp)# mac address-table static 0000.0000.0001 vlan 101 drop
switch1(config-sync-sp)# interface Ethernet1/2
switch1(config-sync-sp-if)# switchport mode trunk
switch1(config-sync-sp-if)# switchport trunk allowed vlan 101
switch1(config-sync-sp-if)# exit
switch1(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

switch1(config-sync-sp)# buffer-move 3 1
switch1(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
```

```

switch1(config-sync-sp)# buffer-delete 1
switch1(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

switch1(config-sync-sp)# buffer-delete all
switch1(config-sync-sp)# show switch-profile sp buffer
switch1(config-sync-sp)#

```

設定のインポート

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

```

switch# show running-config interface Ethernet1/3

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

version 5.0(2)N1(1)

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

switch# configure sync
Enter configuration commands, one per line.  End with CNTL/Z.
sw01(config-sync)# switch-profile sp
Switch-Profile started, Profile ID is 1

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

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

```

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

```

switch(config-sync)# switch-profile sp
Switch-Profile started, Profile ID is 1
switch(config-sync-sp)# import running-config
switch(config-sync-sp-import)# show switch-profile sp buffer
-----
Seq-no  Command
-----
1      logging event link-status default
2      vlan 1
3      port-profile type ethernet ppl
3.1    bandwidth 5000
3.2    bandwidth inherit
3.3    speed 10000
3.4    state enabled
4      interface port-channel3
4.1    switchport mode trunk
4.2    vpc peer-link
4.3    spanning-tree port type network
5      interface port-channel30

```

```

5.1      switchport mode trunk
5.2      vpc 30
5.3      switchport trunk allowed vlan 2-10
6        interface port-channel31
6.1      switchport mode trunk
6.2      vpc 31
6.3      switchport trunk allowed vlan 11-20
7        interface port-channel101
7.1      switchport mode fex-fabric
7.2      fex associate 101
8        interface port-channel102
8.1      switchport mode fex-fabric
8.2      vpc 102
8.3      fex associate 102
9        interface port-channel103
9.1      switchport mode fex-fabric
9.2      vpc 103
9.3      fex associate 103
10       interface Ethernet1/1
11       interface Ethernet1/2
12       interface Ethernet1/3
13       interface Ethernet1/4
13.1     switchport mode trunk
13.2     channel-group 3
14       interface Ethernet1/5
14.1     switchport mode trunk
14.2     channel-group 3
15       interface Ethernet1/6
15.1     switchport mode trunk
15.2     channel-group 3
16       interface Ethernet1/7
16.1     switchport mode trunk
16.2     channel-group 3
17       interface Ethernet1/8
18       interface Ethernet1/9
18.1     switchport mode trunk
18.2     switchport trunk allowed vlan 11-20
18.3     channel-group 31 mode active
19       interface Ethernet1/10
19.1     switchport mode trunk
19.2     switchport trunk allowed vlan 11-20
19.3     channel-group 31 mode active
20       interface Ethernet1/11
21       interface Ethernet1/12
...
45       interface Ethernet2/4
45.1     fex associate 101
45.2     switchport mode fex-fabric
45.3     channel-group 101
46       interface Ethernet2/5
46.1     fex associate 101
46.2     switchport mode fex-fabric
46.3     channel-group 101
47       interface Ethernet2/6
47.1     fex associate 101
47.2     switchport mode fex-fabric
47.3     channel-group 101
48       interface Ethernet2/7
48.1     fex associate 101
48.2     switchport mode fex-fabric
48.3     channel-group 101
49       interface Ethernet2/8
49.1     fex associate 101
...
89       interface Ethernet100/1/32
90       interface Ethernet100/1/33
91       interface Ethernet100/1/34
92       interface Ethernet100/1/35
93       interface Ethernet100/1/36
...
105      interface Ethernet100/1/48
switch(config-sync-sp-import)#

```

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

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

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

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

switch#

switch# configure sync
Enter configuration commands, one per line.  End with CNTL/Z.
sw01(config-sync)# switch-profile sp
Switch-Profile started, Profile ID is 1
switch(config-sync-sp)# import
switch(config-sync-sp-import)# port-profile type ethernet ppl
switch(config-sync-sp-import-if)# bandwidth 5000
switch(config-sync-sp-import-if)# bandwidth inherit
switch(config-sync-sp-import-if)# speed 10000
switch(config-sync-sp-import-if)# state enabled
switch(config-sync-sp-import-if)# show switch-profile sp buffer
-----
Seq-no  Command
-----
1       port-profile type ethernet ppl
1.1    bandwidth 5000
1.2    bandwidth inherit
1.3    speed 10000
1.4    state enabled

switch(config-sync-sp-import-if)# verify
Verification Successful
switch(config-sync-sp-import)# commit
Commit Successful
sw01(config-sync)# show running-config switch-profile
switch-profile sp
  sync-peers destination 10.193.194.52
  port-profile type ethernet ppl
  bandwidth 5000
  bandwidth inherit
  speed 10000
  state enabled
switch(config-sync)#
```

import コマンドを使用したサンプル移行

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

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

手順の概要

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

手順の詳細

-
- ステップ 1** 設定が両方のスイッチで同じであることを確認します。
- ステップ 2** 両方のスイッチで、同じ名前を持つスイッチ プロファイルを設定します。
- ステップ 3** 両方のスイッチで **import running config** コマンドを入力します。
- ステップ 4** **switch-profile name buffer** コマンドを入力し、すべての設定が両方のスイッチで正しくインポートされていることを確認します。
- ステップ 5** バッファを編集して不要な設定を削除します。
詳細については、[スイッチ プロファイル バッファの表示](#)、(34 ページ) を参照してください。
- ステップ 6** 両方のスイッチで **commit** コマンドを入力します。
- ステップ 7** 両方のスイッチでピア スイッチを設定するには、**sync-peers destination IP-address** コマンドを入力します。
- ステップ 8** 両方のスイッチが同期されていることを確認するには、**switch-profile name status** コマンドを入力します。
-

ファブリックエクステンダのストレート型トポロジでのCisco NX-OS Release 5.0(2)N1(1)の移行例

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

手順の概要

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

手順の詳細

-
- ステップ 1** vPC ポートチャネルの設定が、両方のスイッチで同じであることを確認します。
- ステップ 2** 両方のスイッチで、同じ名前を持つスイッチ プロファイルを設定します。
- ステップ 3** 両方のスイッチのすべての vPC ポートチャネルについて、**import interface port-channel *x-y*, port-channel *z*** コマンドを入力します。
- ステップ 4** **show switch-profile *name* buffer** コマンドを入力し、すべての設定が両方のスイッチで正しくインポートされていることを確認します。
- ステップ 5** バッファを編集して不要な設定を削除します。
詳細については、[スイッチ プロファイル バッファの表示](#)、(34 ページ) を参照してください。
- ステップ 6** 両方のスイッチで **commit** コマンドを入力します。
- ステップ 7** 両方のスイッチでピア スイッチを設定するには、**sync-peers destination *IP-address*** コマンドを入力します。
- ステップ 8** 両方のスイッチが同期されていることを確認するには、**show switch-profile *name* status** コマンドを入力します。
-

設定の同期

スイッチのリブート後の設定の同期

新しい設定をスイッチ プロファイルを使用してピア スイッチにコミットする間に 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ように、次の手順を実行します。

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

vPC ピア リンクに障害が発生した場合の設定の同期化

ピアリンクに失敗したが、両方のスイッチが動作状態であれば、セカンダリ スイッチはその vPC ポートをシャットダウンします。ファブリック エクステンダ A/A トポロジでは、A/A ファブリック エクステンダがセカンダリで切断されます。設定がプライマリ スイッチのスイッチ プロファイルで変更された場合、設定はセカンダリ スイッチで A/A ファブリック エクステンダが事前プロビジョニングされていない限り受け入れられません。したがって、設定の同期機能を使用する際に、すべての A/A ファブリック エクステンダを事前プロビジョニングすることを推奨します。

mgmt0 インターフェイスの接続が失われた場合の設定の同期化

mgmt0 インターフェイスの接続が失われ、設定変更が必要な場合は、スイッチ プロファイルを使用して、両方のスイッチ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、両方のスイッチが同期されます。

このシナリオで設定変更が1台のスイッチのみで実行された場合、マージは、mgmt0 インターフェイスが起動し、設定が他のスイッチに適用されたときに成功します。

ISSU が1台のスイッチで実行され、設定変更がピア スイッチ上で行われた場合の設定の同期

vPC トポロジでは、ISSU が一方のスイッチで実行されている場合は、ピア スイッチで設定の変更はできません。vPC のないトポロジでは、設定変更は許可され、アップグレードが完了すると、ISSU を実行しているスイッチは新しい設定を同期します。



第 4 章

モジュールの事前プロビジョニングの設定

この章の内容は、次のとおりです。

- [モジュールの事前プロビジョニングに関する情報, 41 ページ](#)
- [注意事項および制約事項, 42 ページ](#)
- [モジュールの事前プロビジョニングのイネーブル化, 42 ページ](#)
- [モジュールの事前プロビジョニングの削除, 43 ページ](#)
- [事前プロビジョニングした設定の確認, 45 ページ](#)
- [事前プロビジョニングの設定例, 45 ページ](#)

モジュールの事前プロビジョニングに関する情報

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

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

サポートされているハードウェア

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

アップグレードおよびダウングレード

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

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

注意事項および制約事項

事前プロビジョニング設定時の注意事項と制限事項は次のとおりです。

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

モジュールの事前プロビジョニングのイネーブル化

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



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

手順の概要

1. `configuration terminal`
2. `slot slot`
3. `provision model model`
4. `exit`
5. (任意) `copy running-config startup-config`

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configuration terminal 例： switch# config t switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	slot slot 例： switch(config)# slot 101 switch(config-slot)#	事前プロビジョニングするスロットを選択し、スロット コンフィギュレーション モードを開始します。
ステップ 3	provision model model 例： switch(config-slot)# provision model N2K-C2248T switch(config-slot)#	事前プロビジョニングするモジュールを選択します。
ステップ 4	exit 例： switch(config-slot)# exit switch#	スロット コンフィギュレーション モードを終了します。
ステップ 5	copy running-config startup-config 例： switch# copy running-config startup-config	(任意) 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

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

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

モジュールの事前プロビジョニングの削除

事前プロビジョニングされたモジュールを削除できます。

手順の概要

1. **configuration terminal**
2. **slot slot**
3. **no provision model model**
4. **exit**
5. (任意) **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configuration terminal 例： switch# config t switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	slot slot 例： switch(config)# slot 101 switch(config-slot)#	事前プロビジョニングするスロットを選択し、スロット コンフィギュレーション モードを開始します。
ステップ 3	no provision model model 例： switch(config-slot)# no provision model N2K-C2248T switch(config-slot)#	モジュールから事前プロビジョニングを削除します。
ステップ 4	exit 例： switch(config-slot)# exit switch#	スロット コンフィギュレーション モードを終了します。
ステップ 5	copy running-config startup-config 例： switch# copy running-config startup-config	(任意) 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

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

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

事前プロビジョニングした設定の確認

事前プロビジョニングした設定を表示するには、次のいずれかの作業を行います。

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

事前プロビジョニングの設定例

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

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

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

version 5.0(2)N1(1)

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

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

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

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

```
interface Ethernet101/1/2
  service-policy input test
```

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

次に、スロットから事前プロビジョニングされたすべてのモジュールを削除する例を示します。

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



第 5 章

CFS の使用

この章の内容は、次のとおりです。

- [CFS について, 47 ページ](#)
- [CFS 配信, 48 ページ](#)
- [アプリケーションの CFS サポート, 53 ページ](#)
- [CFS リージョン, 57 ページ](#)
- [IP を介した CFS の設定, 61 ページ](#)
- [CFS 配信情報の表示, 65 ページ](#)
- [CFS のデフォルト設定, 67 ページ](#)

CFS について

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

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

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

CFS には次の機能があります。

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

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

IP を介した CFS 配信では、次の機能がサポートされます。

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

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

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

CFS 配信

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

CFS の配信モード

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

- 非協調型配信
- 協調型配信
- 無制限の非協調型配信

常に 1 つのモードだけを適用できます。

非協調型配信

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

協調型配信

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

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

協調型配信には、次の 2 種類があります。

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

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

無制限の非協調型配信

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

スイッチ上での CFS 配信のディセーブル化またはイネーブル化

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

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# no cfs distribute	スイッチ上のすべてのアプリケーションに対して、CFS 配信（ファイバチャネルまたは IP を介した CFS）をグローバルにディセーブルにします。
ステップ 3	switch(config)# cfs distribute	(任意) スイッチ上の CFS 配信をイネーブルにします。これはデフォルトです。

CFS 配信ステータスの確認

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

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

IP を介した CFS 配信

IP を介した CFS 配信は次の機能をサポートしています。

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



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

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

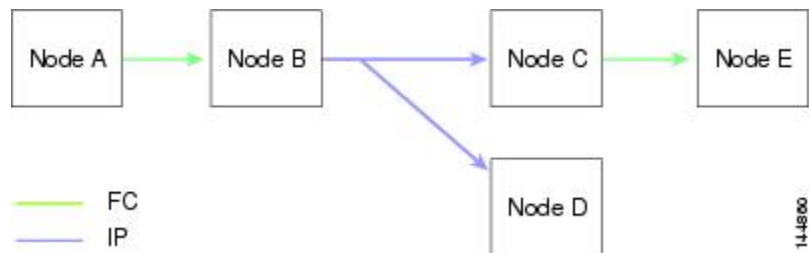


(注) CFS は同じスイッチから IPv4 と IPv6 の両方を介しては配信できません。

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

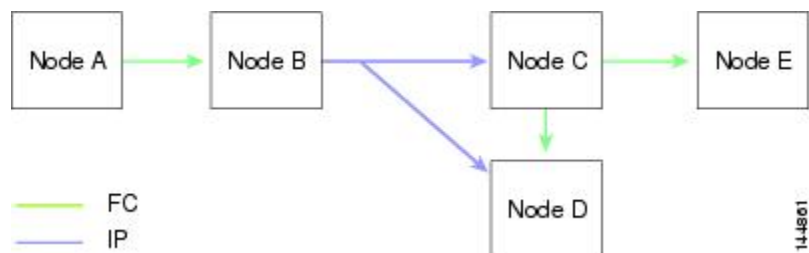
次の図 (ネットワーク例 1) は、ファイバチャネル接続と IP 接続の両方を使用したネットワークを示します。ノード A はファイバチャネルを介してノード B にイベントを転送します。ノード B はユニキャスト IP を使用してノード C とノード D にイベントを転送します。ノード C はファイバチャネルを介してノード E にイベントを転送します。

図 1: ファイバチャネル接続と IP 接続を使用するネットワーク例 1



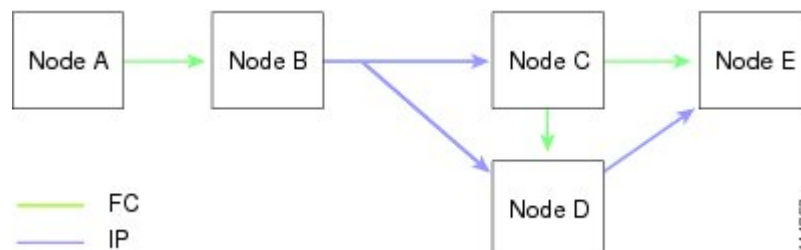
次の図 (ネットワーク例 2) は前の図と同じです。ただし、ノード C とノード D はファイバチャネルを使用して接続しています。ノード B にはノード C とノード D の IP 用配信リストがあるので、この例のすべてのプロセスは同じです。ノード D はすでにノード B からの配信リストに入っているため、ノード C はノード D に転送しません。

図 2: ファイバチャネル接続と IP 接続を使用するネットワーク例 2



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

図 3: ファイバチャネル接続と IP 接続を使用するネットワーク例 3



ファイバチャネルを介した CFS 配信

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

CFS 配信の範囲

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

- VSAN レベル（論理スコープ）

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



（注） IP を介した CFS 配信では、論理範囲はサポートされません。

- 物理トポロジ レベル（物理スコープ）

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

- 選択された 2 つのスイッチ間

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

CFS 結合のサポート

CFS 結合は、ファイバチャネルを介した CFS 配信でサポートされます。

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

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

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

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

アプリケーションの CFS サポート

CFS のアプリケーション要件

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

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

- アプリケーション単位でイネーブル化またはディセーブル化される CFS 配信：CFS 配信ステータスのデフォルト（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、一時的な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テータスの確認

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 番目のカラムは、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（logical、physical、またはその両方）。



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

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

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

```
switch# show cfs application name fscm

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

ネットワークのロック

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

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

CFS ロック ステータスの確認

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

```
switch# show cfs lock

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

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

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

```
switch# show cfs lock name ntp

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

Total number of entries = 1
```

変更のコミット

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

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

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

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

commit コマンドを入力すると、指定した機能の変更をコミットできます。

変更の廃棄

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

abort コマンドを入力すると、指定した機能の変更を廃棄できます。

設定の保存

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



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

ロック済みセッションのクリア

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



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

CFS リージョン

CFS リージョンの概要

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



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

シナリオ例

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

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

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

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

CFS リージョンの管理

CFS リージョンの作成

CFS リージョンを作成できます。

手順の概要

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

手順の詳細

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

CFS リージョンへのアプリケーションの割り当て

スイッチでリージョンにアプリケーションを割り当てることができます。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# cfs region region-id	リージョンを作成します。
ステップ 3	switch(config-cfs-region)# <i>application</i>	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、 「Application already present in the same region」 というエラーメッセージが表示されます。

次に、リージョンにアプリケーションを割り当てる例を示します。

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

別の CFS リージョンへのアプリケーションの移動

あるリージョンから別のリージョンにアプリケーションを移動できます。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# configure	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# cfs region region-id	CFS リージョン サブモードを開始します。
ステップ 3	switch(config-cfs-region)# <i>application</i>	あるリージョンから別のリージョンに移動するアプリケーションを示します。 (注) 同じリージョンにアプリケーションを複数回移動しようとする、 「Application already present in the same region」 というエラーメッセージが表示されます。

	コマンドまたはアクション	目的
--	--------------	----

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

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

リージョンからのアプリケーションの削除

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

手順の概要

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

手順の詳細

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

CFS リージョンの削除

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

手順の概要

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

手順の詳細

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

IP を介した CFS の設定

IPv4 を介した CFS のイネーブル化

IPv4 を介した CFS をイネーブルまたはディセーブルにできます。



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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# configure	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# cfs ipv4 distribute	スイッチのすべてのアプリケーションに対して IPv6 を介した CFS をグローバルでイネーブルにします。

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

IPv6 を介した CFS のイネーブル化

IPv6 を介した CFS をイネーブルまたはディセーブルにできます。



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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# configure	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# cfs ipv6 distribute	スイッチのすべてのアプリケーションに対して IPv6 を介した CFS をグローバルでイネーブルにします。
ステップ 3	switch(config)# no cfs ipv6 distribute	(任意) スイッチの IPv6 を介した CFS をディセーブルにします (デフォルト)。

IP を介した CFS 設定の確認

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

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

IP を介した CFS の IP マルチキャストアドレスの設定

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



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

CFS の IPv4 マルチキャストアドレスの設定

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

手順の概要

1. switch# **configure**
2. switch(config)# **cfs ipv4 mcast-address ipv4-address**
3. (任意) switch(config)# **no cfs ipv4 mcast-address ipv4-address**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# configure	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# cfs ipv4 mcast-address ipv4-address	IPv4 を介した CFS 配信の IPv4 マルチキャストアドレスを設定します。 有効な IPv4 アドレスの範囲は 239.255.0.0 ~ 239.255.255.255 および 239.192/16 ~ 239.251/16 です。

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

CFS の IPv6 マルチキャストアドレスの設定

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

手順の概要

1. `switch# configure`
2. `switch(config)# cfs ipv6 mcast-address ipv4-address`
3. (任意) `switch(config)# no cfs ipv6 mcast-address ipv4-address`

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<code>switch# configure</code>	コンフィギュレーションモードを開始します。
ステップ 2	<code>switch(config)# cfs ipv6 mcast-address ipv4-address</code>	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	<code>switch(config)# no cfs ipv6 mcast-address ipv4-address</code>	(任意) IPv6 を介した CFS 配信のデフォルトの IPv6 マルチキャストアドレスに戻します。IP を介した CFS のデフォルトの IPv6 マルチキャストアドレスは ff15::efff:4653 です。

IP を介した CFS の IP マルチキャストアドレス設定の確認

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

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

CFS 配信情報の表示

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

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

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

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

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

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

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

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

```

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

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

```

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

```

switch# show cfs peers

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

Total number of entries = 2

```

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

```

switch# show cfs peers name ntp

Scope      : Physical

-----

Switch WWN                IP Address
-----

20:00:00:44:22:00:4a:9e  172.22.92.27    [Local]
20:00:00:05:30:01:1b:c2  172.22.92.215

```

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

```

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

-----

Domain   Switch WWN                IP Address
-----

124      20:00:00:44:22:00:4a:9e  172.22.92.27    [Local]
98       20:00:00:05:30:01:1b:c2  172.22.92.215

Total number of entries = 2

```

```

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

Total number of entries = 2

```

CFS のデフォルト設定

次の表に、CFS のデフォルト設定を示します。

表 2: デフォルトの CFS パラメータ

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

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



第 6 章

ユーザアカウントと RBAC の設定

この章の内容は、次のとおりです。

- [ユーザアカウントと RBAC の概要, 69 ページ](#)
- [ユーザアカウントの注意事項および制約事項, 72 ページ](#)
- [ユーザアカウントの設定, 72 ページ](#)
- [RBAC の設定, 74 ページ](#)
- [ユーザアカウントと RBAC の設定の確認, 79 ページ](#)
- [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, 80 ページ](#)

ユーザアカウントと RBAC の概要

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

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

ユーザ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	ftuser
games	gdm	gopher	halt	lp
mail	mailnull	man	mtsuser	news

nobody	nscd	operator	rpc	rpcuser
shutdown	sync	sys	uucp	xfs

**注意**

Cisco Nexus 5000 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 5000 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 5000 シリーズ スイッチはパスワードを拒否します。各ユーザアカウントには強力なパスワードを設定するようにしてください。強固なパスワードは、次の特性を持ちます。

- 長さが 8 文字以上である
- 複数の連続する文字 (「abcd」など) を含んでいない
- 複数の同じ文字の繰返し (「aaabbb」など) を含んでいない
- 辞書に載っている単語を含んでいない
- 固有名詞を含んでいない
- 大文字および小文字の両方が含まれている
- 数字が含まれている

強固なパスワードの例を次に示します。

- If2CoM18
- 2009AsdfLkj30
- Cb1955S21

**(注)**

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

ユーザーロール

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

Cisco Nexus 3000 シリーズ スイッチは、次のデフォルトのユーザーロールを提供します。

- **network-admin** (スーパーユーザー) : スイッチ全体に対して完全な読み取りと書き込みのアクセス権を持ちます。
- **network-operator** : スイッチに対して完全な読み取りアクセス権を持ちます。



(注) 複数のロールに属するユーザーは、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、ユーザーが、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、同じユーザーがロール **B** も持ち、このロールではコンフィギュレーションコマンドにアクセスできるとします。この場合、このユーザーはコンフィギュレーションコマンドにアクセスできます。

ルール

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

- **Command** : コマンドまたは正規表現で定義された一連のコマンド。
- **Feature** : Cisco Nexus 5000 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。
- **Feature group** : デフォルトまたはユーザー定義の機能グループ。
 - **show role feature-group** コマンドを入力すれば、このパラメータに指定できるデフォルトの機能グループが表示されます。

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

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

ユーザロールポリシー

ユーザロールポリシーを定義することにより、ユーザがアクセスできるスイッチリソースを制限できます。インターフェイス、VLAN、およびVSAN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ルールで制約されます。たとえば、特定のインターフェイスへのアクセスを許可するインターフェイスポリシーを定義した場合、**interface** コマンドを許可するコマンドルールをロールに設定しないと、ユーザはインターフェイスにアクセスできません。

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

ユーザアカウントの注意事項および制約事項

ユーザアカウントとRBACには、次の設定ガイドラインと制限事項があります。

- ユーザロールには最大 256 個の規則を追加できます。
- 1つのユーザアカウントに最大 64 個のユーザロールを割り当てられます。



(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

1台のCisco Nexus シリーズスイッチ上に最大 256 個のユーザアカウントを作成できます。ユーザアカウントは、次の属性を持ちます。

- ユーザ名
- パスワード
- 失効日
- ユーザロール

ユーザアカウントは、最大 64 個のユーザロールを持つことができます。



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

手順の概要

1. (任意) switch(config)# **show role**
2. switch# **configure terminal**
3. switch(config)# **username user-id [password password] [expire date] [role role-name]**
4. (任意) switch# **show user-account**
5. (任意) switch# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch(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 2	switch# configure terminal	コンフィギュレーションモードに入ります。
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。 <i>user-id</i> は、最大 28 文字の英数字のストリングで、大文字と小文字が区別されます。 デフォルト パスワードは定義されていません。 (注) パスワードを指定しなかった場合、ユーザは Cisco Nexus 5000 シリーズ スイッチにログインできない場合があります。 <i>expire date</i> オプションの形式は、YYYY-MM-DD です。デフォルトでは、失効日はありません。
ステップ 4	switch# show user-account	(任意) ロール設定を表示します。
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、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

各ユーザ ロールが、最大 256 個のルールを持つことができます。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。

指定するルール番号は、適用する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 つのルールが 3 つのルールを持っている場合、ルール 3 がルール 2 よりも前に適用され、ルール 2 はルール 1 よりも前に適用されます。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **role name** *role-name*
3. switch(config-role)# **rule number** {deny | permit} **command** *command-string*
4. switch(config-role)# **rule number** {deny | permit} {read | read-write}
5. switch(config-role)# **rule number** {deny | permit} {read | read-write} **feature** *feature-name*
6. switch(config-role)# **rule number** {deny | permit} {read | read-write} **feature-group** *group-name*
7. (任意) switch(config-role)# **description** *text*
8. (任意) switch# **show role**
9. (任意) switch# **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
		必要なルールの数だけこのコマンドを繰り返します。
ステップ 4	<code>switch(config-role)# rule number {deny permit} {read read-write}</code>	すべての操作の読み取り専用ルールまたは読み取り/書き込みルールを設定します。
ステップ 5	<code>switch(config-role)# rule number {deny permit} {read read-write} feature feature-name</code>	機能に対して、読み取り専用ルールか読み取りと書き込みのルールかを設定します。 show role feature コマンドを使用すれば、機能のリストが表示されます。 必要なルールの数だけこのコマンドを繰り返します。
ステップ 6	<code>switch(config-role)# rule number {deny permit} {read read-write} feature-group group-name</code>	機能グループに対して、読み取り専用ルールか読み取りと書き込みのルールかを設定します。 show role feature-group コマンドを使用すれば、機能グループのリストが表示されます。 必要なルールの数だけこのコマンドを繰り返します。
ステップ 7	<code>switch(config-role)# description text</code>	(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	<code>switch# show role</code>	(任意) ユーザロールの設定を表示します。
ステップ 9	<code>switch# copy running-config startup-config</code>	(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、ユーザロールを作成して規則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

機能グループを作成できます。

手順の概要

1. `switch# configure terminal`
2. `switch(config)# role feature-group group-name`
3. (任意) `switch# show role feature-group`
4. (任意) `switch# copy running-config startup-config`

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<code>switch# configure terminal</code>	コンフィギュレーション モードを開始します。
ステップ 2	<code>switch(config)# role feature-group group-name</code>	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。 <i>group-name</i> は、最大 32 文字の英数字のストリングで、大文字と小文字が区別されます。
ステップ 3	<code>switch# show role feature-group</code>	(任意) ロール機能グループ設定を表示します。
ステップ 4	<code>switch# copy running-config startup-config</code>	(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。

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。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# role name <i>role-name</i>	ユーザ ロールを指定し、ロール コンフィギュレーション モードを開始します。
ステップ 3	switch(config-role)# 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 <i>interface-list</i>	<p>ロールがアクセスできるインターフェイスのリストを指定します。</p> <p>必要なインターフェイスの数だけこのコマンドを繰り返します。</p> <p>このコマンドの場合、イーサネットインターフェイス、ファイバチャネルインターフェイス、および仮想ファイバチャネルインターフェイスを指定できます。</p>
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	<p>(任意)</p> <p>ロール設定を表示します。</p>
ステップ 7	switch(config-role)# copy running-config startup-config	<p>(任意)</p> <p>実行コンフィギュレーションを、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。</p>

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
```

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できます。これを必要なインターフェイスの数だけ指定できます。

ユーザ ロール VLAN ポリシーの変更

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	コンフ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# show role	(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。

ユーザロール VSAN ポリシーの変更

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

手順の概要

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

手順の詳細

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

ユーザアカウントとRBACの設定の確認

ユーザアカウントおよびRBAC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 role	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。

コマンド	目的
<code>show startup-config security</code>	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。
<code>show running-config security [all]</code>	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。
<code>show user-account</code>	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 3: デフォルトのユーザアカウントと RBAC パラメータ

パラメータ	デフォルト
ユーザアカウントパスワード	未定義。
ユーザアカウントの有効期限	なし。
インターフェイスポリシー	すべてのインターフェイスにアクセス可能。
VLAN ポリシー	すべての VLAN にアクセス可能。
VFC ポリシー	すべての VFC にアクセス可能。
VETH ポリシー	すべての VETH にアクセス可能。



第 7 章

Session Manager の設定

この章の内容は、次のとおりです。

- [Session Manager の概要, 81 ページ](#)
- [Session Manager の注意事項および制約事項, 82 ページ](#)
- [Session Manager の設定, 82 ページ](#)
- [Session Manager 設定の確認, 85 ページ](#)

Session Manager の概要

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

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

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

Session Manager の注意事項および制約事項

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

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

Session Manager の設定

セッションの作成

作成できるコンフィギュレーションセッションの最大数は 32 です。

手順の概要

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

手順の詳細

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

セッションでの ACL の設定

コンフィギュレーションセッションで ACL を設定できます。

手順の概要

1. switch# **configure session** *name*
2. switch(config-s)# **ip access-list** *name*
3. (任意) switch(config-s-acl)# **permit protocol source destination**
4. switch(config-s-acl)# **interface interface-type number**
5. switch(config-s-if)# **ip port access-group name in**
6. (任意) switch# **show configuration session** [*name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# configure session <i>name</i>	コンフィギュレーションセッションを作成し、セッションコンフィギュレーションモードを開始します。名前は任意の英数字ストリングです。
ステップ 2	switch(config-s)# ip access-list <i>name</i>	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 [<i>name</i>]	(任意) セッションの内容を表示します。

セッションの確認

セッションを確認するには、セッションモードで次のコマンドを使用します。

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

セッションのコミット

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

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

セッションの保存

セッションを保存するには、セッション モードで次のコマンドを使用します。

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

セッションの廃棄

セッションを廃棄するには、セッション モードで次のコマンドを使用します。

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

Session Manager のコンフィギュレーション例

この例では、ACL 用の設定セッションを作成する方法を示します。

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

Session Manager 設定の確認

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

コマンド	目的
<code>show configuration session [name]</code>	コンフィギュレーションファイルの内容を表示します。
<code>show configuration session status [name]</code>	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。
<code>show configuration session summary</code>	すべてのコンフィギュレーションセッションのサマリーを表示します。



第 8 章

オンライン診断の設定

この章の内容は、次のとおりです。

- [オンライン診断について, 87 ページ](#)
- [オンライン診断の設定, 90 ページ](#)
- [オンライン診断設定の確認, 91 ページ](#)
- [オンライン診断のデフォルト設定, 91 ページ](#)

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。起動時診断では、スーパーバイザと ASIC の間のデータパスと制御バ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 4: 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タス（on、off、pass、または fail）を示します。

起動時診断をバイパスするか、完全な起動時診断セットを実行するよう Cisco Nexus 5000 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 5: 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 6: 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 7: 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 8: 拡張モジュールのヘルスモニタリング診断

診断	説明
LED	ポートおよびシステムのステータス LED をモニタします。
温度センサー	温度センサーの読み取り値をモニタします。

オンライン診断の設定

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



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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<code>switch# configure terminal</code>	コンフィギュレーションモードを開始します。
ステップ 2	<code>switch(config)# diagnostic bootup level [complete bypass]</code>	デバイスの起動時に診断を実行するよう起動時診断レベルを次のように設定します。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • complete : すべての起動時診断を実行します。これがデフォルト値です。 • bypass : 起動時診断を実行しません。
ステップ 3	switch# show diagnostic bootup level	(任意) 現在、スイッチで実行されている起動時診断レベル (bypass または complete) を表示します。

次に、完全な診断を実行するよう起動時診断レベルを設定する例を示します。

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

オンライン診断設定の確認

オンライン診断設定情報を表示するには、次の作業を行います。

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

オンライン診断のデフォルト設定

次の表に、オンライン診断パラメータのデフォルト設定を示します。

表 9: デフォルトのオンライン診断パラメータ

パラメータ	デフォルト
起動時診断レベル	complete



第 9 章

システム メッセージ ログिंगの設定

この章の内容は、次のとおりです。

- システム メッセージ ログिंगの概要, 93 ページ
- システム メッセージ ログिंगのライセンス要件, 95 ページ
- システム メッセージ ログिंगの注意事項および制約事項, 95 ページ
- システム メッセージ ログिंगのデフォルト設定, 95 ページ
- システム メッセージ ログिंगの設定, 96 ページ
- システム メッセージ ログिंगの設定確認, 108 ページ

システム メッセージ ログिंगの概要

システム メッセージ ログ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 サーバへのログングを設定できます。

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

デフォルトでは、Cisco Nexus 5000 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 10: 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 へのログは設定できません。

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

syslog サーバ

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

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



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

システムメッセージロギングのライセンス要件

製品	ライセンス要件
Cisco NX-OS	システムメッセージロギングにライセンスは不要です。ライセンスパッケージに含まれていない機能はすべて Cisco NX-OS システムイメージにバンドルされており、追加費用は一切発生しません。Cisco NX-OS ライセンス方式の詳細については、『 <i>Cisco NX-OS Licensing Guide</i> 』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 11: 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 ログの設定

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

デフォルトでは、ターミナルセッションでログはイネーブルです。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# terminal monitor	コンソールから現在の端末セッションに syslog メッセージをコピーします。
ステップ 2	switch# configure terminal	コンフィギュレーション モードを開始します。
ステップ 3	switch(config)# logging console [severity-level]	指定された重大度（またはそれ以上）に基づくコンソールセッションへのメッセージの記録をイネーブルにします（数字が小さいほうが大きい重大度を示します）。重大度は 0～7 の範囲です。 <ul style="list-style-type: none"> • 0：緊急 • 1：アラート • 2：クリティカル • 3：エラー • 4：警告 • 5：通知

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • 6 : 情報 • 7 : デバッグ <p>重大度が指定されていない場合、デフォルトの 2 が使用されます。</p>
ステップ 4	switch(config)# no logging console [severity-level]	(任意) コンソールへのログギングメッセージをディセーブルにします。
ステップ 5	switch(config)# logging monitor [severity-level]	<p>指定された重大度（またはそれ以上）に基づくモニタへのメッセージの記録をイネーブルにします（数字が小さいほうが大きい重大度を示します）。重大度は 0 ~ 7 の範囲です。</p> <ul style="list-style-type: none"> • 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 <p>重大度が指定されていない場合、デフォルトの 2 が使用されます。</p> <p>設定は Telnet および SSH セッションに適用されます。</p>
ステップ 6	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グ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 ログ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 ログギング設定を表示します。
ステップ 9	switch# copy running-config startup-config	(任意) 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

次に、コンソールのロギングレベルを3に設定する例を示します。

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

次に、コンソールのロギングの設定を表示する例を示します。

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

次に、コンソールのロギングをディセーブルにする例を示します。

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

次に、ターミナルセッションのロギングレベルを4に設定する例を示します。

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

次に、ターミナルセッションのロギングの設定を表示する例を示します。

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

次に、ターミナルセッションのロギングをディセーブルにする例を示します。

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

ファイルへのシステムメッセージロギングの設定

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<code>switch# configure terminal</code>	コンフィギュレーションモードを開始します。
ステップ 2	<code>switch(config)# logging logfile logfile-name severity-level [size bytes]</code>	システムメッセージを保存するのに使用するログファイルの名前と、記録する最小重大度を設定します。任意で最大ファイルサイズを指定できます。デフォルトの重大度は5です。ファイルサイズは4194304です。

	コマンドまたはアクション	目的
		<p>重大度は 0 ～ 7 の範囲です。</p> <ul style="list-style-type: none"> • 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 <p>ファイルサイズは 4096 ～ 10485760 バイトです。</p>
ステップ 3	<code>switch(config)# no logging logfile [logfile-name severity-level [size bytes]]</code>	<p>(任意)</p> <p>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。</p>
ステップ 4	<code>switch# show logging info</code>	<p>(任意)</p> <p>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。</p>
ステップ 5	<code>switch# copy running-config startup-config</code>	<p>(任意)</p> <p>実行コンフィギュレーションを、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。</p>

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

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

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

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

```

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

```

モジュールおよびファシリティメッセージのロギングの設定

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	コンフィギュレーションモードを開始します。
ステップ 2	switch(config)# logging module [<i>severity-level</i>]	指定された重大度またはそれ以上の重大度であるモジュールログメッセージをイネーブルにします。重大度は 0～7 の範囲です。 <ul style="list-style-type: none"> • 0 : 緊急 • 1 : アラート • 2 : クリティカル • 3 : エラー • 4 : 警告 • 5 : 通知 • 6 : 情報

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • 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	<code>switch(config)# logging level facility severity-level</code>	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。 <ul style="list-style-type: none"> • 0: 緊急 • 1: アラート • 2: クリティカル • 3: エラー • 4: 警告 • 5: 通知 • 6: 情報 • 7: デバッグ 同じ重大度をすべてのファシリティに適用するには、all ファシリティを使用します。デフォルト値については、 show logging level コマンドを参照してください。
ステップ 4	<code>switch(config)# no logging module [severity-level]</code>	(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	<code>switch(config)# no logging level [facility severity-level]</code>	(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	<code>switch# show logging module</code>	(任意) モジュール ロギング設定を表示します。
ステップ 7	<code>switch# show logging level [facility]</code>	(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	<code>switch# copy running-config startup-config</code>	(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
```

ログ タイムスタンプの設定

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

手順の概要

1. switch# **configure terminal**
2. switch(config)# **logging timestamp {microseconds | milliseconds | seconds}**
3. (任意) switch(config)# **no logging timestamp {microseconds | milliseconds | seconds}**
4. (任意) switch# **show logging timestamp**
5. (任意) switch# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	コンフィギュレーションモードを開始します。
ステップ 2	switch(config)# logging timestamp {microseconds milliseconds seconds}	ログ タイムスタンプ単位を設定します。デフォルトでは、単位は秒です。
ステップ 3	switch(config)# no logging timestamp {microseconds milliseconds seconds}	(任意) ログ 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
```

syslog サーバの設定

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： <pre>switch# configure terminal switch(config)#</pre>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	logging server host [severity-level [use-vrf vrf-name [facility facility]]] 例： <pre>switch(config)# logging server 172.28.254.254 5 use-vrf default facility local3</pre>	<p>ホストが syslog メッセージを受信するように設定します。</p> <ul style="list-style-type: none"> • host 引数は、syslog サーバ ホストのホスト名または IPv4 または IPv6 アドレスを示します。 • severity-level 引数は、指定したレベルに syslog サーバへのメッセージのロギングを制限します。重大度は 0～7 の範囲です。表 10：システムメッセージの重大度，(94 ページ) を参照してください。 • use vrf vrf-name キーワードと引数は、仮想ルーティングおよび転送 (VRF) 名の <i>default</i> または <i>management</i> 値を示します。特定の VRF が指定されない場合は、<i>management</i> がデフォルトです。ただし、<i>management</i> 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。 <p>(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。</p> • 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 <i>local7</i> です。

	コマンドまたはアクション	目的
		<p>ファシリティは、使用している Cisco Nexus シリーズ ソフトウェアのコマンドリファレンスに記載されています。Nexus 5000 用の入手可能なコマンドリファレンスは http://www.cisco.com/en/US/products/ps9670/prod_command_reference_list.html にあります。</p> <p>(注) デバッグは CLI ファシリティですが、デバッグの syslog にはサーバに送信されません。</p>
ステップ 3	no logging server host 例： <pre>switch(config)# no logging server 172.28.254.254 5</pre>	(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： <pre>switch# show logging server</pre>	(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： <pre>switch(config)# copy running-config startup-config</pre>	(任意) リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を永続的に保存します。

次に、syslog サーバを設定する例を示します。

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

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

UNIX または Linux システムでの syslog の設定

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

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

次の表に、設定可能な syslog フィールドを示します。

表 12: *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。

手順の概要

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

手順の詳細

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

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

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

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

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

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

syslog サーバ設定の配布の設定

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

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



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

はじめる前に

1 つまたは複数の syslog サーバを設定しておく必要があります。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **logging distribute**
3. switch(config)# **logging commit**
4. switch(config)# **logging abort**
5. (任意) switch(config)# **no logging distribute**
6. (任意) switch# **show logging pending**
7. (任意) switch# **show logging pending-diff**
8. (任意) switch# **show logging internal info**
9. (任意) switch# **copy running-config startup-config**

手順の詳細

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

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

ログファイルの表示およびクリア

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# show logging last number-lines	ログイング 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 ログिंगの設定確認

システム メッセージ ログिंग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 ログイング設定を表示します。
show logging info	ログイング設定を表示します。
show logging internal info	syslog 配布情報を表示します。
show logging last number-lines	ログ ファイルの末尾から指定行数を表示します。

コマンド	目的
show logging level [<i>facility</i>]	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 <i>yyyy mmm dd hh:mm:ss</i>] [end-time <i>yyyy mmm dd hh:mm:ss</i>]	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 [<i>last number-lines</i>]	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。
show logging pending-diff	syslog サーバの保留中の配布設定の違いを表示します。
show logging server	syslog サーバ設定を表示します。
show logging session	ロギングセッションのステータスを表示します。
show logging status	ロギングステータスを表示します。
show logging timestamp	ロギングタイムスタンプ単位設定を表示します。



第 10 章

Smart Call Home の設定

この章の内容は、次のとおりです。

- [Smart Call Home に関する情報, 111 ページ](#)
- [Smart Call Home の注意事項および制約事項, 121 ページ](#)
- [Smart Call Home の前提条件, 122 ページ](#)
- [Call Home のデフォルト設定, 122 ページ](#)
- [Smart Call Home の設定, 123 ページ](#)
- [Smart Call Home 設定の確認, 136 ページ](#)
- [フルテキスト形式での syslog アラート通知の例, 137 ページ](#)
- [XML 形式での syslog アラート通知の例, 137 ページ](#)

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 サービス用のデバイスを登録できます。Smart Call Home は、ご使用のデバイスから送信された Smart Call Home メッセージを分析し、背景情報および推奨事項を提供して、システムの問題を迅速に解決します。既知と特定できる問題、特に GOLD 診断エラーについては、Cisco Technical Assistance Center (TAC) によって自動サービス リクエストが生成されます。

Smart Call Home には、次の機能があります。

- 継続的なデバイス ヘルス モニタリングとリアルタイムの診断アラート。

- ご使用のデバイスからの Smart Call Home メッセージの分析と、必要に応じた自動サービスリクエストの生成は、問題を迅速に解決するための詳細な診断情報とともに、適切な TAC チームにルーティングされます。
- セキュアなメッセージ転送が、ご使用のデバイスから直接、またはダウンロード可能な Transport Gateway (TG; トランスポートゲートウェイ) 集約ポイントを経由して行われます。複数のデバイスでサポートを必要としている場合、またはセキュリティ要件の関係でご使用のデバイスをインターネットに直接接続できない場合は、TG 集約ポイントを使用できます。
- Smart Call Home メッセージと推奨事項、すべての Smart Call Home デバイスのインベントリおよび設定情報、および Field Notice、セキュリティ勧告、およびサポート終了日情報への Web ベースのアクセス。

Smart Call Home の概要

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

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

Smart Call Home 機能には、次のものがあります。

- 関連する CLI コマンド出力の実行および添付が自動化されます。
- 次のような、複数のメッセージフォーマットオプションがあります。
 - ショートテキスト：ポケットベルまたは印刷形式のレポートに最適。
 - フルテキスト：人間が判読しやすいように完全にフォーマットされたメッセージ情報です。
 - XML：Extensible Markup Language (XML) および Adaptive Messaging Language (AML) XML スキーマ定義 (XSD) を使用した、判読可能なフォーマットです。XML 形式では、Cisco TAC と通信できます。
- 複数のメッセージ宛先への同時配信が可能。それぞれの宛先プロファイルには、最大 50 個の電子メール宛先アドレスを設定できます。

Smart Call Home 宛先プロファイル

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

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

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

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

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

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

Smart Call Home アラートグループ

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

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

表 13：アラートグループおよび実行されるコマンド

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

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

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

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

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

Smart Call Home のメッセージ レベル

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

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



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

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

表 14：重大度と *syslog* レベルのマッピング

Smart Call Home レベル	キーワード	syslog レベル	説明
9	Catastrophic	なし	ネットワーク全体に及ぶ深刻な障害。
8	Disaster	なし	ネットワークへの重大な影響。
7	Fatal	緊急 (0)	システムは使用不能。
6	Critical	アラート (1)	クリティカルな状況で、すぐに対応する必要があります。
5	Major	クリティカル (2)	メジャーな状態です。
4	Minor	エラー (3)	マイナーな状態。

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

Call Home のメッセージ形式

Call Home では、次のメッセージフォーマットがサポートされます。

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

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

表 15: ショートテキストメッセージフォーマット

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

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

表 16: すべてのフルテキストと XML メッセージに共通のフィールド

データ項目 (プレーンテキストおよび XML)	説明 (プレーンテキストおよび XML)	XML タグ (XML のみ)
タイムスタンプ	ISO 時刻通知でのイベントの日付とタイムスタンプ YYYY-MM-DD HH:MM:SS GMT+HH:MM	/aml/header/time
メッセージ名	メッセージの名前。特定のイベント名は上記の表に記載。	/aml/header/name
メッセージタイプ	リアクティブまたはプロアクティブなどのメッセージタイプの名前。	/aml/header/type
メッセージグループ	syslog などのアラートグループの名前。	/aml/header/group
重大度	メッセージの重大度。	/aml/header/level
送信元 ID	ルーティングのための製品タイプ。	/aml/header/source
デバイス ID	メッセージを生成したエンドデバイスの固有デバイス識別情報 (UDI)。メッセージがデバイスに対して固有でない場合は、このフィールドを空にする必要があります。形式は、 <i>type@Sid@serial</i> 。 <ul style="list-style-type: none"> • <i>type</i> は、バックプレーン IDPROM からの製品の型番。 • <i>@</i> は区切り文字。 • <i>Sid</i> は C で、シリアル ID をシャーシシリアル番号として特定します。 • <i>serial</i> は、[Sid] フィールドによって特定される数字。 例: WS-C6509@C@12345678	/aml/ header/deviceID

データ項目（プレーンテキストおよびXML）	説明（プレーンテキストおよびXML）	XML タグ（XML のみ）
カスタマー ID	サポート サービスによって契約情報やその他の ID に使用されるオプションのユーザ設定可能なフィールド。	/aml/ header/customerID
連絡先 ID	サポート サービスによって契約情報やその他の ID に使用されるオプションのユーザ設定可能なフィールド。	/aml/ header /contractID
サイト ID	シスコが提供したサイト ID または別のサポート サービスにとって意味のあるその他のデータに使用されるオプションのユーザ設定可能なフィールド。	/aml/ header/siteID
サーバ ID	<p>デバイスからメッセージが生成された場合、これはデバイスの Unique Device Identifier (UDI) フォーマットです。</p> <p>形式は、<i>type@Sid@serial</i>。</p> <ul style="list-style-type: none"> • <i>type</i> は、バックプレーン IDPROM からの製品の型番。 • <i>@</i> は区切り文字。 • <i>Sid</i> は C で、シリアル ID をシャーシシリアル番号として特定します。 • <i>serial</i> は、[Sid] フィールドによって特定される数字。 <p>例：WS-C6509@C@12345678</p>	/aml/header/serverID
メッセージの説明	エラーを説明するショートテキスト。	/aml/body/msgDesc
デバイス名	イベントが発生したノード（デバイスのホスト名）。	/aml/body/sysName

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

次の表に、フルテキストまたはXMLのリアクティブイベントメッセージ形式について説明します。

表 17: 対処的または予防的イベントメッセージに挿入されるフィールド

データ項目 (プレーンテキストおよびXML)	説明 (プレーンテキストおよびXML)	XML タグ (XML のみ)
シャーシのハードウェアバージョン	シャーシのハードウェアバージョン。	/aml/body/chassis/hwVersion
スーパーバイザモジュールのソフトウェアバージョン	最上位ソフトウェアバージョン。	/aml/body/chassis/swVersion
影響のある FRU 名	イベントメッセージを生成する関連 FRU の名前。	/aml/body/fru/name
影響のある FRU のシリアル番号	関連 FRU のシリアル番号。	/aml/body/fru/serialNo
影響のある FRU の部品番号	影響のある FRU の部品番号。	/aml/body/fru/partNo
FRU スロット	イベントメッセージを生成する FRU のスロット番号。	/aml/body/fru/slot
FRU ハードウェアバージョン	影響のある FRU のハードウェアバージョン。	/aml/body/fru/hwVersion
FRU ソフトウェアのバージョン	関連 FRU で稼働しているソフトウェアバージョン。	/aml/body/fru/swVersion

次の表に、フルテキストまたはXMLのコンポーネントイベントメッセージ形式について説明します。

表 18: コンポーネントイベントメッセージの挿入フィールド

データ項目 (プレーンテキストおよびXML)	説明 (プレーンテキストおよびXML)	XML タグ (XML のみ)
シャーシのハードウェアバージョン	シャーシのハードウェアバージョン。	/aml/body/chassis/hwVersion
スーパーバイザモジュールのソフトウェアバージョン	最上位ソフトウェアバージョン。	/aml/body/chassis/swVersion

データ項目（プレーンテキストおよび XML）	説明（プレーンテキストおよび XML）	XML タグ（XML のみ）
FRU 名	イベント メッセージを生成する関連 FRU の名前。	/aml/body/fru/name
FRU s/n	FRU のシリアル番号。	/aml/body/fru/serialNo
FRU 部品番号	FRU の部品番号。	/aml/body/fru/partNo
FRU スロット	FRU のスロット番号。	/aml/body/fru/slot
FRU ハードウェア バージョン	FRU のハードウェア バージョン。	/aml/body/fru/hwVersion
FRU ソフトウェアのバージョン	FRU で稼働しているソフトウェア バージョン。	/aml/body/fru/swVersion

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

表 19: ユーザが作成したテストメッセージの挿入フィールド

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

Smart Call Home の注意事項および制約事項

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

Smart Call Home の前提条件

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

Call Home のデフォルト設定

表 20: デフォルトの *Call Home* パラメータ

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

Smart Call Home の設定

Smart Call Home の登録

はじめる前に

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

手順の概要

1. ブラウザでは、Smart Call Home Web ページに移動します。
2. [Getting Started] で、Smart Call Home の登録指示に従ってください。

手順の詳細

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

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

次の作業

連絡先情報を設定します。

担当者情報の設定

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# snmp-server contact <i>sys-contact</i>	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 <i>email-address</i>	スイッチの担当者の電子メールアドレスを設定します。 <i>email-address</i> には、電子メールアドレスの形式で、最大 255 の英数字を使用できます。 (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 <i>international-phone-number</i>	デバイスの担当者の電話番号を国際電話フォーマットで設定します。 <i>international-phone-number</i> は、最大 17 文字の英数字で、国際電話フォーマットにする必要があります。 (注) 電話番号には、空白を含めることはできません。番号の前にプラス (+) プレフィックスを使用します。
ステップ 6	switch(config-callhome)# streetaddress <i>address</i>	スイッチの主担当者の住所を設定します。 <i>address</i> には、最大 255 の英数字を使用できます。スペースを使用できます。
ステップ 7	switch(config-callhome)# contract-id <i>contract-number</i>	(任意) サービス契約からこのスイッチの契約番号を設定します。

	コマンドまたはアクション	目的
		<i>contract-number</i> には最大 255 の英数字を使用できます。
ステップ 8	<code>switch(config-callhome)# customer-id customer-number</code>	(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。 <i>customer-number</i> には最大 255 の英数字を使用できます。
ステップ 9	<code>switch(config-callhome)# site-id site-number</code>	(任意) このスイッチのサイト番号を設定します。 <i>site-number</i> は、最大 255 文字の英数字を自由なフォーマットで指定できます。
ステップ 10	<code>switch(config-callhome)# switch-priority number</code>	(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	<code>switch# show callhome</code>	(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	<code>switch(config)# copy running-config startup-config</code>	(任意) リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を永続的に保存します。

次に、Call Home に関する契約情報を設定する例を示します。

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

次の作業

宛先プロファイルを作成します。

宛先プロファイルの作成

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

手順の概要

1. switch# **configure terminal**
2. switch(config)# **callhome**
3. switch(config-callhome)# **destination-profile** {ciscoTAC-1 {alert-group group | email-addr address | http URL | transport-method {email | http}} | profile-name {alert-group group | email-addr address | format {XML | full-txt | short-txt} | http URL | message-level level | message-size size | transport-method {email | http}} | full-txt-destination {alert-group group | email-addr address | http URL | message-level level | message-size size | transport-method {email | http}} | short-txt-destination {alert-group group | email-addr address | http URL | message-level level | message-size size | transport-method {email | http}}}
4. (任意) switch# **show callhome destination-profile** [profile name]
5. (任意) switch(config)# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# callhome	Smart Call Home コンフィギュレーション モードを開始します。
ステップ 3	switch(config-callhome)# destination-profile {ciscoTAC-1 {alert-group group email-addr address http URL transport-method {email http}} profile-name {alert-group group email-addr address format {XML full-txt short-txt} http URL message-level level message-size size transport-method {email http}} full-txt-destination {alert-group group email-addr address http URL message-level level message-size size transport-method {email http}} short-txt-destination {alert-group group email-addr address http URL message-level level message-size size transport-method {email http}}}	新しい宛先プロファイルを作成し、そのプロファイルのメッセージフォーマットを設定します。プロファイル名は、最大 31 文字の英数字で指定できます。 このコマンドの詳細については、使用している Cisco Nexus シリーズ ソフトウェアのコマンドリファレンスを参照してください。Nexus 5000 用の入手可能なコマンドリファレンスは http://www.cisco.com/en/US/products/ps9670/prod_command_reference_list.html にあります。
ステップ 4	switch# show callhome destination-profile [profile name]	(任意) 1つまたは複数の宛先プロファイルに関する情報を表示します。
ステップ 5	switch(config)# copy running-config startup-config	(任意) リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

次に、Smart Call Home の宛先プロフィー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
```

宛先プロフィールの変更

定義済みまたはユーザ定義の宛先プロフィー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：この宛先プロフィールの Call Home メッセージの重大度。
- メッセージサイズ：この宛先プロフィー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 宛先プロフィールは変更または削除できません。

手順の概要

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

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	<code>switch(config-callhome)# destination-profile {name full-txt-destination short-txt-destination} email-addr address</code>	ユーザ定義または定義済みの宛先プロフィールに電子メールアドレスを設定します。宛先プロフィールには、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	<code>destination-profile {name full-txt-destination short-txt-destination} message-level number</code>	この宛先プロフィールの 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、このプロフィールの宛先に送信されます。 <code>number</code> に指定できる範囲は 0～9 です。9 は最大の重大度を示します。
ステップ 5	<code>switch(config-callhome)# destination-profile {name full-txt-destination short-txt-destination} message-size number</code>	この宛先プロフィールの最大メッセージサイズを設定します。 <code>full-txt-destination</code> の値の範囲は 0～5000000 で、デフォルトは 2500000 です。 <code>short-txt-destination</code> の値の範囲は 0～100000 で、デフォルトは 4000 です。CiscoTAC-1 では、値は 5000000 で、これは変更不可能です。
ステップ 6	<code>switch# show callhome destination-profile [profile name]</code>	(任意) 1 つまたは複数の宛先プロフィールに関する情報を表示します。
ステップ 7	<code>switch(config)# copy running-config startup-config</code>	(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 の宛先プロフィールを変更する例を示します。

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

次の作業

アラートグループと宛先プロフィールをアソシエートします。

アラートグループと宛先プロファイルのアソシエーション

手順の概要

1. switch# **configure terminal**
2. switch(config)# **callhome**
3. switch(config-callhome)# **destination-profile** *name* **alert-group** {**All** | **Cisco-TAC** | **Configuration** | **Diagnostic** | **Environmental** | **Inventory** | **License** | **Linecard-Hardware** | **Supervisor-Hardware** | **Syslog-group-port** | **System** | **Test**}
4. (任意) switch# **show callhome destination-profile** [*profile name*]
5. (任意) switch(config)# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	グローバルコンフィギュレーションモードを開始します。
ステップ 2	switch(config)# callhome	Smart Call Home コンフィギュレーションモードを開始します。
ステップ 3	switch(config-callhome)# destination-profile <i>name</i> alert-group { All Cisco-TAC Configuration Diagnostic Environmental Inventory License Linecard-Hardware Supervisor-Hardware Syslog-group-port System Test }	アラートグループをこの宛先プロファイルにアソシエートします。キーワード All を使用して、すべてのアラートグループをこの宛先プロファイルにアソシエートします。
ステップ 4	switch# show callhome destination-profile [<i>profile name</i>]	(任意) 1 つまたは複数の宛先プロファイルに関する情報を表示します。
ステップ 5	switch(config)# copy running-config startup-config	(任意) リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を永続的に保存します。

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

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

次の作業

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

アラートグループへの show コマンドの追加

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

手順の概要

1. switch# **configure terminal**
2. switch(config)# **callhome**
3. switch(config-callhome)# **alert-group {Configuration | Diagnostic | Environmental | Inventory | License | Linecard-Hardware | Supervisor-Hardware | Syslog-group-port | System | Test} user-def-cmd show-cmd**
4. (任意) switch# **show callhome user-def-cmds**
5. (任意) switch(config)# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	グローバルコンフィギュレーションモードを開始します。
ステップ 2	switch(config)# callhome	Smart Call Home コンフィギュレーションモードを開始します。
ステップ 3	switch(config-callhome)# alert-group {Configuration Diagnostic Environmental Inventory License Linecard-Hardware Supervisor-Hardware Syslog-group-port System Test} user-def-cmd show-cmd	show コマンド出力を、このアラートグループに送信された Call Home メッセージに追加します。有効な show コマンドだけが受け入れられます。 (注) CiscoTAC-1 宛先プロファイルには、ユーザ定義の CLI show コマンドを追加できません。
ステップ 4	switch# show callhome user-def-cmds	(任意) アラートグループに追加されたすべてのユーザ定義 show コマンドに関する情報を表示します。
ステップ 5	switch(config)# copy running-config startup-config	(任意) リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を永続的に保存します。

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

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

次の作業

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

電子メール サーバの詳細の設定

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	グローバルコンフィギュレーションモードを開始します。
ステップ 2	switch(config)# callhome	Smart Call Home コンフィギュレーションモードを開始します。
ステップ 3	switch(config-callhome)# transport email smtp-server ip-address [port number] [use-vrf vrf-name]	SMTP サーバを、ドメイン ネーム サーバ (DNS) 名、IPv4 アドレス、または IPv6 アドレスのいずれかとして設定します。 portnumber の範囲は 1 ~ 65535 です。デフォルトのポート番号は 25 です。 この SMTP サーバと通信する際に使用するよう任意で VRF を設定できます。

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

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

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

次の作業

定期的なインベントリ通知を設定します。

定期的なインベントリ通知の設定

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

手順の概要

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

手順の詳細

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

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

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

次の作業

重複メッセージ抑制をディセーブルにします。

重複メッセージ抑制のディセーブル化

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

手順の概要

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

手順の詳細

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

次に、重複メッセージ抑制をディセーブルにする例を示します。

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

次の作業

Smart Call Home をイネーブルにします。

Smart Call Home のイネーブル化またはディセーブル化

手順の概要

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

手順の詳細

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

次に、Smart Call Home をイネーブルにする例を示します。

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

次の作業

任意でテスト メッセージを生成します。

Smart Call Home 設定のテスト

はじめる前に

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



重要

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

手順の概要

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

手順の詳細

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

次に、Smart Call Home をイネーブルにする例を示します。

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

Smart Call Home 設定の確認

設定を確認するには、次のいずれかのコマンドを使用します。

コマンド	目的
switch# show callhome	Call Home のステータスを表示します。
switch# show callhome destination-profile name	1 つまたは複数の Call Home 宛先プロファイルを表示します。
switch# show callhome pending-diff	保留中の Smart Call Home 設定と実行中の Smart Call Home 設定の違いを表示します。
switch# show callhome status	Smart Call Home ステータスを表示します。
switch# show callhome transport-email	Smart Call Home の電子メール設定を表示します。

コマンド	目的
switch# show callhome user-def-cmds	任意のアラートグループに追加された CLI コマンドを表示します。
switch# show running-config [callhome callhome-all]	Smart Call Home の実行コンフィギュレーションを表示します。
switch# show startup-config callhome	Smart Call Home のスタートアップコンフィギュレーションを表示します。
switch# show tech-support callhome	Smart Call Home のテクニカル サポート出力を表示します。

フルテキスト形式での syslog アラート通知の例

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

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

XML 形式での syslog アラート通知の例

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

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

```

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

```

```

</ch:Call Home>
</aml-block:Content>
<aml-block:Attachments>
<aml-block:Attachment type="inline">
<aml-block:Name>show logging</aml-block:Name>
<aml-block:Data encoding="plain">
<![CDATA[Syslog logging: enabled (0 messages dropped, 0 messages
rate-limited, 0 flushes, 0 overruns, xml disabled, filtering disabled)
Console logging: level debugging, 53 messages logged, xml disabled,
filtering disabled Monitor logging: level debugging, 0 messages logged,
xml disabled,filtering disabled Buffer logging: level debugging,
53 messages logged, xml disabled, filtering disabled Exception
Logging: size (4096 bytes) Count and timestamp logging messages: disabled
Trap logging: level informational, 72 message lines logged
Log Buffer (8192 bytes):
00:00:54: curr is 0x20000
00:00:54: RP: Currently running ROMMON from F2 region
00:01:05: %SYS-5-CONFIG_I: Configured from memory by console
00:01:09: %SYS-5-RESTART: System restarted --Cisco IOS Software,
s72033_rp Software (s72033_rp-ADVENTERPRISEK9_DBG-VM), Experimental
Version 12.2(20070421:012711) Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Thu 26-Apr-07 15:54 by xxx
Firmware compiled 11-Apr-07 03:34 by integ Build [100]00:01:01: %PFREDUN-6-ACTIVE:
Initializing as ACTIVE processor for this switch00:01:01: %SYS-3-LOGGER_FLUSHED:
System was paused for 00:00:00 to ensure console debugging output.00:03:00: SP: SP:
Currently running ROMMON from F1 region00:03:07: %C6K_PLATFORM-SP-4-CONFREG_BREAK
_ENABLED: The default factory setting for config register is 0x2102.It is advisable
to retain 1 in 0x2102 as it prevents returning to ROMMON when break is issued.00:03:18:
%SYS-SP-5-RESTART: System restarted --Cisco IOS Software, s72033_sp Software
(s72033_sp-ADVENTERPRISEK9_DBG-VM), Experimental Version 12.2(20070421:012711)Copyright
(c) 1986-2007 by Cisco Systems, Inc.
Compiled Thu 26-Apr-07 18:00 by xxx
00:03:18: %SYS-SP-6-BOOTTIME: Time taken to reboot after reload = 339 seconds
00:03:18: %OIR-SP-6-INSPS: Power supply inserted in slot 1
00:03:18: %C6KPWR-SP-4-PSOK: power supply 1 turned on.
00:03:18: %OIR-SP-6-INSPS: Power supply inserted in slot00:01:09: %SSH-5-ENABLED:
SSH 1.99 has been enabled
00:03:18: %C6KPWR-SP-4-PSOK: power supply 2 turned on.
00:03:18: %C6KPWR-SP-4-PSREDUNDANTMISMATCH: power supplies rated outputs do not match.
00:03:18: %C6KPWR-SP-4-PSREDUNDANTBOTHSUPPLY: in power-redundancy mode, system is
operating on both power supplies.
00:01:10: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
00:01:10: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
00:03:20: %C6KENV-SP-4-FANHIOUTPUT: Version 2 high-output fan-tray is in effect
00:03:22: %C6KPWR-SP-4-PSNOREDUNDANCY: Power supplies are not in full redundancy,
power usage exceeds lower capacity supply
00:03:26: %FABRIC-SP-5-FABRIC_MODULE_ACTIVE: The Switch Fabric Module in slot 6
became active.
00:03:28: %DIAG-SP-6-RUN_MINIMUM: Module 6: Running Minimal Diagnostics...
00:03:50: %DIAG-SP-6-DIAG_OK: Module 6: Passed Online Diagnostics
00:03:50: %OIR-SP-6-INSCARD: Card inserted in slot 6, interfaces are now online
00:03:51: %DIAG-SP-6-RUN_MINIMUM: Module 3: Running Minimal Diagnostics...
00:03:51: %DIAG-SP-6-RUN_MINIMUM: Module 7: Running Minimal Diagnostics...
00:03:51: %DIAG-SP-6-RUN_MINIMUM: Module 9: Running Minimal Diagnostics...
00:01:51: %MFIB_CONST_RP-6-REPLICATION_MODE_CHANGE: Replication Mode Change Detected.
Current system replication mode is Ingress
00:04:01: %DIAG-SP-6-DIAG_OK: Module 3: Passed Online Diagnostics
00:04:01: %OIR-SP-6-DOWNGRADE: Fabric capable module 3 not at an appropriate hardware
revision level, and can only run in flowthrough mode
00:04:02: %OIR-SP-6-INSCARD: Card inserted in slot 3, interfaces are now online
00:04:11: %DIAG-SP-6-DIAG_OK: Module 7: Passed Online Diagnostics
00:04:14: %OIR-SP-6-INSCARD: Card inserted in slot 7, interfaces are now online
00:04:35: %DIAG-SP-6-DIAG_OK: Module 9: Passed Online Diagnostics
00:04:37: %OIR-SP-6-INSCARD: Card inserted in slot 9, interfaces are now online
00:00:09: DaughterBoard (Distributed Forwarding Card 3)
Firmware compiled 11-Apr-07 03:34 by integ Build [100]
00:00:22: %SYS-DFC4-5-RESTART: System restarted --
Cisco DCOS Software, c61c2 Software (c61c2-SPDBG-VM), Experimental Version 4.0
(20080421:012711)Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 26-Apr-08 17:20 by xxx
00:00:23: DFC4: Currently running ROMMON from F2 region
00:00:25: %SYS-DFC2-5-RESTART: System restarted --
Cisco IOS Software, c6slc Software (c6slc-SPDBG-VM), Experimental Version 12.2

```

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



第 11 章

ロールバックの設定

この章の内容は、次のとおりです。

- [ロールバックの概要, 141 ページ](#)
- [注意事項および制約事項, 141 ページ](#)
- [チェックポイントの作成, 142 ページ](#)
- [ロールバックの実装, 143 ページ](#)
- [ロールバック コンフィギュレーションの確認, 144 ページ](#)

ロールバックの概要

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

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

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

注意事項および制約事項

ロールバックに関する設定時の注意事項および制約事項は、次のとおりです。

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

チェックポイントの作成

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

手順の概要

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

手順の詳細

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

ロールバックの実装

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



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

手順の概要

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

手順の詳細

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

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

```
switch# checkpoint stable
switch# rollback running-config checkpoint stable atomic
```

ロールバック コンフィギュレーションの確認

ロールバックの設定を表示するには、次のいずれかの作業を行います。

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



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



第 12 章

DNS の設定

この章の内容は、次のとおりです。

- [DNS クライアントの概要, 147 ページ](#)
- [DNS クライアントの前提条件, 148 ページ](#)
- [DNS クライアントのライセンス要件, 148 ページ](#)
- [デフォルト設定値, 149 ページ](#)
- [DNS クライアントの設定, 149 ページ](#)

DNS クライアントの概要

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

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

ネーム サーバ

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

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

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

DNS の動作

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

- 権限ネームサーバは、その権限ゾーン内のドメイン名を求める DNS ユーザ照会に、自身のホストテーブル内にキャッシュされた永久的なエントリを使用して応答します。照会で求められているのが、自身の権限ゾーン内であるが、設定情報が登録されていないドメイン名の場合、権限ネームサーバは単に、その情報が存在しないと返信します。
- 権限ネームサーバとして設定されていないネームサーバは、以前に受信した照会への返信からキャッシュした情報を使用して、DNS ユーザ照会に応答します。ゾーンの権限ネームサーバとして設定されたルータがない場合は、ローカルに定義されたホストを求める DNS サーバへの照会には、正規の返信は送信されません。

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

ハイアベイラビリティ

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

DNS クライアントの前提条件

DNS クライアントには次の前提条件があります。

- ネットワーク上に DNS ネームサーバが必要です。

DNS クライアントのライセンス要件

次の表に、この機能のライセンス要件を示します。

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

デフォルト設定値

次の表に、DNS クライアント パラメータのデフォルト設定を示します。

パラメータ	デフォルト
DNS クライアント	イネーブル

DNS クライアントの設定

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

はじめる前に

- ネットワーク上にドメイン ネーム サーバがあることを確認します。

手順の概要

1. configuration terminal
2. vrf context managment
3. ip host name *address1* [*address2... address6*]
4. ip domain name *name* [**use-vrf** *vrf-name*]
5. ip domain-list *name* [**use-vrf** *vrf-name*]
6. ip name-server *server-address1* [*server-address2... server-address6*] [**use-vrf** *vrf-name*]
7. ip domain-lookup
8. show hosts
9. exit
10. copy running-config startup-config

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configuration terminal 例 : <pre>switch# configuration terminal switch(config)#</pre>	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 : <pre>switch(config)# vrf context management switch(config)#</pre>	設定可能な VRF 名を指定します。
ステップ 3	ip host name address1 [address2... address6] 例 : <pre>switch# ip host cisco-rtp 192.0.2.1 switch(config)#</pre>	ホスト名キャッシュに、6つまでのスタティックホスト名/アドレスマッピングを定義します。
ステップ 4	ip domain name name [use-vrf vrf-name] 例 : <pre>switch(config)# ip domain-name myserver.com switch(config)#</pre>	(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 : <pre>switch(config)# ip domain-list mycompany.com switch(config)#</pre>	(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 : <pre>switch(config)# ip name-server 192.0.2.1 switch(config)#</pre>	(任意) 最大6つのネームサーバを定義します。使用可能なアドレスは、IPv4 アドレスまたは IPv6 アドレスです。

	コマンドまたはアクション	目的
	例： switch(config)# ip name-server 192.0.2.22	この名前サーバを設定した VRF でこの名前サーバに到達できない場合は、任意で、Cisco NX-OS がこの名前サーバに到達するために使用する VRF を定義することもできます。
ステップ 7	ip domain-lookup 例： switch(config)# ip domain-lookup	(任意) DNS ベースのアドレス変換をイネーブルにします。デフォルトでは、イネーブルです。
ステップ 8	show hosts 例： switch(config)# show hosts	(任意) DNS に関する情報を表示します。
ステップ 9	exit 例： switch(config)# exit switch#	コンフィギュレーションモードを終了し、EXEC モードに戻ります。
ステップ 10	copy running-config startup-config 例： switch# copy running-config startup-config switch#	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

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

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




第 13 章

SNMP の設定

この章の内容は、次のとおりです。

- [SNMP について, 153 ページ](#)
- [SNMP のライセンス要件, 158 ページ](#)
- [SNMP の注意事項および制約事項, 158 ページ](#)
- [SNMP のデフォルト設定, 158 ページ](#)
- [SNMP の設定, 159 ページ](#)
- [SNMP のディセーブル化, 172 ページ](#)
- [SNMP の設定の確認, 173 ページ](#)

SNMP について

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

SNMP 機能の概要

SNMP フレームワークは 3 つの部分で構成されます。

- **SNMP マネージャ**：SNMP を使用してネットワーク デバイスのアクティビティを制御し、モニタリングするシステム。
- **SNMP エージェント**：デバイスのデータを維持し、必要に応じてこれらのデータを管理システムに報告する、管理対象デバイス内のソフトウェア コンポーネント。Cisco Nexus 5000 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 5000 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。

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

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

SNMP 通知

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

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

トラップの信頼性はインフォームより低くなります。SNMP マネージャはトラップを受信しても Acknowledgment (ACK; 確認応答) を送信しないからです。このため、トラップが受信されたかどうかをスイッチが判断できません。インフォーム要求を受信する SNMP マネージャは、SNMP 応答 Protocol Data Unit (PDU; プロトコルデータ ユニット) でメッセージの受信を確認します。Cisco Nexus 5000 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 21：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 AAA 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爾またはディセーブ爾に設定できます。

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、ライセンスは必要ありません。ライセンスパッケージに含まれていない機能はすべて Cisco NX-OS システムイメージにバンドルされており、追加費用は一切発生しません。Cisco NX-OS 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 22: 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	イネーブ爾
linkUp/Down 通知タイプ	ietf-extended

SNMP の設定

SNMP ユーザの設定



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

手順の概要

1. **configure terminal**
2. `switch(config)# snmp-server user name [auth {md5 | sha} passphrase [auto] [priv [aes-128] passphrase] [engineID id] [localizedkey]]`
3. (任意) `switch# show snmp user`
4. (任意) `copy running-config startup-config`

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： <pre>switch# configure terminal switch(config)#</pre>	グローバルコンフィギュレーションモードを開始します。
ステップ 2	<code>switch(config)# snmp-server user name [auth {md5 sha} passphrase [auto] [priv [aes-128] passphrase] [engineID id] [localizedkey]]</code> 例： <pre>switch(config)# snmp-server user Admin auth sha abcd1234 priv abcdefgh</pre>	認証およびプライバシー パラメータのある SNMP ユーザを設定します。 パスフレーズには最大 64 文字の英数字を使用できます。大文字と小文字を区別します。 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	<code>switch# show snmp user</code> 例： <pre>switch(config) # show snmp user</pre>	(任意) 1 人または複数の SNMP ユーザに関する情報を表示します。

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

次の例は、SNMP ユーザを設定します。

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

SNMP メッセージ暗号化の適用

着信要求に認証または暗号化が必要となるよう SNMP を設定できます。デフォルトでは、SNMP エージェントは、認証と暗号化なしで SNMPv3 メッセージを受け入れます。プライバシーを適用する場合、Cisco NX-OS は、**noAuthNoPriv** または **authNoPriv** のいずれかのセキュリティレベルパラメータを使用しているすべての SNMPv3 PDU 要求に対して、許可エラーで応答します。

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

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

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

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

SNMPv3 ユーザに対する複数のロールの割り当て

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



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

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

SNMP コミュニティの作成

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

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

コマンド	目的
<code>switch(config)# snmp-server community name group {ro rw}</code>	SNMP コミュニティストリングを作成します。

SNMP 要求のフィルタリング

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

ACL は次のパラメータで作成します。

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

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



ヒント

ACL の作成の詳細については、使用している Cisco Nexus シリーズ ソフトウェアの『*NX-OS Security Configuration Guide*』を参照してください。Nexus 5000 用の入手可能なセキュリティ設定ガイドラインは http://www.cisco.com/en/US/products/ps9670/products_installation_and_configuration_guides_list.html にあります。

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

コマンド	目的
<pre>switch(config)# snmp-server community <i>community name</i> use-acl <i>acl-name</i></pre> <p>Example: <pre>switch(config)# snmp-server community public use-acl my_acl_for_public</pre></p>	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
<pre>switch(config)# snmp-server host <i>ip-address</i> traps version 1 <i>community</i> [<i>udp_port number</i>]</pre>	SNMPv1 トラップのホスト レシーバを設定します。 <i>ip-address</i> は IPv4 または IPv6 アドレスを使用できます。 <i>community</i> 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
<code>switch(config)# snmp-server host ip-address {traps informs} version 2c community [udp_port number]</code>	SNMPv2c トラップまたはインフォームのホスト レシーバを設定します。 <i>ip-address</i> は IPv4 または IPv6 アドレスを使用できます。 <i>community</i> 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
<code>switch(config)# snmp-server host ip-address {traps informs} version 3 {auth noauth priv} username [udp_port number]</code>	SNMPv2c トラップまたはインフォームのホスト レシーバを設定します。 <i>ip-address</i> は IPv4 または IPv6 アドレスを使用できます。 <i>username</i> には最大 255 の英数字を使用できます。 UDP ポート番号の範囲は 0 ~ 65535 です。



- (注) SNMP マネージャは、SNMPv3 メッセージを認証し暗号解除するために、Cisco Nexus 5000 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
```

すべての SNMP 通知を送信するための送信元インターフェイスの設定

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： <pre>switch# configure terminal switch(config)#</pre>	グローバルコンフィギュレーションモードを開始します。
ステップ 2	<pre>switch(config) # snmp-server source-interface {traps informs} if-type if-number</pre> 例： <pre>switch(config) # snmp-server source-interface traps ethernet 2/1</pre>	SNMPv2c トラップまたは応答要求を送信するよう発信元インターフェイスを設定します。?を使用して、サポートされているインターフェイスタイプを特定します。

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

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

次の作業

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

SNMP 通知のホスト レシーバの設定



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

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config) # snmp-server host ip-address source-interface if-type if-number [udp_port number] 例： switch(config) # snmp-server host 192.0.2.1 source-interface traps ethernet 2/1	SNMPv2c トラップまたはインフォームのホスト レシーバを設定します。 <i>ip-address</i> は IPv4 または IPv6 アドレスを使用できます。 ? を使用して、サポートされているインターフェイス タイプを特定します。

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

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

次の作業

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

インバンド アクセスのための SNMP の設定

次のものを使用して、インバンドアクセス用に SNMP を設定できます。

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

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **snmp-server context context-name vrf vrf-name**
3. switch(config)# **snmp-server community community-name group group-name**
4. switch(config)# **snmp-server mib community-map community-name context context-name**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# configuration terminal	グローバルコンフィギュレーションモードを開始します。
ステップ 2	switch(config)# snmp-server context context-name vrf vrf-name	管理 VRF またはデフォルト VRF に SNMP コンテキストをマッピングします。カスタム VRF はサポートされません。 名前には最大 32 の英数字を使用できます。
ステップ 3	switch(config)# snmp-server community community-name group group-name	SNMPv2c コミュニティと SNMP コンテキストにマッピングし、コミュニティが属するグループを識別します。名前には最大 32 の英数字を使用できます。
ステップ 4	switch(config)# snmp-server mib community-map community-name context context-name	SNMPv2c コミュニティを SNMP コンテキストにマッピングします。名前には最大 32 の英数字を使用できます。

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

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

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

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

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

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

SNMP 通知のイネーブル化

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



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

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

表 23: 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
ENTITY-MIB、 CISCO-ENTITY-FRU-CONTROL-MIB、 CISCO-ENTITY-SENSOR-MIB	snmp-server enable traps entity snmp-server enable traps entity fru
CISCO-LICENSE-MGR-MIB	snmp-server enable traps license
IF-MIB	snmp-server enable traps link
CISCO-PSM-MIB	snmp-server enable traps port-security
SNMPv2-MIB	snmp-server enable traps snmp snmp-server enable traps snmp authentication
CISCO-FCC-MIB	snmp-server enable traps fcc
CISCO-DM-MIB	snmp-server enable traps fcdomain
CISCO-NS-MIB	snmp-server enable traps fens
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

MIB	関連コマンド
CISCO-RSCN-MIB	snmp-server enable traps rscn snmp-server enable traps rscn els snmp-server enable traps rscn ils
CISCO-ZS-MIB	snmp-server enable traps zone snmp-server enable traps zone default-zone-behavior-change snmp-server enable traps zone merge-failure snmp-server enable traps zone merge-success snmp-server enable traps zone request-reject snmp-server enable traps zone unsupp-mem



(注) ライセンス通知は、デフォルトではイネーブルです。

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

コマンド	目的
switch(config)# snmp-server enable traps	すべての SNMP 通知をイネーブルにします。
switch(config)# snmp-server enable traps aaa [server-state-change]	AAA SNMP 通知をイネーブルにします。
switch(config)# snmp-server enable traps entity [fru]	ENTITY-MIB SNMP 通知をイネーブルにします。
switch(config)# snmp-server enable traps license	ライセンス SNMP 通知をイネーブルにします。
switch(config)# snmp-server enable traps port-security	ポートセキュリティ SNMP 通知をイネーブルにします。
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。
- IETF 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。
- IETF 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。
- IETF extended Cisco : Cisco NX-OS は、インターフェイスに対して ifLinkUpDownTrapEnable (IF-MIB で定義) がイネーブルの場合は、IF-MIB に定義された通知 (linkUp、linkDown) および CISCO-IF-EXTENSION-MIB.my に定義された通知 (cieLinkUp、cieLinkDown) を送信します。Cisco NX-OS は、linkUp および linkDown 通知の IF-MIB に定義されている変数バインドに加え、シスコ固有の変数バインドも送信します。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	snmp-server enable traps link [cisco] [ietf ietf-extended] 例 : <pre>switch(config)# snmp-server enable traps link cisco</pre>	リンク SNMP 通知をイネーブルにします。

インターフェイスでのリンク通知のディセーブル化

個別のインターフェイスで linkUp および linkDown 通知をディセーブルにできます。フラッピングインターフェイス（Up と Down の間を頻繁に切り替わるインターフェイス）で、この制限通知を使用できます。

手順の概要

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

手順の詳細

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

TCP での SNMP に対するワンタイム認証のイネーブル化

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

コマンド	目的
switch(config)# snmp-server tcp-session [auth]	TCP セッション上で SNMP に対するワンタイム認証をイネーブルにします。デフォルトはディセーブルです。

SNMP スイッチの連絡先および場所の情報の割り当て

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# configuration terminal	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# snmp-server contact name	sysContact (SNMP 担当者名) を設定します。
ステップ 3	switch(config)# snmp-server location name	sysLocation (SNMP ロケーション) を設定します。
ステップ 4	switch# show snmp	(任意) 1つまたは複数の宛先プロファイルに関する情報を表示します。
ステップ 5	switch# copy running-config startup-config	(任意) この設定変更を保存します。

コンテキストとネットワーク エンティティ間のマッピング設定

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

手順の概要

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

手順の詳細

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

SNMP のディセーブル化

手順の概要

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

手順の詳細

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

	コマンドまたはアクション	目的
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 14 章

RMON の設定

この章の内容は、次のとおりです。

- [RMON について, 175 ページ](#)
- [RMON の設定時の注意事項および制約事項, 177 ページ](#)
- [RMON の設定, 177 ページ](#)
- [RMON の設定の確認, 179 ページ](#)
- [デフォルトの RMON 設定, 180 ページ](#)

RMON について

RMON は、各種のネットワーク エージェントおよびコンソール システムがネットワーク モニタリングデータを交換できるようにするためのインターネット技術特別調査委員会 (IETF) 標準モニタリング仕様です。Cisco NX-OS は、Cisco Nexus 5000 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で使用し、RMON アラームが発生したときにログ エントリまたは Simple Network Management Protocol (SNMP; 簡易ネットワーク管理プロトコル) 通知を生成できます。

Cisco Nexus 5000 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 5000 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 5000 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 5000 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 5000 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 アラームにアソシエートさせることができます。RMON は次のイベントタイプをサポートします。

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

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

下限アラームおよび上限アラームに異なるイベントを指定できます。

RMON の設定時の注意事項および制約事項

RMON には、次の注意事項および制限事項があります。

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

RMON の設定

RMON アラームの設定

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

次のパラメータを任意で指定することもできます。

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

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

手順の概要

1. `switch# configure terminal`
2. `switch(config)# rmon alarm index mib-object sample-interval {absolute | delta} rising-threshold value [event-index] falling-threshold value [event-index] [owner name]`
3. `switch(config)# rmon hcalarm index mib-object sample-interval {absolute | delta} rising-threshold-high value rising-threshold-low value [event-index] falling-threshold-high value falling-threshold-low value [event-index] [owner name] [storagetype type]`
4. (任意) `switch# show rmon {alarms | hcalarms}`
5. (任意) `switch# copy running-config startup-config`

手順の詳細

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

次に、RMON アラームを設定する例を示します。

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

RMON イベントの設定

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

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# rmon event index [description string] [log] [trap] [owner name]	RMON イベントを設定します。説明のストリングおよびオーナー名は、任意の英数字ストリングです。
ステップ 3	switch(config)# show rmon {alarms hcalarms}	(任意) RMON アラームまたは高容量アラームに関する情報を表示します。
ステップ 4	switch# copy running-config startup-config	(任意) この設定変更を保存します。

RMON の設定の確認

RMON 設定情報を表示するには、次のいずれかの作業を行います。

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

デフォルトの RMON 設定

次の表に、RMON パラメータのデフォルト設定を示します。

表 24: デフォルトの RMON パラメータ

パラメータ	デフォルト
アラーム	未設定。
イベント	未設定。



第 15 章

SPAN の設定

この章の内容は、次のとおりです。

- [SPAN に関する情報, 182 ページ](#)
- [SPAN 送信元, 182 ページ](#)
- [送信元ポートの特性, 183 ページ](#)
- [SPAN 宛先, 183 ページ](#)
- [宛先ポートの特性, 184 ページ](#)
- [SPAN の注意事項および制約事項, 184 ページ](#)
- [SPAN セッションの作成または削除, 184 ページ](#)
- [イーサネット宛先ポートの設定, 185 ページ](#)
- [SPAN セッションごとの MTU の切り捨ての設定, 186 ページ](#)
- [SPAN トラフィックのレート制限の設定, 187 ページ](#)
- [ファイバチャネル宛先ポートの設定, 188 ページ](#)
- [送信元ポートの設定, 190 ページ](#)
- [送信元ポートチャネル、VSAN、または VLAN の設定, 191 ページ](#)
- [SPAN セッションの説明の設定, 192 ページ](#)
- [SPAN セッションのアクティブ化, 193 ページ](#)
- [SPAN セッションの一時停止, 193 ページ](#)
- [SPAN 情報の表示, 194 ページ](#)

SPAN に関する情報

スイッチドポートアナライザ (SPAN) 機能 (ポートミラーリングまたはポートモニタリングとも呼ばれる) は、ネットワークアナライザによる分析のためのネットワークトラフィックを選択します。ネットワークアナライザは、Cisco SwitchProbe、ファイバチャネルアナライザ、またはその他のリモートモニタリング (RMON) プローブです。

SPAN 送信元

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

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

SPAN送信元インターフェイスが6Gbpsよりも大きいトラフィックを送信した場合、またはトラフィックがあまりにも急増した場合、デバイスは送信元インターフェイスでトラフィックをドロップします。送信元インターフェイスの実際のトラフィックのドロップを減らすために、SPAN宛先に対して **switchport monitor rate-limit 1G** コマンドを使用できます。ただし、SPANトラフィックは1Gbpsに制限されます。詳細は、[SPANトラフィックのレート制限の設定](#)、(187ページ)を参照してください。



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



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

送信元ポートの特性

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

送信元ポートの特性は、次のとおりです。

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

SPAN 宛先

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

送信元 SPAN	宛先 SPAN
イーサネット	イーサネット
ファイバチャネル	ファイバチャネル
ファイバチャネル	イーサネット (FCoE)
仮想ファイバチャネル	ファイバチャネル

送信元 SPAN	宛先 SPAN
仮想ファイバ チャンネル	イーサネット (FCoE)

宛先ポートの特性

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

- すべての物理ポートが可能です。イーサネット、イーサネット (FCoE)、またはファイバチャンネル、および仮想ファイバチャンネルポートは、宛先ポートにできません。
- 送信元ポートにはなれません。
- ポートチャンネルまたは SAN ポートチャンネルグループにはできません。
- SPAN セッションがアクティブなときは、スパニングツリーに参加しません。
- 任意の SPAN セッションのソース VLAN に属する場合、送信元リストから除外され、モニタリングされません。
- すべてのモニタリング対象送信元ポートの送受信トラフィックのコピーを受信します。宛先ポートがオーバーサブスクライブ型の場合、輻輳が発生する可能性があります。輻輳が発生すると、1 つまたは複数の送信元ポートでのトラフィック転送に影響を及ぼす可能性があります。

SPAN の注意事項および制約事項

SPAN トラフィックは、実稼働トラフィックに悪影響を及ぼさないように、次のように Nexus 5500 シリーズのスイッチでレート制限されます。

- SPAN は 8 ポート (1 ASIC) ごとに 5 Gbps にレート制限されます。
- RX-SPAN は、ポートの RX トラフィックが 5 Gbps を超える場合は、ポートごとに 0.71 Gbps にレート制限されます。

SPAN セッションの作成または削除

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

手順の概要

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

手順の詳細

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

次に、SPAN モニタ セッションを設定する例を示します。

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

イーサネット宛先ポートの設定

SPAN 宛先ポートとしてイーサネットインターフェイスを設定できます。



(注) SPAN 宛先ポートは、スイッチ上の物理ポートにのみ設定できます。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface ethernet** *slot/port*
3. switch(config-if)# **switchport monitor**
4. switch(config-if)# **exit**
5. switch(config)# **monitor session** *session-number*
6. switch(config-monitor)# **destination interface ethernet** *slot/port*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	グローバルコンフィギュレーションモードを開始します。
ステップ 2	switch(config)# interface ethernet slot/port	指定されたスロットとポートでイーサネットインターフェイスのインターフェイス コンフィギュレーションモードを開始します。
ステップ 3	switch(config-if)# switchport monitor	指定されたイーサネット インターフェイスのモニタ モードを開始します。ポートが SPAN 宛先として設定されている場合、プライオリティフロー制御はディセーブルです。
ステップ 4	switch(config-if)# exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	switch(config)# monitor session session-number	指定した SPAN セッションのモニタ コンフィギュレーション モードを開始します。
ステップ 6	switch(config-monitor)# destination interface ethernet slot/port	イーサネット SPAN 宛先ポートを設定します。

次に、イーサネット SPAN 宛先ポートを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/3
switch(config-if)# switchport monitor
switch(config-if)# exit
switch(config)# monitor session 2
switch(config-monitor)# destination interface ethernet 1/3
switch(config-monitor)#
```

SPAN セッションごとの MTU の切り捨ての設定

SPAN トラフィック帯域幅を減らすには、SPAN セッションの各複製パケットで許可される最大バイト数を設定できます。この値は、最大伝送単位 (MTU) の切り捨てサイズと呼ばれます。設定されたサイズよりも大きい SPAN パケットはすべて、設定されたサイズに切り捨てられます。

手順の概要

1. switch# **configure terminal**
2. switch(config) # **monitor session session-number**
3. switch(config-monitor) # **[no] mtu**
4. (任意) switch(config-monitor) # **show monitor session session-number**
5. (任意) switch(config-monitor) # **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config) # monitor session session-number	モニタ コンフィギュレーション モードを開始し、MTU 切り捨てサイズが設定された SPAN セッションを指定します。
ステップ 3	switch(config-monitor) # [no] mtu	指定した SPAN セッションのパケットの MTU 切り捨てサイズを設定します。指定できる範囲は 64 ~ 1518 バイトです。
ステップ 4	switch(config-monitor) # show monitor session session-number	(任意) MTU 切り捨ての設定ステータス、セッションごとに各パケットで許可される最大バイト数、MTU 切り捨てがサポートされるモジュールとサポートされないモジュールを含む、SPAN セッションのステータスを表示します。
ステップ 5	switch(config-monitor) # copy running-config startup-config	(任意) 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

次に、SPAN セッションの MTU 切り捨てを設定する例を示します。

```
switch# configure terminal
switch(config) # monitor session 3
switch(config-monitor) # mtu
switch(config-monitor) # copy running-config startup-config
switch(config-monitor) #
```

SPAN トラフィックのレート制限の設定

モニタセッション全体で SPAN トラフィックのレート制限を 1Gbps に設定することで、モニタされた実稼働トラフィックへの影響を回避できます。Nexus 5000 シリーズスイッチの場合は次のようになります。

- 1 Gbps を超えるトラフィックを 1 Gb の SPAN 宛先インターフェイスに分散させる場合、SPAN 送信元トラフィックはドロップされません。
- 6 Gbps を超える (ただし 10 Gbps 未満) のトラフィックを 10 Gb の SPAN 宛先インターフェイスに分散させる場合、SPAN トラフィックは、宛先またはスニファで 10 Gbps が可能な場合でも、1 Gbps に制限されます。

Nexus 5500 シリーズで、SPAN トラフィックはデフォルトで 1Gbps にレート制限されるため、**switchport monitor rate-limit 1G** インターフェイス コマンドはサポートされません。また、モニタ対象実稼働トラフィックへの影響を回避するため、次のようになります。

- SPAN は 8 ポート (1 ASIC) ごとに 5 Gbps にレート制限されます。
- RX-SPAN は、ポートの RX トラフィックが 5 Gbps を超える場合は、ポートごとに 0.71 Gbps にレート制限されます。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# interface ethernet slot/port	スロット値およびポート値による選択で指定されたイーサネット インターフェイスで、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# switchport monitor rate-limit 1G	レート制限が 1 Gbps であることを指定します。 (注) トラフィックはデフォルトで 1 Gbps にレート制限されているため、このコマンドは Nexus 5500 プラットフォームではサポートされません。
ステップ 4	switch(config-if)# exit	グローバル コンフィギュレーション モードに戻ります。

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

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

ファイバチャネル宛先ポートの設定



(注) SPAN 宛先ポートは、スイッチ上の物理ポートにのみ設定できます。

ファイバチャネルポートを SPAN 宛先ポートとして設定できます。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface fc slot/port**
3. switch(config-if)# **switchport mode SD**
4. switch(config-if)# **switchport speed 1000**
5. switch(config-if)# **exit**
6. switch(config)# **monitor session session-number**
7. switch(config-monitor)# **destination interface fc slot/port**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# interface fc slot/port	スロット値およびポート値による選択で指定されたファイバチャネルインターフェイスで、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# switchport mode SD	インターフェイスを SPAN 宛先 (SD) モードに設定します。
ステップ 4	switch(config-if)# switchport speed 1000	インターフェイス速度を 1000 に設定します。自動速度オプションは使用できません。
ステップ 5	switch(config-if)# exit	グローバルコンフィギュレーションモードに戻ります。
ステップ 6	switch(config)# monitor session session-number	モニタ コンフィギュレーション モードを開始します。
ステップ 7	switch(config-monitor)# destination interface fc slot/port	ファイバチャネル宛先ポートを設定します。

次に、イーサネット SPAN 宛先ポートを設定する例を示します。

```
switch# configure terminal
switch(config)# interface fc 2/4
switch(config-if)# switchport mode SD
switch(config-if)# switchport speed 1000
switch(config-if)# exit
switch(config)# monitor session 2
switch(config-monitor)# destination interface fc 2/4
```

送信元ポートの設定

送信元ポートは、イーサネット、ファイバチャネル、または仮想ファイバチャネルのポートに設定できます。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config) # monitor session session-number	指定したモニタリングセッションのモニタ コンフィギュレーション モードを開始します。
ステップ 3	switch(config-monitor) # source interface type slot/port [rx tx both]	送信元およびパケットをコピーするトラフィック方向を設定します。イーサネット、ファイバチャネル、または仮想ファイバチャネルのポート範囲を入力できます。コピーするトラフィック方向を、入力 (rx)、出力 (tx)、または両方向 (both) として指定できます。デフォルトは both です。

次に、イーサネット SPAN 送信元ポートを設定する例を示します。

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

次に、ファイバチャネル SPAN 送信元ポートを設定する例を示します。

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

次に、仮想ファイバチャネル SPAN 送信元ポートを設定する例を示します。

```
switch# configure terminal
switch(config)# monitor session 2
switch(config-monitor)# source interface vfc 129
switch(config-monitor)#
```

送信元ポート チャンネル、VSAN、または VLAN の設定

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



(注) Cisco Nexus 5000 シリーズ スイッチは、2 つのアクティブな SPAN セッションをサポートします。Cisco Nexus 5548 スイッチは、4 つのアクティブな SPAN セッションをサポートします。2 つを超える SPAN セッションを設定すると、最初の 2 つのセッションがアクティブになります。起動中にアクティブなセッションの順序が逆になり、最後の 2 つのセッションがアクティブになります。たとえば、セッション 1 ~ 10 を設定して、1 と 2 がアクティブな場合、リブート後はセッション 9 と 10 がアクティブになります。確定した動作を可能にするには、**monitor session session-number shut** コマンドを使用して、セッション 3 ~ 10 を明示的に一時停止します。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config) # monitor session session-number	指定した SPAN セッションのモニタ コンフィギュレーション モードを開始します。
ステップ 3	switch(config-monitor) # source {interface {port-channel san-port-channel} channel-number [rx tx both] vlan vlan-range vsan vsan-range }	ポート チャンネル、SAN ポートチャンネル、VLAN、または VSAN 送信元を設定します。VLAN または VSAN 送信元の場合、モニタ方向は暗黙的です。

次に、ポート チャンネル SPAN 送信元を設定する例を示します。

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

次に、SAN ポート チャネル SPAN 送信元を設定する例を示します。

```
switch(config-monitor)#switch# configure terminal
switch(config)# monitor session 2
switch(config-monitor)# source interface san-port-channel 3 rx
switch(config-monitor)#
```

次に、VLAN の SPAN 送信元を設定する例を示します。

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

switch(config-monitor)# 次に、VSAN SPAN 送信元を設定する例を示します。

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

SPAN セッションの説明の設定

参照しやすいように、SPAN セッションにわかりやすい名前を付けることができます。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	グローバルコンフィギュレーションモードを開始します。
ステップ 2	switch(config) # monitor session session-number	指定した SPAN セッションのモニタ コンフィギュレーションモードを開始します。
ステップ 3	switch(config-monitor) # description description	SPAN セッションのわかりやすい名前を作成します。

次に、SPAN セッションの説明を設定する例を示します。

```
switch# configure terminal
switch(config) # monitor session 2
switch(config-monitor) # description monitoring ports eth2/2-eth2/4
switch(config-monitor) #
```


SPAN セッションのアクティブ化

デフォルトでは、セッション ステートは **shut** に保持されます。送信元から宛先へパケットをコピーするセッションを開くことができます。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<code>switch# configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>switch(config) # no monitor session {all session-number} shut</code>	指定された SPAN セッションまたはすべてのセッションを開始します。

次に、SPAN セッションをアクティブにする例を示します。

```
switch# configure terminal
switch(config) # no monitor session 3 shut
```

SPAN セッションの一時停止

デフォルトでは、セッション ステートは **shut** です。



- (注) Cisco Nexus スイッチは、2つのアクティブな SPAN セッションをサポートします。Cisco Nexus 5548 スイッチは、4つのアクティブな SPAN セッションをサポートします。2つを超える SPAN セッションを設定すると、最初の 2 つのセッションがアクティブになります。起動中にアクティブなセッションの順序が逆になり、最後の 2 つのセッションがアクティブになります。たとえば、セッション 1～10 を設定して、1 と 2 がアクティブな場合、リブート後はセッション 9 と 10 がアクティブになります。確定した動作を可能にするには、**monitor session session-number shut** コマンドを使用して、セッション 3～10 を明示的に一時停止します。

手順の概要

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

手順の詳細

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

次に、SPAN セッションを一時停止する例を示します。

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

SPAN 情報の表示

手順の概要

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

手順の詳細

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

次に、SPAN セッションの情報を表示する例を示します。

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

次に、SPAN セッションの詳細を表示する例を示します。

```
switch# show monitor session 2
session 2
-----
type : local
state : up
source intf :
rx : fc3/1
tx : fc3/1
both : fc3/1
source VLANs :
rx :
```

```
source VSANs      :  
  rx              : 1  
destination ports : Eth3/1
```




索引

C

- Call Home の通知 [137](#)
 - syslog の XML 形式 [137](#)
 - syslog のフル テキスト形式 [137](#)

G

- GOLD 診断 [87, 88, 89](#)
 - 拡張モジュール [89](#)
 - 設定 [89](#)
 - ヘルス モニタリング [88](#)
 - ランタイム [87](#)

I

- ID [116](#)
 - シリアル ID [116](#)

L

- linkDown 通知 [168, 170](#)
- linkUp 通知 [168, 170](#)

S

- Session Manager [81, 82, 83, 84, 85](#)
 - ACL セッションの設定例 [85](#)
 - 制限事項 [82](#)
 - セッションの確認 [83](#)
 - セッションのコミット [84](#)
 - セッションの廃棄 [84](#)
 - セッションの保存 [84](#)
 - 設定の確認 [85](#)
 - 説明 [81](#)

Session Manager (続き)

- 注意事項 [82](#)
- show コマンドの追加、アラート グループ [130](#)
 - Smart Call Home [130](#)
- Smart Call Home [111, 112, 113, 121, 122, 123, 125, 127, 129, 130, 131, 132, 133, 134, 135, 136](#)
 - show コマンドの追加、アラート グループ [130](#)
 - 宛先プロファイル [112](#)
 - 宛先プロファイル、作成 [125](#)
 - 宛先プロファイル、変更 [127](#)
 - アラート グループ [113](#)
 - アラート グループのアソシエート [129](#)
 - 確認 [136](#)
 - 設定のテスト [135](#)
 - 説明 [111](#)
 - 前提条件 [122](#)
 - 担当者情報、設定 [123](#)
 - 注意事項および制約事項 [121](#)
 - 重複メッセージ抑制、ディセーブル化 [133, 134](#)
 - 定期的なインベントリ通知 [132](#)
 - デフォルト設定 [122](#)
 - 電子メールの詳細、設定 [131](#)
 - 登録 [123](#)
 - メッセージ フォーマット オプション [112](#)
- Smart Call Home のメッセージ [112, 115](#)
 - フォーマット オプション [112](#)
 - レベルの設定 [115](#)
- SNMP [153, 154, 156, 157, 158, 159, 160, 161, 162, 163, 164, 165, 172](#)
 - CLI を使用したユーザの同期 [157](#)
 - アクセス グループ [158](#)
 - インバンド アクセス [165](#)
 - 機能の概要 [153](#)
 - グループ ベースのアクセス [158](#)
 - セキュリティ モデル [156](#)
 - 送信元インターフェイス [163, 164](#)
 - 注意事項および制約事項 [158](#)
 - 通知 レシーバ [162](#)

SNMP (続き)

- ディセーブル化 [172](#)
- デフォルト設定 [158](#)
- トラップ通知 [154](#)
- バージョン3のセキュリティ機能 [154](#)
- メッセージの暗号化 [160](#)
- ユーザの設定 [159](#)
- ユーザベースのセキュリティ [156](#)
 - SNMP [156](#)
- 要求のフィルタリング [161](#)
- ライセンス [158](#)

SNMPv3 [154, 160](#)

- セキュリティ機能 [154](#)
- 複数のロールの割り当て [160](#)

SNMP (簡易ネットワーク管理プロトコル) [155](#)

- バージョン [155](#)

SNMP のデフォルト設定 [158](#)SNMP 要求のフィルタリング [161](#)SPAN [182, 183, 184, 185, 187, 188, 190, 191, 192, 193, 194](#)

- VLAN、設定 [191](#)
- VSAN、設定 [191](#)
- 宛先 [183](#)
- 宛先ポート、特性 [184](#)
- イーサネット宛先ポート、設定 [185](#)
- 作成、セッションの削除 [184](#)
- 出力送信元 [182](#)
- 情報の表示 [194](#)
- セッションのアクティブ化 [193](#)
- 説明、設定 [192](#)
- 送信元ポート、設定 [190](#)
- 送信元ポートチャネル、設定 [191](#)
- 注意事項および制約事項 [184](#)
- 特性、送信元ポート [183](#)
- 入力送信元 [182](#)
- ファイバチャネル宛先ポート、設定 [188](#)
- モニタリングの送信元 [182](#)
- レート制限、設定 [187](#)

SPAN 送信元 [182](#)

- 出力 [182](#)
- 入力 [182](#)

syslog [103](#)

- 設定 [103](#)

あ

- 宛先 [183](#)
 - SPAN [183](#)

宛先プロファイル [112](#)

- Smart Call Home [112](#)

宛先プロファイル、作成 [125](#)

- Smart Call Home [125](#)

宛先プロファイル、変更 [127](#)

- Smart Call Home [127](#)

宛先ポート、特性 [184](#)

- SPAN [184](#)

アラートグループ [113](#)

- Smart Call Home [113](#)

アラートグループのアソシエート [129](#)

- Smart Call Home [129](#)

い

イーサネット宛先ポート、設定 [185](#)

- SPAN [185](#)

か

確認 [136](#)

- Smart Call Home [136](#)

関連情報 [41](#)

- モジュールの事前プロビジョニング [41](#)

さ

サーバ ID [116](#)

- 説明 [116](#)

作成、セッションの削除 [184](#)

- SPAN [184](#)

し

システムメッセージロギング [93, 95](#)

- 関連情報 [93](#)
- 注意事項および制約事項 [95](#)
- ライセンス [95](#)

システムメッセージロギングの設定 [95](#)

- デフォルト [95](#)

情報の表示 [194](#)

- SPAN [194](#)

シリアル ID [116](#)

- 説明 [116](#)

新規情報 1

説明 1

診断 87, 88, 89, 91

拡張モジュール 89

設定 89

デフォルト設定 91

ヘルス モニタリング 88

ランタイム 87

す

スイッチドポートアナライザ 182

せ

制約事項 69

ユーザアカウント 69

セッションのアクティブ化 193

SPAN 193

セッションの実行 84

設定のテスト 135

Smart Call Home 135

説明、設定 192

SPAN 192

そ

送信元 ID 116

Call Home イベントの形式 116

送信元ポート、設定 190

SPAN 190

送信元ポート、特性 183

SPAN 183

た

担当者情報、設定 123

Smart Call Home 123

ち

注意事項および制約事項 95, 121, 158, 184

Smart Call Home 121

SNMP 158

注意事項および制約事項 (続き)

SPAN 184

システムメッセージロギング 95

重複メッセージ抑制、ディセーブル化 133, 134

Smart Call Home 133, 134

つ

通知レシーバ 162

SNMP 162

て

定期的なインベントリ通知、設定 132

Smart Call Home 132

デバイス ID 116

Call Home の形式 116

デフォルト設定 85, 122

Smart Call Home 122

ロールバック 85

電子メール通知 111

Smart Call Home 111

電子メールの詳細、設定 131

Smart Call Home 131

と

登録 123

Smart Call Home 123

トラップ通知 154

は

パスワード要件 70

ふ

ファイバチャネル宛先ポート、設定 188

SPAN 188

へ

- ヘルス モニタリング診断 [88](#)
 - 情報 [88](#)
- 変更情報 [1](#)
 - 説明 [1](#)

め

- メッセージの暗号化 [160](#)
 - SNMP [160](#)

も

- モジュールの事前プロビジョニング [41](#)
 - 関連情報 [41](#)

ゆ

- ユーザ [69](#)
 - 説明 [69](#)
- ユーザアカウント [69, 70](#)
 - 制約事項 [69](#)
 - パスワード [70](#)

よ

- 要件 [70](#)
 - ユーザ パスワード [70](#)

ら

- ライセンス [95, 158](#)
 - SNMP [158](#)
 - システム メッセージ ロギング [95](#)
- ランタイム診断 [87](#)
 - 情報 [87](#)

れ

- レート制限、設定 [187](#)
 - SPAN [187](#)

ろ

- ロール [69](#)
 - 認証 [69](#)
- ロールバック [81, 82, 85](#)
 - 制限事項 [82](#)
 - 設定の確認 [85](#)
 - 設定例 [82](#)
 - 説明 [81](#)
 - チェックポイント コピーの作成 [82](#)
 - チェックポイントのコピー [81](#)
 - チェックポイントファイルの削除 [82](#)
 - チェックポイントファイルへの復帰 [82](#)
 - 注意事項 [82](#)
 - デフォルト設定 [85](#)
 - ハイ アベイラビリティ [81](#)
 - ロールバックの実装 [82](#)