Cisco DCNM for SAN システム管理コンフィギュレーション ガイド

Cisco DCNM for SAN、Release 5.x
2011 年 6 月

Text Part Number: OL-24960-01-J

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

Cisco DCNM for SAN システム管理コンフィギュレーション ガイド

CONTENTS

新機能および変更情報

Cisco DCNM Release 5.2 以降、Cisco Fabric Manager と Cisco Data Center Network Manager for LAN は、Cisco Data Center Network Manager（DCNM）と呼ばれる 1 つの製品に統合されており、LAN 環境と SAN 環境の両方を管理できるようになっています。この製品統合に伴い、Cisco Fabric Manager の名称は、Cisco DCNM for SAN という名称に変更されています。

次のマニュアルの変更は、統合された Cisco DCNM 製品に対応しています。

- Cisco DCNM Release 5.2 の Cisco DCNM 製品のマニュアルは、Cisco DCNM for LAN という名称でタイトルが変更されています。
- Cisco DCNM Release 5.2 の Cisco Fabric Manager 製品のマニュアルは、Cisco DCNM for SAN という名称でタイトルが変更されています。
- Cisco DCNM for SAN 製品のマニュアルは、Cisco.com の http://www.cisco.com/en/US/products/ps9369/tsd_products_support_configure.html にある Data Center Network Manager の一覧ページで現在公開されています。

  この URL は、Cisco DCNM for LAN 製品のマニュアルの一覧ページでもあります。
- Cisco DCNM Release 5.2 よりも前のソフトウェア リリースに対する Cisco Fabric Manager のマニュアルは、Cisco Fabric Manager という名称のままであり、現行の Cisco.com の一覧ページからまだ入手できます。
  http://www.cisco.com/en/US/products/ps10495/tsd_products_support_configure.html

  Cisco DCNM Release 5.2 よりも前の Cisco Fabric Manager ソフトウェアのリリースを使用している場合は、引き続き Cisco Fabric Manager のマニュアルを使用する必要があります。
- DCNM-SAN という名称が、Cisco Data Center Network Manager のユーザ インターフェイスにおいて Cisco DCNM for SAN の代わりに使用されます。同様に、DCNM-LAN という名称が、ユーザ インターフェイスにおいて Cisco DCNM for LAN の代わりに使用されます。ユーザ インターフェイスと一致させるために、製品マニュアルでも DCNM-SAN と DCNM-LAN の名称が使用されています。
- 次の新しい資料は、Cisco DCNM for LAN と DCNM for SAN の両方に対応しており、Cisco DCNM の新しいライセンス モデル、新しいインストール プロセス、および新しい機能が説明されています。
  - 『*Cisco DCNM Installation and Licensing Guide*』
  - 『*Cisco DCNM Release Notes*』

Cisco DCNM マニュアルの全リストについては、「はじめに」の「関連資料」を参照してください。

Cisco MDS NX-OS Release 4.2(1) より、新機能に固有のコンフィギュレーション ガイドでソフトウェア設定に関する次の情報を入手できます。

- システム管理

- インターフェイス
- ファブリック
- Quality of Service
- セキュリティ
- IP サービス
- ハイ アベイラビリティおよび冗長性

これらの新しいガイドの情報は、以前は『*Cisco MDS 9000 Family CLI Configuration Guide*』および『*Cisco MDS 9000 Family Fabric Manager Configuration Guide*』に記載されていました。これらのコンフィギュレーション ガイドは、Cisco.com に用意されており、MDS NX-OS Release 4.2(1) 以前のすべてのソフトウェア リリース用に参照できます。各ガイドには、特定のリリースで導入された機能や使用可能な機能が記載されています。ご使用のスイッチにインストールされているソフトウェアに対応したコンフィギュレーション ガイドを選択して参照してください。

『*Cisco MDS 9000 Family CLI Configuration Guide*』と『*Cisco MDS 9000 Family Fabric Manager Configuration Guide*』は、現在、Nexus オペレーティング システムを実行する製品で共通の次のガイドにあります。

- 『*Cisco NX-OS Family Licensing Guide*』: ライセンス モデルと機能ライセンスについて説明します。
- 『*Cisco NX-OS Fundamentals Configuration Guide*』: スイッチ セットアップ ユーティリティについて説明し、一般的な CLI、ファイル システム、およびコンフィギュレーション情報について説明します。

資料のタイトルの一覧表については、「はじめに」の「関連資料」を参照してください。

Cisco MDS NX-OS Release 4.2(x) に関する詳細については、『*Cisco MDS 9000 Family Release Notes*』を次のシスコ Web サイトから入手して参照してください。

http://www.cisco.com/en/US/products/ps5989/prod_release_notes_list.htm

このマニュアルについて

新しい『*Cisco Fabric Manager System Management Configuration Guide*』の情報は、以前は『*Cisco MDS 9000 Family Fabric Manager Configuration Guide*』の次の場所にありました。

- Part 2 :「Installation and Switch Management」
- Part 5 :「Security」
- Part 8 :「Network and Switch Monitoring」
- Part 9 :「Troubleshooting」

表 1 に、このガイドで取り上げる MDS NX-OS Release 4.2(1) 以降の新機能および変更された機能を示します。

表 1　新機能および変更された機能

機能	追加または変更された内容	変更されたリリース	参照先
Call Home HTTP プロキシ サーバ	Cisco DCNM-SAN を使用して Call Home HTTP プロキシ サーバを設定する方法についての情報が追加されました。	5.2(1)	第 4 章「Call Home の設定」
Call Home ウィザード	Cisco DCNM-SAN を使用して Call Home ウィザードを設定する方法についての情報が追加されました。	5.2(1)	第 4 章「Call Home の設定」
通知の拡張	Device Manager を使用したイベント フィルタの通知の拡張が追加されました。	5.0(1a)	第 4 章「Call Home の設定」
Syslog の拡張	Fabric Manager からの Syslog のモニタリングが追加されました。	5.0(1a)	第 3 章「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 ロギング情報が追加されました。		
CFS の保留の差異	CFS の保留の差異のスクリーンショットが新しく追加されました。	5.0(1a)	第 2 章「CFS インフラストラクチャの使用」
[Call Home Destination] タブ	[Destination] タブの拡張を追加。	4.2(1)	第 4 章「Call Home の設定」
Call Home HTTP のサポート	Call Home HTTP 拡張を追加。	4.2(1)	第 4 章「Call Home の設定」
[SNMP Trap] の [Control] タブ	NX-OS Release 4.2(1) で追加された新しい [Control] タブの詳細を追加。	4.2(1)	第 9 章「SNMP の設定」
Domain Manager のターボ モード	Domain Manager のターボ モードの設定手順を追加。	4.2(1)	第 10 章「ドメイン パラメータの設定」

はじめに

ここでは、『Cisco DCNM for SAN システム管理コンフィギュレーション ガイド』の対象読者、構成、および表記法について説明します。また、関連マニュアルの入手方法についても説明します。

対象読者

このマニュアルは、マルチレイヤ ディレクタおよびファブリック スイッチの Cisco MDS 9000 ファミリの設定および保守を担当する、経験豊富なネットワーク管理者を対象にしています。

マニュアルの構成

このマニュアルは、次の章で構成されています。

章	タイトル	説明
第 1 章	「システム管理の概要」	CLI を使用してスイッチを監視および管理するための、システム管理機能の概要について説明します。
第 2 章	「CFS インフラストラクチャの使用」	効率的なデータベースの配布を実現するための Cisco Fabric Services（CFS）インフラストラクチャの使用方法について説明します。
第 3 章	「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 ロギングの設定手順および表示方法を説明します。
第 4 章	「Call Home の設定」	Call Home サービスの詳細と、Call Home、イベント トリガー、連絡先情報、宛先プロファイル、E メール オプションについて説明します。
第 5 章	「メンテナンス ジョブのスケジューリング」	すべての Cisco MDS 9000 ファミリ スイッチの設定およびメンテナンス作業をスケジューリングするのに役立つ Cisco MDS コマンド スケジューラ機能について説明します。
第 6 章	「システム プロセスおよびログのモニタ」	システム プロセスおよびステータスの表示方法を説明します。さらに、コア ファイルおよびログ ファイルの設定手順、HA ポリシー、ハートビートおよび Watchdog チェック、アップグレードのリセットについても説明します。

章	タイトル	説明
第 7 章	「Embedded Event Manager の設定」	デバイス上の重要なイベントを検出し、処理する Embedded Event Manager の詳細について説明します。
第 8 章	「RMON の設定」	RMON を使用してアラームおよびイベントを設定する手順を説明します。
第 9 章	「SNMP の設定」	CLI を使用して作成したロールの SNMP による変更方法について詳述します。
第 10 章	「ドメイン パラメータの設定」	プリンシパル スイッチの選出、ドメイン ID の配布、FC ID の割り当て、ファブリック再設定機能などのファイバ チャネル ドメイン（fcdomain）機能について説明します。
第 11 章	「SPAN を使用したネットワーク トラフィックのモニタリング」	Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）、SPAN 送信元、フィルタ、SPAN セッション、SD ポート特性、および設定について説明します。
第 12 章	「Fabric Configuration Server の設定」	Fabric Configuration Server（FCS）機能の設定方法と表示方法について説明します。

表記法

コマンドの説明では、次の表記法を使用しています。

太字	コマンドおよびキーワードは太字で示しています。
イタリック体	ユーザが値を指定する引数は、イタリック体で示しています。
[ ]	角カッコの中の要素は、省略可能です。
[x | y | z]	どれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。

出力例では、次の表記法を使用しています。

`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*」を意味します。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

Cisco MDS 9000 ファミリのマニュアル セットには次のマニュアルが含まれます。オンラインでドキュメントを検索するには、次の Web サイトにある Cisco MDS NX-OS Documentation Locator を使用してください。

http://www.cisco.com/en/US/docs/storage/san_switches/mds9000/roadmaps/doclocater.htm

リリース ノート

- 『*Cisco MDS 9000 Family Release Notes for Cisco MDS NX-OS Releases*』
- 『*Cisco MDS 9000 Family Release Notes for MDS SAN-OS Releases*』
- 『*Cisco MDS 9000 Family Release Notes for Cisco MDS 9000 EPLD Images*』
- 『*Cisco DCNM Release Notes*』

規制の順守と安全に関する情報

- 『*Regulatory Compliance and Safety Information for the Cisco MDS 9000 Family*』

互換性に関する情報

- 『*Cisco Data Center Interoperability Support Matrix*』
- 『*Cisco MDS 9000 NX-OS Hardware and Software Compatibility Information and Feature Lists*』
- 『*Cisco MDS 9000 Family Switch-to-Switch Interoperability Configuration Guide*』

ハードウェアの設置

- 『*Cisco MDS 9500 Series Hardware Installation Guide*』
- 『*Cisco MDS 9200 Series Hardware Installation Guide*』
- 『*Cisco MDS 9100 Series Hardware Installation Guide*』
- 『*Cisco MDS 9124 and Cisco MDS 9134 Multilayer Fabric Switch Quick Start Guide*』

ソフトウェアのインストールおよびアップグレード

- 『*Cisco MDS 9000 NX-OS Software Upgrade and Downgrade Guide*』

Cisco NX-OS

- 『*Cisco MDS 9000 Family NX-OS Licensing Guide*』
- 『*Cisco MDS 9000 Family NX-OS Fundamentals Configuration Guide*』
- 『*Cisco MDS 9000 Family NX-OS System Management Configuration Guide*』
- 『*Cisco MDS 9000 Family NX-OS Interfaces Configuration Guide*』
- 『*Cisco MDS 9000 Family NX-OS Fabric Configuration Guide*』
- 『*Cisco MDS 9000 Family NX-OS Quality of Service Configuration Guide*』
- 『*Cisco MDS 9000 Family NX-OS Security Configuration Guide*』
- 『*Cisco MDS 9000 Family NX-OS IP Services Configuration Guide*』
- 『*Cisco MDS 9000 Family NX-OS Intelligent Storage Services Configuration Guide*』
- 『*Cisco MDS 9000 Family NX-OS High Availability and Redundancy Configuration Guide*』
- 『*Cisco MDS 9000 Family NX-OS Inter-VSAN Routing Configuration Guide*』
- 『*Cisco MDS 9000 Family Cookbook for Cisco MDS SAN-OS*』

Cisco DCNM-SAN

- 『*Cisco DCNM Fundamentals Guide, Release 5.x*』
- 『*System Management Configuration Guide, Cisco DCNM for SAN, Release 5.x*』
- 『*Interfaces Configuration Guide, Cisco DCNM for SAN, Release 5.x*』
- 『*Fabric Configuration Guide, Cisco DCNM for SAN, Release 5.x*』
- 『*Quality of Service Configuration Guide, Cisco DCNM for SAN, Release 5.x*』
- 『*Security Configuration Guide, Cisco DCNM for SAN, Release 5.x*』
- 『*IP Services Configuration Guide, Cisco DCNM for SAN, Release 5.x*』
- 『*Intelligent Storage Services Configuration Guide, Cisco DCNM for SAN, Release 5.x*』
- 『*High Availability and Redundancy Configuration Guide, Cisco DCNM for SAN, Release 5.x*』
- 『*Inter-VSAN Routing Configuration Guide, Cisco DCNM for SAN, Release 5.x*』
- 『*SMI-S and Web Services Programming Guide, Cisco DCNM for SAN, Release 5.x*』

コマンドライン インターフェイス

- 『*Cisco MDS 9000 Family Command Reference*』

インテリジェント ストレージ ネットワーキング サービス コンフィギュレーション ガイド

- 『*Cisco MDS 9000 Family I/O Acceleration Configuration Guide*』
- 『*Cisco MDS 9000 Family SANTap Deployment Guide*』
- 『*Cisco MDS 9000 Family Data Mobility Manager Configuration Guide*』
- 『*Cisco MDS 9000 Family Storage Media Encryption Configuration Guide*』

トラブルシューティングおよび参考資料

- 『*Cisco MDS 9000 Family and Nexus 7000 Series System Messages Reference*』
- 『*Cisco MDS 9000 Family SAN-OS Troubleshooting Guide*』
- 『*Cisco MDS 9000 Family NX-OS MIB Quick Reference*』
- 『*Cisco DCNM for SAN Database Schema Reference*』

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は、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 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。

CHAPTER 1

システム管理の概要

システム管理機能を使用し、Cisco DCNM-SAN を使用してスイッチをモニタおよび管理できます。そのような機能には、Call Home、SNMP、RMON、SPAN、および Embedded Event Manager（EEM）があります。

この章では、これらの機能について説明します。この章の内容は次のとおりです。

Cisco Fabric Service

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、Cisco Fabric Services（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。

CFS の設定方法については、第 2 章「CFS インフラストラクチャの使用」を参照してください。

システム メッセージ

システム メッセージは、Telnet、SSH、コンソール ポートのいずれかを通じてスイッチにアクセスするか、システム メッセージ ロギング サーバ上のログを参照することにより、リモートでモニタされます。ログ メッセージは、システム再起動後には消去されています。

システム メッセージの設定方法については、第 3 章「システム メッセージ ロギングの設定」を参照してください。

Call Home

Call Home は、重要なシステム イベントを E メールで通知します。ポケットベル サービス、通常の電子メール、または XML ベースの自動解析アプリケーションとの適切な互換性のために、さまざまなメッセージの形式が使用できます。この機能の一般的な用途としては、ネットワーク サポート技術者を直接ポケットベルで呼び出したり、Network Operations Center（NOC; ネットワーク オペレーション センター）に E メールで通知したり、Technical Assistance Center で直接ケースを作成するために Cisco Smart Call Home サービスを使用することが挙げられます。

Call Home の設定方法については、第 4 章「Call Home の設定」を参照してください。

スケジューラ

Cisco MDS コマンド スケジューラ機能を使用すると、Cisco MDS 9000 ファミリのすべてのスイッチで、設定およびメンテナンス ジョブをスケジュールできます。この機能を使用して、一度だけ実行するジョブや定期的に実行するジョブをスケジュールできます。Cisco NX-OS コマンド スケジューラは、将来の指定した時刻に 1 つ以上のジョブ（CLI コマンドのセット）をスケジュールするための機構を提供します。ジョブは、将来の指定した時刻に一度だけ実行することも、定期的に実行することもできます。

Cisco MDS コマンド スケジューラ機能の設定方法については、第 5 章「メンテナンス ジョブのスケジューリング」を参照してください。

システム プロセスとログ

スイッチの状態は、さまざまなシステム プロセスとログによってモニタできます。Online Health Management System（システム ヘルス）は、ハードウェア障害検出および復旧機能です。この Health Management System は、Cisco MDS 9000 ファミリの任意のスイッチング、サービス、スーパーバイザ モジュールの全般的な状態を確認します。

スイッチの状態のモニタリングについては、第 6 章「システム プロセスおよびログのモニタ」を参照してください。

SNMP

Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）は、ネットワーク デバイス間で管理情報をやり取りするためのアプリケーション層プロトコルです。すべての Cisco MDS 9000 ファミリ スイッチで、SNMPv1、SNMPv2c、および SNMPv3 の 3 つの SNMP バージョンが使用できます。CLI と SNMP は、Cisco MDS 9000 ファミリのすべてのスイッチで共通のロールを使用します。SNMP を使用して CLI で作成したロールを変更したり、その逆を行うことができます。

CLI ユーザと SNMP ユーザのユーザ、パスワード、ロールは、すべて同じです。CLI を通じて設定されたユーザは SNMP（たとえば、DCNM-SAN や Device Manager）を使用してスイッチにアクセスでき、その逆も可能です。

SNMP の設定方法については、第 7 章「SNMP の設定」を参照してください。

RMON

RMON は、各種のネットワーク エージェントおよびコンソール システムがネットワーク モニタリング データを交換できるようにするための、Internet Engineering Task Force（IETF）標準モニタリング仕様です。RMON のアラームとイベントを使用し、Cisco SAN-OS Release 2.0(1b) 以降または Cisco Release NX-OS 4.1(3) 以降のソフトウェアが動作する Cisco MDS 9000 ファミリ スイッチをモニタできます。

RMON の設定方法については、第 8 章「RMON の設定」を参照してください。

ドメイン パラメータ

Fibre Channel domain（fcdomain; ファイバ チャネル ドメイン）機能では、FC-SW-2 標準で記述されているように、主要スイッチ選択、ドメイン ID 配信、FC ID 割り当て、ファブリック再設定機能が実行されます。ドメインは VSAN 単位で設定されます。ドメイン ID を設定しない場合、ローカル スイッチはランダムな ID を使用します。

ファイバ チャネル ドメイン機能の設定方法については、第 9 章「ドメイン パラメータの設定」を参照してください。

SPAN

Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）機能は、Cisco MDS 9000 ファミリのスイッチ専用の機能です。SPAN は、ファイバ チャネル インターフェイスを通じてネットワーク トラフィックをモニタします。任意のファイバ チャネル インターフェイスを通るトラフィックは、SPAN 宛先ポート（SD ポート）という専用ポートに複製することができます。スイッチの任意のファイバ チャネル ポートを SD ポートとして設定できます。SD ポート モードに設定したインターフェイスは、標準データ トラフィックには使用できません。ファイバ チャネル アナライザを SD ポートに接続して、SPAN トラフィックをモニタできます。

SPAN 機能については、第 10 章「SPAN を使用したネットワーク トラフィックのモニタリング」を参照してください。

Fabric Configuration Server

Fabric Configuration Server（FCS）を使用すると、トポロジ属性を検出したり、ファブリック要素の設定情報リポジトリを維持したりすることができます。通常、管理アプリケーションは N ポートを通してスイッチの FCS に接続されます。Cisco MDS 9000 ファミリ スイッチ環境では、複数の VSAN がファブリックを構成し、VSAN ごとに 1 つの FCS インスタンスが存在します。

FCS の設定方法については、第 11 章「Fabric Configuration Server の設定」を参照してください。

CHAPTER 2

CFS インフラストラクチャの使用

Cisco Fabric Service（CFS）は、ファブリック内で自動的に設定を同期化するための、共通のインフラストラクチャを提供します。CFS は、転送機能と、さまざまな共通サービスをアプリケーションに提供します。CFS はファブリック内の CFS 対応スイッチを検出したり、すべての CFS 対応スイッチのアプリケーション機能を検出したりできます。

この章の内容は、次のとおりです。

CFS について

Cisco MDS NX-OS ソフトウェアは Cisco Fabric Services（CFS）インフラストラクチャを使用して、効率的なデータベース配信を実現し、デバイスの柔軟性を高めます。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 プロビジョニングが簡単になります。

複数の Cisco MDS NX-OS アプリケーションが、CFS インフラストラクチャを使用して、特定のアプリケーションのデータベースの内容を維持および配信します。

Cisco MDS スイッチの機能の多くでは、ファブリック内のすべてのスイッチで設定が同期している必要があります。ファブリック全体で設定を維持することは、ファブリックの一貫性を維持するうえで重要です。共通のインフラストラクチャがない場合、そのような同期を行うには、ファブリック内の各スイッチで手動で設定することになります。これは、退屈で誤りが起きやすい作業です。

ここで説明する内容は、次のとおりです。

CFS を使用した Cisco MDS NX-OS 機能

次の Cisco NX-OS の機能は、CFS インフラストラクチャを使用します。

- N ポート バーチャライゼーション
- FlexAttach 仮想 pWWN
- NTP
- ダイナミック ポート VLAN メンバーシップ
- Distributed Device Alias Service
- IVR トポロジ
- SAN デバイス バーチャライゼーション
- TACACS+ および RADIUS
- ユーザおよび管理者ロール
- ポート セキュリティ
- iSNS
- Call Home
- Syslog
- fctimer
- SCSI フロー サービス
- Fabric Startup Configuration Manager（FSCM）を使用した、保存されたスタートアップ コンフィギュレーション
- 許可ドメイン ID リスト
- RSCN タイマー
- iSLB

CFS の機能

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
- 3 つの配信スコープ
  - 論理スコープ：配信は、VSAN のスコープ内で発生します。
  - 物理スコープ：配信は、物理トポロジ全体におよびます。
  - 選択した VSAN セットを超える場合：Inter-VSAN Routing（IVR）などの一部のアプリケーションは、一部の特定の VSAN を超えた設定の配信を必要とします。これらのアプリケーションは、配信を制限する VSAN セットを CFS に指定できます。
- 3 つの配信モード
  - 協調型配信：ファブリック内で同時に 1 つの配信だけが許可されます。
  - 非協調型配信：協調型配信が進行中である場合を除いて、ファブリック内で複数の同時配信を実行できます。
  - 無制限の非協調型配信：既存の協調型配信がある場合でも、ファブリッ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、他のすべての配信タイプの配信と同時に実行できます。
- ファブリック マージ イベント中（2 つの独立したファブリックのマージ中）に、アプリケーション設定のマージを実行するマージ プロトコルをサポートします。

アプリケーションの 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。Cisco SAN-OS Release 2.0(1b) よりも前に存在していた機能では、配信機能がデフォルトでディセーブルになっており、配信機能を明示的にイネーブルにする必要がありました。

Cisco SAN-OS Release 2.0(1b) 以降、または MDS NX-OS Release 4.1(1) 以降で採用されているアプリケーションでは、配信機能がデフォルトでイネーブルになっています。

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。

CFS プロトコル

CFS 機能は、下位層の転送には依存しません。現在、Cisco MDS スイッチでは、CFS プロトコル レイヤは Fiber Channel 2（FC2; ファイバ チャネル 2）レイヤの上に存在し、クライアントとサーバの関係がないピアツーピアのプロトコルになっています。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 アドレスで送受信されます。

CFS は、IP を使用して他のスイッチに情報を送信することもできます。

CFS を使用するアプリケーションは、下位層の転送をまったく認識しません。

CFS 配信のスコープ

Cisco MDS 9000 ファミリ スイッチ上のさまざまなアプリケーションが、さまざまなレベルで設定を配信する必要があります。

- 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。

- 物理トポロジ レベル（物理スコープ）

  アプリケーションは、複数の VSAN にまたがる物理トポロジ全体に設定を配信しなければならない場合があります。そのようなアプリケーションとしては、NTP や DPVM（WWN ベースの VSAN）が挙げられます。これらは VSAN とは無関係です。

- 2 台のスイッチ間

  アプリケーションは、ファブリック内の選択したスイッチ間だけで動作する可能性があります。アプリケーションの例としては、2 台のスイッチ間で動作する SCSI フロー サービスが挙げられます。

CFS の配信モード

CFS は、さまざまなアプリケーション要件をサポートするため、協調型配信と非協調型配信の、2 種類の配信モードをサポートしています。2 つのモードは相互に排他的です。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。例としては、iSNS などのローカル デバイス登録が挙げられます。1 つのアプリケーションで、複数の非協調型配信が可能です。

協調型配信

協調型配信では、同時に 1 つのアプリケーション配信だけを実行できます。CFS はロックを使用してこの機能を実行します。ファブリック内のいずれかの場所にあるアプリケーションによってロックが取得されている場合、協調型配信を開始できません。協調型配信は、次の 3 段階で構成されています。

1. ファブリック ロックが取得されます。
2. 設定が配信され、コミットされます。
3. ファブリック ロックが解放されます。

協調型配信には、次の 2 種類があります。

- CFS によるもの：アプリケーションが介在することなく、アプリケーション要求に応じて CFS が各段階を実行します。
- アプリケーションによるもの：各段階がアプリケーション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でも、ファブリッ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、他のすべての配信タイプの配信と同時に実行できます。

混合ファブリック内での CFS の接続性

CFS は、Cisco Nexus 5000 シリーズ スイッチ上や Cisco MDS 9000 スイッチ上でも動作するインフラストラクチャ コンポーネントです。混合ファブリック内のさまざまなプラットフォーム（Cisco Nexus 7000 シリーズ、Cisco Nexus 5000 シリーズ、Cisco MDS 9000 スイッチなど）は、相互に情報をやりとりすることができます。

CFSoIP と CFSoFC を使用して、各 CFS クライアントは他のプラットフォーム上で動作しているそれぞれのインスタンスと通信することもできます。定義されたドメインと配信スコープの範囲内で、CFS はクライアントのデータと設定を他のプラットフォーム上で動作しているピアに配信できます。

3 種類すべてのプラットフォームで CFSoIP と CFSoFC の両方がサポートされています。ただし、Cisco Nexus 7000 シリーズと Cisco Nexus 5000 シリーズのスイッチでは、CFSoFC が動作するために、FC または FCoE プラグインおよび対応する設定が必要になります。Cisco MDS 9000 スイッチでは、両方のオプションがデフォルトで使用可能になっています。

（注） 一部のアプリケーションは、異なるプラットフォーム上で動作しているそれらのインスタンスと互換性がありません。そのため、設定をコミットする前に、CFS 配信に関するクライアントの注意事項を注意深く読むことを推奨します。

Cisco Nexus 5000 シリーズと Cisco MDS 9000 スイッチに対する CFS の詳細については、『*Cisco Nexus 5000 Series NX-OS System Management Configuration Guide*』と『*Cisco MDS 9000 Family NX-OS System Management Configuration Guide*』をそれぞれ参照してください。

ファブリックのロック

CFS インフラストラクチャを使用する Cisco NX-OS 機能（またはアプリケーション）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、ファブリックをロックします。ファブリックがロックされると、Cisco NX-OS ソフトウェアは、ロックを保持しているスイッチ以外のスイッチからこの Cisco NX-OS 機能への設定変更を許可せず、ロックされたステータスをユーザに通知するためのメッセージを発行します。設定変更は、該当アプリケーションによって保留データベースに保持されます。

ファブリックのロックが必要な CFS セッションを開始した後に、セッションが終了されなかった場合、管理者はセッションをクリアできます。ファブリックをロックしたユーザの名前は、再起動およびスイッチオーバーを行っても保持されます。（同じマシン上で）別のユーザが設定タスクを実行しようとしても、拒否されます。

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。

一般に、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、コミット操作の結果として、ロックを取得し、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 つ以上の外部スイッチが成功ステータスを報告：アプリケーションは変更をローカルに適用し、ファブリック ロックを解除します。
- どの外部スイッチも成功ステートを報告しない：アプリケーションはこのステートを失敗として認識し、ファブリック内のすべてのスイッチに変更を適用しません。ファブリック ロックは解除されません。

CFS マージのサポート

アプリケーションは CFS を通して、設定をファブリック内で継続的に同期します。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 イベント中に調停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 個のアプリケーション ピアがあるファブリックが N 個アプリケーション ピアがある別のファブリックとマージし、アプリケーションが通知のたびにマージ動作を行う場合は、リンク アップ イベントによりファブリック内で M*N 回のマージがトリガーされます。

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動します。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。その他のスイッチは、マージ プロセスで何も役割を果たしません。

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判断し、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。

IP を介した CFS 配信

ファイバ チャネルを介して到達できないスイッチを含むネットワークに対し、IP を介して情報を配信するように CFS を設定できます。IP を介した CFS 配信は次の機能をサポートしています。

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

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

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

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

- 設定可能なマルチキャスト アドレスを使用してネットワーク トポロジの変更を検出するキープアライブ メカニズム
- Cisco MDS SAN-OS Release 2.x との互換性
- 論理スコープ アプリケーションに対する配信は、VSAN の実装がファイバ チャネルに制限されているため、サポートされません。

図 2-1 に、ファイバ チャネル接続と IP 接続の両方を持つ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 2-1　ファイバ チャネル接続と IP 接続を持つネットワーク例 1

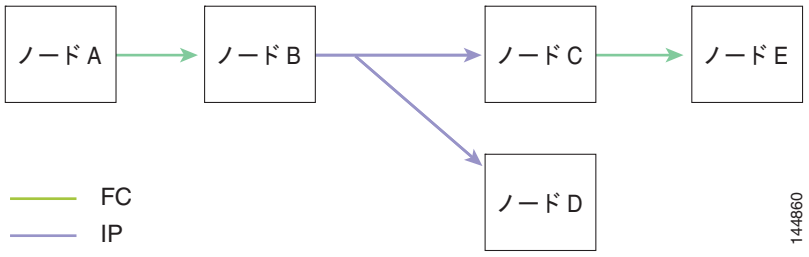


図 2-2 は、ノード D とノード E がファイバ チャネルを使用して接続されていることを除き、図 2-1 と同じです。ノード B にはノード C とノード D の IP 用配信リストがあるので、この例のすべてのプロセスは同じです。ノード D はすでにノード B からの配信リストに入っているため、ノード C はノード D に転送しません。

図 2-2　ファイバ チャネル接続と IP 接続を持つネットワーク例 2

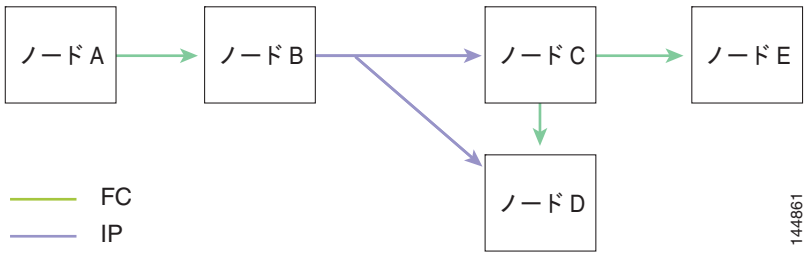
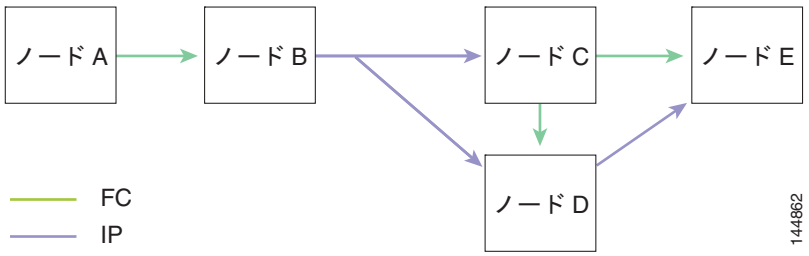


図 2-3 は、ノード D とノード E が IP を使用して接続されていることを除き、図 2-2 と同じです。ノード E はノード B からの配信リストに入っていないため、ノード C とノード D はイベントをノード E に転送します。

図 2-3　ファイバ チャネル接続と IP 接続を持つネットワーク例 3



IP を介した CFS 用のスタティック IP ピア

一部のデバイスでは、マルチキャスト フォワーディングはデフォルトでディセーブルになっています。たとえば、IBM Blade シャーシでは、特に外部イーサネット ポートでマルチキャスト フォワーディングがディセーブルになっており、イネーブルにする方法はありません。N ポート バーチャライゼーション デバイスは、IP だけを転送メディアとして使用し、ISL 接続またはファイバ チャネル ドメインを持っていません。

マルチキャスト フォワーディングをサポートしていないスイッチで IP を介した CFS をイネーブルにするには、スイッチに物理的に接続されているネットワーク全体で、イーサネット IP スイッチに対して、マルチキャスト フォワーディングをイネーブルにする必要があります。その場合、IP を介した CFS 配信のためにスタティック IP ピアを設定できます。

CFS は、設定された IP アドレスのリストを使用して各ピアと通信し、ピア スイッチの WWN を学習します。ピア スイッチの WWN を学習した後、CFS はスイッチを CFS 対応とマークし、アプリケーションレベルのマージとデータベース配信をトリガーします。

次の MDS 9000 の機能では、IP を介した CFS 配信のために、スタティック IP ピア設定が必要です。

- N ポート バーチャライゼーション デバイスは、通信チャネルとして IP を持っています。これは、NPV スイッチに FC ドメインがないためです。NPV デバイスは、IP を介した CFS を転送メディアとして使用します。
- NPV 対応のスイッチだけをリンクする、CFS リージョン 201 上の FlexAttach 仮想 pWWN 配信。

CFS リージョンの概要

CFS リージョンは、物理配信スコープにおける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。SAN が広い範囲におよぶ場合、物理プロキシミティに基づいてスイッチ セット間で特定のプロファイルの配信をローカライズまたは制限しなければならない場合があります。MDS SAN-OS Release 3.2.(1) よりも前のバージョンでは、SAN 内のアプリケーションの配信スコープは、物理ファブリック全体におよんでおり、ファブリック内の特定のスイッチのセットに配信を制限する機能はありませんでした。CFS リージョンの機能では、CFS リージョンを作成することでこの制限を克服できます。CFS リージョンは、CFS 機能またはアプリケーションに対する、ファブリック内の複数の配信アイランドです。CFS リージョンは、機能の設定の配信をファブリックにおける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 リージョンは、SAN 内の物理スイッチに対してだけ設定できます。CFS リージョンの設定は、VSAN では行えません。

CFS シナリオの例：Call Home は、ある状況が発生した場合や、何らかの異常が発生した場合にネットワーク管理者に対してアラートをトリガーするアプリケーションです。ファブリックが広い範囲におよび、ファブリック内のスイッチのサブセットを担当するネットワーク管理者が複数存在する場合、Call Home アプリケーションは、管理者のいる場所にかかわらず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 アプリケーションは、メッセージ アラートを選択してネットワーク管理者に送信するために、CFS リージョンを実装してアプリケーションの物理スコープを調整するか絞り込む必要があります。

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 はデフォルトのリージョンとして予約されており、ファブリッ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。Release 3.2(1) よりも前の SAN-OS が動作するスイッチが同じファブリック上にある場合、これらのスイッチを同期化する際に、リージョン 0 の機能だけがサポートされます。これらのスイッチを同期化する際、他のリージョンの機能は無視されます。

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。

注意事項と制限

ファブリック内のすべてのスイッチは CFS に対応している必要があります。Cisco MDS 9000 ファミリ スイッチは、Cisco SAN-OS Release 2.0(1b) 以降、または MDS NX-OS Release 4.1(1) 以降を実行している場合、CFS に対応しています。CFS に対応していないスイッチは配信を受信できず、ファブリックの一部が目的の配信を受信できなくなります。

CFS には、次の注意事項と制限事項があります。

- 暗黙的な CFS の使用 : CFS 対応アプリケーションに CFS タスクを初めて発行した場合は、設定変更プロセスが開始し、アプリケーションによってファブリックがロックされます。
- 保留データベース：保留データベースはコミットされていない情報を保持する一時的なバッファです。データベースがファブリック内の他のスイッチのデータベースと同期するように、コミットされていない変更はすぐに適用されません。変更をコミットすると、保留データベースはコンフィギュレーション データベース（別名、アクティブ データベースまたは有効データベース）を上書きします。
- アプリケーション単位でイネーブル化またはディセーブル化される CFS 配信 : CFS 配信ステートのデフォルト（イネーブルまたはディセーブル）は、アプリケーション間で異なります。CFS 配信がディセーブル化されたアプリケーションは、設定を配信せず、ファブリック内の他のスイッチからの配信も受信しません。
- 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ファブリックに配信したりファブリック ロックを解放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動作が必要です。コミット操作を実行しないと、一時的バッファ内の変更は適用されません。

デフォルト設定

表 2-1 に、CFS 設定のデフォルト設定値を示します。

表 2-1　デフォルトの CFS パラメータ

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

CFS の設定

ここでは、設定プロセスについて説明します。ここで説明する内容は、次のとおりです。

スイッチの CFS 配信のディセーブル化

デフォルトでは、CFS 配信はイネーブルに設定されています。アプリケーションは、ファブリック内のアプリケーションが存在するすべての CFS 対応スイッチにデータと設定情報を配信できます。これが操作の通常モードです。

物理接続を維持したまま、スイッチで CFS をグローバルにディセーブルにし、CFS を使用するアプリケーションをファブリック全体への配信から隔離することができます。

制約事項

- スイッチで CFS がグローバルにディセーブルになっている場合、CFS 動作はスイッチに制限され、すべての CFS コマンドはスイッチが物理的に隔離されているかのように機能し続けます。

手順の詳細

スイッチ上で CFS 配信をグローバルにディセーブルまたはイネーブルにするには、次の手順を実行します。

ステップ 1　[Physical Attributes] ペインで、[Switches] > [CFS] の順に展開します。

ステップ 2　[information] ペインのドロップダウン メニューで、スイッチに対して [disable] または [enable] を選択します。

ステップ 3　[Apply Changes] アイコンをクリックして、設定の変更をコミットします。

Device Manager を使用して、特定のスイッチ上で CFS 配信をグローバルにディセーブル化またはイネーブル化するには、次の手順を実行します。

ステップ 1　[Admin] > [CFS (Cisco Fabric Services)] を選択します。

そのスイッチのすべての機能の CFS ステータスを示す [CFS] ダイアログボックスが表示されます。

ステップ 2　現在のスイッチで CFS 配信をディセーブル化またはイネーブル化するには、[Globally Enabled] チェックボックスをオフまたはオンにします。

ステップ 3　[Apply] をクリックして、このスイッチの CFS をディセーブルにします。

アプリケーションの CFS のイネーブル化

制約事項

- 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。

手順の詳細

機能に対して CFS をイネーブルにするには、次の手順を実行します。

ステップ 1　CFS をイネーブルにする機能を選択します。たとえば、[Physical Attributes] ペインで [Switches] > [Events] を展開して、[CallHome] を選択します。[Information] ペインに、該当する機能および [CFS] タブが表示されます。[CFS] タブをクリックして、ファブリック内のスイッチごとに、該当機能の CFS ステートを表示します。

ステップ 2　CFS をイネーブルにするスイッチを決定します。CFS をイネーブルにする場合は [Admin] カラムを [enable] に、CFS をディセーブルにする場合は [disable] に設定します。

（注）　CFS を使用する機能について、ファブリック内のすべてのスイッチ、または VSAN 内のすべてのスイッチに対して、CFS をイネーブルにします。

ステップ 3　変更した行を右クリックして、ポップアップ メニューを表示します。[Apply Changes] を選択して、CFS の設定変更を適用します。CFS の変更が有効になると、[CFS] タブが更新されます。

DCNM-SAN が CFS 変更のステータスを取得し、[Last Result] カラムを更新します。

Device Manager を使用し、ある機能に対して CFS をイネーブルにするには、次の手順を実行します。

ステップ 1　[Admin] > [CFS (Cisco Fabric Services)] を選択します。

そのスイッチのすべての機能の CFS ステータスを示す [CFS] ダイアログボックスが表示されます。

ステップ 2　CFS が必要な機能を決定します。CFS をイネーブルにする場合は [Command] カラムを [enable] に、CFS をディセーブルにする場合は [disable] に設定します。

（注）　ファブリックまたは VSAN 内のすべてのスイッチについて、CFS を使用する機能に対し、CFS をイネーブルまたはディセーブルにします。

ステップ 3　[Pending Differences] をクリックして、現在のスイッチのこの機能の設定を、またはこの機能に対して CFS がイネーブルになっている、ファブリックまたは VSAN 内の他のスイッチと比較します。[Show Pending Diff] ポップアップ ウィンドウを閉じます。

ステップ 4　[Apply] をクリックして、CFS 設定変更を適用します。

Device Manager は CFS の変更ステータスを取り込んで、[Last Command] カラムおよび [Result] カラムを更新します。

変更のコミット

手順の詳細

指定した機能に対する変更をコミットするには、その機能に対して、[CFS] > [Config Action] を [commit] に設定します。

CFS 対応機能に対する変更をコミットするには、次の手順を実行します。

ステップ 1　CFS をイネーブルにする機能を選択します。たとえば、[Switch] > [Clock] > [NTP] を選択します。

[Information] ペインに、該当する機能および [CFS] タブが表示されます。

ステップ 2　[CFS] タブをクリックして、ファブリック内のスイッチごとに、該当機能の CFS ステートを表示します。

ステップ 3　[Feature] タブで、NTP の [General] タブをクリックし、設定を変更します。[Apply Changes] アイコンをクリックして、設定をローカル スイッチに適用します。変更内容は、さらに CFS コミットが適用されるまで、ローカル スイッチの保留データベースにとどまります。

ステップ 4　[Pending Differences] をクリックして、現在のスイッチの機能の設定を、またはこの機能に対して CFS がイネーブル化されているファブリックまたは VSAN 内の他のスイッチと比較します。

ステップ 5　[CFS] タブをクリックし、選択されているマスター スイッチの [Config Action] カラム内の値を右クリックし、ドロップダウン メニューからオプションを選択します。([commit]、[clear lock]、[abort])。たとえば、[Config Action] カラム内の値を右クリックし、[commit] を選択することで、その機能に対する CFS の保留中の変更をコミットし、CFS によってそれらの変更を配信します。

DCNM-SAN が CFS 変更のステータスを取得し､機能または VSAN の [Last Command] カラムおよび [Last Result] カラムを更新します。

Device Manager を使用して CFS 対応機能に対する変更をコミットするには、次の手順を実行します。

ステップ 1　Device Manager で、CFS をイネーブルにする機能を選択します。たとえば、[Admin] > [NTP] を選択します。

ステップ 2　[Feature] タブで、NTP の [General] タブをクリックし、設定を変更します。[Apply Changes] アイコンをクリックして、設定をローカル スイッチに適用します。変更内容は、さらに CFS コミットが適用されるまで、ローカル スイッチの保留データベースにとどまります。

ステップ 3　[Admin] > [CFS (Cisco Fabric Services)] を選択します。

ステップ 4　[CFS] テーブルで、[Pending Differences] をクリックして、現在のスイッチの機能の設定を、この機能に対して CFS がイネーブルにされているファブリックまたは VSAN 内の他のスイッチと比較します。

ステップ 5　該当機能の設定変更をコミットし、CFS を通して変更を配信する場合は、該当する機能ごとに、[Command] カラムを [commit] に設定します。該当機能に対する変更を廃棄して、この機能の CFS のファブリック ロックを解除する場合は、[Command] カラムを [abort] に設定します。

Device Manager は CFS の変更ステータスを取り込んで、[Last Command] カラムおよび [Result] カラムを更新します。

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。

変更の破棄

設定変更を廃棄する場合、アプリケーションは保留データベースを消去し、ファブリック内のロックを解除します。中断とコミット機能の両方を使用できるのは、ファブリック ロックが取得されたスイッチだけです。

指定した機能の [Command] カラムの値を [disable] に設定し、[Apply] をクリックすると、その機能に対する変更を廃棄できます。

コンフィギュレーションの保存

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。

CISCO-CFS-MIB には CFS 関連機能の SNMP 設定情報が含まれます。この MIB の詳細については、『*Cisco MDS 9000 Family MIB Quick Reference*』を参照してください。

ロック済みセッションのクリア

アプリケーションによって保持されているロックは、ファブリック内の任意のスイッチからクリアできます。この方法は、ロックが取得されクリアされない状況から復帰するために提供されています。

手順の詳細

ロックをクリアするには、次の手順を実行します。

ステップ 1　[CFS] タブをクリックします。

ステップ 2　ロックをクリアする各スイッチの [Config Action] ドロップダウン リストから [clearLock] を選択します。

ステップ 3　[Apply Changes] アイコンをクリックして、変更を保存します。

トラブルシューティングのヒント

- この機能を使用してファブリック内のロックをクリアする場合は、注意が必要です。ファブリック内の全スイッチのすべての保留データベースの内容は、消去されて失われます。

IP を介した CFS 用のスタティック IP ピアの設定

Cisco DCNM-SAN は、NPV コア スイッチ上のネーム サーバ データベースを読み込んで NPV デバイスを検出します。これは、スタティック ピアを使用した IP を介した CFS 配信のために、NPV スイッチでスタティック ピア リストを管理するためにも使用されます。

DCNM for SAN 4.1(1) 以降では、スイッチ上で検出された NPV ピアのピア リストを管理するための、ワンタイム コンフィギュレーション ウィザードが提供されています。スイッチでピア リストが設定されている場合、CFS は IP スタティック ピアを使用した配信を、リストのすべてのメンバーでイネーブルにし、ピア リストをリストのすべてのメンバーに伝播します。

（注）　新しい NPV スイッチがファブリックに追加された場合、NPV CFS セットアップ ウィザードを起動してリストを更新する必要があります。これは、DCNM-SAN でリストが自動的に更新されないためです。

リストへのピアの追加

手順の詳細

スタティック IP ピア リストを設定するには、次の手順を実行します。

ステップ 1　[DCNM-SAN] メニューから、[Tools] > [NPV CFS Setup] を選択します。

[NPV Device Selection] ダイアログボックスが表示され、スイッチから取得した NPV デバイス ピアの一覧に、デバイス名、デバイスの IP アドレス、ピアの状態が表示されます。

ステップ 2　[NPV Device to retrieve peer list from] ドロップダウン リストから、ピア リストの取得元のデバイスを選択します。

スイッチから取得したリスト内の NPV デバイスがファブリックに存在する場合、ステータスとして、Local、Reachable、Unreachable、Discovery in Progress のいずれかが表示されます。NPV デバイスがファブリック中に存在しない場合、ステータスは「Not in Fabric」と表示されます。

（注）　ステータスが「Not in Fabric」と表示される場合、リストからデバイスを削除する必要があります。

ステップ 3　[Add] をクリックします。

ダイアログボックスに、現在のピア リストに含まれていない、ファブリック内のすべての NPV デバイスの一覧が表示されます。デフォルトでは、リスト内のすべてのスイッチが選択されています。

ステップ 4　ピアを選択し、[OK] をクリックしてピアをリストに追加します。

ピアは、To Be Added ステータスでリストに追加されます。

ステップ 5　ピアをリストに追加する場合は、[Set] をクリックします。これにより、ピア リストが CFS によって伝播されます。

ピア リストからの NPV デバイスの削除

手順の詳細

IP ピア リストからピアを削除するには、次の手順を実行します。

ステップ 1　[DCNM-SAN] メニューから、[Tools] > [NPV CFS Setup] を選択します。

NPV CFS セットアップ ウィザードが起動されます。

ステップ 2　[NPV Device to retrieve peer list from] ドロップダウン リストから、ピアを削除するピア リストを取得するデバイスを選択します。

ステップ 3　次のいずれかの作業を行って、ピアまたはローカル ホストを削除済みとしてマークします。

- ピア リストからピアを削除するには、リストからピアを選択し、[Delete] をクリックします。
- ピア リストからローカル ホストを削除するには、ローカル NPV デバイスを選択して [Delete] をクリックするか、リスト中のすべてのピアを選択して [Delete All] をクリックします。

ステップ 4　[Yes] をクリックしてピアをリストから削除します。

ステップ 5　NPV CFS ウィザードで [Set] をクリックします。メッセージ ボックスが表示されます。

ステップ 6　[Yes] をクリックして、削除されたピアまたはローカル ホストをその他すべての NPV デバイス ピア リストから削除し、削除されたピア内でマルチキャストを使用して動的ピア検出を開始します。

CFS リージョンの設定

ここでは、次の内容について説明します。

CFS リージョンの管理

ここでは、DCNM-SAN を使用して、CFS リージョンを管理する方法について説明します。DCNM-SAN は、すべてのスイッチ、リージョン、およびトポロジの各リージョンに関連付けられた機能の総合的ビューを提供します。次のタスクを完了するには、[All Regions] タブおよび [Feature by Region] タブの下のテーブルを使用します。

（注）　CFS は、CFS リージョンが適用されていない場合は常に個々のファブリック内で動作します。CFS リージョンが存在する場合は、個々の CFS リージョン内で動作します。SAN またはデータセンター（ファブリックより上位）のノードまたはスコープが選択されている場合でも、DCNM-SAN では、選択されたスコープ下の最初のファブリックのスイッチのみが表示されます。

CFS リージョンの作成

手順の詳細

CFS リージョンを作成するには、次の手順を実行します。

ステップ 1　[Physical Attributes] ペインで、[Switches] を展開し、[CFS] を選択します。

[Information] ペインに、[Global]、[IP Multicast]、[Feature by Region]、および [All Regions] タブが表示されます。

ステップ 2　[All Regions] タブをクリックします。

タブにスイッチとリージョン ID のリストが表示されます。

ステップ 3　ツールバーの [Create Row] ボタンをクリックします。

ステップ 4　ドロップダウン リストからスイッチを選択して、範囲からリージョン ID を選択します。

ステップ 5　[Create] をクリックします。

リージョンが正常に作成されると、ダイアログボックスの下部に「Success」と表示されます。

CFS リージョンへの機能の割り当て

制約事項

- [Feature by Region] タブでは、[Create Row] をクリックしてスイッチの機能を別のリージョンに再割り当てしようとすると、操作が失敗したことを示すメッセージが表示されます。このエラーメッセージは、エントリがすでに存在することを示します。別のリージョンへの機能の移動は、「別のリージョンへの機能の移動」（P.2-17）で説明する別のタスクで実行できます。

手順の詳細

リージョンに機能を割り当てるには、次の手順を実行します。

ステップ 1　[Physical Attributes] ペインで、[Switches] を展開し、[CFS] を選択します。

[Information] ペインに、[Global]、[IP Multicast]、[Feature by Region]、および [All Regions] タブが表示されます。

ステップ 2　[Feature by Region] タブをクリックします。

このタブには、すべてのスイッチと、対応する機能およびリージョン ID が表示されます。

[Feature by Region] タブを使用して新しいリージョンに機能が割り当てられると、[All Regions] タブの下のテーブルに、新しいリージョンが示された新しい行が自動的に作成されます。また、[All Regions] タブを使用してリージョンを作成することもできます。

ステップ 3　ツールバーの [Create Row] ボタンをクリックします。

ステップ 4　ドロップダウン リストから、スイッチを選択します。

選択したスイッチで実行されている機能が、[Feature] ドロップダウン リストに表示されます。

ステップ 5　そのスイッチの機能を選択して、リージョンに関連付けます。

ステップ 6　[RegionID] リストからリージョン番号を選択して、リージョンを選択した機能に関連付けます。

ステップ 7　[Create] をクリックすると、リージョンへのスイッチ機能の割り当てが完了します。

機能が正常に割り当てられると、ダイアログボックスの下部に「Success」と表示されます。

別のリージョンへの機能の移動

前提条件

- 機能を新しいリージョンに移動するには、まず [All Regions] タブで新しいリージョンを作成します。つまり、[All Regions] タブに、新しいリージョン ID で新しい行を追加する必要があります。

手順の詳細

別のリージョンに機能を移動するには、次の手順を実行します。

ステップ 1　[Physical Attributes] ペインで、[Switches] を展開し、[CFS] を選択します。

[Information] ペインに、[Global]、[IP Multicast]、[Feature by Region]、および [All Regions] タブが表示されます。

ステップ 2　[Feature by Region] タブをクリックします。

ステップ 3　必要な行の [RegionId] セルをダブルクリックします。

セル中でカーソルが点滅し、値を変更できることを示します。

ステップ 4　[RegionId] の値を必要なリージョンに変更します。

ステップ 5　ツールバーで [Apply Changes] ボタンをクリックして、変更をコミットします。

リージョンからの機能の削除

手順の詳細

リージョンから機能を削除するには、次の手順を実行します。

ステップ 1　[Feature by Region] タブをクリックして、必要な行を選択します。

ステップ 2　ツールバーで [Delete Row] ボタンをクリックします。

ステップ 3　[Yes] をクリックして、ビューのテーブルから行を削除することを確認します。

CFS リージョンの削除

手順の詳細

リージョン全体を削除するには、次の手順を実行します。

ステップ 1　[All Regions] タブをクリックして、必要な行を選択します。

ステップ 2　[Delete Row] をクリックします。

このアクションは、そのスイッチおよびリージョンに関連するすべてのエントリを [Feature by Region] タブのテーブルから削除します。

ステップ 3　[Yes] をクリックして、リージョンの削除を確認します。

CFS 設定の確認

CFS 設定情報を表示するには、次の作業を実行します。

- 「CFS 設定情報の表示」（P.2-18）

CFS 設定情報の表示

手順の詳細

スイッチの CFS 配信のステータスを表示するには、次の手順を実行します。

ステップ 1　[Admin] > [CFS (Cisco Fabric Services)] を選択します。

[CFS] ダイアログボックスが表示されます。このダイアログボックスには、CFS を使用している各機能の配信ステータス、CFS を使用中の現在登録されているアプリケーション、および最後に成功したマージの結果が表示されます。

ステップ 2　行を選択し、[Details] をクリックして、機能の詳細を表示します。

CFS の設定例

ここでは、CFS の設定方法の例を示します。

DCNM for SAN を使用した CFS の例

この手順は、DCNM-SAN を使用して CFS を使用する機能を設定した場合に表示される内容を示した例です。

手順の詳細

ステップ 1　設定する CFS 対応機能を選択します。たとえば、[Logical Domains] ペインで [VSAN] を展開してから、[Port Security] を選択します。

[Information] ペインに、その VSAN のポート セキュリティ設定が表示されます。

ステップ 2　[CFS] タブをクリックします。

各スイッチの CFS の設定およびステータスが表示されます。

ステップ 3　[Feature Admin] ドロップダウン リストで、各スイッチに対して [enable] を選択します。

ステップ 4　ファブリック内のすべてのスイッチに対して、ステップ 3 を繰り返します。

（注）　ファブリック内のすべてのスイッチで、現在の機能に対して CFS をイネーブルにしない場合は、警告が表示されます。

ステップ 5　この機能のマージ マスターとして機能させるスイッチの [Master] チェックボックスをオンにします。

（注）　[information] ペインで他のタブをクリックし、[CFS] タブをクリックした場合、[Master] チェックボックスはオンにならなくなります。DCNM-SAN は、CFS マスター情報をキャッシュしません。

ステップ 6　CFS をイネーブルにしたスイッチごとに、[Config Action] ドロップダウン リストで [commit Changes] を選択します。

ステップ 7　[Information] ペインで、[Servers] タブをクリックします。

マスター スイッチに基づいて、この機能の設定が表示されます。

ステップ 8　機能の設定を変更します。たとえば、[Master] カラムの名前を右クリックし、[Create Row] を選択して、NTP 用のサーバを作成します。

a.　NTP サーバの ID および名前または IP アドレスを設定します。

b.　[Mode] オプション ボタンを設定し、必要に応じて [Preferred] チェックボックスをオンにします。

c.　[Create] をクリックして、サーバを追加します。

ステップ 9　[Delete Row] アイコンをクリックして、行を削除します。

変更を加えると、ステータスが自動的に [Pending] に変わります。

ステップ 10　[Commit CFS Pending Changes] アイコンをクリックして、変更内容を保存します。

ステップ 11　ステータスが [Running] に変わります。

ステップ 12　CFS をイネーブルにしたスイッチごとに、[Config Action] ドロップダウン リストで [abortChanges] を選択します。

（注）　[enable] を選択した場合は、DCNM-SAN はステータスを pending に変更しません。最初の変更が実際に行われるまで、pending ステータスは適用されないためです。

ステップ 13　[Apply Changes] アイコンをクリックして、その機能の設定変更をコミットし、CFS を通じて変更内容を配信します。

（注）　DPVM やデバイス エイリアスなどの機能と CFS を併用する場合は、各設定の終了時に [commit] を選択する必要があります。セッションがロックされている場合は、[abort] を選択して、機能を終了する必要があります。

機能ごとに配信用のマスターまたはシード スイッチを設定するには、次の手順を実行します。

ステップ 1　CFS に対してマージ マスターが必要な機能を選択します。たとえば、[Physical Attributes] ペインから [Events] を展開し、[CallHome] を選択します。

[Information] ペインに、CFS タブを含む該当する機能が表示されます。

ステップ 2　[CFS] タブをクリックして、ファブリック内のスイッチごとに、該当機能の CFS ステートを表示します。

ステップ 3　この機能のマージ マスターとして機能させるスイッチの [Master column] カラムのチェックボックスをオンにします。

ステップ 4　[Apply Changes] アイコンをクリックして、今後の CFS 配信用にこのスイッチをマスターとして選択します。

Device Manager を使用した CFS の例

制約事項

- DPVM やデバイス エイリアスなどの機能と CFS を併用する場合は、各設定の終了時に [commit] を選択する必要があります。セッションがロックされている場合は、[abort] を選択して、機能を終了する必要があります。

手順の詳細

この手順は、Device Manager を使用して CFS を使用する機能を設定した場合に表示される内容を示した例です。CFS を使用する機能の具体的な手順については、該当する機能のマニュアルを参照してください。

CFS を使用する機能を設定するには、次の手順を実行します。

ステップ 1　任意の CFS 対応機能のダイアログボックスを開きます。Device Manager が、CFS がイネーブルになっているかどうかを調べます。また、[Owner] テーブル内のエントリを最低 1 つ調べて、機能がロックされているかどうかも調べます。CFS がイネーブルにされていて、機能がロックされている場合、Device Manager はその機能のステータスを「pending」に設定します。ロック情報を示すダイアログボックスが表示されます。

ステップ 2　プロンプトが表示されたら、[Continue] または [Cancel] をクリックします。継続した場合は、CFS ステータスが復元されます。

ステップ 3　[Admin] > [CFS (Cisco Fabric Services)] を選択して、CFS ロックを保持しているユーザの名前を表示します。

ステップ 4　ロックされた機能をクリックして、[Details] をクリックします。

ステップ 5　[Owners] タブをクリックし、[UserName] カラムを参照します。

（注）　[Refresh] をクリックしない限り、Device Manager はファブリック全体で機能のステータスを監視しません。別の CFS 対応スイッチ上のユーザが同じ機能を設定しようとしても、「pending」ステータスは表示されません。ただし、そのユーザのスイッチで設定変更が拒否されます。

ステップ 6　CFS がイネーブル化されていて、機能がロックされていない場合、Device Manager はその機能のステータスを running に設定します。

その後、この機能に関するダイアログボックスが表示されます。作成、削除、または変更を実行するとすぐに、Device Manager はステータスを pending に変更して、保留データベース内の更新済み情報を表示します。

ステップ 7　機能の CFS テーブルを表示します。Device Manager がステータスを running に変更するのは、[commit]、[clear]、または [abort] を選択して、適用した場合だけです。[enable] を選択した場合は、Device Manager はステータスを「pending」に変更しません。最初の変更が実際に行われるまで、pending ステータスは適用されないためです。

直前のコマンドが **noOp** の場合、[Last Command] および [Result] フィールドはブランクです。

CFS のフィールドの説明

ここでは、CFS のフィールドの説明を示します。

Cisco Fabric Services（CFS）の機能

フィールド	説明
Globally Enabled	このチェックボックスをオンにすると、このスイッチ上の CFS は機能の設定を他のスイッチに配信できるようになります。このチェックボックスをオフにすると、CFS は他のスイッチに設定を配信できなくなります。
Feature	CFS 対応機能の名前。
Status	CFS 対応機能のステータス。
Command	機能に対してトリガーされるアクション。次のアクションがあります。 • [noop]：操作なし。 • [enable]：スイッチ上の CFS 配信をイネーブルにします。 • [disable]：スイッチ上の CFS 配信をディセーブルにします。 • [commit]：セッション開始以降に行われた変更をコミットします。 • [abort]：行われた変更を廃棄し、セッションを閉じます。 • [clear]：行われた変更を廃棄し、セッションは閉じません。
Type	使用された最後の CFS 機能スコープ タイプ。
VSAN Id	この機能が動作中の VSAN の ID。

フィールド	説明
RegionId	この CFS 対応機能がマッピングされている配信リージョン ID。このリージョンは、その使用よりも前に定義される必要があります。
View Config Changes As	変更が実行と保留のいずれであるかを決定します。保留コンフィギュレーションは、その機能に対してコミットまたは中断のアクションがトリガーされるまで存在します。この値が [running] の場合、この機能の後続のすべての設定取得は、ローカル デバイス上の実行コンフィギュレーションから行われます。この値が [pending] の場合、この機能の後続のすべての設定取得は、ローカル デバイス上の保留コンフィギュレーションから行われます。
LastCommand	この機能に対して実行された最後のアクション。
Result	CFS 対応機能に対して実行されたアクションの結果。
Scope	このオブジェクトの値は、CFS インフラストラクチャに登録されている CFS 対応機能の属性を表します。 • [fcFabric]：機能の CFS ベースの配信が FC（ファイバ チャネル）ファブリック全体にわたることを示します。 • [ipNetwork]：機能の CFS ベースの配信が IP ネットワーク全体にわたることを示します。 • [vsanScope]：機能の CFS ベースの配信が VSAN 単位で行われ、FC（ファイバ チャネル）ファブリック内の特定の VSAN に制限されることを示します。
PendingConfOwnerAddr	機能に対する保留コンフィギュレーションが存在する、ファブリック内のデバイスのアドレス。

関連トピック

CFS インフラストラクチャの使用

スイッチの CFS 配信のディセーブル化

アプリケーションの CFS のイネーブル化

Cisco Fabric Services（CFS）の IP マルチキャスト

フィールド	説明
IP Address Type	IP アドレス タイプ（IPv4、IPv6、または DNS）。
Multicast Address Domain	CFS 配信が制限されるマルチキャスト アドレス ドメイン。IP で CFS 対応スイッチを検出するためにキープアライブ メッセージが送受信されるデフォルトのマルチキャスト アドレスが IPv4 と IPv6 の両方に存在します。同じマルチキャスト アドレスを持つすべてのスイッチが 1 つの CFS-over-IP ファブリックを構成します。IPv4 のデフォルトのマルチキャスト アドレスは 239.255.70.83 で、サポートされる範囲は 239.255.0.0 ～ 239.255.255.255 です。IPv6 のデフォルトのマルチキャスト アドレスは ff13::7743:4653 で、サポートされる範囲は ff13::0000:0000 ～ ff13::ffff:ffff です。
Action	対応するタイプのインターネット アドレスを使用した配信について CFS で採用される現在の動作モードを指定します。このオブジェクトの値を [enable] に設定すると、CFS は、対応するタイプのインターネット アドレスを使用してファブリック経由でアプリケーション データを配信する機能をイネーブルにします。このオブジェクトの値を [disable] に設定すると、CFS は、対応するタイプのインターネット アドレスを使用してファブリック経由でデータを配信する機能をディセーブルにします。

Cisco Fabric Services（CFS）のリージョンごとの機能

フィールド	説明
Feature	配信リージョン内の CFS 対応機能の名前を特定します。
RegionId	CFS 配信リージョンを特定します。

Cisco Fabric Services（CFS）のすべてのリージョン

フィールド	説明
RegionId	CFS 配信リージョンを特定します。

Cisco Fabric Services（CFS）のオーナー

フィールド	説明
[Feature]、[VSAN]	CFS 対応機能の名前、およびその機能のイネーブル化やコミットが行われる VSAN。
[Name] または [IP Address]	機能のイネーブル化やコミットが行われるスイッチの名前または IP アドレス。
UserName	機能のイネーブル化またはコミットを実行したユーザの名前。
Type	使用された最後の CFS 機能スコープ タイプ。

Cisco Fabric Services（CFS）のマージ

フィールド	説明
Feature	CFS 対応機能の名前。
CFS Merge Status Value	最後に行われたファブリック マージの結果。

その他の参考資料

CFS の実装に関する詳細情報については、次の項を参照してください。

- 「MIB」（P.2-24）

MIB

MIB	MIB のリンク
• CISCO-CFS-CAPABILITY-MIB • CISCO-CFS-MIB	MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 http://www.cisco.com/en/US/products/ps5989/prod_technical_reference_list.html

CFS の機能履歴

表 2-2 に、この機能のリリース履歴を示します。Release 3.x 以降のリリースで導入または変更された機能のみが表に記載されています。

表 2-2　CFS の機能履歴

機能名	リリース	機能情報
CFS の保留の差異	5.0(1a)	CFS の保留の差異のスクリーン ショットが新しく追加されました。
CFS リージョン	3.2(1)	CFS に追加された [Region] タブ、およびリージョンの作成とリージョンへの機能の割り当てを行うためのダイアログボックス スイッチ ファブリック内の一部のスイッチで構成される CFS リージョンをユーザが設定できます。
許可ドメイン ID リストの CFS サポート	3.0(1)	[VSAN]、[Domain Manager] の下の [Allowed DomainIds] タブ CFS インフラストラクチャを使用して許可ドメイン ID リストをファブリック内で配信できます。
IP を介した CFS	3.0(1)	IP 接続を介した CFS 配信を可能にします。
RCSN の CFS サポート	3.0(1)	[VSAN]、[Domain Manager]、[Advanced] の下の [CFS] タブ CFS インフラストラクチャを使用して RSCN タイマー値をファブリック内で配信できます。
CFS リージョン	3.2.(1)	[All Regions] タブと [Feature by Region] タブの追加 CFS リージョンの表示と管理が可能です。[All Regions] タブと [Feature by Region] タブを使用して、リージョンを作成したり、機能をリージョンに割り当てたり、リージョン間で機能を移動させたりできます。

CHAPTER 3

システム メッセージ ロギングの設定

この章では、Cisco DCNM-SAN 上でシステム メッセージ ロギングを設定する方法について説明します。内容は次のとおりです。

システム メッセージ ロギングについて

システム メッセージ ロギング ソフトウェアでは、メッセージをログ ファイルに保存したり、メッセージを他のデバイスに転送したりできます。デフォルトでは、スイッチにより、正常だが重要なシステム メッセージがログ ファイルに記録され、それらのメッセージがシステム コンソールに送信されます。この機能には次の特徴があります。

- モニタリングおよびトラブルシューティングに使用するロギング情報を提供
- 取得したロギング情報のタイプが選択可能
- キャプチャされたロギング情報を適切に設定されたシステム メッセージ ロギング サーバに転送するために宛先サーバを選択可能。

システム メッセージを監視するには、DCNM-SAN の [Events] タブをクリックするか、Device Manager で [Logs] > [Events] > [Current] を選択します。システム メッセージは、Telnet、SSH、コンソール ポートのいずれかを通じてスイッチにアクセスするか、システム メッセージ ロギング サーバ上のログを参照することにより、リモートで監視することもできます。

（注） 最初にスイッチを初期化するとき、初期化が完了するまでネットワークは接続されません。そのため、メッセージはシステム メッセージ ロギング サーバに数秒間リダイレクトされます。

ログ メッセージは、システム再起動後には消去されています。ただし、重大度が Critical 以下（レベル 0、1、2）の最大 100 個のログ メッセージは NVRAM に保存されます。

表 3-1 では、システム メッセージ ログでサポートされているファシリティの例について説明します。

表 3-1　内部ロギング ファシリティ

ファシリティ キーワード	説明	標準であるか、または Cisco MDS 固有であるか
acl	ACL マネージャ	Cisco MDS 9000 ファミリ固有
all	すべてのファシリティ	Cisco MDS 9000 ファミリ固有
auth	許可システム	標準
authpriv	認証（プライベート）システム	標準
bootvar	Bootvar	Cisco MDS 9000 ファミリ固有
callhome	Call Home	Cisco MDS 9000 ファミリ固有
cron	cron ファシリティまたは at ファシリティ	標準
daemon	システム デーモン	標準
fcc	FCC	Cisco MDS 9000 ファミリ固有
fcdomain	fcdomain	Cisco MDS 9000 ファミリ固有
fcns	ネーム サーバ	Cisco MDS 9000 ファミリ固有
fcs	FCS	Cisco MDS 9000 ファミリ固有
flogi	FLOGI	Cisco MDS 9000 ファミリ固有
fspf	FSPF	Cisco MDS 9000 ファミリ固有
ftp	ファイル転送プロトコル	標準
ipconf	IP 設定	Cisco MDS 9000 ファミリ固有
ipfc	IPFC	Cisco MDS 9000 ファミリ固有
kernel	カーネル	標準
local0 ～ local7	ローカルに定義されたメッセージ	標準
lpr	ライン プリンタ システム	標準
mail	メール システム	標準
mcast	マルチキャスト	Cisco MDS 9000 ファミリ固有
module	スイッチング モジュール	Cisco MDS 9000 ファミリ固有
news	USENET ニュース	標準
ntp	NTP	Cisco MDS 9000 ファミリ固有
platform	プラットフォーム マネージャ	Cisco MDS 9000 ファミリ固有
port	ポート	Cisco MDS 9000 ファミリ固有
port-channel	PortChannel	Cisco MDS 9000 ファミリ固有
qos	QoS	Cisco MDS 9000 ファミリ固有
rdl	RDL	Cisco MDS 9000 ファミリ固有
rib	RIB	Cisco MDS 9000 ファミリ固有
rscn	RSCN	Cisco MDS 9000 ファミリ固有
securityd	セキュリティ	Cisco MDS 9000 ファミリ固有
syslog	内部システム メッセージ	標準
sysmgr	システム マネージャ	Cisco MDS 9000 ファミリ固有
tlport	TL ポート	Cisco MDS 9000 ファミリ固有

表 3-1　内部ロギング ファシリティ （続き）

ファシリティ キーワード	説明	標準であるか、または Cisco MDS 固有であるか
user	ユーザ プロセス	標準
uucp	UNIX 間コピー プログラム	標準
vhbad	仮想ホスト ベース アダプタ デーモン	Cisco MDS 9000 ファミリ固有
vni	仮想ネットワーク インターフェイス	Cisco MDS 9000 ファミリ固有
vrrp_cfg	VRRP の設定	Cisco MDS 9000 ファミリ固有
vrrp_eng	VRRP エンジン	Cisco MDS 9000 ファミリ固有
vsan	VSAN システム メッセージ	Cisco MDS 9000 ファミリ固有
vshd	vshd	Cisco MDS 9000 ファミリ固有
wwn	WWN マネージャ	Cisco MDS 9000 ファミリ固有
xbar	クロスバー システム メッセージ	Cisco MDS 9000 ファミリ固有
zone	ゾーン サーバ	Cisco MDS 9000 ファミリ固有

表 3-2 に、システム メッセージ ログでサポートされている重大度を示します。

表 3-2　エラー メッセージの重大度

レベル キーワード	レベル	説明	システム メッセージ定義
emergencies	0	システムが使用不可	LOG_EMERG
alerts	1	即時処理が必要	LOG_ALERT
critical	2	クリティカルな状態	LOG_CRIT
errors	3	エラー状態	LOG_ERR
warnings	4	警告状態	LOG_WARNING
notifications	5	正常だが注意を要する状態	LOG_NOTICE
informational	6	情報メッセージだけ	LOG_INFO
debugging	7	デバッグ メッセージ	LOG_DEBUG

（注）　エラー ログ メッセージ フォーマットの詳細については、『*Cisco MDS 9000 Family and Nexus 7000 Series System Messages Reference*』を参照してください。

ここで説明する内容は、次のとおりです。

- 「DCNM-SAN からの Syslog サーバのモニタリング」（P.3-4）
- 「システム メッセージ ロギング」（P.3-4）
- 「SFP 診断」（P.3-5）
- 「出力されるシステム メッセージ ロギング サーバ ファシリティ」（P.3-5）
- 「システム メッセージ ロギング サーバ」（P.3-6）
- 「システム メッセージ ロギング設定の配信」（P.3-6）
- 「ファブリックのロックの上書き」（P.3-7）

DCNM-SAN からの Syslog サーバのモニタリング

Cisco DCNM-SAN は、自身をロギング サーバとして登録し、Syslog メッセージを受信し、それらをスイッチごとに独立したファイルに保管します。

Cisco NX-OS Release 5.0(1a) 以降の DCNM-SAN は、ファブリック内のすべてのスイッチからの Syslog メッセージをデータベースに保管し、Web クライアントには集約された Syslog 情報のみを表示します。この機能は、イネーブルまたはディセーブルにできます。データベースに保管された Syslog は、設定可能な重大度によってフィルタリングされます。

DCNM-SAN が syslog レシーバを通じて Syslog メッセージを受信すると、それらの未処理メッセージが解析され、データベース内でそのメッセージを永続化させるためのフラグがオンにされます。解析されたフィールドからこのメッセージの重大度がチェックされ、Syslog メッセージはデータベースに送信されます。

未処理の Syslog メッセージは、switch time、facility、severity、event、および Vsan Id フィールドに解析されます。説明はデータベースに保管され、重大度でフィルタリングされます。

次のフィールドが server.properties に追加されます。

- syslog.dblog.enable = false

  このフィールドは、Syslog メッセージをデータベースに保管する機能をオンにするために使用されます。このフラグをオンにすると、Syslog メッセージがデータベースにも書き込まれます。

- syslog.dblog.severity = warnings

  このフィールドは、Syslog メッセージを重大度に基づいてフィルタリングするために使用されます。このプロパティを設定すると、Syslog メッセージが重大度に基づいてフィルタリングされます。

システム メッセージ ロギング

システム メッセージ ロギング ソフトウェアは、メッセージをログ ファイルに保存したり、他のデバイスにメッセージを転送したりします。この機能では、次のことができます。

- モニタリングおよびトラブルシューティングのためにロギング情報を提供します。
- ユーザが、キャプチャされたロギング情報のタイプを選択できます。
- ユーザが、キャプチャされたロギング情報を転送するために宛先サーバを選択できます。

デフォルトでは、スイッチにより、正常だが重要なシステム メッセージがログ ファイルに記録され、それらのメッセージがシステム コンソールに送信されます。ファシリティおよび重大度に基づいて保存するシステム メッセージを指定できます。リアルタイムのデバッグおよび管理を強化するために、メッセージにはタイムスタンプが付加されます。

ロギングされたシステム メッセージには CLI を使用してアクセスできます。あるいは、それらのメッセージを正しく設定されたシステム メッセージ ロギング サーバに保存してアクセスすることもできます。スイッチ ソフトウェアは、システム メッセージを、1200 エントリまで保存可能なファイルに保存します。システム メッセージは、Telnet、SSH、コンソール ポートのいずれかを通じてスイッチにアクセスするか、システム メッセージ ロギング サーバ上でログを表示することにより、リモートで監視できます。

SFP 診断

SFP 障害に関連したエラー メッセージは、Syslog に書き込まれます。SFP 障害に関連したイベントについて Syslog をリッスンできます。次のパラメータについて、値（下限または上限アラーム）と警告がチェックされます。

- TX 電力
- RX 電力
- 温度
- 電圧
- 電流

SFP 通知トラップは、デジタル診断モニタリング情報に基づいて、すべてのセンサーのアラームおよび警告のモニタリング パラメータの最新ステータスを示します。この通知は、インターフェイス内のトランシーバ上でセンサーのモニタリング パラメータが 1 つでもステータスを変化させると生成されます。

SFP 通知トラップ情報は、CISCO-INTERFACE-XCVR-MONITOR-MIB に格納されます。この MIB の詳細については、『*Cisco MDS 9000 Family MIB Quick Reference*』を参照してください。

出力されるシステム メッセージ ロギング サーバ ファシリティ

すべてのシステム メッセージには、ロギング ファシリティとレベルがあります。ロギング ファシリティは*場所*、レベルは*対象*と考えることができます。

単一のシステム メッセージ ロギング デーモン（syslogd）が、設定されている **facility** オプションに基づいて情報を送信します。ファシリティが指定されていない場合、local7 がデフォルトの送信ファシリティとなります。

内部ファシリティの一覧は表 3-1 に記載されており、送信ロギング ファシリティの一覧は表 3-3 に記載されています。

表 3-3　送信ロギング ファシリティ

ファシリティ キーワード	説明	標準であるか、または Cisco MDS 固有であるか
auth	許可システム	標準
authpriv	認証（プライベート）システム	標準
cron	cron ファシリティまたは at ファシリティ	標準
daemon	システム デーモン	標準
ftp	ファイル転送プロトコル	標準
kernel	カーネル	標準
local0 ～ local7	ローカルに定義されたメッセージ	標準（デフォルトは local7）
lpr	ライン プリンタ システム	標準
mail	メール システム	標準
news	USENET ニュース	標準
syslog	内部システム メッセージ	標準

表 3-3　送信ロギング ファシリティ （続き）

ファシリティ キーワード	説明	標準であるか、または Cisco MDS 固有であるか
user	ユーザ プロセス	標準
uucp	UNIX 間コピー プログラム	標準

システム メッセージ ロギング サーバ

Device Manager を使用すると、スイッチ上のイベント ログだけでなく、ローカル PC 上のイベント ログも参照できます。スイッチで発生するすべてのイベントを永続的に記録するには、これらのメッセージをスイッチから取得して保存する必要があります。そのためには、Syslog メッセージをローカル PC に送信するように Cisco MDS 9000 ファミリ スイッチを設定し、それらのメッセージを受信するためにその PC 上で Syslog サーバを動作させる必要があります。これらのメッセージは、次の 4 つのクラスに分類されます。

- ハードウェア：ラインカードまたは電源の問題
- リンク インシデント：FICON ポートの状態変化
- アカウンティング：ユーザ変更イベント
- イベント：その他すべてのイベント

（注）　DHCP によってランダムに IP アドレスが割り当てられた PC を使用するのは避けてください。スイッチは、手動で変更するまで古い IP アドレスを使用し続けます。ただし、Device Manager では、この状況を検出するとプロンプトが表示されます。UNIX ワークステーションには syslog サーバが組み込まれています。組み込み syslog デーモンを停止しシスコの syslog サーバを起動するには、root のアクセス権が必要です（または、シスコの syslog サーバを root の seuid として実行します）。

システム メッセージ ロギング設定の配信

ファブリック内のすべての Cisco MDS 9000 ファミリ スイッチに対してファブリック配信をイネーブルにできます。システム メッセージ ロギングを設定した場合、配信がイネーブルになっていると、その設定がファブリック内のすべてのスイッチに配信されます。

スイッチでの配信をイネーブルにした後で最初のコンフィギュレーション コマンドを発行すると、ファブリック全体が自動的にロックされます。システム メッセージ ロギング サーバは、有効/保留データベース モデルを使用して、設定をベースにコマンドを保存またはコミットします。設定の変更を確定すると、有効データベースが保留データベースの設定変更で上書きされ、ファブリック内のすべてのスイッチで設定が同じになります。設定を変更した後、変更を廃棄するには、変更を確定せずに中断します。いずれの場合でも、ロックは解除されます。CFS アプリケーションの詳細については、第 2 章「CFS インフラストラクチャの使用」を参照してください。

ファブリックのロックの上書き

システム メッセージ ロギングで作業を行い、変更の確定か廃棄を行ってロックを解除するのを忘れた場合、管理者はファブリック内の任意のスイッチからロックを解除できます。管理者がこの操作を行うと、ユーザによる保留データベースの変更は廃棄され、ファブリックのロックは解除されます。

ヒント　変更は volatile ディレクトリだけで使用でき、スイッチを再起動すると廃棄されます。

注意事項と制限

概念の詳細については、「CFS マージのサポート」（P.2-6）を参照してください。

2 つのシステム メッセージ ロギング データベースをマージする場合は、次の注意事項に従ってください。

- マージされたデータベースは、ファブリック内のスイッチごとに存在する受信データベースを結合したものになることに注意してください。
- マージされたデータベースに、最大で 3 つのシステム メッセージ ロギング サーバしか含まれないことを確認してください。

注意　マージされたデータベースに含まれるサーバが 3 台を超えると、そのマージは失敗します。

デフォルト設定

表 3-4 に、システム メッセージ ロギングのデフォルト設定値の一覧を示します。

表 3-4　システム メッセージ ログのデフォルト設定値

パラメータ	デフォルト
コンソールへのシステム メッセージ ロギング	Critical 重大度のメッセージに対してイネーブル。
Telnet セッションへのシステム メッセージ ロギング	ディセーブル。
ロギング ファイル サイズ	4194304。
ログ ファイル名	メッセージ（最大 200 文字の名前に変更可能）。
ロギング サーバ	ディセーブル。
Syslog サーバの IP アドレス	設定されていません。
サーバ数	3 台。
サーバ機能	local7。

システム メッセージ ロギングの設定

システム ロギング メッセージは、デフォルトの（または設定された）ロギング ファシリティと重大度に基づいてコンソールに送信されます。

ここでは、次の内容について説明します。

システム メッセージ ロギングを設定するためのタスク フロー

システム メッセージ ロギングを設定するには、次の手順を実行します。

ステップ 1　メッセージ ロギングをイネーブルまたはディセーブルにします。

ステップ 2　モニタ重大度を設定します。

ステップ 3　ファシリティ重大度を設定します。

ステップ 4　ログ ファイルを送信します。

ステップ 5　システム メッセージ ロギング サーバを設定します。

メッセージ ロギングのイネーブル化またはディセーブル化

コンソールへのロギングをディセーブルにしたり、特定された Telnet セッションまたは SSH セッションへのロギングをイネーブルにできます。

- コンソール セッションへのロギングをディセーブルまたはイネーブルにすると、その状態は将来のすべてのコンソール セッションに適用されます。セッションを終了して新しいセッションに再度ログインした場合、状態は保持されます。
- Telnet セッションまたは SSH セッションへのロギングをイネーブルまたはディセーブルにした場合、その状態はそのセッションだけに適用されます。セッションを終了して新しいセッションに再度ログインした場合、状態は保持されません。

手順の詳細

Telnet セッションまたは SSH セッションのロギング状態をイネーブルまたはディセーブルにするには、次の手順を実行します。

ステップ 1　[Fabric] ペインでスイッチを選択します。

ステップ 2　[Physical Attributes] ペインで [Events] を展開し、[SysLog] を選択します。

[Information] ペインに、SysLog 情報が表示されます。

ステップ 3　[Switch Logging] タブをクリックします。

スイッチ情報が表示されます。

ステップ 4　[Information] ペインでスイッチを選択します。

ステップ 5　[Console Enable] チェックボックスをオン（イネーブル）またはオフ（ディセーブル）にします。

ステップ 6　[Apply Changes] アイコンをクリックします。

コンソール重大度の設定

コンソール セッションに対するロギングがイネーブルになっている場合（デフォルト）、コンソールに表示されるメッセージの重大度を設定できます。コンソール ロギングのデフォルトの重大度は 2（Critical）です。

コンソールのボー レートが 9600 ボー（デフォルト）の場合、現在の Critical（デフォルト）ロギング レベルが維持されます。コンソール ロギング レベルを変更しようとすると、必ずエラー メッセージが生成されます。ロギング レベルを上げる（Critical よりも上に）には、コンソールのボー レートを 38400 ボーに変更する必要があります。

モニタ重大度の設定

モニタ セッションに対するロギングがイネーブルになっている場合（デフォルト）、モニタに表示されるメッセージの重大度を設定できます。モニタ ロギングのデフォルトの重大度は 5（notifications）です。

手順の詳細

ロギング ファシリティの重大度を設定するには、次の手順を実行します。

ステップ 1　[Fabric] ペインでスイッチを選択します。

ステップ 2　[Physical Attributes] ペインで [Events] を展開し、[SysLog] を選択します。

[Information] ペインに、SysLog 情報が表示されます。

ステップ 3　[Switch Logging] タブをクリックします。

スイッチ情報が表示されます。

ステップ 4　[Information] ペインでスイッチを選択します。

ステップ 5　そのスイッチの行の [Console Severity] ドロップダウン リストから重大度を選択します。

ステップ 6　[Apply Changes] アイコンをクリックします。

モジュール ロギングの設定

デフォルトでは、すべてのモジュールに対してレベル 7 でロギングが有効になっています。各モジュールの対するロギングを、特定のレベルでイネーブルまたはディセーブルにできます。

ファシリティ重大度の設定

手順の詳細

ロギング ファシリティの重大度を設定するには、次の手順を実行します。

ステップ 1　[Physical Attributes] ペインで [Events] を展開し、[SysLog] を選択します。

Device Manager で、[Logs] > [Syslog] > [Setup] の順に選択し、[Syslog] ダイアログボックスの [Switch Logging] タブをクリックします。

スイッチ情報が表示されます。

ステップ 2　メッセージ ロギングを行うチェックボックスをオンにします（[ConsoleEnable]、[TerminalEnable]、[LineCardEnable]）。

ステップ 3　DCNM-SAN で、各スイッチに対するメッセージ重大度しきい値を [Console Severity] ドロップダウン ボックスから選択します。または、Device Manager で、適切なメッセージ重大度のオプション ボタンをクリックします。

ステップ 4　DCNM-SAN で [Apply Changes] アイコンをクリックするか、Device Manager で [Apply] をクリックし、変更内容を保存して適用します。

ログ ファイルの送信

デフォルトでは、スイッチにより、正常だが重要なシステム メッセージがログ ファイルに記録され、それらのメッセージがシステム コンソールに送信されます。ログ メッセージは、システムの再起動時に保存されません。ロギング メッセージは生成時にログ ファイルに保存できます。必要に応じてこのファイルの名前を設定したり、そのサイズを制限できます。デフォルトのログ ファイル名は messages です。

ファイル名の最大文字数は 80 文字で、ファイル サイズの範囲は 4096 ～ 4194304 バイトです。

制約事項

設定したログ ファイルは、/var/log/external ディレクトリに保存されます。ログ ファイルの場所は変更できません。

手順の詳細

ログ メッセージをファイルに送るには、次の手順を実行します。

ステップ 1　[Fabric] ペインでスイッチを選択します。

ステップ 2　[Physical Attributes] ペインで [Events] を展開し、[SysLog] を選択します。

[Information] ペインに、SysLog 情報が表示されます。

ステップ 3　[Information] ペインでスイッチを選択します。

ステップ 4　[Switch Logging] タブをクリックします。

ステップ 5　ログ ファイルの名前を、そのスイッチの行の [LogFile Name] カラムに入力します。

ステップ 6　[Apply Changes] アイコンをクリックします。

システム メッセージ ロギング サーバの設定

最大 3 台のシステム メッセージ ロギング サーバを設定できます。DCNM-SAN の [Event] タブからシステム メッセージを参照するには、これらの Syslog サーバの 1 台を DCNM-SAN にする必要があります。

ログ メッセージを UNIX システム メッセージ ロギング サーバに送るには、UNIX サーバ上でシステム メッセージ ロギング デーモンを設定する必要があります。root でログインし、次の手順を実行します。

ステップ 1　次の行を /etc/syslog.conf ファイルに追加します。

```
local1.debug                    /var/log/myfile.log
```

（注）　**local1.debug** と **/var/log/*myfile*.log** の間には、必ず 5 個のタブ文字を追加してください。詳細な例については、/etc/syslog.conf ファイルのエントリを参照してください。

スイッチは、指定されたファシリティ タイプと重大度に基づいて、メッセージを送信します。**local1** キーワードは、UNIX のロギング ファシリティを使用することを指定します。スイッチからのメッセージは、ユーザ プロセスによって生成されます。**debug** キーワードは、ログに記録される状態の重大度を指定します。スイッチからのすべてのメッセージを受信するように UNIX システムを設定できます。

ステップ 2　UNIX シェル プロンプトに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　次のコマンドを実行して、システム メッセージ ロギング デーモンに新しい変更を読み込ませます。

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

（注）　CFS を使用している機能の [Information] ペインのほとんどのタブは、[CFS] タブをクリックするまで薄く表示されます。[CFS] タブには、CFS がイネーブルになっているスイッチと、この機能のマスター スイッチが表示されます。[CFS] タブをクリックすると、CFS を使用している [Information] ペインの他のタブがアクティブになります。

手順の詳細

システム メッセージ ロギング サーバを設定するには、次の手順を実行します。

ステップ 1　[Physical Attributes] ペインで [Events] を展開し、[SysLog] を選択します。

ステップ 2　[Information] ペインで、[Servers] タブをクリックします。

Device Manager で、[Logs] > [Syslog] > [Setup] の順に選択し、[syslog] ダイアログボックスの [Servers] タブをクリックします。

ステップ 3　新しい Syslog サーバを追加するには、DCNM-SAN で [Create Row] アイコンをクリックするか、Device Manager で [Create] をクリックします。

ステップ 4　syslog サーバの名前またはドット付き 10 進表記の IP アドレス（たとえば 192.168.2.12）を、[Name or IP Address] フィールドに入力します。

ステップ 5　[MsgSeverity] オプション ボタンをクリックしてメッセージ重大度のしきい値を設定し、[Facility] オプション ボタンをクリックしてファシリティを設定します。

ステップ 6　DCNM-SAN で [Apply Changes] アイコンをクリックするか、Device Manager で [Create] をクリックし、変更を保存して適用します。

ログ設定の確認

ここでは、システム メッセージ ロギング設定情報を表示する方法について説明します。

DCNM-SAN Web サーバからの Syslog サーバの確認

Syslog サーバを、DCNM-SAN Web サーバを使用してリモートで確認するには、次の手順を実行します。

ステップ 1　ブラウザで DCNM-SAN Web サーバにアクセスします。

ステップ 2　[Events] > [Syslog] を選択して、各スイッチの syslog サーバ情報を表示します。テーブル内のカラムはソートできます。

ログのモニタリング

この項では、次の項目について説明します。

- 「DCNM-SAN Web サーバからのログの表示」（P.3-12）
- 「Device Manager からのログの表示」（P.3-13）

DCNM-SAN Web サーバからのログの表示

DCNM-SAN Web サーバを使用してシステム メッセージをリモートで表示するには、次の手順を実行します。

ステップ 1　ブラウザで DCNM-SAN Web サーバにアクセスします。

ステップ 2　[Events] タブ、[Details] の順にクリックするとシステム メッセージが表示されます。イベント テーブル内のカラムはソートできます。また、[Filter] ボタンを使用して、テーブル内のメッセージの範囲を制限できます。

Device Manager からのログの表示

DCNM-SAN と同じワークステーションから Device Manager を実行している場合には、Device Manager からシステム メッセージを表示できます。Device Manager で [Logs] > [Events] > [current] を選択すると、システム メッセージが表示されます。イベント テーブル内のカラムはソートできます。また、[Find] ボタンを使用して、テーブル内のテキストを検索できます。

スイッチに保存されているログは、ローカル Syslog サーバが設定されていなくても、またはスイッチの Syslog サーバ リストにローカル PC が含まれていなくても表示できます。ただし、メモリに制限があるため、特定のサイズに達すると古いログは消去されます。スイッチの Syslog には、2 つのログがあります。Critical 以上の重大度のメッセージが限定数だけ保存される NVRAM ログ、および Notice 以上の重大度のメッセージが保存される非永続的なログです。ハードウェア メッセージは、これらのログに含まれます。

その他の参考資料

システム メッセージ ロギングの実装に関する詳細情報については、次の項を参照してください。

- 「MIB」（P.3-13）

MIB

MIB	MIB のリンク
• CISCO-SYSLOG-EXT-MIB • CISCO-SYSLOG-MIB	MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 http://www.cisco.com/en/US/products/ps5989/prod_technical_reference_list.html

システム メッセージ ロギングの機能履歴

表 3-5 に、この機能のリリース履歴を示します。Release 3.x 以降のリリースで導入または変更された機能のみが表に記載されています。

表 3-5　システム メッセージ ロギングの機能履歴

機能名	リリース	機能情報
Syslog の拡張	5.0(1a)	DCNM-SAN からの Syslog サーバのモニタリングが追加されました。 システム メッセージ ロギング情報が追加されました。

CHAPTER 4

Call Home の設定

Call Home は、重要なシステム イベントを E メールで通知します。ポケットベル サービス、通常の電子メール、または XML ベースの自動解析アプリケーションとの適切な互換性のために、さまざまなメッセージの形式が使用できます。

（注） Cisco Autonotify は、Smart Call Home と呼ぶ新機能にアップグレードされています。Smart Call Home は、Autonotify に比べて機能が大幅に改良されており、シスコの製品レンジ全体にわたって使用できます。Smart Call Home の詳細については、Smart Call Home のページ（http://www.cisco.com/go/smartcall/）を参照してください。

この章の内容は、次のとおりです。

Call Home について

Call Home 機能は、メッセージ スロットリング機能を備えています。定期的なコンポーネント メッセージ、ポート syslog メッセージ、および RMON アラート メッセージが、配信可能な Call Home メッセージの一覧に追加されています。必要に応じて、Cisco Fabric Services アプリケーションを使用して、Call Home 設定を、ファブリック内の他のすべてのスイッチに配信することもできます。

Call Home サービスでは、重要なシステム イベントに関する電子メール ベースの通知が提供されます。ポケットベル サービス、通常の電子メール、または XML ベースの自動解析アプリケーションとの適切な互換性のために、さまざまなメッセージの形式が使用できます。

一般的な機能として次のものがあります。

- ポケットベルによるネットワーク サポート技術者の呼び出し
- ネットワーク オペレーション センターへの電子メールの送信
- Technical Assistance Center の直接ケースの提出

Call Home 機能は、Cisco MDS 9000 ファミリ スイッチと Cisco Nexus 5000 シリーズ スイッチから直接利用できます。複数の Call Home メッセージが提供され、それぞれに個別の宛先があります。事前に定義されたプロファイルに加えて、独自の宛先プロファイルを定義できます。各宛先プロファイルには最大 50 件の電子メール アドレスを設定できます。柔軟なメッセージの配信オプションとフォーマット オプションにより、個別のサポート要件を簡単に統合できます。

Call Home 機能には、次の利点があります。

- スイッチ上のトリガー イベント用に事前に定義された一連の固定のアラート。
- 関連するコマンドの自動的な実行と出力の添付。

ここで説明する内容は、次のとおりです。

Call Home の機能

Call Home 機能は、Cisco MDS 9000 ファミリ スイッチと Cisco Nexus 5000 シリーズ スイッチから直接利用できます。複数の Call Home プロファイル（*Call Home 宛先プロファイル*とも呼びます）が提供され、それぞれに個別の宛先があります。事前に定義されたプロファイルに加えて、独自の宛先プロファイルを定義できます。

Call Home 機能では、シスコまたは別のサポート パートナーによるサポートも利用できます。柔軟なメッセージの配信オプションとフォーマット オプションにより、個別のサポート要件を簡単に統合できます。

Call Home 機能には、次の利点があります。

- スイッチ上の固定の事前に定義されたアラートおよびトリガー イベント。
- 関連するコマンドの自動的な実行と出力の添付。
- 複数のメッセージ フォーマット オプション
  - 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。

  - プレーン テキスト：人間が読むのに適した形式に完全整形されたメッセージ情報。
  - XML：Extensible Markup Language（XML）と、Messaging Markup Language（MML）と呼ぶ Document Type Definitions（DTD）を使用した、機械で読み取り可能なフォーマット。MML DTD は、Cisco.com の Web サイト http://www.cisco.com/ で公開されています。XML フォーマットでは、シスコの Technical Assistance Center との通信が可能になります。
- 複数のメッセージ宛先への同時配信が可能。各宛先プロファイルには最大 50 件の電子メール宛先アドレスを設定できます。
- システム、環境、スイッチング モジュール ハードウェア、スーパーバイザ モジュール、ハードウェア、コンポーネント、syslog、RMON、テストなど、複数のメッセージ カテゴリ。
- お使いのデバイスから直接、または HTTP プロキシ サーバやダウンロード可能な転送ゲートウェイ（TG）を介した、セキュアなメッセージ転送。TG 集約ポイントは、複数のデバイスをサポートする場合またはセキュリティ要件によって、デバイスをインターネットに直接接続できない場合に使用できます。

Smart Call Home の概要

Smart Call Home は、Cisco SMARTnet Service のコンポーネントであり、選択したシスコ デバイス上での予防的診断、リアルタイム アラート、パーソナライズされた Web ベースのレポート機能を提供します。

Smart Call Home は、デバイスから送信された Call Home メッセージを解析し、シスコ カスタマー サポートへの直接通知パスを提供することにより、システムの問題を迅速に解決します。

Smart Call Home には、次の機能があります。

- 連続的なデバイスのヘルス モニタリングとリアルタイム診断アラート。
- 使用しているデバイスからの Call Home メッセージの分析と、必要に応じた自動的なサービス リクエストの生成と適切な TAC チームへの送信。これには、すばやい問題解決のための詳細な診断情報が含まれます。
- Call Home メッセージと推奨事項、すべての Call Home デバイスのコンポーネントと設定情報への Web アクセス。関連付けられたフィールド通告、セキュリティ勧告、およびサポート終了日情報にアクセスできます。

表 4-1 に Smart Call Home の利点の一覧を示します。

表 4-1　Smart Call Home の Autonotify と比較した利点

機能	Smart Call Home	Autonotify
簡単な登録	登録処理が大幅に簡素化されます。デバイス シリアル番号や連絡先情報を知っている必要はありません。デバイスからメッセージを送信することで、シスコの手動の介入なしにデバイスを登録できます。手順の概要については www.cisco.com/go/smartcall を参照してください。	各シリアル番号をデータベースに追加するようにシスコに依頼する必要があります。
推奨事項	Smart Call Home は、SR が提起された問題や、SR が該当しないものの、お客様による対処が必要となる可能性がある、既知の問題に対する推奨事項を提供します。	Autonotify は、一連の障害状況に対する SR を提起しますが、それらの対する推奨事項は提供しません。
デバイス レポート	デバイス レポートには、完全なコンポーネントと設定の詳細が含まれています。これらのレポート内の情報は、Field Notice、PSIRT、EoX notices、コンフィグレーション ベスト プラクティスとバグにマッピングされます。	なし。
履歴レポート	履歴レポートは、メッセージとその内容を探すために使用できます。これには、過去 3 か月の間に送信されたすべてのメッセージに対する、**show** コマンド、メッセージ処理、分析結果、推奨事項とサービス リクエスト番号が含まれます。	基本的なレポートが使用できますが、メッセージの内容は含まれていません。
ネットワーク要約レポート	カスタマー ネットワーク内のデバイスとモジュールの構成の要約を示すレポート（Smart Call Home に登録されているデバイスが対象です）	なし。
シスコ デバイスのサポート	デバイスのサポートはシスコの製品レンジ全体に拡張されます。サポートされている製品の表については、www.cisco.com/go/smartcall を参照してください。	Smart Call Home への移行を推進するため、2008 年 10 月に廃止されました。

Smart Call Home の取得

シスコと直接サービス契約を結んでいる場合は、Smart Call Home サービスに登録することで、Technical Assistance Center から自動的なケース生成を受け取ることができます。

次の項目を登録する必要があります。

- 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

Smart Call Home の詳細と、クイック スタート コンフィギュレーションおよび登録手順については、次の場所にある Smart Call Home のページを参照してください。

http://www.cisco.com/go/smartcall/

Call Home 宛先プロファイル

宛先プロファイルには、アラート通知に必要な送信情報が含まれています。宛先プロファイルは、一般にネットワーク管理者によって設定されます。

アラート グループを使用して、（定義済みまたはユーザ定義の）宛先プロファイルで受信される Call Home アラートのセットを選択できます。アラート グループは、Call Home アラートの事前に定義されたサブセットであり、Cisco MDS 9000 ファミリと Cisco Nexus 5000 シリーズのすべてのスイッチでサポートされています。Call Home アラートはタイプごとに別のアラート グループにグループ化されます。ネットワークの必要性に応じて、1 つ以上のアラート グループを各プロファイルに関連付けることができます。

Call Home アラート グループ

アラート グループは、事前に定義された Call Home アラートのサブセットで、Cisco MDS 9000 ファミリと Cisco Nexus 5000 シリーズのすべてのスイッチでサポートされています。アラート グループを使用することで、（定義済みまたはユーザ定義の）宛先プロファイルで受信される Call Home アラートのセットを選択できます。Call Home アラートが、宛先プロファイル内の E メールの宛先に送信されるのは、その Call Home アラートが、その宛先プロファイルに関連付けられているいずれかのアラート グループに属する場合だけです。

定義済みの Call Home アラート グループを使用して、スイッチに特定のイベントが発生したときに通知メッセージを生成できます。定義済みのアラート グループは、特定のイベントが発生した際に追加の **show** コマンドを実行したり、定義済みの **show** コマンド以外からの出力を通知したりするようにカスタマイズできます。

カスタマイズされたアラート グループ メッセージ

アラート グループは、事前に定義された Call Home アラートのサブセットで、Cisco MDS 9000 ファミリと Cisco Nexus 5000 シリーズ スイッチのすべてのスイッチでサポートされています。アラート グループを使用することで、（定義済みまたはユーザ定義の）宛先プロファイルで受信される Call Home アラートのセットを選択できます。定義済みの Call Home アラート グループは、スイッチ上で特定のイベントが発生したときに通知メッセージを生成します。定義済みのアラート グループをカスタマイズして、特定のイベントが発生したときに、**show** コマンドを追加で実行できます。

Call Home のメッセージ レベル機能

Call Home のメッセージ レベル機能を使用すると、緊急度に基づいてメッセージをフィルタできます。各宛先プロファイル（定義済みおよびユーザ定義）は、Call Home メッセージ レベルしきい値に関連付けられます。緊急度しきい値よりも値が小さいメッセージは送信されません。Call Home の重大度は、システム メッセージ ロギングの重大度とは異なります。

Syslog ベースのアラート

特定の syslog メッセージを Call Home メッセージとして送信するようにスイッチを設定できます。これらのメッセージは、宛先プロファイルとアラート グループ マッピングの間のマッピング、および生成された Syslog メッセージの重大度に基づいて送信されます。

Syslog ベースの Call Home アラートを受信するには、宛先プロファイルと Syslog アラート グループを関連付けて（現在は syslog-group-port という 1 つの Syslog アラート グループだけが存在する）、適切なメッセージ レベルを設定する必要があります。

syslog-group-port アラート グループは、そのポート ファシリティの syslog メッセージを選択します。Call Home アプリケーションは、syslog の重大度を対応する Call Home の重大度にマッピングします（「Call Home のメッセージ レベル」（P.4-10）を参照）。たとえば、Call Home メッセージ レベルに対してレベル 5 を選択すると、レベル 0、1、2 の syslog メッセージが Call Home ログに追加されます。

syslog メッセージが生成されるたびに、Call Home アプリケーションは、宛先プロファイルとアラート グループ マッピングの間のマッピングに従い、生成された syslog メッセージの重大度に基づいて、Call Home メッセージを送信します。Syslog ベースの Call Home アラートを受信するには、宛先プロファイルと Syslog アラート グループを関連付けて（現在は syslog-group-port という 1 つの Syslog アラート グループだけが存在する）、適切なメッセージ レベルを設定する必要があります（「Call Home のメッセージ レベル」（P.4-10）を参照）。

（注）　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。Call Home ログ内の Syslog メッセージ テキストは、『*Cisco MDS 9000 Family and Nexus 7000 Series System Messages Reference*』の記載どおりに出力されます。

RMON ベースのアラート

RMON アラート トリガーに対応する Call Home 通知を送信するようにスイッチを設定できます。RMON ベースの Call Home メッセージのメッセージ レベルは、すべて NOTIFY（2）に設定されます。RMON アラート グループは、すべての RMON ベースの Call Home アラートに対して定義されます。RMON ベースの Call Home アラートを受信するには、宛先プロファイルを RMON アラート グループに関連付ける必要があります。

HTTPS サポートを使用した一般的な電子メール オプション

Call Home の HTTPS サポートは、HTTP と呼ばれる転送方式を提供します。HTTPS サポートはセキュアな通信で使用され、HTTP はノンセキュアな通信で使用されます。Call Home 宛先プロファイルに対し、HTTP URL を宛先として設定できます。URL リンクは、セキュア サーバでもノンセキュア サーバでも構いません。HTTP URL を使用して設定された宛先プロファイルでは、Call Home メッセージは、HTTP URL リンクにポストされます。

（注）　Call Home HTTP 設定は、NX-OS Release 4.2(1) 以降が動作するスイッチに、CFS を通じて配信できます。Call Home HTTP 設定は、配信不可能な HTTP 設定をサポートしているスイッチには配布できません。NX-OS Release 4.2(1) よりも前のバージョンが動作しているスイッチでは、HTTP 設定は無視されます。

定期的なコンポーネント通知

スイッチ上で現在イネーブルかつ動作中のすべてのソフトウェア サービスの一覧と、ハードウェア コンポーネント情報とともに、定期的にメッセージを送信するようにスイッチを設定できます。コンポーネントは、スイッチを停止せずに再起動するたびに変更されます。

重複するメッセージのスロットリング

同じイベントに対して受信する Call Home メッセージの数を制限するために、スロットリング メカニズムを設定できます。短時間のうちにスイッチから何度も同じメッセージが送信される場合、重複する多数のメッセージであふれることがあります。

Call Home 設定の配信

ファブリック内のすべての Cisco MDS 9000 ファミリ スイッチと Cisco Nexus 5000 シリーズ スイッチに対して、ファブリック配信をイネーブルにできます。Call Home を設定した場合、配信がイネーブルになっていると、その設定がファブリック内のすべてのスイッチに配信されます。ただし、スイッチ プライオリティと Syscontact 名は配信されません。

スイッチで配信をイネーブルにしてから初めてコンフィギュレーション コマンド操作を入力するとき、ファブリック全体が自動的にロックされます。Call Home アプリケーションは、設定の変更を保存または確定するために、有効および保留データベース モデルを使用します。設定の変更を確定すると、有効データベースが保留データベースの設定変更で上書きされ、ファブリック内のすべてのスイッチで設定が同じになります。設定を変更した後、変更を廃棄するには、変更を確定せずに中断します。いずれの場合でも、ロックは解除されます。CFS アプリケーションの詳細については、第 2 章「CFS インフラストラクチャの使用」を参照してください。

（注）　スイッチ プライオリティと Syscontact 名は配信されません。

ファブリックのロックの上書き

Call Home で作業を行い、変更の確定か廃棄を行ってロックを解除するのを忘れた場合、管理者はファブリック内の任意のスイッチからロックを解除できます。管理者がこの操作を行うと、ユーザによる保留データベースの変更は廃棄され、ファブリックのロックは解除されます。

ヒント　変更は volatile ディレクトリだけで使用でき、スイッチを再起動すると廃棄されます。

Call Home ネーム サーバ データベースのクリア

Call Home ネーム サーバ データベースが一杯になると、新しいエントリを追加できなくなります。デバイスがオンラインになることはできません。ネーム サーバ データベースをクリアするには、データベース サイズを増やすか、使用していないデバイスを削除してクリーンアップを実行します。合計 20,000 個のネーム サーバ エントリがサポートされています。

EMC E-mail Home 遅延トラップ

DCNM-SAN は、EMC E-mail Home XML 電子メール メッセージを生成するように設定できます。SAN-OS Release 3.x およびそれよりも前のリリースでは、DCNM-SAN はインターフェイス トラップを受信し、EMC E-mail Home 電子メール メッセージを生成します。リンク トラップは、インターフェイスがアップからダウンに移行する場合、またはその逆の場合に生成されます。たとえば、サーバのリブートがスケジュールされている場合、リンクがダウンし DCNM-SAN が電子メール通知を生成します。

Cisco NX-OS Release4.1(3) には、生成される E メール メッセージの数を減らすために、遅延トラップを生成する機能が備わっています。この方法は、サーバのリブートをフィルタし、無駄な EMC E-mail Home E メール メッセージの生成を回避します。NX-OS Release 4.1(3) では、ユーザは既存の機能か、もしくはこの新しい遅延トラップ機能を選択できます。

イベント トリガー

ここでは、Call Home のトリガー イベントについて説明します。トリガー イベントは複数のカテゴリにわかれており、各カテゴリには、イベントが発生したときに実行される CLI コマンドが割り当てられています。

表 4-2　イベント トリガー

イベント	アラート グループ	イベント名	説明	Call Home メッセージ レベル
Call Home	システムおよび CISCO_TAC	SW_CRASH	ソフトウェア プロセスがステートレス再起動を伴ってクラッシュしました。サービスの中断を示します。	5
	システムおよび CISCO_TAC	SW_SYSTEM_INCONSISTENT	ソフトウェアまたはファイル システムで不整合が検出されました。	5
	環境および CISCO_TAC	TEMPERATURE_ALARM	温度センサーが、温度が動作しきい値に達したことを示しています。	6
		POWER_SUPPLY_FAILURE	電源が障害になりました。	6
		FAN_FAILURE	冷却ファンが障害になりました。	5
	ラインカード ハードウェアおよび CISCO_TAC	LINECARD_FAILURE	ラインカード ハードウェアが障害になりました。	7
		POWER_UP_DIAGNOSTICS_FAILURE	ラインカード ハードウェアの電源投入診断に失敗しました。	7
	ラインカード ハードウェアおよび CISCO_TAC	PORT_FAILURE	インターフェイス ポートのハードウェア障害。	6
	ラインカード ハードウェア、スーパーバイザ ハードウェア、および CISCO_TAC	BOOTFLASH_FAILURE	ブート コンパクト フラッシュ カードの障害。	6
	スーパーバイザ ハードウェアおよび CISCO_TAC	NVRAM_FAILURE	スーパーバイザ ハードウェア上の NVRAM のハードウェア障害。	6
	スーパーバイザ ハードウェアおよび CISCO_TAC	FREEDISK_FAILURE	スーパーバイザ ハードウェア上の空きディスク スペースがしきい値未満。	6
	スーパーバイザ ハードウェアおよび CISCO_TAC	SUP_FAILURE	スーパーバイザ ハードウェアの動作失敗。	7
		POWER_UP_DIAGNOSTICS_FAILURE	スーパーバイザ ハードウェアの電源投入診断に失敗しました。	7
	スーパーバイザ ハードウェアおよび CISCO_TAC	INBAND_FAILURE	インバンド通信パスの障害。	7
	スーパーバイザ ハードウェアおよび CISCO_TAC	EOBC_FAILURE	イーサネット アウトオブバンド チャネル通信障害。	6

表 4-2　イベント トリガー （続き）

イベント	アラート グループ	イベント名	説明	Call Home メッセージ レベル
Call Home	スーパーバイザ ハードウェアおよび CISCO_TAC	MGMT_PORT_FAILURE	管理イーサネット ポートのハードウェア障害。	5
	ライセンス	LICENSE_VIOLATION	使用中の機能のライセンスがなく、猶予期間の後にオフになります。	6
コンポーネント	コンポーネントおよび CISCO_TAC	COLD_BOOT	スイッチの電源が投入され、コールド ブート シーケンスにリセットされます。	2
		HARDWARE_INSERTION	シャーシに新しいハードウェアが挿入されました。	2
		HARDWARE_REMOVAL	シャーシからハードウェアが除去されました。	2
テスト	テストおよび CISCO_TAC	TEST	ユーザがテストを生成しました。	2
ポート syslog	syslog-group-ポート	SYSLOG_ALERT	ポート ファシリティに対応する syslog メッセージ。	2
RMON	RMON	RMON_ALERT	RMON アラート トリガー メッセージ。	2

Call Home のメッセージ レベル

Call Home メッセージ（syslog アラート グループに対して送信）には、Call Home メッセージ レベルにマッピングされた syslog 重大度があります（「Syslog ベースのアラート」（P.4-6）を参照）。

ここでは、Cisco MDS 9000 ファミリと Cisco Nexus 5000 シリーズのスイッチを 1 つ以上使用する場合の Call Home メッセージの重大度について説明します。Call Home メッセージ レベルは、イベント タイプごとに事前に割り当てられています。

重大度の範囲は 0 ～ 9 で、9 の緊急度が最も高くなっています。各 syslog レベルには、表 4-3 に示すように、キーワードと対応する syslog レベルがあります。

（注）　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。Call Home ログ内の Syslog メッセージ テキストは、『*Cisco MDS 9000 Family and Nexus 7000 Series System Messages Reference*』の記載どおりに出力されます。

（注）　Call Home の重大度は、システム メッセージ ロギングの重大度と同じではありません（『*Cisco MDS 9000 Family and Nexus 7000 Series System Messages Reference*』を参照）。

表 4-3　重大度と Syslog レベルのマッピング

Call Home レベル	使用されるキーワード	Syslog レベル	説明
Catastrophic (9)	**Catastrophic**	該当なし	ネットワーク全体の破滅的な障害。
Disaster (8)	**Disaster**	該当なし	ネットワークへの重大な影響。

表 4-3　重大度と Syslog レベルのマッピング （続き）

Call Home レベル	使用されるキーワード	Syslog レベル	説明
Fatal (7)	**Fatal**	緊急（0）	システムが使用不可能な状態。
Critical (6)	**Critical**	アラート（1）	クリティカルな状態、ただちに注意が必要。
Major (5)	**Major**	重要（2）	重大な状態。
Minor (4)	**Minor**	エラー（3）	軽微な状態。
Warning (3)	**Warning**	警告（4）	警告状態。
Notify (2)	**Notification**	通知（5）	基本的な通知と情報メッセージ。他と関係しない、重要性の低い障害。
Normal (1)	**Normal**	情報（6）	標準状態に戻ることを示す標準イベント。
Debug (0)	**Debugging**	デバッグ（7）	デバッグ メッセージ。

メッセージの内容

スイッチ上で次の連絡先情報を設定できます。

- 連絡先担当者の名前
- 連絡先担当者の電話番号
- 連絡先担当者の E メール アドレス
- 交換部品の送付先の住所（必要な場合）
- サイトが展開されているネットワークのサイト ID
- お客様とサービス プロバイダーの間のサービス契約を識別するコンタクト ID

表 4-4 に、すべてのメッセージ タイプのショート テキスト フォーマット オプションを示します。

表 4-4　ショート テキスト メッセージ

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

表 4-5、表 4-6、および表 4-7 に、プレーンテキスト メッセージおよび XML メッセージに含まれる情報を示します。

表 4-5　対処的イベント メッセージ フォーマット

データ項目（プレーンテキストと XML）	説明（プレーン テキストと XML）	XML タグ（XML のみ）
タイム スタンプ	ISO 時刻表記（*YYYY-MM-DDTHH:MM:SS*）による日付とタイム スタンプ。 **（注）** UTC からの時間帯または夏時間（DST）オフセットは、すでに適用済みです。T は、ハードコードされた時刻の区切りです。	/mml/header/time - ch:EventTime
メッセージ名	メッセージの名前。具体的なイベント名のリストは「イベント トリガー」（P.4-9）に示されています。	/mml/header/name
メッセージ タイプ	「Call Home」となります。	/mml/header/type - ch:Type
メッセージ グループ	「reactive」となります。	/mml/header/group
重大度	メッセージの重大度（表 4-3 を参照）。	/mml/header/level - aml-block:Severity
送信元 ID	ルーティングのための製品タイプ。	/mml/header/source - ch:Series
デバイス ID	メッセージを生成するエンド デバイスの Unique Device Identifier（UDI）。メッセージがファブリック スイッチ専用でない場合、このフィールドは空白になります。フォーマットは *type@Sid@serial* です。各項目の意味は次のとおりです。 • *type* は、バックプレーン SEEPROM から取得した製品モデル番号です。 • *@* は区切り文字です。 • *Sid* は「C」です。それにより、シリアル ID をシャーシ シリアル番号と見なします。 • *serial* は、Sid フィールドによって識別される番号です。 例：DS-C9509@C@12345678	/mml/ header/deviceId
カスタマー ID	任意のサポート サービスによって、連絡先情報またはその他の ID に使用される、オプションのユーザ設定可能フィールド。	/mml/header/customerID - ch:CustomerId
契約 ID	任意のサポート サービスによって、連絡先情報またはその他の ID に使用される、オプションのユーザ設定可能フィールド。	/mml/header/contractId - ch: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。	/mml/header/siterId - ch:SiteId

表 4-5　対処的イベント メッセージ フォーマット （続き）

データ項目（プレーンテキストと XML）	説明（プレーン テキストと XML）	XML タグ（XML のみ）
サーバ ID	メッセージがファブリック スイッチから生成される場合、そのスイッチの Unique Device Identifier（UDI）。 フォーマットは *type@Sid@serial* です。各項目の意味は次のとおりです。 • *type* は、バックプレーン SEEPROM から取得した製品モデル番号です。 • *@* は区切り文字です。 • *Sid* は「C」です。それにより、シリアル ID をシャーシ シリアル番号と見なします。 • *serial* は、Sid フィールドによって識別される番号です。 例：DS-C9509@C@12345678	/mml/header/serverId - -blank-
メッセージの説明	エラーを説明する短い文章。	/mml/body/msgDesc - ch:MessageDescription
デバイス名	イベントが発生するノード。これは、デバイスのホスト名です。	/mml/body/sysName - ch:SystemInfo/Name
担当者名	イベント発生中のノードに関する問題の問い合わせ先の担当者名。	/mml/body/sysContact - ch:SystemInfo/Contact
連絡先電子メール	このユニットの連絡先である人物の電子メール アドレス。	/mml/body/sysContacte-mail - ch:SystemInfo/Contacte-mail
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。	/mml/body/sysContactPhoneNumber - ch:SystemInfo/ContactPhoneNumber
住所	このユニットに関連した RMA 部品の送付先住所を格納しているオプションのフィールド。	/mml/body/sysStreetAddress - ch:SystemInfo/StreetAddress
モデル名	スイッチのモデル名。製品ファミリ名の一部である固有モデルです。	/mml/body/chassis/name - rme:Chassis/Model
シリアル番号	ユニットのシャーシのシリアル番号。	/mml/body/chassis/serialNo - rme:Chassis/SerialNumber
シャーシの部品番号	シャーシの最上アセンブリ番号。	/mml/body/fru/partNo - rme:chassis/Card/PartNumber
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。	/mml/body/chassis/hwVersion - rme:Chassis/HardwareVersion
スーパーバイザ モジュール ソフトウェア バージョン	トップ レベル ソフトウェア バージョン。	/mml/body/fru/swVersion - rme:chassis/Card/SoftwareIdentity
影響のある FRU の名前	イベント メッセージを生成する、影響のある FRU の名前。	/mml/body/fru/name - rme:chassis/Card/Model
影響のある FRU のシリアル番号	影響のある FRU のシリアル番号。	/mml/body/fru/serialNo - rme:chassis/Card/SerialNumber

表 4-5　対処的イベント メッセージ フォーマット （続き）

データ項目（プレーンテキストと XML）	説明（プレーン テキストと XML）	XML タグ（XML のみ）
影響のある FRU の製品番号	影響のある FRU の製品番号。	/mml/body/fru/partNo - rme:chassis/Card/PartNumber
FRU スロット	イベント メッセージを生成している FRU のスロット番号。	/mml/body/fru/slot - rme:chassis/Card/LocationWithinContainer
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。	/mml/body/fru/hwVersion - rme:chassis/Card/SoftwareIdentity
FRU ソフトウェア バージョン	影響のある FRU 上で動作しているソフトウェア バージョン。	/mml/body/fru/swVersion - rme:chassis/Card/SoftwareIdentity
コマンド出力名	実行されたコマンドの正確な名前。	/mml/attachments/attachment/name - aml-block:Attachment/Name
添付タイプ	コマンド出力を指定します。	/mml/attachments/attachment/type - aml-block:Attachment type
MIME タイプ	通常は、テキスト、プレーン、符号化タイプのいずれか。	/mml/attachments/attachment/mime - aml-block:Attachment/Data encoding
コマンド出力テキスト	自動的に実行されたコマンドの出力（表 4-3 を参照）。	/mml/attachments/attachment/atdata - aml-block:Attachment/Data

表 4-6　コンポーネント エラー メッセージのフォーマット

データ項目（プレーンテキストと XML）	説明（プレーン テキストと XML）	XML タグ（XML のみ）
タイム スタンプ	ISO 時刻表記（*YYYY-MM-DD*T*HH:MM:SS*）による日付とタイム スタンプ。 （注）　UTC からの時間帯または夏時間（DST）オフセットは、すでに適用済みです。T は、ハードコードされた時刻の区切りです。	/mml/header/time - ch:EventTime
メッセージ名	メッセージの名前。「Inventory Update」となります。具体的なイベント名については、「イベント トリガー」（P.4-9）を参照してください。	/mml/header/name
メッセージ タイプ	「Inventory Update」となります。	/mml/header/type - ch-inv:Type
メッセージ グループ	「proactive」となります。	/mml/header/group
重大度	コンポーネント イベントの重大度はレベル 2 です（表 4-3 を参照）。	/mml/header/level - aml-block:Severity

表 4-6　コンポーネント エラー メッセージのフォーマット （続き）

データ項目（プレーンテキストと XML）	説明（プレーン テキストと XML）	XML タグ（XML のみ）
送信元 ID	シスコでのルーティングのための製品タイプ。「MDS 9000」となります。	/mml/header/source - ch-inv:Series
デバイス ID	メッセージを生成するエンド デバイスの Unique Device Identifier（UDI）。メッセージがファブリック スイッチ専用でない場合、このフィールドは空白になります。フォーマットは *type@Sid@serial* です。各項目の意味は次のとおりです。 • *type* は、バックプレーン SEEPROM から取得した製品モデル番号です。 • *@* は区切り文字です。 • *Sid* は「C」です。それにより、シリアル ID をシャーシ シリアル番号と見なします。 • *serial* は、Sid フィールドによって識別される番号です。 例：DS-C9509@C@12345678	/mml/ header /deviceId
カスタマー ID	任意のサポート サービスによって、連絡先情報またはその他の ID に使用される、オプションのユーザ設定可能フィールド。	/mml/header/customerID - ch-inv:CustomerId
契約 ID	任意のサポート サービスによって、連絡先情報またはその他の ID に使用される、オプションのユーザ設定可能フィールド。	/mml/header/contractId - ch-inv:ContractId>
サイト ID	シスコが提供するサイト ID で使用されるオプションのユーザ設定可能フィールドか、他のサポート サービスにとって意味のあるその他のデータ。	/mml/header/siterId - ch-inv:SiteId
サーバ ID	メッセージがファブリック スイッチから生成される場合、そのスイッチの Unique Device Identifier（UDI）。 フォーマットは *type@Sid@serial* です。各項目の意味は次のとおりです。 • *type* は、バックプレーン SEEPROM から取得した製品モデル番号です。 • *@* は区切り文字です。 • *Sid* は「C」です。それにより、シリアル ID をシャーシ シリアル番号と見なします。 • *serial* は、Sid フィールドによって識別される番号です。 例：DS-C9509@C@12345678	/mml/header/serverId - -blank-
メッセージの説明	エラーを説明する短い文章。	/mml/body/msgDesc - ch-inv:MessageDescription
デバイス名	イベントが発生するノード。	/mml/body/sysName - ch-inv:SystemInfo/Name
担当者名	イベント発生中のノードに関する問題の問い合わせ先の担当者名。	/mml/body/sysContact - ch-inv:SystemInfo/Contact
連絡先電子メール	このユニットの連絡先である人物の電子メール アドレス。	/mml/body/sysContacte-mail - ch-inv:SystemInfo/Contacte-mail

表 4-6　コンポーネント エラー メッセージのフォーマット （続き）

データ項目（プレーンテキストと XML）	説明（プレーン テキストと XML）	XML タグ（XML のみ）
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。	/mml/body/sysContactPhoneNumber - ch-inv:SystemInfo/ContactPhoneNumber
住所	このユニットに関連した RMA 部品の送付先住所を格納しているオプションのフィールド。	/mml/body/sysStreetAddress - ch-inv:SystemInfo/StreetAddress
モデル名	ユニットのモデル名。製品ファミリ名の一部である固有モデルです。	/mml/body/chassis/name - rme:Chassis/Model
シリアル番号	ユニットのシャーシのシリアル番号。	/mml/body/chassis/serialNo - rme:Chassis/SerialNumber
シャーシの部品番号	シャーシの最上アセンブリ番号。	/mml/body/fru/partNo - rme:chassis/Card/PartNumber
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。	/mml/body/fru/hwVersion - rme:chassis/Card/SoftwareIdentity
スーパーバイザ モジュール ソフトウェア バージョン	トップ レベル ソフトウェア バージョン。	/mml/body/fru/swVersion - rme:chassis/Card/SoftwareIdentity
FRU 名	イベント メッセージを生成する、影響のある FRU の名前。	/mml/body/fru/name - rme:chassis/Card/Model
FRU s/n	FRU のシリアル番号。	/mml/body/fru/serialNo - rme:chassis/Card/SerialNumber
FRU 製品番号	FRU の製品番号。	/mml/body/fru/partNo - rme:chassis/Card/PartNumber
FRU スロット	FRU のスロット番号。	/mml/body/fru/slot - rme:chassis/Card/LocationWithinContainer
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。	/mml/body/fru/hwVersion - rme:chassis/Card/SoftwareIdentity
FRU ソフトウェア バージョン	FRU 上で動作しているソフトウェア バージョン。	/mml/body/fru/swVersion - rme:chassis/Card/SoftwareIdentity
コマンド出力名	実行されたコマンドの正確な名前。	/mml/attachments/attachment/name - aml-block:Attachment/Name
添付タイプ	コマンド出力を指定します。	/mml/attachments/attachment/type - aml-block:Attachment type

表 4-6　コンポーネント エラー メッセージのフォーマット （続き）

データ項目（プレーンテキストと XML）	説明（プレーン テキストと XML）	XML タグ（XML のみ）
MIME タイプ	通常は、テキスト、プレーン、符号化タイプのいずれか。	/mml/attachments/attachment/mime - aml-block:Attachment/Data encoding
コマンド出力テキスト	イベント カテゴリに従って自動的に実行されるコマンドの出力（「イベント トリガー」（P.4-9）を参照）。	/mml/attachments/attachment/atdata - aml-block:Attachment/Data

表 4-7　ユーザが生成したテスト メッセージのフォーマット

データ項目（プレーンテキストと XML）	説明（プレーン テキストと XML）	XML タグ（XML のみ）
タイム スタンプ	ISO 時刻表記（*YYYY-MM-DDTHH:MM:SS*）による日付とタイム スタンプ。 **（注）** UTC からの時間帯または夏時間（DST）オフセットは、すでに適用済みです。T は、ハードコードされた時刻の区切りです。	/mml/header/time - ch:EventTime
メッセージ名	メッセージの名前。特に、テスト タイプ メッセージのテスト メッセージ。具体的なイベント名については、「イベント トリガー」（P.4-9）を参照してください。	/mml/header/name
メッセージ タイプ	「Test Call Home」となります。	/mml/header/type - ch:Type
メッセージ グループ	このフィールドは、受信側の Call Home 処理アプリケーションによって無視されますが、「proactive」または「reactive」を設定できます。	/mml/header/group
重大度	メッセージ、テスト Call Home メッセージの重大度（表 4-3 を参照）。	/mml/header/level - aml-block:Severity
送信元 ID	ルーティングのための製品タイプ。	/mml/header/source - ch:Series
デバイス ID	メッセージを生成するエンド デバイスの Unique Device Identifier（UDI）。メッセージがファブリック スイッチに固有のものでない場合、このフィールドは空です。フォーマットは *type@Sid@serial* です。各項目の意味は次のとおりです。 • *type* は、バックプレーン SEEPROM から取得した製品モデル番号です。 • @ は区切り文字です。 • *Sid* は「C」です。それにより、シリアル ID をシャーシ シリアル番号と見なします。 • *serial* は、Sid フィールドによって識別される番号です。 例：DS-C9509@C@12345678	/mml/ header /deviceId
カスタマー ID	任意のサポート サービスによって、連絡先情報またはその他の ID に使用される、オプションのユーザ設定可能フィールド。	/mml/header/customerID - ch:CustomerId

表 4-7　ユーザが生成したテスト メッセージのフォーマット （続き）

データ項目（プレーンテキストと XML）	説明（プレーン テキストと XML）	XML タグ（XML のみ）
契約 ID	任意のサポート サービスによって、連絡先情報またはその他の ID に使用される、オプションのユーザ設定可能フィールド。	/mml/header/contractId - ch: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。	/mml/header/siterId - ch:SiteId
サーバ ID	メッセージがファブリック スイッチから生成される場合、そのスイッチの Unique Device Identifier（UDI）。 フォーマットは *type@Sid@serial* です。各項目の意味は次のとおりです。 • *type* は、バックプレーン SEEPROM から取得した製品モデル番号です。 • @ は区切り文字です。 • *Sid* は「C」です。それにより、シリアル ID をシャーシ シリアル番号と見なします。 • *serial* は、Sid フィールドによって識別される番号です。 例：DS-C9509@C@12345678	/mml/header/serverId - -blank-
メッセージの説明	エラーを説明する短い文章。	/mml/body/msgDesc - ch:MessageDescription
デバイス名	イベントが発生したスイッチ。	/mml/body/sysName - ch:SystemInfo/Name
担当者名	イベント発生中のノードに関する問題の問い合わせ先の担当者名。	/mml/body/sysContact - ch:SystemInfo/Contact
連絡先電子メール	このユニットの連絡先である人物の電子メール アドレス。	/mml/body/sysContacte-mail - ch:SystemInfo/Contacte-mail
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。	/mml/body/sysContactPhoneNumber - ch:SystemInfo/ContactPhoneNumber
住所	このユニットに関連した RMA 部品の送付先住所を格納しているオプションのフィールド。	/mml/body/sysStreetAddress - ch:SystemInfo/StreetAddress
モデル名	スイッチのモデル名。製品ファミリ名の一部である固有モデルです。	/mml/body/chassis/name - rme:Chassis/Model
シリアル番号	ユニットのシャーシのシリアル番号。	/mml/body/chassis/serialNo - rme:Chassis/SerialNumber
シャーシの部品番号	シャーシの最上アセンブリ番号。例：800-xxx-xxxx	/mml/body/fru/partNo - rme:chassis/Card/PartNumber
コマンド出力テキスト	イベント カテゴリに従って自動的に実行されるコマンドの出力（表 4-3 を参照）。	/mml/attachments/attachment/atdata - aml-block:Attachment/Data

表 4-7　ユーザが生成したテスト メッセージのフォーマット （続き）

データ項目（プレーンテキストと XML）	説明（プレーン テキストと XML）	XML タグ（XML のみ）
MIME タイプ	通常は、テキスト、プレーン、符号化タイプのいずれか。	/mml/attachments/attachment/mime - aml-block:Attachment/Data encoding
添付タイプ	コマンド出力を指定します。	/mml/attachments/attachment/type - aml-block:Attachment type
コマンド出力名	実行されたコマンドの正確な名前。	/mml/attachments/attachment/name - aml-block:Attachment/Name

注意事項と制限

Call Home データベースのマージに関する注意事項

2 つの Call Home データベースをマージする場合は、次の注意事項に従ってください。

- マージされたデータベースには次の情報が格納されることに注意してください。
  - マージ プロトコルに参加する、上位スイッチと下位スイッチのすべての宛先プロファイルのスーパーセット。
  - 宛先プロファイルの E メール アドレスとアラート グループ。
  - マージ前に上位スイッチ内に存在した、スイッチからのその他の設定情報（メッセージ スロットリング、定期的コンポーネントなど）。
- 上位スイッチと下位スイッチに、同じ名前の宛先プロファイルがないことを確認してください（設定情報が異なる場合も含みます）。同じ名前が含まれている場合、マージ操作は失敗します。その場合、必要なスイッチで衝突する宛先プロファイルを変更または削除する必要があります。

概念の詳細については、「CFS マージのサポート」（P.2-6）を参照してください。

Call Home の設定に関する注意事項

Call Home を設定する場合は、次の注意事項に従ってください。

- E メール サーバと少なくとも 1 つの宛先プロファイル（事前定義またはユーザ定義）が設定されている必要があります。使用する宛先プロファイルは、受信エンティティがポケットベル、電子メール、Cisco Smart Call Home のような自動サービスのいずれであるかによって異なります。
- スイッチは、イベント（SNMP トラップ/インフォーム）を、最大 10 件の宛先に転送できます。
- Call Home をイネーブルにする前に、連絡先名（SNMP サーバの連絡先）、電話、住所の情報を設定する必要があります。この設定は、受信したメッセージの送信元を特定するために必要です。
- Cisco MDS 9000 ファミリ スイッチと Cisco Nexus 5000 シリーズ スイッチは、電子メール サーバへの IP 接続が確立されている必要があります。
- Cisco Smart Call Home を使用する場合、設定しようとしているデバイスが、アクティブ サービス契約の対象になっている必要があります。

デフォルト設定

表 4-8 に、Call Home のデフォルト設定を示します。

表 4-8　Call Home のデフォルト設定

パラメータ	デフォルト
フル テキスト形式で送信されるメッセージの宛先メッセージ サイズ。	500,000
XML 形式で送信されるメッセージの宛先メッセージ サイズ。	500,000
ショート テキスト形式で送信されるメッセージの宛先メッセージ サイズ。	4000
ポートが指定されていない場合にサーバに到達するための、SMTP サーバの DNS または IP アドレス	25
プロファイルとのアラート グループの関連付け	All
形式タイプ	XML
Call Home メッセージ レベル。	0（ゼロ）
HTTP プロキシ サーバの使用。	ディセーブルであり、プロキシ サーバは設定されていません。
HTTP プロキシ サーバのフル テキストの宛先のメッセージ サイズ。	1 MB
HTTP プロキシ サーバの XML のメッセージ サイズ。	1 MB

Call Home の設定

Call Home プロセスの設定方法は、この機能の利用目的によって変わります。

ここで説明する内容は、次のとおりです。

- 「Cisco Device Manager を使用した遅延トラップのイネーブル化」（P.4-32）
- 「イベント フィルタ通知の表示」（P.4-32）

Call Home を設定するためのタスク フロー

次の手順を実行して、Call Home を設定します。

ステップ 1　連絡先情報を設定します。

ステップ 2　Call Home をイネーブルまたはディセーブルにします。

ステップ 3　宛先プロファイルを設定します。

ステップ 4　ネットワークの必要性に応じて、1 つ以上のアラート グループを各プロファイルに関連付けます。必要に応じてアラート グループをカスタマイズします。

ステップ 5　E メール オプションを設定します。

ステップ 6　Call Home メッセージをテストします。

連絡先情報の設定

スイッチ プライオリティは、ファブリック内のスイッチごとにユーザが設定します。このプライオリティは、運用要員または TAC サポート要員によって、最初に対処すべき Call Home メッセージを決定するために使用されます。各スイッチから送信される重大度が同じ Call Home アラートに優先順位を設定できます。

前提条件

- 各スイッチには、E メール、電話、住所の情報が含まれている必要があります。オプションで、コントラクト ID、カスタマー ID、スイッチ プライオリティ情報を含めることができます。

手順の詳細

連絡先情報を割り当てるには、次の手順を実行します。

ステップ 1　[Events] を展開し、[Physical Attributes] ペインから [Call Home] を選択します。

[Information] ペインに [Call Home] タブが表示されます。

ステップ 2　Device Manager で、[Admin] > [Events] > [Call Home] の順にクリックします。

ステップ 3　[General] タブをクリックし、連絡先情報を割り当てて Call Home 機能をイネーブルにします。Call Home はデフォルトではイネーブルになっていません。Call Home 通知の送信元を識別する E メール アドレスを入力する必要があります。

ステップ 4　[Destination(s)] タブをクリックし、Call Home 通知の宛先 E メール アドレスを設定します。Call Home 通知を受信する E メール アドレスを 1 つ以上設定できます。

（注）　スイッチは、イベント（SNMP トラップ/インフォーム）を、最大 10 件の宛先に転送できます。

a. [Create] タブをクリックして、新しい宛先を作成します。[create destination] ウィンドウが表示されます。

b. 宛先のプロファイル名、ID、およびタイプを入力します。[Type] フィールドでは、[email] または [http] を選択できます。

[email] を選択した場合、[EmailAddress] フィールドに E メール アドレスを入力します。[HttpUrl] フィールドはディセーブルになります。

[http] を選択した場合、[HttpUrl] フィールドに HTTP URL を入力します。[EmailAddress] フィールドはディセーブルになります。

c. [Create] をクリックして、宛先プロファイルの作成を完了します。

ステップ 5　[e-mail Setup] タブをクリックし、SMTP サーバを設定します。スイッチがアクセスできるメッセージ サーバを設定します。このメッセージ サーバは、Call Home 通知を宛先に転送します。

ステップ 6　DCNM-SAN で、[Apply Changes] アイコンをクリックします。Device Manager で、[Apply] をクリックします。

Call Home 機能のイネーブル化

連絡先情報を設定したら、Call Home 機能をイネーブルにする必要があります。

手順の詳細

Call Home 機能をイネーブルにするには、次の手順を実行します。

ステップ 1　[Fabric] ペインでスイッチを選択します。

ステップ 2　[Physical Attributes] ペインで [Events] を展開し、[Call Home] を選択します。

[Information] ペインに、Call Home 情報が表示されます。

ステップ 3　[Control] タブをクリックします。

ステップ 4　[information] ペインでスイッチを選択します。

ステップ 5　[Duplicate Message Throttle] チェックボックスをオンにします。

ステップ 6　[Apply Changes] アイコンをクリックします。

宛先プロファイルの設定

宛先プロファイルには、アラート通知に必要な送信情報が含まれています。宛先プロファイルは、一般にネットワーク管理者によって設定されます。

宛先プロファイルには、次の属性を設定できます。

- プロファイル名：各ユーザ定義宛先プロファイルを一意に識別する文字列で、最大 32 文字の英数字で指定します。ユーザ定義の宛先プロファイルのフォーマット オプションは、フル テキスト、ショート テキスト、XML（デフォルト）のいずれかです。
- 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）。

（注）　Cisco Smart Call Home サービスを使用する場合、XML 宛先プロファイルが必要です（http://www.cisco.com/en/US/partner/products/hw/ps4159/ps4358/products_configuration_example09186a0080108e72.shtml を参照）。

前提条件

- 少なくとも 1 つの宛先プロファイルが必要です。1 つまたは複数のタイプの複数の宛先プロファイルを設定できます。事前に定義された宛先プロファイルのいずれかを使用するか、目的のプロファイルを定義できます。新しいプロファイルを定義する場合、プロファイル名を割り当てる必要があります。

手順の詳細

定義済みの宛先プロファイルのメッセージング オプションを設定するには、次の手順を実行します。

ステップ 1　[Physical Attributes] ペインで [Events] を展開し、[Call Home] を選択します。

（注）　[Destination] タブは、[Profiles] タブをクリックするまでディセーブルになります。[Destination] タブに内容を設定するには、プロファイルをロードしておく必要があります。

ステップ 2　[Information] ペインで [Profiles] タブをクリックします。

複数のスイッチに対する Call Home プロファイルが表示されます。

ステップ 3　プロファイル名、メッセージ フォーマット、メッセージ サイズ、重大度を設定します。

ステップ 4　[Alert Groups] 列をクリックし、アラート グループを選択または削除します。

ステップ 5　[Apply Changes] アイコンをクリックし、選択したスイッチ上でこのプロファイルを作成します。

新しい宛先プロファイル（および関連するパラメータ）を設定するには、次の手順を実行します。

ステップ 1　[Physical Attributes] ペインで [Events] を展開し、[Call Home] を選択します。

（注）　[Destination] タブは、[Profiles] タブをクリックするまでディセーブルになります。[Destination] タブに内容を設定するには、プロファイルをロードしておく必要があります。

ステップ 2　[Information] ペインで [Profiles] タブをクリックします。

複数のスイッチに対する Call Home プロファイルが表示されます。

ステップ 3　[Create Row] アイコンをクリックして新しいプロファイルを追加します。

ステップ 4　プロファイル名、メッセージ フォーマット、サイズ、重大度を設定します。

ステップ 5　アラート グループをクリックし、このプロファイルで送信する各グループを選択します。

ステップ 6　転送方式をクリックします。[email]、[http]、[emailandhttp] のいずれかを選択できます。

ステップ 7　[Create] をクリックして、選択したスイッチ上でこのプロファイルを作成します。

アラート グループの関連付け

Call Home アラートはタイプごとに別のアラート グループにグループ化されます。ネットワークの必要性に応じて、1 つ以上のアラート グループを各プロファイルに関連付けることができます。

アラート グループ機能を使用することで、宛先プロファイル（定義済みまたはユーザ定義）が受信する Call Home アラートのセットを選択できます。複数のアラート グループを 1 つの宛先プロファイルに関連付けることができます。

制約事項

- Call Home アラートが、宛先プロファイル内の E メールの宛先に送信されるのは、その Call Home アラートが、その宛先プロファイルに関連付けられているいずれかのアラート グループに属する場合だけです。

手順の詳細

アラート グループを宛先プロファイルに関連付けるには、次の手順を実行します。

ステップ 1　[Physical Attributes] ペインで [Events] を展開し、[Call Home] を選択します。

ステップ 2　[Information] ペインで [Profiles] タブをクリックします。

複数のスイッチに対する Call Home プロファイルが表示されます。

ステップ 3　関連付けるプロファイルの行の [Alert Groups] カラムをクリックします。

[alert groups] ドロップダウン メニューが表示されます。

ステップ 4　関連付けるアラート グループをクリックして選択します。

ステップ 5　そのアラート グループの横にチェックが表示されます。選択を解除してチェックを外すには、再度クリックします。

ステップ 6　[Apply Changes] アイコンをクリックします。

アラート グループ メッセージのカスタマイズ

手順の詳細

Call Home アラート グループ メッセージをカスタマイズするには、次の手順を実行します。

ステップ 1　[Physical Attributes] ペインで [Events] を展開し、[Call Home] を選択します。

ステップ 2　[Information] ペインの [User Defined Command] タブをクリックします。

ユーザ定義コマンドの情報が表示されます。

ステップ 3　[Create Row] アイコンをクリックします。

ステップ 4　受信するアラートの送信元となるスイッチの前にあるチェックボックスをオンにします。

ステップ 5　[Alert Group Type] ドロップダウン リストからアラート グループ タイプを選択します。

ステップ 6　CLI コマンドの ID（1 ～ 5）を選択します。ID は、メッセージを追跡するために使用します。

ステップ 7　CLI **show** コマンドを [CLI Command] フィールドに入力します。

ステップ 8　[Create] をクリックします。

ステップ 9　プロファイルに関連付ける各コマンドに対し、ステップ 3 ～ 7 を繰り返します。

ステップ 10　[Close] をクリックして、ダイアログボックスを閉じます。

Call Home メッセージ レベルの設定

制約事項

- 緊急度の範囲は 0（最も緊急度が低い）から 9（最も緊急度が高い）であり、デフォルトは 0 です（すべてのメッセージが送信されます）。

手順の詳細

Call Home の各宛先プロファイルに対してメッセージ レベルを設定するには、次の手順を実行します。

ステップ 1　[Physical Attributes] ペインで [Events] を展開し、[Call Home] を選択します。
[Information] ペインに、Call Home 情報が表示されます。
Device Manager で、[Admin] > [Events] > [Call Home] の順に選択します。

ステップ 2　[Information] ペインで [Profiles] タブをクリックします。
Call Home プロファイルが表示されます。

ステップ 3　[MsgLevel] 列のドロップダウン メニューを使用して、各スイッチのメッセージ レベルを設定します。

ステップ 4　[Apply Changes] アイコンをクリックして変更を保存します。

Syslog ベースのアラートの設定

手順の詳細

syslog-group-port アラート グループを設定するには、次の手順を実行します。

ステップ 1　[Fabric] ペインでスイッチを選択します。

ステップ 2　[Physical Attributes] ペインで [Events] を展開し、[Call Home] を選択します。
[Information] ペインに、Call Home 情報が表示されます。

ステップ 3　[Profiles] タブをクリックします。
Call Home プロファイルが表示されます。

ステップ 4　[Create Row] アイコンをクリックします。
[Create Call Home Profile] ダイアログボックスが表示されます。

ステップ 5　アラートを送信するスイッチを選択します。

ステップ 6　プロファイル名を [Name] フィールドに入力します。

ステップ 7　メッセージ フォーマット、メッセージ サイズ、メッセージの重大度を選択します。

ステップ 8　[AlertGroups] セクションの [syslogGroupPort] チェックボックスをオンにします。

ステップ 9　[Create] をクリックして、syslog ベースのアラートのプロファイルを作成します。

ステップ 10　ダイアログボックスを閉じます。

RMON アラートの設定

手順の詳細

RMON アラート グループを設定するには、次の手順を実行します。

ステップ 1　[Fabric] ペインでスイッチを選択します。

ステップ 2　[Physical Attributes] ペインで [Events] を展開し、[Call Home] を選択します。

[Information] ペインに、Call Home 情報が表示されます。

ステップ 3　[Profiles] タブをクリックします。

Call Home プロファイルが表示されます。

ステップ 4　[Create Row] アイコンを選択します。

[Create Call Home Profile] ダイアログボックスが表示されます。

ステップ 5　アラートを送信するスイッチを選択します。

ステップ 6　プロファイル名を入力します。

ステップ 7　メッセージ フォーマット、メッセージ サイズ、メッセージの重大度を選択します。

ステップ 8　[AlertGroups] セクションの [ROMN] チェックボックスをオンにします。

ステップ 9　[Create] をクリックして、RMON ベースのアラートのプロファイルを作成します。

ステップ 10　ダイアログボックスを閉じます。

一般的な電子メール オプションの設定

from、reply-to、return-receipt の E メール アドレスを設定できます。ほとんどの E メール アドレス設定はオプションですが、Call Home 機能を使用するには、SMTP サーバのアドレスを設定する必要があります。

手順の詳細

一般的な電子メール オプションを設定するには、次の手順を実行します。

ステップ 1　[Fabric] ペインでスイッチを選択します。

ステップ 2　[Physical Attributes] ペインで [Events] を展開し、[Call Home] を選択します。

[Information] ペインに、Call Home 情報が表示されます。

ステップ 3　[e-mail Setup] タブをクリックします。

ステップ 4　[Information] ペインでスイッチを選択します。

ステップ 5　一般的な E メール情報を入力します。

ステップ 6　SMTP サーバの IP アドレス タイプ、IP アドレスまたは名前、ポートを入力します。

ステップ 7　[Apply Changes] アイコンをクリックして、E メール オプションを更新します。

HTTP プロキシ サーバの設定

手順の詳細

Call Home HTTP プロキシ サーバを設定するには、次の手順を実行します。

ステップ 1　[Fabric] ペインでスイッチを選択します。

ステップ 2　[Physical Attributes] ペインで [Events] を展開し、[Call Home]、[HTTP Proxy Server] を選択します。

[Information] ペインに Call Home HTTP プロキシ サーバの情報が表示されます。

ステップ 3　[Address Type] タブをクリックします。

アドレス タイプのオプションが表示されます。

ステップ 4　[Address] タブをクリックし、HTTP プロキシ サーバのアドレスを入力します。

ステップ 5　[Port] タブをクリックし、整数値を入力して、HTTP プロキシ サーバのポートを指定します。

ステップ 6　[Enable] チェックボックスをオンにして、Call Home 用に設定された HTTP プロキシをイネーブルにします。

ステップ 7　（オプション）空の値を [Address] タブに設定して、MDS スイッチから HTTP プロキシ サーバを削除します。

ステップ 8　アドレス タイプを選択します。[ipv4]、[ipv6]、または [DNS] を選択できます。

（注）　アドレスが空の場合、プロキシ サーバは設定されません。

ステップ 9　[Apply] をクリックして、HTTP プロキシ サーバのオプションを更新します。

Call Home ウィザードの設定

Call Home ウィザードを設定するためのタスク フロー

次の手順を実行して、Call Home ウィザードを設定します。

ステップ 1　連絡先情報を設定します。

ステップ 2　SMTP 情報を設定します。

ステップ 3　電子メールの送信元と宛先の情報を設定します。

ステップ 4　CFS を使用して、設定データを読み込みます。

ステップ 5　ステータスを表示します。

Call Home ウィザードの起動

はじめる前に

- DCNM-SAN 設定テーブルからスイッチ上のグローバル CFS をイネーブルにします。
- スイッチ上の CFS ロックをクリアします。
- スイッチ上の CFS のマージ ステータスを確認します。マージの失敗が検出されると、ウィザードは、実行中にバックエンド プロセスでマージの失敗を解決します。

手順の詳細

Call Home ウィザードを設定するには、次の手順を実行します。

ステップ 1　論理ドメイン ツリー内のファブリックを選択します。

ステップ 2　[Tools]、[Events]、[Call Home] を選択します。

[master switch] ペインが表示されます。

ステップ 3　（オプション）Call Home の [Control] タブで [CallHome Wizard] アイコンをクリックして Call Home ウィザードを起動することもできます。

ステップ 4　[Master Switch] を選択し、[Next] をクリックします。

[contact information] ペインが表示されます。

ステップ 5　[Contact]、[Phone Number]、[Email Address]、および [Street Address] の情報を入力します。

（注）　[Next] をクリックする前に、4 つのパラメータをすべて指定する必要があります。

ステップ 6　[Next] をクリックします。

[Email Setup] ペインが表示されます。

ステップ 7　[Email SMTP Servers] タブで、[Primary SNTP Server] アドレスを入力します。

マスター スイッチがバージョン 5.0 以上ならば、SMTP サーバを 2 台まで指定できます。マスター スイッチのバージョンが 5.0 未満の場合は、セカンダリ SMTP サーバを指定することはできません。

ウィザードは、SMTP サーバ テーブルに新しい行を作成します。

ステップ 8　[Destination] タブで、[Add] をクリックして Call Home 宛先を入力します。

Call Home 宛先は 3 つまで入力できます。

ステップ 9　（オプション）[Remove] をクリックして Call Home 宛先のエントリを削除します。

ステップ 10　ドロップダウン リストから、[Protocol] と [Profile] を選択します。

[Profile] ドロップダウンには、[xml]、[short_txt]、および [full_txt] の 3 つのデフォルト プロファイルがリスト表示されます。

ステップ 11　[Finish] をクリックしてウィザードを設定します。

[Status Dialog] ウィンドウが表示されます。

すべての重要な設定手順およびエラーが [Status Dialog] ウィンドウに表示されます。

ステップ 12　[Run Test] をクリックして Call Home テストを実行します。

ステップ 13　[Yes] をクリックして選択ファブリック内のすべてのスイッチ上でコマンドをテストするか、[No] をクリックしてウィンドウを閉じます。

定期的なコンポーネント通知のイネーブル化

間隔の値を設定せずにこの機能をイネーブルにすると、Call Home メッセージは 7 日間おきに送信されます。この値の範囲は、1 ～ 30 日間です。デフォルトでは、Cisco MDS 9000 ファミリと Cisco Nexus 5000 シリーズのすべてのスイッチにおいてこの機能はディセーブルになっています。

手順の詳細

Cisco MDS 9000 ファミリ スイッチまたは Cisco Nexus 5000 シリーズ スイッチで定期的なコンポーネント通知をイネーブルにするには、次の手順を実行します。

ステップ 1　[Fabric] ペインでスイッチを選択します。

ステップ 2　[Physical Attributes] ペインで [Events] を展開し、[Call Home] を選択します。

[Information] ペインに、Call Home 情報が表示されます。

ステップ 3　[Periodic Inventory] タブをクリックします。

Call Home 定期的なコンポーネント情報が表示されます。

ステップ 4　[Information] ペインでスイッチを選択します。

ステップ 5　[Enable] チェックボックスをオンにします。

ステップ 6　コンポーネントをチェックする間隔を日単位で入力します。

ステップ 7　[Apply Changes] アイコンをクリックします。

重複するメッセージのスロットリングの設定

同じイベントに対して受信する Call Home メッセージの数を制限するために、スロットリング メカニズムを設定できます。短時間のうちにスイッチから何度も同じメッセージが送信される場合、重複する多数のメッセージであふれることがあります。

制約事項

- デフォルトでは、Cisco MDS 9000 ファミリと Cisco Nexus 5000 シリーズのすべてのスイッチにおいてこの機能はイネーブルになっています。この機能をイネーブルにすると、送信されるメッセージの数が、2 時間あたりの最大値である 30 メッセージを超えると、そのアラート タイプの以降のメッセージは、その間廃棄されます。時間間隔やメッセージ カウンタの上限は変更できません。

- 最初に該当するメッセージが送信されてから 2 時間が経過し、新しいメッセージを送信する必要がある場合、新しいメッセージが送信され、その時刻に時間間隔がリセットされ、カウントが 1 にリセットされます。

手順の詳細

Cisco MDS 9000 ファミリ スイッチまたは Cisco Nexus 5000 シリーズ スイッチでメッセージ スロットリングをイネーブルにするには、次の手順を実行します。

ステップ 1　[Fabric] ペインでスイッチを選択します。

ステップ 2　[Physical Attributes] ペインで [Events] を展開し、[Call Home] を選択します。

[Information] ペインに、Call Home 情報が表示されます。

ステップ 3　[Control] タブをクリックします。

ステップ 4　[Information] ペインでスイッチを選択します。

ステップ 5　[Duplicate Msg Throttle] チェックボックスをオンにします。

ステップ 6　[Apply Changes] アイコンをクリックします。

Call Home ファブリック配信のイネーブル化

手順の詳細

Call Home ファブリック配信をイネーブルにするには、次の手順を実行します。

ステップ 1　[Fabric] ペインでスイッチを選択します。

ステップ 2　[Physical Attributes] ペインで [Events] を展開し、[Call Home] を選択します。

[Information] ペインに、Call Home 情報が表示されます。

ステップ 3　[CFS] タブをクリックします。

Call Home の CFS 情報が表示されます。

ステップ 4　[Information] ペインでスイッチを選択します。

ステップ 5　そのスイッチの行の [Admin] カラムのドロップダウン リストから、[Enable] を選択します。

ステップ 6　[Apply Changes] アイコンをクリックして、変更を確定します。

Call Home 通信テスト

テスト メッセージを設定された宛先に送信するか、テスト コンポーネント メッセージを設定された宛先に送信することで、Call Home の通信をテストできます。

手順の詳細

Call Home の機能をテストし、メッセージ生成をシミュレートするには、次の手順を実行します。

ステップ 1　[Fabric] ペインでスイッチを選択します。

ステップ 2　[Physical Attributes] ペインで [Events] を展開し、[Call Home] を選択します。

[Information] ペインに、Call Home 情報が表示されます。

ステップ 3　[Test] タブをクリックします。

スイッチに対して設定されているテストと、最後のテストのステータスが表示されます。

ステップ 4　[Information] ペインでスイッチを選択します。

ステップ 5　そのスイッチの行の [TestAction] ドロップダウン リストから、[test] または [testWithInventory] を選択します。

ステップ 6　[Apply Changes] アイコンをクリックして、テストを実行します。

表 4-9 に、EMC Call Home 用のトラップをすべて示します。

表 4-9　EMC Call Home のトラップ

SNMP トラップ	EMC Call Home の送信条件
connUnitStatusChange	operStatus == failed(5)
cefcModuleStatusChange	operStatus != {ok(2), boot(5), selfTest(6), poweredUp(16), syncInProgress(21)}
cefcPowerStatusChange	operStatus = {offDenied(4), offEnvPower(5),offEnvTemp(6),offEnvFan(7),failed(8)}
cefcFRURemoved	すべて
cefcFanTrayStatusChange	すべて
cieDelayedLinkUpDown	operStatusReason != {linkFailure, adminDown, portGracefulShutdown}
cefcFRUInserted	すべて
entSensorThresholdNotification	値 >= しきい値

遅延トラップの設定

server.callhome.delayedtrap.enable プロパティが、server.properties コンフィギュレーション ファイルのセクション 9 Call Home に追加されています。プロパティ ファイルでは、DCNM-SAN サーバが、EMC E-mail Home メッセージに対し、通常の linkDown トラップではなく遅延トラップを使用するように設定できます。

前提条件

この機能をイネーブルにするには、遅延トラップをスイッチ レベルで有効にし、server.properties コンフィギュレーション ファイルで server.callhome.delayedtrap.enable プロパティを true に設定する必要があります。デフォルトでは、server.callhome.delayedtrap.enable オプションはディセーブルになっており、通常の linkDown トラップが使用されます。

手順の詳細

NX-OS Release 4.1(3) 以降が動作するスイッチ上で遅延トラップをイネーブルにするには、次の手順を実行します。

ステップ 1　[Physical Attributes] ペインで [Events] を展開し、[SNMP Traps] を選択します。

DCNM-SAN のマップ レイアウトの上にあるテーブルで、[Delayed Traps] タブをクリックします。

ステップ 2　遅延トラップをイネーブルにするスイッチの [Enable] チェックボックスをオンにします。

ステップ 3　[Delay] カラムに**タイマー**値を入力します。

ステップ 4　[Apply] をクリックして変更を保存します。

（注）　値を入力しないと、デフォルト値の 4 分が使用されます。

遅延トラップをディセーブルにするには、次の手順を実行します。

ステップ 1　[Enable] チェックボックスをオフにします。

ステップ 2　[Apply] をクリックします。

Cisco Device Manager を使用した遅延トラップのイネーブル化

手順の詳細

遅延トラップ機能をイネーブルにするには、次の手順を実行します。

ステップ 1　Device Manager で、[Admin] > [Events] > [Filters] > [Delayed Traps] の順に選択します。

[Information] ペインにイベント フィルタの情報が表示されます。

ステップ 2　[Delayed Traps] タブをクリックします。

ステップ 3　[Enable] チェックボックスをオンにし、遅延トラップをイネーブルにします。

遅延時間は、この機能をイネーブルにしないと設定できません。

ステップ 4　遅延トラップをディセーブルにするには、[Enable] チェックボックスをオフにして [Apply] をクリックします。

イベント フィルタ通知の表示

手順の詳細

通知の説明を表示するには、次の手順を実行します。

ステップ 1　Device Manager で、[Admin] > [Events] > [Filters] の順に選択します。

[Information] ペインにイベント フィルタの情報が表示されます。

[Event Filters] 画面に、通知に関する説明が表示されます。

Call Home のモニタリング

ここで説明する内容は、次のとおりです。

フルテキスト形式の Syslog アラート通知の例

```
source:MDS9000
Switch Priority:7
Device Id:DS-C9506@C@FG@07120011
Customer Id:basu
Contract Id:123
Site Id:San Jose
Server Id:DS-C9506@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:Basavaraj B
Contact e-mail:admin@yourcompany.com
Contact Phone:+91-80-310-1718
Street Address:#71 , Miller's Road
Event Description:2004 Oct  8 11:10:44 10.76.100.177 %PORT-5-IF_TRUNK_UP: %$VSAN 1%$
Interface fc2/5, vsan 1 is up

syslog_facility:PORT
start chassis information:
Affected Chassis:DS-C9506
Affected Chassis Serial Number:FG@07120011
Affected Chassis Hardware Version:0.104
Affected Chassis Software Version:3.1(1)
Affected Chassis Part No:73-8607-01
end chassis information:
```

XML 形式の Syslog アラート通知の例

```
<?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.cisco.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.cisco.com/neddce/services/DDCEService</aml-session:To>
<aml-session:Path>
<aml-session:Via>http://www.cisco.com/appliance/uri</aml-session:Via>
</aml-session:Path>
<aml-session:From>http://www.cisco.com/appliance/uri</aml-session:From>
```

```
<aml-session:MessageId>1004:FOX090306QT:3E55A81A</aml-session:MessageId>
</aml-session:Session>
</soap-env:Header>
<soap-env:Body>
<aml-block:Block xmlns:aml-block="http://www.cisco.com/2004/01/aml-block">
<aml-block:Header>
<aml-block:Type>http://www.cisco.com/2005/05/callhome/syslog</aml-block:Type>
<aml-block:CreationDate>2003-02-21 04:16:18 GMT+00:00</aml-block:CreationDate>
<aml-block:Builder>
<aml-block:Name>MDS</aml-block:Name>
<aml-block:Version>4.1</aml-block:Version>
</aml-block:Builder>
<aml-block:BlockGroup>
<aml-block:GroupId>1005:FOX090306QT:3E55A81A</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>6</aml-block:Severity>
</aml-block:Header>
<aml-block:Content>
<ch:CallHome xmlns:ch="http://www.cisco.com/2005/05/callhome" version="1.0">
<ch:EventTime>2003-02-21 04:16:18 GMT+00:00</ch:EventTime>
<ch:MessageDescription>LICENSE_VIOLATION 2003 Feb 21 04:16:18 switch %$
%DAEMON-3-SYSTEM_MSG: &lt;&lt;%LICMGR-3-LOG_LICAPP_NO_LIC&gt;&gt; License file is missing
for feature SAN_EXTN_OVER_IP</ch:MessageDescription>
<ch:Event>
<ch:Type>syslog</ch:Type>
<ch:SubType>LICENSE_VIOLATION</ch:SubType>
<ch:Brand>Cisco</ch:Brand>
<ch:Series>MDS9000</ch:Series>
</ch:Event>
<ch:CustomerData>
<ch:UserData>
<ch:e-mail>esajjana@cisco.com</ch:e-mail>
</ch:UserData>
<ch:ContractData>
<ch:CustomerId>eeranna</ch:CustomerId>
<ch:SiteId>Bangalore</ch:SiteId>
<ch:ContractId>123</ch:ContractId>
<ch:DeviceId>DS-C9216I-K9@C@FOX090306QT</ch:DeviceId>
</ch:ContractData>
<ch:SystemInfo>
<ch:Name>switch</ch:Name>
<ch:Contact>Eeranna</ch:Contact>
<ch:Contacte-mail>esajjana@cisco.com</ch:Contacte-mail>
<ch:ContactPhoneNumber>+91-80-310-1718</ch:ContactPhoneNumber>
<ch:StreetAddress>#71, Miller&apos;s Road</ch:StreetAddress> </ch:SystemInfo>
</ch:CustomerData> <ch:Device> <rme:Chassis xmlns:rme="http://www.cisco.com/rme/4.0">
<rme:Model>DS-C9216I-K9</rme:Model>
<rme:HardwareVersion>1.0</rme:HardwareVersion>
<rme:SerialNumber>FOX090306QT</rme:SerialNumber>
</rme:Chassis>
</ch:Device>
</ch:CallHome>
</aml-block:Content>
<aml-block:Attachments>
<aml-block:Attachment type="inline">
<aml-block:Name>show logging logfile | tail -n 200</aml-block:Name> <aml-block:Data
encoding="plain">
<![CDATA[syslog_show:: command: 1055 param_count: 0
2003 Feb 21 04:11:48  %KERN-2-SYSTEM_MSG: Starting kernel... - kernel
2003 Feb 21 04:11:48  %KERN-3-SYSTEM_MSG: CMOS: Module initialized - kernel
```

```
2003 Feb 21 04:11:48  %KERN-2-SYSTEM_MSG: CARD TYPE: KING BB Index = 2344 - kernel
2003 Feb 21 04:12:04  %MODULE-5-ACTIVE_SUP_OK: Supervisor 1 is active (serial:
JAB100700MC)
2003 Feb 21 04:12:04  %PLATFORM-5-MOD_STATUS: Module 1 current-status is
MOD_STATUS_ONLINE/OK
2003 Feb 21 04:12:06  %IMAGE_DNLD-SLOT1-5-ADDON_IMG_DNLD_COMPLETE:  Addon module image
download process completed. Addon Image download completed, installing image please wait..
2003 Feb 21 04:12:07  %IMAGE_DNLD-SLOT1-5-ADDON_IMG_DNLD_SUCCESSFUL:  Addon module image
download and install process successful. Addon image installed.
2003 Feb 21 04:12:08  %KERN-3-SYSTEM_MSG: klm_af_xipc: Unknown parameter `start&apos; -
kernel
2003 Feb 21 04:12:08  %KERN-3-SYSTEM_MSG: klm_ips_portcfg: Unknown parameter `start&apos;
- kernel
2003 Feb 21 04:12:08  %KERN-3-SYSTEM_MSG: klm_flamingo: Unknown parameter `start&apos; -
kernel
2003 Feb 21 04:12:10  %PORT-5-IF_UP: Interface mgmt0 is up
2003 Feb 21 04:12:21 switch %LICMGR-3-LOG_LIC_FILE_MISSING: License file(s) missing for
feature ENTERPRISE_PKG.
2003 Feb 21 04:12:21 switch %LICMGR-3-LOG_LIC_FILE_MISSING: License file(s) missing for
feature SAN_EXTN_OVER_IP.
2003 Feb 21 04:12:21 switch %LICMGR-3-LOG_LIC_FILE_MISSING: License file(s) missing for
feature ENTERPRISE_PKG.
2003 Feb 21 04:12:21 switch %LICMGR-3-LOG_LIC_FILE_MISSING: License file(s) missing for
feature SAN_EXTN_OVER_IP.
2003 Feb 21 04:12:23 switch %PLATFORM-5-MOD_STATUS: Module 1 current-status is
MOD_STATUS_ONLINE/OK
2003 Feb 21 04:12:23 switch %MODULE-5-MOD_OK: Module 1 is online (serial: JAB100700MC)
2003 Feb 21 04:12:25 switch %PORT-5-IF_DOWN_ADMIN_DOWN: %$VSAN 1%$ Interface fc1/1 is down
(Administratively down)
2003 Feb 21 04:12:25 switch %PORT-5-IF_DOWN_ADMIN_DOWN: %$VSAN 1%$ Interface fc1/2 is down
(Administratively down)
2003 Feb 21 04:12:25 switch %PORT-5-IF_DOWN_ADMIN_DOWN: %$VSAN 1%$ Interface fc1/3 is down
(Administratively down)
2003 Feb 21 04:12:25 switch %PORT-5-IF_DOWN_ADMIN_DOWN: %$VSAN 1%$ Interface fc1/4 is down
(Administratively down)
2003 Feb 21 04:12:26 switch %PLATFORM-5-PS_STATUS: PowerSupply 1 current-status is PS_FAIL
2003 Feb 21 04:12:26 switch %PLATFORM-2-PS_FAIL: Power supply 1 failed or shut down
(Serial number QCS1007109F)
2003 Feb 21 04:12:26 switch %PLATFORM-5-PS_FOUND: Power supply 2 found (Serial number
QCS1007109R)
2003 Feb 21 04:12:26 switch %PLATFORM-2-PS_OK: Power supply 2 ok (Serial number
QCS1007109R)
2003 Feb 21 04:12:26 switch %PLATFORM-5-PS_STATUS: PowerSupply 2 current-status is PS_OK
2003 Feb 21 04:12:26 switch %PLATFORM-2-PS_FANOK: Fan in Power supply 2 ok
2003 Feb 21 04:12:26 switch %PLATFORM-5-FAN_DETECT: Fan module 1 (Serial number
NWG0901031X) ChassisFan1 detected
2003 Feb 21 04:12:26 switch %PLATFORM-2-FAN_OK: Fan module ok
2003 Feb 21 04:12:26 switch %PLATFORM-2-CHASSIS_CLKMODOK: Chassis clock module A ok
2003 Feb 21 04:12:26 switch %PLATFORM-2-CHASSIS_CLKSRC: Current chassis clock source is
clock-A
2003 Feb 21 04:12:26 switch %PORT-5-IF_DOWN_ADMIN_DOWN: %$VSAN 1%$ Interface fc1/5 is down
(Administratively down)
2003 Feb 21 04:12:26 switch %PORT-5-IF_DOWN_ADMIN_DOWN: %$VSAN 1%$ Interface fc1/6 is down
(Administratively down)
2003 Feb 21 04:12:26 switch %PORT-5-IF_DOWN_ADMIN_DOWN: %$VSAN 1%$ Interface fc1/7 is down
(Administratively down)
2003 Feb 21 04:12:26 switch %PORT-5-IF_DOWN_ADMIN_DOWN: %$VSAN 1%$ Interface fc1/8 is down
(Administratively down)
2003 Feb 21 04:12:26 switch %PORT-5-IF_DOWN_ADMIN_DOWN: %$VSAN 1%$ Interface fc1/9 is down
(Administratively down)
2003 Feb 21 04:12:26 switch %PORT-5-IF_DOWN_ADMIN_DOWN: %$VSAN 1%$ Interface fc1/10 is
down (Administratively down)
2003 Feb 21 04:12:27 switch %PORT-5-IF_DOWN_ADMIN_DOWN: %$VSAN 1%$ Interface fc1/11 is
down (Administratively down)
```

```
2003 Feb 21 04:12:27 switch %PORT-5-IF_DOWN_ADMIN_DOWN: %$VSAN 1%$ Interface fc1/12 is
down (Administratively down)
2003 Feb 21 04:12:27 switch %PORT-5-IF_DOWN_ADMIN_DOWN: %$VSAN 1%$ Interface fc1/13 is
down (Administratively down)
2003 Feb 21 04:12:27 switch %PORT-5-IF_DOWN_ADMIN_DOWN: %$VSAN 1%$ Interface fc1/14 is
down (Administratively down)
2003 Feb 21 04:12:30 switch %PLATFORM-2-MOD_DETECT: Module 2 detected (Serial number
JAB0923016X) Module-Type IP Storage Services Module Model DS-X9304-SMIP
2003 Feb 21 04:12:30 switch %MODULE-2-MOD_UNKNOWN: Module type [25] in slot 2 is not
supported
2003 Feb 21 04:12:45 switch %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configured from vty by root on
console0
2003 Feb 21 04:14:06 switch %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configured from vty by admin on
console0
2003 Feb 21 04:15:12 switch %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configured from vty by admin on
console0
2003 Feb 21 04:15:52 switch %SYSMGR-3-BASIC_TRACE: core_copy: PID 1643 with message Core
not generated by system for licmgr(0). WCOREDUMP(9) returned zero .
2003 Feb 21 04:15:52 switch %SYSMGR-2-SERVICE_CRASHED: Service \"licmgr\" (PID 2272)
hasn&amp;apos;t caught signal 9 (no core).
2003 Feb 21 04:16:18 switch %LICMGR-3-LOG_LIC_FILE_MISSING: License file(s) missing for
feature ENTERPRISE_PKG.
2003 Feb 21 04:16:18 switch %LICMGR-3-LOG_LIC_FILE_MISSING: License file(s) missing for
feature SAN_EXTN_OVER_IP.
2003 Feb 21 04:16:18 switch %LICMGR-3-LOG_LIC_FILE_MISSING: License file(s) missing for
feature ENTERPRISE_PKG.
2003 Feb 21 04:16:18 switch %LICMGR-3-LOG_LIC_FILE_MISSING: License file(s) missing for
feature SAN_EXTN_OVER_IP.
2003 Feb 21 04:16:18 switch %CALLHOME-2-EVENT: LICENSE_VIOLATION
2003 Feb 21 04:16:18 switch %CALLHOME-2-EVENT: LICENSE_VIOLATION
2003 Feb 21 04:16:18 switch %CALLHOME-2-EVENT: LICENSE_VIOLATION
2003 Feb 21 04:16:18 switch %CALLHOME-2-EVENT: LICENSE_VIOLATION ]]> </aml-block:Data>
</aml-block:Attachment> <aml-block:Attachment type="inline"> <aml-block:Name>show license
usage</aml-block:Name> <aml-block:Data encoding="plain">
<![CDATA[Feature                     Ins  Lic   Status Expiry Date Comments
                                Count
--------------------------------------------------------------------------------
DMM_184_PKG                   No    0   Unused             Grace expired
FM_SERVER_PKG                 No    -   Unused             Grace expired
MAINFRAME_PKG                 No    -   Unused             Grace expired
ENTERPRISE_PKG                Yes   -   Unused never       license missing
DMM_FOR_SSM_PKG               No    0   Unused             Grace expired
SAN_EXTN_OVER_IP              Yes   8   Unused never       8 license(s) missing
PORT_ACTIVATION_PKG           No    0   Unused             -
SME_FOR_IPS_184_PKG           No    0   Unused             Grace expired
STORAGE_SERVICES_184          No    0   Unused             Grace expired
SAN_EXTN_OVER_IP_18_4         No    0   Unused             Grace expired
SAN_EXTN_OVER_IP_IPS2         No    0   Unused             Grace expired
SAN_EXTN_OVER_IP_IPS4         No    0   Unused             Grace expired
STORAGE_SERVICES_SSN16        No    0   Unused             Grace expired
10G_PORT_ACTIVATION_PKG       No    0   Unused             -
STORAGE_SERVICES_ENABLER_PKG  No    0   Unused             Grace expired
--------------------------------------------------------------------------------
**** WARNING: License file(s) missing. **** ]]> </aml-block:Data> </aml-block:Attachment>
</aml-block:Attachments> </aml-block:Block> </soap-env:Body> </soap-env:Envelope>
```

XML 形式の RMON 通知の例

```
<?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.cisco.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.cisco.com/neddce/services/DDCEService</aml-session:To>
<aml-session:Path>
<aml-session:Via>http://www.cisco.com/appliance/uri</aml-session:Via>
</aml-session:Path>
<aml-session:From>http://www.cisco.com/appliance/uri</aml-session:From>
<aml-session:MessageId>1086:FHH0927006V:48BA26BD</aml-session:MessageId>
</aml-session:Session>
</soap-env:Header>
<soap-env:Body>
<aml-block:Block xmlns:aml-block="http://www.cisco.com/2004/01/aml-block">
<aml-block:Header>
<aml-block:Type>http://www.cisco.com/2005/05/callhome/diagnostic</aml-block:Type>
<aml-block:CreationDate>2008-08-31 05:06:05 GMT+00:00</aml-block:CreationDate>
<aml-block:Builder>
<aml-block:Name>MDS</aml-block:Name>
<aml-block:Version>4.1</aml-block:Version>
</aml-block:Builder>
<aml-block:BlockGroup>
<aml-block:GroupId>1087:FHH0927006V:48BA26BD</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:CallHome xmlns:ch="http://www.cisco.com/2005/05/callhome" version="1.0">
<ch:EventTime>2008-08-31 05:06:05 GMT+00:00</ch:EventTime>
<ch:MessageDescription>RMON_ALERT WARNING(4) Falling:iso.3.6.1.4.1.9.9.305.1.1.1.0=1 &lt;=
89:1, 4</ch:MessageDescription>
<ch:Event>
<ch:Type>diagnostic</ch:Type>
<ch:SubType>GOLD-major</ch:SubType>
<ch:Brand>Cisco</ch:Brand>
<ch:Series>MDS9000</ch:Series>
</ch:Event>
<ch:CustomerData>
<ch:UserData>
<ch:e-mail>mchinn@cisco.com</ch:e-mail>
</ch:UserData>
<ch:ContractData>
<ch:CustomerId>12ss</ch:CustomerId>
<ch:SiteId>2233</ch:SiteId>
<ch:ContractId>rrr55</ch:ContractId>
<ch:DeviceId>DS-C9513@C@FHH0927006V</ch:DeviceId>
</ch:ContractData>
<ch:SystemInfo>
<ch:Name>sw172-22-46-174</ch:Name>
<ch:Contact>Mani</ch:Contact>
<ch:Contacte-mail>mchinn@cisco.com</ch:Contacte-mail>
<ch:ContactPhoneNumber>+1-800-304-1234</ch:ContactPhoneNumber>
<ch:StreetAddress>1234 wwee</ch:StreetAddress>
</ch:SystemInfo>
</ch:CustomerData>
<ch:Device>
<rme:Chassis xmlns:rme="http://www.cisco.com/rme/4.0">
<rme:Model>DS-C9513</rme:Model>
<rme:HardwareVersion>0.205</rme:HardwareVersion>
<rme:SerialNumber>FHH0927006V</rme:SerialNumber>
</rme:Chassis>
```

```
</ch:Device>
</ch:CallHome>
</aml-block:Content>
</aml-block:Block>
</soap-env:Body>
</soap-env:Envelope>
```

Call Home のフィールドの説明

ここでは、Call Home のフィールドの説明を示します。

Call Home 一般

フィールド	説明
Contact	このスイッチの連絡先担当者。この担当者への連絡方法に関する情報も含む。
phoneNumber	連絡先担当者の電話番号。電話番号は、「+」で始まり、空白と「-」以外はすべて数字にする必要があります。+44 20 8332 9091、+45 44886556、+81-46-215-4678、+1-650-327-2600 などの電話番号が有効です。
EmailAddress	連絡先担当者の電子メール アドレス。raj@helpme.com、bob@service.com、mtom@abc.caview.ca.us などの電子メール アドレスが有効です。
StreetAddress	このスイッチの送付先住所です。
CustomerId	お客様を識別するための任意の適切な形式の文字列です。
ContractId	お客様とサポート パートナーの間のサポート契約を識別するための任意の適切な形式の文字列です。
SiteId	このデバイスのロケーション ID です。
DeviceServicePriority	デバイスのサービス プライオリティです。これにより、デバイスにサービスが提供される速さが決定されます。
Enable	ローカル デバイス上で Call Home インフラストラクチャをイネーブルまたはディセーブルにします。

関連トピック

Call Home について

Call Home 宛先

フィールド	説明
E-mailAddress	この宛先プロファイルに関連付けられる電子メール アドレス。raj@helpme.com、bob@service.com、mtom@abc.caview.ca.us などになります。

関連トピック

Call Home 宛先プロファイル

Call Home SMTP サーバ

フィールド	説明
[Address Type]、[Address]	SMTP サーバの IP アドレス。
Port	SMTP サーバの TCP ポート。
Priority	プライオリティ値。

Call Home 電子メール セットアップ

フィールド	説明
From	SMTP を使用して電子メールを送信する際に、From フィールドに使用される電子メール アドレス。raj@helpme.com、bob@service.com、mtom@abc.caview.ca.us などになります。
ReplyTo	SMTP を使用して電子メールを送信する際に、Reply-To フィールドに使用される電子メール アドレス。raj@helpme.com、bob@service.com、mtom@abc.caview.ca.us などになります。
IP Address Type	IP アドレス タイプ（IPv4、IPv6、または DNS）。
[Name] または [IP Address]	SMTP サーバの名前または IP アドレス。
Port	SMTP サーバの TCP ポート。

関連トピック

一般的な電子メール オプションの設定

Call Home アラート

フィールド	説明
Action	[Test]：Call Home メッセージを送信します。 [TestWithInventory]：コンポーネントの詳細付きメッセージを送信します。
Status	最後の Call Home アクション呼び出しのステータス。
FailureCause	最後の Call Home テスト呼び出しの失敗原因。
LastTimeSent	最後の Call Home アラートが送信された時刻。
NumberSent	Call Home アラートの送信数。
Interval	定期的なソフトウェア コンポーネント Call Home メッセージを送信するためのタイム フレーム。

フィールド	説明
Throttling Enable	オンの場合、システムに実装されているメッセージ スロットリング メカニズムがイネーブルになり、一定のタイム フレーム内での特定のアラート タイプの Call Home メッセージの数が制限されます。最大は 2 時間のタイム フレーム内で 30 件であり、それ以上のそのアラート タイプのメッセージは廃棄されます。
Enable	オンの場合、システム上での定期的なソフトウェア コンポーネント Call Home メッセージの送信がイネーブルになります。

関連トピック

Call Home アラート グループ

アラート グループ メッセージのカスタマイズ

Call Home ユーザ定義コマンド

フィールド	説明
User Defined Command	Call Home アラート グループ タイプのユーザ定義コマンドを設定します。

遅延トラップ

フィールド	説明
Enable	遅延トラップをイネーブルまたはディセーブルにします。
Delay	分単位の遅延時間（有効な値の範囲は 1 ～ 60）。

Call Home プロファイル

フィールド	説明
MsgFormat	XML、フル テキスト、またはショート テキスト。
MaxMsgSize	この宛先プロファイルで示される宛先に送信可能な最大メッセージ サイズ。
MsgLevel	しきい値レベル。宛先に送信されるアラート メッセージのフィルタリングに使用されます。設定されたしきい値レベルよりも低い重大度の Callhome アラート メッセージは送信されなくなります。デフォルトのしきい値レベルはデバッグ (1) です。この場合、すべてのアラート メッセージが送信されます。
AlertGroups	この宛先プロファイルに設定されているアラート グループのリスト。

イベント宛先アドレス

フィールド	説明
Address/Port	イベントを送信する IP アドレスとポート。
Security Name	このアドレスに送信されるメッセージを生成する際に使用される SNMP パラメータ。
Security Model	このエントリを使用して SNMP メッセージを生成する際に使用されます。
Inform Type	• [Trap]：未確認応答イベント • [Inform]：確認応答イベント
Inform Timeout	このアドレスとの通信に求められる最大ラウンドトリップ時間。
RetryCount	生成したメッセージに対する応答が受信されない場合に行われる再試行の回数。

イベント宛先セキュリティ（詳細）

フィールド	説明
MPModel	このエントリを使用して SNMP メッセージを生成する際に使用されるメッセージ処理モデル。
SecurityModel	このエントリを使用して SNMP メッセージを生成する際に使用されるセキュリティ モデル。
SecurityName	このエントリを使用して SNMP メッセージが生成される対象者を識別します。
SecurityLevel	このエントリを使用して SNMP メッセージを生成する際に使用されるセキュリティ レベル。

イベント フィルター般

フィールド	説明
FSPF - Nbr State Changes	ローカル スイッチが VSAN 上のインターフェイスでネイバーの状態（FSPF ネイバー有限状態マシンの状態）の変化を検出したときに通知を発行するかどうかを指定します。
Domain Mgr - ReConfig Fabrics	ローカル スイッチが VSAN 上での ReConfigureFabric（RCF）の送受信時に通知を発行するかどうかを指定します。
Zone Server - Request Rejects	ゾーン サーバが拒否時に通知を発行するかどうかを指定します。
Zone Server - Merge Failures	ゾーン サーバがマージ失敗時に通知を発行するかどうかを指定します。
Zone Server - Merge Successes	ゾーン サーバがマージ成功時に通知を発行するかどうかを指定します。

フィールド	説明
Zone Server - Default Zone Behavior Change	伝播ポリシーが変化した場合にゾーン サーバが通知を発行するかどうかを指定します。
Zone Server - Unsupp Mode	ゾーン サーバが unsupp モードの変化時に通知を発行するかどうかを指定します。
FabricConfigServer - Request Rejects	ファブリック コンフィギュレーション サーバが拒否時に通知を発行するかどうかを指定します。
RSCN - ILS Request Rejects	SW_RSCN 要求が拒否されるときに RSCN モジュールが通知を生成するかどうかを指定します。
RSCN - ILS RxRequest Rejects	SW_RSCN 要求が拒否されるときに RSCN モジュールが通知を生成するかどうかを指定します。
RSCN - ELS Request Rejects	SCR または RSCN 要求が拒否されるときに RSCN モジュールが通知を生成するかどうかを指定します。
FRU Changes	false 値の場合、このシステムによって現場交換可能ユニット（FRU）通知は生成されません。
SNMP - Community Auth Failure	SNMP エンティティが authenticationFailure トラップの生成を許可されているかどうかを示します。
VRRP	VRRP 対応ルータがこの MIB に定義されているイベントに対して SNMP トラップを生成するかどうかを示します。
FDMI	登録要求が拒否されるときに FDMI が通知を生成するかどうかを指定します。
License Manager	システムが通知を生成するかどうかを示します。
Port/Fabric Security	ポート/ファブリック セキュリティの問題が発生したときにシステムが通知を生成するかどうかを指定します。
FCC	エージェントが通知を生成するかどうかを指定します。
Name Server	オンの場合、要求が拒否されるときにネーム サーバが通知を生成します。オフの場合、通知は生成されません。

イベント フィルタ インターフェイス

フィールド	説明
EnableLinkTrap	このインターフェイスに対して linkUp/linkDown トラップが生成されるかどうかを示します。

イベント フィルタ制御

フィールド	説明
Variable	制御される通知を表します。
Descr	通知に関する説明。
Enabled	オンにすると、コントロールの通知がイネーブルになります。コントロールのステータスを表示します。

（注）　[Descr] カラムは、Cisco NX-OS Release 5.0 以降が動作しているスイッチ上でのみ表示されます。

その他の参考資料

Call Home の実装に関連した情報については、次を参照してください。

- 「MIB」（P.4-43）

MIB

MIB	MIB のリンク
• CISCO-CALLHOME-CAPABILITY-MIB • CISCO-CALLHOME-MIB	MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 http://www.cisco.com/en/US/products/ps5989/prod_technical_reference_list.html

Call Home の機能履歴

表 4-10 に、この機能のリリース履歴を示します。Release 3.x 以降のリリースで導入または変更された機能のみが表に記載されています。

表 4-10　Call Home の機能履歴

機能名	リリース	機能情報
Call Home HTTP プロキシ サーバ	5.2	Call Home HTTP プロキシ サーバ サポートの詳細が追加されました。
Call Home ウィザード	5.2	Call Home ウィザード設定の詳細が追加されました。

機能名	リリース	機能情報
複数 SMTP サーバ サポート	5.0(1a)	複数 SMTP サーバ サポートの詳細が追加されました。 Callhome 転送を確認するコマンドが追加されました。
通知の拡張	5.0(1a)	Device Manager を使用したイベント フィルタの通知の拡張が追加されました。
Call Home	4.1(1b)	Call Home の HTTPS サポートが追加されました。
DCNM-SAN における [Call Home - Delayed Traps for EMC Call Home] 設定ウィンドウ	4.1(1a)	EMC Call Home の遅延トラップの拡張が追加されました。
[Call Home Destination] タブ	4.2(1)	[Destination] タブの拡張を追加。
Call Home HTTP のサポート	4.2(1)	Call Home HTTP 拡張を追加。
EMC Email Home	3.3(3)	この章に EMC Email Home 設定情報が追加されました。
EMC Call Home	3.0(1)	EMC 仕様に従い、電子メールを使用してトラップを XML データとして転送できるようになります。
Call Home の拡張	3.0(1)	アラート グループ メッセージをカスタマイズできるようになります。

CHAPTER 5

メンテナンス ジョブのスケジューリング

Cisco MDS コマンド スケジューラ機能は、Cisco MDS 9000 ファミリの任意のスイッチで設定ジョブとメンテナンス ジョブをスケジュールするのに役立ちます。この機能を使用して、一度だけ実行するジョブや定期的に実行するジョブをスケジュールできます。

この章の内容は、次のとおりです。

コマンド スケジューラについて

Cisco NX-OS コマンド スケジューラは、将来の指定した時刻に 1 つ以上のジョブ（CLI コマンドのセット）をスケジュールするための機構を提供します。ジョブは、将来の指定した時刻に一度だけ実行することも、定期的に実行することもできます。

この機能を使用すると、ゾーンセットの変更、QoS ポリシーの変更、データのバックアップ、設定の保存などのジョブをスケジューリングできます。

スケジューラの用語

この章では次の用語を使用します。

- ジョブ：スケジュールの定義どおりに実行される NX-OS の CLI コマンド一式（EXEC および config モード）。
- スケジュール：スケジュールは割り当てたジョブを実行する時刻を決定します。スケジュールには複数のジョブを割り当てることができます。スケジュールは、一時モードまたは定期モードで実行されます。
- 定期モード：ユーザが指定した間隔でジョブを実行します。これは、管理者によって削除されるまで継続されます。サポートされている間隔は、次のとおりです。
  - 毎日：ジョブを 1 日に 1 回実行します。
  - 毎週：ジョブを 1 週間に 1 回実行します。
  - 毎月：ジョブを 1 か月に 1 回実行します。
  - 差分：ジョブをユーザ指定の開始時刻から一定間隔（日、時、分）ごとに実行します。

- 一時モード：ジョブをユーザ指定時刻に 1 回実行します。

注意事項と制限

Cisco MDS 9000 スイッチでジョブをスケジュールする前に、次の注意事項を確認してください。

- Cisco MDS SAN-OS Release 3.0(3) よりも前のリリースでは、スイッチに対してローカルなユーザだけがスケジューラを設定できました。Cisco MDS SAN-OS Release 3.0(3) から、リモート ユーザが AAA 認証を使用してジョブのスケジューリングを実行できるようになりました。
- ジョブの実行時に次のいずれかの状況になると、スケジュールされたジョブは実行されません。
  - ジョブの実行予定時刻に、スケジュールされたジョブに含まれるコマンドに関連する機能のライセンスが切れている場合。
  - ジョブの実行予定時刻に、スケジュールされたジョブに含まれるコマンドに関連する機能がディセーブルになっている場合。
  - スロットからモジュールを取り外したときに、そのモジュールまたはスロットに関連するコマンドがジョブに含まれている場合。
- 時刻が設定されていることを確認します。スケジューラにはデフォルトの設定時刻はありません。スケジュールを作成してジョブを割り当てても、時刻を設定しないと、スケジュールは開始されません。
- ジョブを定義する場合、ジョブの中に対話型コマンドや中断型コマンド（**copy bootflash:** *file* **ftp:** *URI*、**write erase** など）が指定されていないことを確認します。これは、ジョブがスケジュールされた時刻に対話なしで実行されるためです。

デフォルト設定

表 5-1 に、コマンド スケジューリング パラメータのデフォルト設定値の一覧を示します。

表 5-1　コマンド スケジューラのパラメータのデフォルト

パラメータ	デフォルト
コマンド スケジューラ	ディセーブル。
ログ ファイル サイズ	16 KB。

コマンド スケジューラの設定

コマンド スケジューラを設定するためのタスク フロー

次の手順を実行して、コマンド スケジューラを設定します。

ステップ 1　スケジューラをイネーブルにします。

ステップ 2　リモート ユーザ アクセスを許可します（オプション）。

ステップ 3　ジョブを定義します。

ステップ 4　スケジュールを定義して、スケジュールにジョブを割り当てます。

ステップ 5　スケジュールの時刻を指定します。

ステップ 6　スケジューリングされた設定を確認します。

コマンド スケジューラのイネーブル化

スケジューリング機能を使用するには、ファブリック内の目的のスイッチ上でこの機能を明示的にイネーブルにする必要があります。デフォルトでは、この機能は Cisco MDS 9000 ファミリのすべてのスイッチでディセーブルになっています。

スケジュールの指定

ジョブを定義したら、スケジュールを作成してスケジュールにジョブを割り当てることができます。その後、実行時刻を設定できます。ジョブは、必要に応じて、1 回だけまたは定期的に実行できます。スケジュールの時刻が設定されていないと、ジョブは実行されません。

定期的なジョブの実行は、間隔（毎日、毎週、毎月、または差分）を指定できます。

CHAPTER 6

システム プロセスおよびログのモニタ

この章では、スイッチのヘルスのモニタリングについて詳細に説明します。この章の内容は次のとおりです。

システム プロセスおよびログについて

ここで説明する内容は、次のとおりです。

コアの保存

次の方法のいずれかで、（アクティブ スーパーバイザ モジュール、スタンバイ スーパーバイザ モジュール、または任意のスイッチング モジュールの）コアを外部 CompactFlash（スロット 0）または TFTP サーバに保存できます。

- オンデマンド：与えられたプロセス ID に基づいて 1 つのファイルをコピーします。
- 定期的：ユーザの設定に従ってコア ファイルを定期的にコピーします。

新しい方式が実行されると、その前に実行された方式は新しい方式で上書きされます。たとえば、別のコア ログ コピー タスクを実行すると、コアは、その新しい場所またはファイルに定期的に保存されます。

ブートフラッシュへの最後のコアの保存

この最後のコア ダンプは、スイッチオーバーまたはリブートが起こる前に、/mnt/pss/ パーティションにあるブートフラッシュに自動的に保存されます。スーパーバイザ モジュールがリブートしてから 3 分間後に、保存された最後のコアがフラッシュ パーティション（/mnt/pss）から元のメモリ上に復元されます。この復元はバックグラウンド プロセスであり、ユーザからは見えません。

ヒント　復元された最後のコア ファイルのタイムスタンプは、最後のコアが実際にダンプされた時刻ではなく、スーパーバイザのブート時刻を表します。最後のコア ダンプの正確な時刻を知るには、PID が同じ、対応するログ ファイルを確認してください。

最初と最後のコア

最初と最後のコアの機能は、限られたシステム リソースで最も重要なコア ファイルを保持します。一般に、最初のコアと最後に生成されたコアにデバッグの情報が格納されています。最初と最後のコアの機能は、最初と最後のコア情報を保持しようとします。

アクティブ スーパーバイザ モジュールからコア ファイルが生成される場合、サービスのコア ファイルの数は、service.conf ファイルで定義されます。アクティブ スーパーバイザ モジュールのコア ファイルの総数に上限はありません。

オンラインでのシステム ヘルス管理

Online Health Management System（OHMS、システム ヘルス）は、ハードウェア障害検出および復旧機能です。OHMS は、Cisco MDS 9000 ファミリのすべてのスイッチのスイッチング モジュール、サービス モジュール、スーパーバイザ モジュールの全般的な状態を確認します。

OHMS は、システム ハードウェアを次のようにモニタリングします。

- アクティブ スーパーバイザ稼動する OHMS コンポーネントは、スイッチ内の他のモジュール上で稼動する他のすべての OHMS コンポーネントを制御します。
- スタンバイ スーパーバイザ モジュール上で稼動するシステム ヘルス アプリケーションは、そのモジュールが HA スタンバイ モードで使用できる場合でも、スタンバイ スーパーバイザ モジュールだけを監視します。

OHMS アプリケーションはすべてのモジュールでデーモン プロセスを起動して、各モジュール上で複数のテストを実行し、モジュールの個々のコンポーネントをテストします。これらのテストは、事前に設定されたインターバルで実行され、すべての主要な障害ポイントを対象として、障害が発生している MDS スイッチのコンポーネントを隔離します。アクティブ スーパーバイザ上で稼動する OHMS は、スイッチ内の他のすべてのモジュール上で稼動する他のすべての OHMS コンポーネントを制御します。

障害を検出すると、システム ヘルス アプリケーションは次のリカバリ アクションを試行します。

- 障害のあるコンポーネントを隔離するため、追加のテストを実行します。
- 永続的ストレージから設定情報を取得し、コンポーネントの再設定を試みます。
- 復旧できない場合、コール ホーム通知、システム メッセージ、および例外ログを送信します。障害の発生しているモジュールまたはコンポーネント（インターフェイスなど）をシャットダウンし、テストを中止します。
- 障害を検出すると、ただちに Call Home メッセージ、システム メッセージ、および例外ログを送信します。
- 障害の発生しているモジュールまたはコンポーネント（インターフェイスなど）をシャットダウンします。
- 詳細なテストが実行されないように、障害が発生したポートを隔離します。
- その障害を適切なソフトウェア コンポーネントに報告します。
- スタンバイ スーパーバイザ モジュールに切り替えます（障害がアクティブ スーパーバイザ モジュールで検出され、Cisco MDS スイッチにスタンバイ スーパーバイザ モジュールが搭載されている場合）。スイッチオーバーが完了すると、新しいアクティブ スーパーバイザ モジュールはアクティブ スーパーバイザ テストを再開します。
- スイッチをリロードします（スイッチにスタンバイ スーパーバイザ モジュールが搭載されていない場合）。
- テストの実行統計情報を表示、テスト、および取得したり、スイッチのシステム ヘルス テスト設定を変更したりするための CLI サポートを提供します。
- 問題領域に焦点を当てるためのテストを実行します。

各モジュールはそれぞれに対応するテストを実行するように設定されています。必要に応じて、各モジュールのデフォルト パラメータを変更できます。

ループバック テストの頻度の設定

ループバック テストは、モジュール内のデータ パスおよびスーパーバイザ内の制御パスにおいてハードウェア エラーを特定するように設計されています。事前に設定された頻度でループバック フレームが各モジュールに 1 つずつ送信されます。このフレームは、それぞれに設定されたインターフェイスを通過した後、スーパーバイザ モジュールに戻ります。

ループバック テストは 5（デフォルト）～ 255 秒の範囲の頻度で実行できます。ループバック頻度の値を設定しなければ、デフォルトの頻度である 5 秒がスイッチ内のすべてのモジュールに対して使用されます。ループバック テストの頻度は、モジュールごとに変更できます。

ループバック テストのフレーム長の設定

ループバック テストは、モジュール内のデータ パスおよびスーパーバイザ内の制御パスにおいてハードウェア エラーを特定するように設計されています。事前に設定されたサイズでループバック フレームが各モジュールに 1 つずつ送信されます。このフレームは、それぞれに設定されたインターフェイスを通過した後、スーパーバイザ モジュールに戻ります。

ループバック テストは、0 ～ 128 バイトの範囲のフレーム サイズで実行できます。ループバック フレーム長の値を設定しなければ、スイッチ内のすべてのモジュールに対してランダムなフレーム長がスイッチによって生成されます（自動モード）。ループバック テストのフレーム長は、モジュールごとに変更できます。

ハードウェアの障害処理

failure-action コマンドは、テストの実行中にハードウェア障害が発見された場合に、Cisco NX-OS ソフトウェアによる処理の実行を抑制します。

デフォルトでは、Cisco MDS 9000 ファミリのすべてのスイッチでこの機能はイネーブルになります。障害が発見されると処理が実行され、障害が発生したコンポーネントはそれ以降のテストから隔離されます。

障害処理は、個々のテスト レベル（モジュール単位）、モジュール レベル（すべてのテスト）、またはスイッチ全体で制御されます。

テストの実行要件

テストをイネーブルにしても、テストの実行が保障されるわけではありません。

特定のインターフェイスまたはモジュールのテストが実行されるのは、次のすべての項目に対してシステム ヘルスをイネーブルにしている場合だけです。

- スイッチ全体
- 必要なモジュール
- 必要なインターフェイス

ヒント　上記のいずれかによってシステム ヘルスがディセーブルになっている場合、テストは実行されません。システム ヘルスでテストの実行がディセーブルになっている場合、テスト ステータスはディセーブル（Disabled）と表示されます。

ヒント　特定のモジュールまたはインターフェイスでテストの実行がイネーブルになっているが、システム ヘルスがディセーブルであるためにテストが実行されない場合、テストはイネーブル（Enabled）と表示されます（実行中（Running）にはなりません）。

指定モジュールのテスト

NX-OS ソフトウェアのシステム ヘルス機能は、次の領域のテストを実行します。

- アクティブ スーパーバイザのファブリックへのインバンド接続。
- スタンバイ スーパーバイザのアービターの可用性。
- すべてのモジュール上でのブートフラッシュの接続性とアクセシビリティ。
- すべてのモジュール上での EOBC の接続性とアクセシビリティ。
- すべてのモジュール上の各インターフェイスのデータ パスの完全性。
- 管理ポートの接続性。
- 外部接続性検証のためのユーザによるテスト。テスト中はポートがシャットダウンされます（ファイバ チャネル ポートのみ）。
- 内部接続性検証のためのユーザによるテスト（ファイバ チャネル ポートと iSCSI ポート）。

古いエラー通知のクリア

ファイバ チャネル インターフェイス、iSCSI インターフェイス、モジュール全体、またはモジュール全体の特定の 1 つのテストについて、エラー履歴をクリアできます。履歴をクリアすると、障害が発生してテストから除外されていたコンポーネントはすべて再度テストされます。

障害発生時に OHMS が一定期間（たとえば、1 週間）の間処理を実行しないようにオプション failure-action オプションをイネーブルにしていて、指定期間が経過した後でエラー受信を再開する準備が整った場合には、それぞれのテストのシステム ヘルス エラー ステータスをクリアする必要があります。

ヒント　管理ポート テストは、スタンバイ スーパーバイザ モジュール上で実行することはできません。

現在のステータスの説明

各モジュールまたはテストのステータスは、その特定のモジュールでの OHMS テストの現在の設定状態によって異なります（表 6-1 を参照）。

オンボード障害ロギング

第 2 世代ファイバ チャネル スイッチング モジュールでは、障害データを永続的ストレージに記録する機能が提供されます。この記録は、分析用に取得したり、表示したりできます。このオンボード障害ロギング（OBFL）機能は、障害および環境情報をモジュールの不揮発性メモリに保管します。この情報は、障害が発生したカードの事後分析に役立ちます。

OBFL データは、モジュール上の既存の CompactFlash に保存されます。OBFL では、モジュールのファームウェアで使用できる永続的ロギング（PLOG）機能を使用して CompactFlash にデータを保存します。保存されたデータを取得するためのメカニズムも提供されます。

OBFL 機能によって保存されるデータは、次のとおりです。

- 最初の電源投入時刻
- カードのシャーシ スロット番号

- カードの初期温度
- ファームウェア、BIOS、FPGA、および ASIC のバージョン
- カードのシリアル番号
- クラッシュのスタック トレース
- CPU hog 情報
- メモリ リーク情報
- ソフトウェア エラー メッセージ
- ハードウェア例外ログ
- 環境履歴
- OBFL 固有の履歴情報
- ASIC 割り込みおよびエラー統計の履歴
- ASIC レジスタ ダンプ

デフォルト設定

表 6-1 に、システム ヘルスおよびログのデフォルト設定値を示します。

表 6-1　システム ヘルスおよびログのデフォルト設定値

パラメータ	デフォルト
カーネル コアの生成	1 つのモジュール
システム ヘルス	イネーブル
ループバック頻度	5 秒
障害処理	イネーブル

コア ディレクトリのクリア

前提条件

- このスイッチ上で SSH2 がイネーブルになっていることを確認します。

手順の詳細

スイッチ上でコアをクリアするには、次の手順を実行します。

ステップ 1　[Clear] をクリックしてコアをクリアします。

ソフトウェアは、過去数世代のコア（サービス単位とスロット単位）を保持し、アクティブ スーパーバイザ モジュール上に存在するすべてのコア ファイルとその他のコアをクリアします。

ステップ 2　[Close] をクリックして、ダイアログボックスを閉じます。

システム ヘルスの設定

Online Health Management System（OHMS、システム ヘルス）は、ハードウェア障害検出および復旧機能です。OHMS は、Cisco MDS 9000 ファミリのすべてのスイッチのスイッチング モジュール、サービス モジュール、スーパーバイザ モジュールの全般的な状態を確認します。

ここで説明する内容は、次のとおりです。

内部ループバック テストの実行

手動ループバック テストを実行すると、スイッチング モジュールまたはサービス モジュールのデータパスや、スーパーバイザ モジュールの制御パスにおけるハードウェア エラーを特定できます。内部ループバック テストは同一のポートに対して FC2 フレームを送受信し、ラウンドトリップ時間をマイクロ秒単位で示します。このテストは、ファイバ チャネル インターフェイス、IPS インターフェイス、iSCSI インターフェイスで使用できます。

Device Manager から内部ループバック テストを実行するには、[Interface] > [Diagnostics] > [Internal] の順に選択します。

外部ループバック テストの実行

手動ループバック テストを実行すると、スイッチング モジュールまたはサービス モジュールのデータパスや、スーパーバイザ モジュールの制御パスにおけるハードウェア エラーを特定できます。外部ループバック テストは、同一のポートの間または 2 つのポート間で FC2 フレームを送受信します。

テストを実行する前に、Rx ポートから Tx ポートへループさせるためにケーブル（またはプラグ）を接続する必要があります。同じポートの間でテストする場合は、特殊なループ ケーブルが必要です。異なるポートとの間でテストする場合は、通常のケーブルを使用できます。このテストを使用できるのは、ファイバ チャネル インターフェイスだけです。

Device Manager から外部ループバック テストを実行するには、[Interface] > [Diagnostics] > [External] を選択します。

システム プロセスおよびログの設定の確認

ここで説明する内容は、次のとおりです。

システム プロセスの表示

すべてのプロセスに関する一般的な情報を表示するには、次の手順を実行します。

ステップ 1　[Admin] > [Running Processes] を選択します。

[Running Processes] ダイアログボックスが表示されます。

各記号の意味は次のとおりです。

- ProcessId = プロセス ID
- Name = プロセス名
- MemAllocated = このプロセスがシステムから動的に割り当てられているすべてのメモリの合計。すでにシステムに返されたメモリが含まれている場合があります。
- CPU Time (ms) = プロセスが使用した CPU 時間（ミリ秒）

ステップ 2　[Close] をクリックして、ダイアログボックスを閉じます。

システム ステータスの表示

Device Manager でシステム ステータスを表示するには、次の手順を実行します。

ステップ 1　[Physical] > [System] を選択します。

[System] ダイアログボックスが表示されます。

ステップ 2　[Close] をクリックして、ダイアログボックスを閉じます。

コア ステータスの表示

スイッチ上でコアを表示するには、次の手順を実行します。

（注）　このスイッチ上で SSH2 がイネーブルになっていることを確認します。

ステップ 1　[Admin] > [Show Cores] を選択します。

[Show Cores] ダイアログボックスが表示されます。

Module-num は、コアが生成されたスロット番号を示します。

ステップ 2　[Close] をクリックして、ダイアログボックスを閉じます。

その他の参考資料

システム プロセスとログの実装に関する詳細情報については、次の項を参照してください。

- 「MIB」（P.6-9）

MIB

MIB	MIB のリンク
• CISCO-SYSTEM-EXT-MIB • CISCO-SYSTEM-MIB	MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 http://www.cisco.com/en/US/products/ps5989/prod_technical_reference_list.html

CHAPTER 7

Embedded Event Manager の設定

ここでは、デバイス上の重要なイベントを検出し、処理するように、EEM を設定する方法について説明します。

この章の内容は、次のとおりです。

EEM について

Embedded Event Manager はデバイス上で発生するイベントをモニタし、設定に基づいて各イベントの回復またはトラブルシューティングのためのアクションを実行します。

ここで説明する内容は、次のとおりです。

EEM の概要

EEM は次の 3 種類の主要コンポーネントからなります。

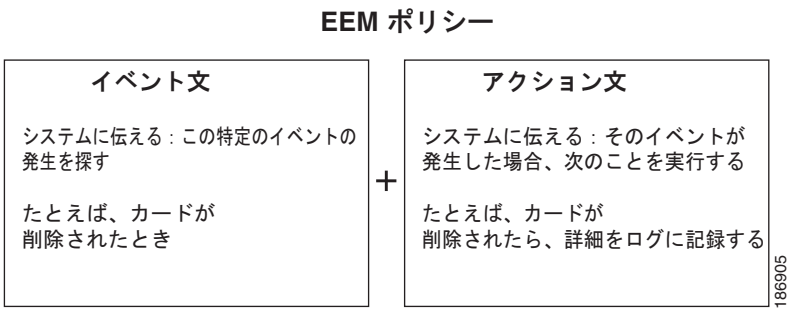
- イベント文：別の Cisco NX-OS コンポーネントからモニタし、アクション、回避策、または通知が必要になる可能性のあるイベント。
- アクション文：電子メールの送信、インターフェイスのディセーブル化など、イベントから回復するために EEM が実行できるアクション。
- ポリシー：イベントのトラブルシューティングまたはイベントからの回復を目的とした 1 つまたは複数のアクションとペアになったイベント。

ポリシー

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

図 7-1 に、EEM ポリシーの基本的な 2 種類の文を示します。

図 7-1　EEM ポリシー文



EEM ポリシーを設定するには、CLI または VSH スクリプトを使用します。

（注） EEM ポリシー照合は、MDS スイッチ上ではサポートされません。

EEM はスーパーバイザ上でイベント ログを維持します。

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

使用するネットワークに合わせてユーザ ポリシーを作成できます。ユーザ ポリシーを作成すると、そのポリシーと同じイベントに関連するシステム ポリシー アクションが EEM によって発生したあと、ユーザ ポリシーで指定したアクションが行われます。

一部のシステム ポリシーは上書きすることもできます。設定した上書き変更がシステム ポリシーの代わりになります。イベントまたはアクションの上書きが可能です。

（注） 上書きポリシーには、必ずイベント文を指定します。上書きポリシーにイベント文が含まれていないと、システム ポリシーで可能性のあるイベントがすべて上書きされます。

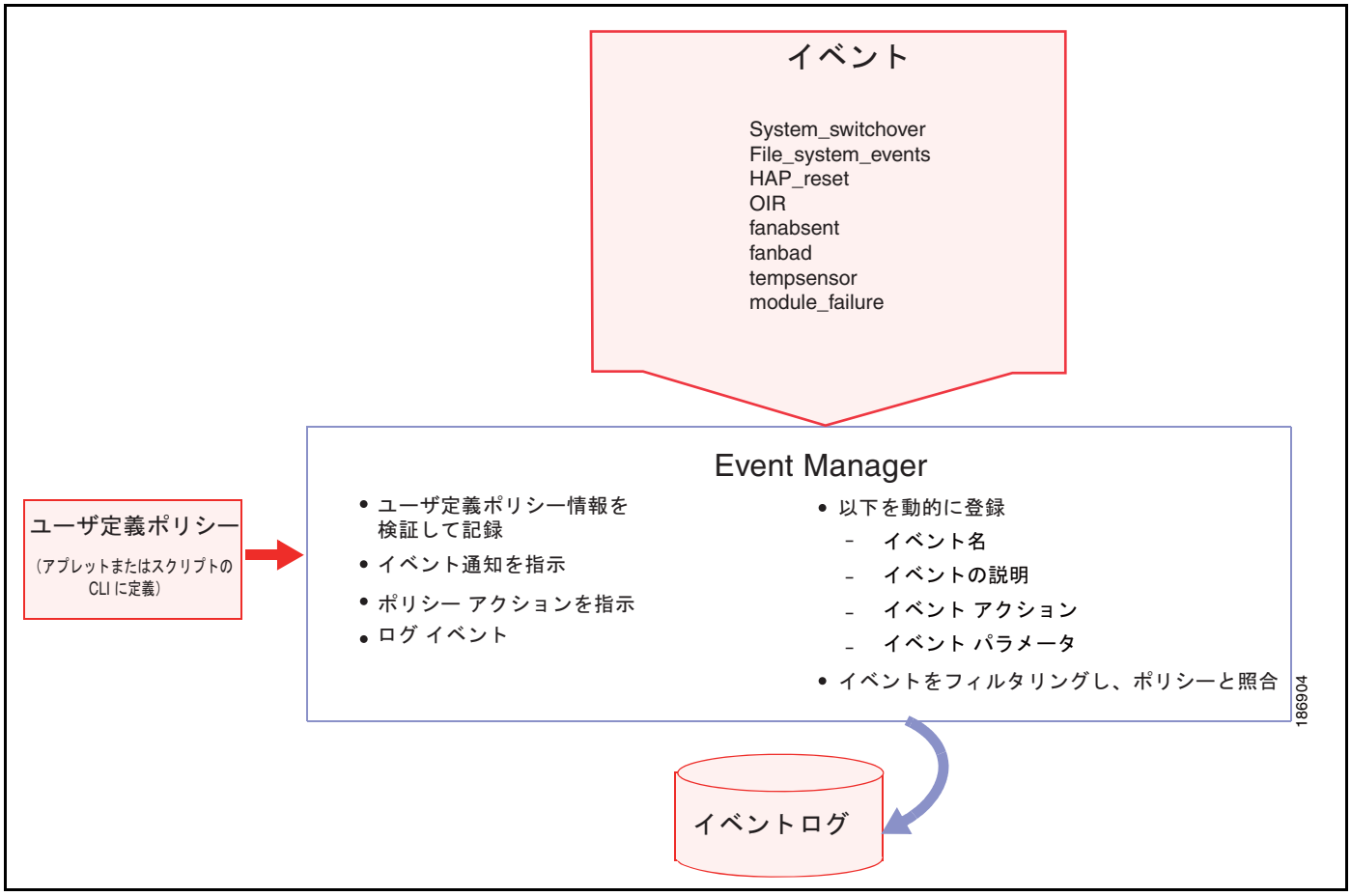
イベント文

イベントは、回避、通知など、何らかのアクションが必要なデバイス アクティビティです。これらのイベントは通常、インターフェイスやファンの誤動作といったデバイスの障害に関連します。

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

図 7-2 に、EEM が処理するイベントを示します。

図 7-2　EEM の概要



イベント文では、ポリシー実行のトリガーになるイベントを指定します。設定できるイベント文は、1 つのポリシーに 1 つだけです。

EEM はイベント文に基づいてポリシーをスケジューリングし、実行します。EEM はイベントおよびアクション コマンドを検証し、定義に従ってコマンドを実行します。

（注） トリガーされたイベントでデフォルト アクションも処理されるようにする場合は、EEM アクションをポリシーのタイプに応じて「event-default」または「policy-default」で明示的に設定する必要があります。

アクション文

アクション文では、ポリシーによって実行されるアクションを記述します。各ポリシーに複数のアクション文を設定できます。ポリシーにアクションを関連付けなかった場合、EEM はイベント観察を続けますが、アクションは実行されません。

EEM がアクション文でサポートするアクションは、次のとおりです。

- CLI コマンドの実行。
- カウンタのアップデート。
- 例外の記録。
- モジュールの強制的シャットダウン。
- デバイスのリロード。
- 電力のバジェット超過による特定モジュールのシャットダウン。
- Syslog メッセージの生成。
- Call Home イベントの生成。
- SNMP 通知の生成。
- システム ポリシー用デフォルト アクションの使用。

（注）　トリガーされたイベントでデフォルト アクションも処理されるようにする場合は、EEM アクションをポリシーのタイプに応じて **event-default** または **policy-default** で明示的に設定する必要があります。たとえば、match 文で CLI コマンドを照合する場合、EEM ポリシーに event-default アクション文を追加する必要があります。この文がないと、EEM では CLI コマンドを実行できません。

（注）　ユーザ ポリシーまたは上書きポリシーの中に、相互に否定したり、関連付けられたシステム ポリシーに悪影響を与えたりするようなアクション文がないかどうかを確認してください。

VSH スクリプト ポリシー

テキスト エディタを使用し、VSH スクリプトでポリシーを作成することもできます。このようなポリシーにも、他のポリシーと同様、イベント文およびアクション文（複数可）を使用します。また、これらのポリシーでシステム ポリシーを補うことも上書きすることもできます。スクリプト ポリシーの作成後、そのポリシーをデバイスにコピーしてアクティブにします。

環境変数

すべてのポリシーに使用できる、EEM の環境変数を定義できます。環境変数は、複数のポリシーで使用できる共通の値を設定する場合に便利です。たとえば、外部電子メール サーバの IP アドレスに対応する環境変数を作成できます。

パラメータ置換フォーマットを使用することによって、アクション文で環境変数を使用できます。

ハイ アベイラビリティ

Cisco NX-OS は、EEM 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に、Cisco NX-OS は実行コンフィギュレーションを適用します。

EEM の前提条件

EEM の前提条件は、次のとおりです。

- EEM を設定するには、network-admin のユーザ権限が必要です。

注意事項と制限

EEM 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。

- ユーザ ポリシーまたは上書きポリシー内のアクション文が、相互に否定したり、関連付けられたシステム ポリシーに悪影響を与えたりするようなことがないようにする必要があります。
- トリガーされたイベントでデフォルト アクションも処理されるようにする場合は、EEM アクションをポリシーのタイプに応じて **event-default** または **policy-default** で明示的に設定する必要があります。たとえば、match 文で CLI コマンドを照合する場合、EEM ポリシーに event-default アクション文を追加する必要があります。この文がないと、EEM では CLI コマンドを実行できません。
- イベント文が指定されていて、アクション文が指定されていない上書きポリシーを設定した場合、アクションは開始されません。また、障害も通知されません。
- 上書きポリシーにイベント文が含まれていないと、システム ポリシーで可能性のあるイベントがすべて上書きされます。

デフォルト設定

表 7-1 に、EEM パラメータのデフォルト設定を示します。

表 7-1　デフォルトの EEM パラメータ

パラメータ	デフォルト
システム ポリシー	アクティブ

その他の参考資料

EEM の実装に関する詳細情報については、次の項を参照してください。

- 「MIB」（P.7-6）

MIB

MIB	MIB のリンク
• CISCO-EMBEDDED-EVENT-MGR-MIB	MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 http://www.cisco.com/en/US/products/ps5989/prod_technical_reference_list.html

EEM の機能履歴

表 7-2 に、この機能のリリース履歴を示します。Release 3.x 以降のリリースで導入または変更された機能のみが表に記載されています。

表 7-2　EEM の機能履歴

機能名	リリース	機能情報
Embedded Event Manager（EEM）	4.1(3)	Embedded Event Manager（EEM）の設定方法に関する新しい章が追加されました。

CHAPTER 8

RMON の設定

RMON は、各種のネットワーク エージェントおよびコンソール システムがネットワーク モニタリング データを交換できるようにするための、Internet Engineering Task Force（IETF）標準モニタリング仕様です。RMON のアラームとイベントを使用し、Cisco SAN-OS Release 2.0(1b) 以降または Cisco NX-OS Release 4.1(3) 以降のソフトウェアが動作する Cisco MDS 9000 ファミリ スイッチを監視できます。

この章の内容は、次のとおりです。

RMON について

スイッチでは 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。

Cisco MDS 9000 ファミリのすべてのスイッチは、次の RMON 機能（RFC 2819 で定義）をサポートしています。

- アラーム：指定された期間、特定の Management Information Base（MIB; 管理情報ベース）オブジェクトを監視します。MIB オブジェクトの値が指定された値（上昇しきい値）を超えた場合、アラーム状態がセットされ、条件がどれだけ長い時間存在したかにかかわらず 1 つのイベントだけをトリガーします。MIB オブジェクトの値が特定の値（下限しきい値）を下回った場合、アラーム状態がクリアされます。これにより、上昇しきい値を再度超えた場合に、再度アラームがトリガーされます。
- イベント：アラームによってイベントが発生したときのアクションを決定します。アクションは、ログ エントリ、SNMP トラップ、またはその両方を生成できます。

エージェントおよび管理については、『*Cisco MDS 9000 Family MIB Quick Reference*』を参照してください。

SNMP 互換ネットワーク管理ステーションの詳細については、「SNMP の設定」（P.9-1）を参照してください。

ここで説明する内容は、次のとおりです。

RMON 設定情報

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

ヒント　RMON のネットワーク管理機能を活用するために、ネットワーク管理ステーション（NMS）で追加の汎用 RMON コンソール アプリケーションを使用することを推奨します。

Threshold Manager を使用した RMON 設定

スイッチでは 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 を使用するか、Device Manager の Threshold Manager を使用します。

Threshold Monitor では、選択した統計情報が設定されたしきい値を超えた場合に、SNMP イベントをトリガーするか、メッセージをログに取得できます。RMON では、これを上昇しきい値と呼びます。設定可能な内容は次のとおりです。

- 変数：しきい値を設定する統計情報。
- 値：アラームをトリガーする変数の値。この値は、Device Manager が変数を連続して 2 度ポーリングしたときの差分です。
- サンプル：変数の連続する 2 度のポーリングの間のサンプル周期（秒単位）。サンプル周期は、変数が通常の動作状態でしきい値を超えないように選択してください。
- 警告：Device Manager によって使用される、トリガーされたアラームの重大度を示す警告レベル。これは、RMON に対する DCNM-SAN と Device Manager の拡張です。

（注）　任意の種類の RMON アラーム（absolute または delta、rising threshold または falling threshold）を設定するには、[Threshold Manager] ダイアログボックスで [More] をクリックします。これらの高度なアラーム タイプを設定する前に、RMON がこれらの概念を定義する方法について理解しておく必要があります。RMON アラームの設定方法については、RMON-MIB（RFC 2819）を参照してください。

（注）　RMON MIB オブジェクトにアクセスするために、スイッチ上で SNMP を設定することも必要です。

RMON アラーム設定情報

Threshold Manager では、RMON しきい値とアラームを設定する、一般的な MIB オブジェクトのリストが提供されています。アラーム機能は、特定の MIB オブジェクトを指定された間隔でモニタし、指定された値（上昇しきい値）でアラームをトリガーし、別の値（下限しきい値）でアラームをリセットします。

また、任意の MIB オブジェクトにアラームを設定できます。指定する MIB は、標準のドット付き表記（ifInOctets.167772161616777216 の場合、1.3.6.1.2.1.2.2.1.14.16777216 16 16777216）の既存の SNMP MIB でなければなりません。

次のいずれかのオプションを使用して、MIB 変数を監視する間隔（1 ～ 4294967295 秒）を指定します。

- **delta** オプションを使用して、MIB 変数サンプル間の変化をテストします。
- **absolute** オプションを使用して、各 MIB 変数を直接テストします。
- **delta** オプションを使用して、カウンタである任意の MIB オブジェクトをテストします。

rising threshold および **falling threshold** の値の範囲は、-2147483647 ～ 2147483647 です。

注意　**falling threshold** の値には、**rising threshold** よりも小さい値を指定してください。

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。

デフォルト設定

表 8-1 に、スイッチのすべての RMON 機能のデフォルト設定値を示します。

表 8-1　RMON のデフォルト設定値

パラメータ	デフォルト
RMON アラーム	ディセーブル
RMON イベント	ディセーブル

RMON の設定

スイッチでは 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。

ここで説明する内容は、次のとおりです。

ポートごとの RMON アラームのイネーブル化

手順の詳細

1 つ以上のポートに対して RMON アラームを設定するには、次の手順を実行します。

ステップ 1　[Admin] > [Events] > [Threshold Manager] の順に選択し、[FC Interfaces] タブをクリックします。

[Threshold Manager] ダイアログボックスが表示されます。

ステップ 2　[Select] オプション ボタンを選択し、このしきい値アラームに対する個別のポートを選択します。

a. [Selected] フィールドの右にある [...] ボタンをクリックし、すべてのポートを表示します。

b. 監視するポートを選択します。

c. [OK] をクリックして選択内容を受け入れます。

または、適切なオプション ボタンをクリックし、種類（[All] ポート、[xE] ポート、[Fx] ポート）ごとにポートを選択します。

ステップ 3　監視する各変数のチェックボックスをオンにします。

ステップ 4　[Value] カラムにしきい値を入力します。

ステップ 5　サンプリング周期を秒単位で入力します。これは、変数の各スナップショット間の時間です。

ステップ 6　アラームに割り当てる重大度を選択します。[Fatal]、[Warning]、[Critical]、[Error]、[Information] があります。

ステップ 7　[Create] をクリックします。

ステップ 8　システムから重大度イベントを定義するよう求められたら、操作を確定して、アラームとログ イベントを定義します。操作を確定しない場合は、ログ イベントだけが定義されます。

ステップ 9　[More] をクリックし、[Threshold Manager] ダイアログボックスで [Alarms] タブをクリックして、作成したアラームを確認します。

ステップ 10　両方のダイアログボックスのポップアップ ウィンドウを閉じます。

32 ビット アラームと 64 ビット アラームのイネーブル化

手順の詳細

1 つ以上のポートに対して RMON アラームを設定するには、次の手順を実行します。

ステップ 1　[Admin] > [Events] > [Threshold Manager] を選択し、[FC Interfaces] > [Create] タブをクリックします。

32 ビットおよび 64 ビット アラーム作成ダイアログボックスが表示されます。

ステップ 2　[Select] オプション ボタンをクリックし、このしきい値アラームに対する個別のポートを選択します。

a. [Selected] フィールドの右にある [...] ボタンをクリックし、すべてのポートを表示します。

b. 監視するポートを選択します。

c. [OK] をクリックして選択内容を受け入れます。

または、適切なオプション ボタンをクリックし、種類（[All] ポート、[xE] ポート、[Fx] ポート）ごとにポートを選択します。

ステップ 3　監視する各変数のチェックボックスをオンにします。

ステップ 4　[Value] カラムにしきい値を入力します。

ステップ 5　サンプリング周期を秒単位で入力します。これは、変数の各スナップショット間の時間です。

ステップ 6　アラームに割り当てる重大度を選択します。[Fatal]、[Warning]、[Critical]、[Error]、[Information] があります。

ステップ 7　[Create] をクリックします。

ステップ 8　システムから重大度イベントを定義するよう求められたら、操作を確定して、アラームとログ イベントを定義します。操作を確定しない場合は、ログ イベントだけが定義されます。

ステップ 9　[More] をクリックし、[Threshold Manager] ダイアログボックスで [Alarms] タブをクリックして、作成したアラームを確認します。32 ビットおよび 64 ビットのアラームの [Interval] カラムに、間隔が秒単位で表示されます。

ステップ 10　両方のダイアログボックスのポップアップ ウィンドウを閉じます。

RMON アラームの作成

手順の詳細

64 ビット RMON アラームを作成するには、次の手順を実行します。

ステップ 1　[Physical Attributes] ペインから [Events] を展開し、[RMON] を選択します。

64 ビット アラームのダイアログボックスが表示されます。

ステップ 2　[64-bit alarms] タブをクリックします。

ステップ 3　[Create Row] タブをクリックします。[Create Row] ウィンドウが表示されます。

ステップ 4　[Variable] フィールドのドロップダウン メニューで、Threshold Manager によって提供されている MIB 変数の一覧から選択します。

（注）　[Variable] フィールドの入力を完了するには、ドロップダウン リストから選択した変数に加え、ifHCInOctets のように、インターフェイスの詳細を入力する必要があります。

ステップ 5　[32-bit alarms] タブをクリックします。

ステップ 6　[Create Row] タブをクリックします。

ステップ 7　[Variable] フィールドのドロップダウン メニューで、Threshold Manager によって提供されている MIB 変数の一覧から選択します。

ステップ 8　オプション ボタンをクリックして作成する RMON アラームを選択します（32 ビットまたは 64 ビット HC アラーム）。

VSAN に対する 32 ビット RMON アラームのイネーブル化

手順の詳細

1 つ以上の VSAN に対して RMON アラームをイネーブルにするには、次の手順を実行します。

ステップ 1　[Admin] > [Events] > [Threshold Manager] を選択し、[Services] タブをクリックします。

[Threshold Manager] ダイアログボックスが表示されます。

ステップ 2　[Services] タブをクリックします。

[Threshold Manager] ダイアログボックスの [Services] タブに、32 ビット アラームが選択された状態で表示されます。

ステップ 3　[32-bit] オプション ボタンをクリックします。

ステップ 4　[VSAN ID(s)] フィールドに、モニタする VSAN を 1 つまたは複数入力します（複数の VSAN はカンマで区切ります）。選択可能な VSAN のリストを表示するには、下矢印を使用します。

ステップ 5　モニタする変数ごとに [Select] カラムのチェックボックスをオンにします。

ステップ 6　[Value] カラムにしきい値を入力します。

ステップ 7　サンプリング周期を秒単位で入力します。

ステップ 8　アラームに割り当てる重大度を選択します（[Fatal]、[Critical]、[Error]、[Warning]、[Information]）。

ステップ 9　[Create] をクリックします。

ステップ 10　システムから重大度イベントを定義するよう求められたら、操作を確定して、アラームとログ イベントを定義します。

操作を確定しない場合は、ログ イベントだけが定義されます。

ステップ 11　[More] をクリックし、[Threshold Manager] ダイアログボックスの [Alarms] タブをクリックして、作成したアラームを確認します。

物理コンポーネントに対する 32 ビットおよび 64 ビット RMON アラームのイネーブル化

手順の詳細

物理コンポーネントの 64 ビット RMON アラームを設定するには、次の手順を実行します。

ステップ 1　[Admin] > [Events] > [Threshold Manager] を選択し、[Physical] タブをクリックします。

[Threshold Manager] ダイアログボックスの [Physical] タブに、64 ビット アラームが選択された状態で表示されます。

ステップ 2　モニタする変数ごとに [Select] カラムのチェックボックスをオンにします。

ステップ 3　[Value] カラムにしきい値を入力します。

ステップ 4　サンプリング周期を秒単位で入力します。

ステップ 5　アラームに割り当てる重大度を選択します（[Fatal(1)]、[Warning(2)]、[Critical(3)]、[Error(4)]、[Information(5)]）。

ステップ 6　[Create] をクリックします。

ステップ 7　システムから重大度イベントを定義するよう求められたら、操作を確定して、アラームとログ イベントを定義します。

操作を確定しない場合は、ログ イベントだけが定義されます。

ステップ 8　[More] をクリックし、[Threshold Manager] ダイアログボックスの [64-bit Alarms] タブをクリックして、作成したアラームを確認します。

（注）　バックエンド サポートのため、[MaxAlarm] オプションは編集できません。最大 RMON アラームは、CLI では設定できません。

Device Manager の Threshold Manager からの新しい RMON の作成

制約事項

RMON は、スイッチを設定する前に RMON アラームの設定を確認しません。

手順の詳細

Device Manager の Threshold Manager から RMON アラームを設定するには、次の手順を実行します。

ステップ 1　[Events] を展開し、[RMON] を選択し、[Control] タブをクリックします。

[create RMON alarm Threshold Manager] ダイアログボックスが表示されます。

新規アラームの追加が最大アラームを超えた場合、ユーザ エラーのプロンプトが表示されます。

（注）　この機能は、Release 4.1(1b) 以降のスイッチを管理する場合に適用されます。Device Manager は、既存のアラーム番号を、チェック用に必ず 0 として扱います。

RMON イベントの管理

手順の詳細

カスタマイズされた RMON イベントを定義するには、次の手順を実行します。

ステップ 1　[Admin] > [Events] > [Threshold Manager] を選択し、[Threshold Manager] ダイアログボックスで [More] をクリックします。

ステップ 2　[RMON Thresholds] ダイアログボックスで [Events] タブをクリックします。

[RMON Thresholds Events] タブが表示されます。

ステップ 3　[Create] をクリックしてイベント エントリを作成します。

[Create RMON Thresholds Events] ダイアログボックスが表示されます。

ステップ 4　イベントのタイプ（[log]、[snmptrap]、または [logandtrap]）を選択して、RMON しきい値イベントの属性を設定します。

ステップ 5　インデックスを 1 だけ増やします。既存のインデックスを持つイベントを作成しようとすると、エントリ重複のエラー メッセージが表示されます。

ステップ 6　（オプション）説明とコミュニティを指定します。

ステップ 7　[Create] をクリックして、ダイアログボックスを閉じます。

ステップ 8　作成したイベントが [RMON Thresholds] ダイアログボックスのリストに表示されていることを確認します。

ステップ 9　[Close] をクリックして、[RMON Thresholds] ダイアログボックスを閉じます。

RMON アラームの管理

手順の詳細

すでにイネーブルになっているアラームを表示するには、次の手順を実行します。

ステップ 1　[Admin] > [Events] > [Threshold Manager] を選択し、[Threshold Manager] ダイアログボックスで [More] をクリックします。

ステップ 2　[Alarms] タブをクリックします。

[RMON Thresholds] ダイアログボックスが表示されます。

ステップ 3　アラームを削除するには、アラームを選択し、[Delete] をクリックします。

RMON ログの表示

手順の詳細

RMON ログを表示するには、次の手順を実行します。

ステップ 1　[Admin] > [Events] > [Threshold Manager] を選択し、[Threshold Manager] ダイアログボックスで [More] をクリックします。

ステップ 2　[RMON Thresholds] ダイアログボックスで [Log] タブをクリックします。

[RMON Thresholds] の [Log] タブが表示されます。これは、Threshold Manager によってトリガーされた RMON イベントのログです。

RMON のフィールドの説明

ここでは、RMON のフィールドの説明を示します。

RMON しきい値制御

フィールド	説明
AlarmEnable	true の場合、RMON アラーム機能はイネーブルになります。RMON 機能をディセーブルにすると、RMON アラームに関連したポーリングはすべて停止されます。これは、RMON の CPU 使用率が悪影響を及ぼすことがないようにするために、RMON アラーム機能を一時的にディセーブルにする場合にのみ使用します。この機能を永続的にディセーブルにする場合は、alarmTable 内のすべてのエントリを削除することが推奨されます。
MaxAlarms	alarmTable の最大許容エントリ数。

関連トピック

RMON アラーム設定情報

RMON しきい値 64 ビット アラーム

フィールド	説明
Interval	データを上昇しきい値および下限しきい値と比較するためのデータのサンプリング間隔の秒数。deltaValue サンプリングの場合、この変数を設定する際に注意が必要です。サンプリングされた変数が 1 つのサンプリング間隔において 2^31 - 1 を上回る幅で増減することがないように、間隔を十分短く設定する必要があります。
Variable	サンプリングされる変数です。INTEGER（INTEGER、Integer32、Counter32、Counter64、Gauge、または TimeTicks）の ASN.1 プリミティブ型になる変数のみがサンプリングされます。
SampleType	選択された変数のサンプリング方式、およびしきい値と比較される値の計算方式。この値が absoluteValue の場合、選択された変数の値は、サンプリング間隔の終了時にしきい値と直接比較されます。この値が deltaValue の場合、選択された変数の直前のサンプリング値が現在の値から減算され、その差がしきい値と比較されます。
Value	最後のサンプリング期間の統計値。たとえば、サンプル タイプが deltaValue の場合、この値は、その期間の開始時のサンプルと終了時のサンプルの差となります。サンプル タイプが absoluteValue の場合、この値は、その期間の終了時にサンプリングされた値になります。この値が、上昇しきい値および下限しきい値と比較されます。現在のサンプリング期間の値は、その期間が完了すると使用可能になり、次の期間が完了するまで使用できます。
StartupAlarm	このエントリが初めて有効に設定されたときに送信されるアラーム。
Rising Threshold	サンプリングされた統計値に対するしきい値。現在のサンプリング値がこのしきい値以上で、最後のサンプリング期間の値がこのしきい値未満であった場合、単一のイベントが生成されます。
Rising EventId	上昇しきい値を超えたときに使用される eventEntry の ID。

フィールド	説明
Falling Threshold	サンプリングされた統計値に対するしきい値。現在のサンプリング値がこのしきい値以下で、最後のサンプリング期間の値がこのしきい値を超えた場合、単一のイベントが生成されます。
Falling EventId	下限しきい値を下回ったときに使用される eventEntry の ID。このインデックスの値で識別される eventEntry は、そのインデックスと同じ値の eventIndex で識別されるものと同じです。eventTable 内に対応するエントリがない場合、関連付けは存在しません。特に、この値が N/A の場合、N/A は有効なイベント インデックスではないので、関連するイベントが生成されることはありません。
FailedAttempts	アラーム変数がポーリングされ（アクティブ状態）、応答が受信されなかった回数。
Owner	このエントリを設定したユーザの ID。

RMON しきい値 32 ビット アラーム

フィールド	説明
Interval	データを上昇しきい値および下限しきい値と比較するためのデータのサンプリング間隔の秒数。deltaValue サンプリングの場合、この変数を設定する際に注意が必要です。サンプリングされた変数が 1 つのサンプリング間隔において 2^31 - 1 を上回る幅で増減することがないように、間隔を十分短く設定する必要があります。
Variable	サンプリングされる変数です。INTEGER（INTEGER、Integer32、Counter32、Counter64、Gauge、または TimeTicks）の ASN.1 プリミティブ型になる変数のみがサンプリングされます。
SampleType	選択された変数のサンプリング方式、およびしきい値と比較される値の計算方式。
Value	最後のサンプリング期間の統計値。
StartupAlarm	このエントリが初めて有効に設定されたときに送信されるアラーム。
Rising Threshold	サンプリングされた統計値に対するしきい値。現在のサンプリング値がこのしきい値以上で、最後のサンプリング期間の値がこのしきい値未満であった場合、単一のイベントが生成されます。
Rising EventId	上昇しきい値を超えたときに使用される eventEntry の ID。
Falling Threshold	サンプリングされた統計値に対するしきい値。現在のサンプリング値がこのしきい値以下で、最後のサンプリング期間の値がこのしきい値を超えた場合、単一のイベントが生成されます。
Falling EventId	下限しきい値を下回ったときに使用される eventEntry の ID。
FailedAttempts	アラーム変数がポーリングされ（アクティブ状態）、応答が受信されなかった回数。
Owner	このエントリを設定したユーザの ID。

RMON しきい値イベント

フィールド	説明
Description	このイベント エントリを説明しているコメント。
Type	プローブがこのイベントに関して行う通知のタイプ。ログの場合、イベントごとにエントリがログ テーブルに作成されます。SNMP トラップの場合、SNMP トラップが 1 つ以上の管理ステーションに送信されます。
LastTimeSent	このイベント エントリによりイベントが最後に送信された時刻。このエントリがイベントを 1 つも生成していない場合、この値は N/A になります。
Owner	このエントリを設定したエンティティ。このエントリに割り当てられたリソースを使用します。

RMON しきい値ログ

フィールド	説明
Time	このログ エントリが作成された時刻。
Description	このログ エントリをアクティブにしたイベントの説明。

その他の参考資料

RMON の実装に関する詳細情報については、次の項を参照してください。

- 「MIB」（P.8-11）

MIB

MIB	MIB のリンク
• CISCO-RMON-CAPABILITY.my • CISCO-RMON-CONFIG-CAPABILITY.my • CISCO-RMON-CONFIG-MIB	MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 http://www.cisco.com/en/US/products/ps5989/prod_technical_reference_list.html

RMON の機能履歴

表 8-2 に、この機能のリリース履歴を示します。Release 3.x 以降のリリースで導入または変更された機能のみが表に記載されています。

表 8-2　RMON の機能履歴

機能名	リリース	機能情報
RMON 32 ビットおよび 64 ビット アラームの設定	3.4(1)	RMON の [32 Alarm] タブおよび [64 bit Alarm] タブ RMON 32 ビットおよび 64 ビット アラームを設定するための新規タブが追加されました。
RMON 32 ビットおよび 64 ビット アラームの設定	4.1(1a)	RMON の [32 Alarm] タブおよび [64 bit Alarm] タブ RMON 32 ビットおよび 64 ビット アラームを設定するための新規タブが追加されました。

CHAPTER 9

SNMP の設定

CLI と SNMP は、Cisco MDS 9000 ファミリのすべてのスイッチで共通のロールを使用します。SNMP を使用して CLI で作成したロールを変更したり、その逆を行うことができます。

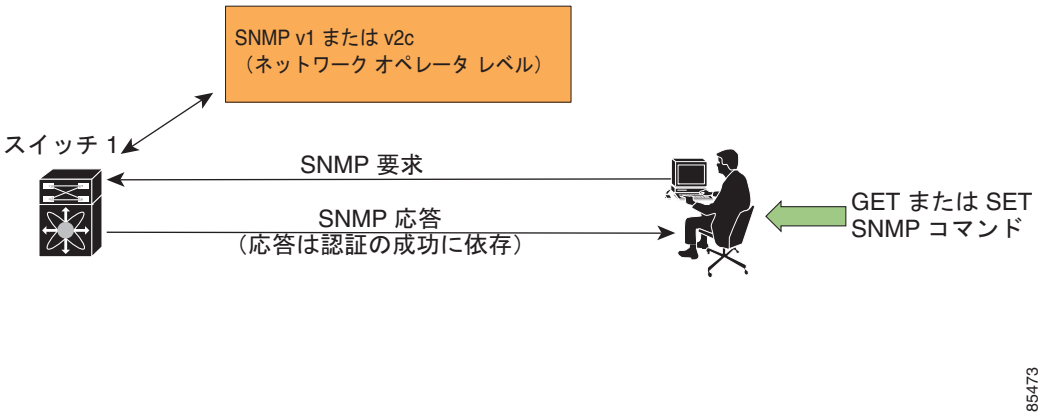
CLI ユーザと SNMP ユーザのユーザ、パスワード、ロールは、すべて同じです。CLI を通じて設定されたユーザは SNMP（たとえば、DCNM-SAN や Device Manager）を使用してスイッチにアクセスでき、その逆も可能です。

この章の内容は、次のとおりです。

SNMP セキュリティについて

SNMP は、ネットワーク デバイス間での管理情報の交換を容易にするアプリケーション層プロトコルです。すべての Cisco MDS 9000 ファミリ スイッチで、SNMPv1、SNMPv2c、および SNMPv3 の 3 つの SNMP バージョンが使用できます（図 9-1 を参照）。

図 9-1　SNMP セキュリティ



ここで説明する内容は、次のとおりです。

SNMP バージョン 1 およびバージョン 2c

SNMP バージョン 1（SNMPv1）および SNMP バージョン 2c（SNMPv2c）は、コミュニティ ストリングを使用してユーザ認証を行います。コミュニティ ストリングは、SNMP の初期のバージョンで使用されていた弱いアクセス コントロール方式です。SNMPv3 は、強力な認証を使用することによってアクセス コントロールを大幅に改善しています。したがって、SNMPv3 がサポートされている場合は、SNMPv1 および SNMPv2c に優先して使用してください。

SNMP バージョン 3

SNMP バージョン 3（SNMPv3）は、ネットワーク管理のための相互運用可能な標準ベースのプロトコルです。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 で提供され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。

SNMPv3 CLI のユーザ管理および AAA の統合

Cisco NX-OS ソフトウェアは RFC 3414 と RFC 3415 を実装しています。これには、User-based Security Model（USM; ユーザベース セキュリティ モデル）とロール ベースのアクセス コントロールが含まれています。SNMP と CLI のロール管理は共通化されており、同じ証明書とアクセス権限を共有しますが、以前のリリースではローカル ユーザ データベースは同期化されませんでした。

SNMPv3 のユーザ管理を AAA サーバ レベルで一元化できます。ユーザ管理を一元化すると、Cisco MDS スイッチ上で稼動する SNMP エージェントが 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。また、AAA サーバにはユーザ グループ名も格納されます。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。

CLI および SNMP のユーザ同期

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。

ユーザの同期化は、次のように処理されます。

- いずれかのコマンドを使用してユーザを削除すると、SNMP と CLI の両方の該当ユーザが削除されます。
- 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。

（注） パスフレーズ/パスワードをローカライズド キー/暗号化形式で指定すると、パスワードは同期化されません。

（注） 3.0(1) からは、DCNM-SAN に対して作成された一時的 SNMP ログインは 24 時間ではなく、1 時間になりました。

- 既存の SNMP ユーザは、特に変更しなくても、引き続き auth および priv のパスフレーズを維持できます。
- 管理ステーションが usmUserTable 内に SNMP ユーザを作成する場合、対応する CLI ユーザはパスワードなし（ログインは無効）で作成され、network-operator のロールが付与されます。

スイッチ アクセスの制限

IP アクセス コントロール リスト（IP-ACL）を使用して、Cisco MDS 9000 ファミリ スイッチへのアクセスを制限できます。

グループベースの SNMP アクセス

（注）　グループが業界全体で使用されている標準 SNMP 用語なので、この SNMP の項では、ロールのことをグループと言います。

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

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

ユーザの作成および変更

SNMP、DCNM-SAN、または CLI を使用して、ユーザの作成、または既存のユーザの変更を実行できます。

- SNMP：スイッチ上の usmUserTable に存在するユーザのクローンとして、新規のユーザを作成します。ユーザを作成した後、クローンの秘密キーを変更してから、そのユーザをアクティブにします。RFC 2574 を参照してください。
- DCNM-SAN。
- CLI：**snmp-server user** コマンドを使用して、ユーザの作成または既存のユーザの変更を実行します。

Cisco MDS 9000 ファミリ スイッチ上で使用できるロールは、network-operator および network-admin です。GUI（DCNM-SAN および Device Manager）を使用する場合は、default-role もあります。また、Common Roles データベースに設定されている任意のロールも使用できます。

ヒント　CLI セキュリティ データベースおよび SNMP ユーザ データベースに対する更新はすべて同期化されます。SNMP パスワードを使用して、DCNM-SAN または Device Manager のいずれかにログインできます。ただし、CLI パスワードを使用して DCNM-SAN または Device Manager にログインした場合、その後のログインには必ず CLI パスワードを使用する必要があります。Cisco MDS SAN-OS Release 2.0(1b) にアップグレードする前から SNMP データベースと CLI データベースの両方に存在しているユーザの場合、アップグレードすると、そのユーザに割り当てられるロールは両方のロールを結合したものになります。

AES 暗号ベースの機密保全

Advanced Encryption Standard（AES）は対称暗号アルゴリズムです。Cisco NX-OS ソフトウェアは、SNMP メッセージ暗号化用のプライバシー プロトコルの 1 つとして AES を使用し、RFC 3826 に準拠しています。

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 を指定して、SNMP PDU を暗号化する必要があります。

SNMP 通知のイネーブル化

通知（トラップおよびインフォーム）は、特定のイベントが発生したときにスイッチによって生成されるシステム アラートです。通知をイネーブルまたはディセーブルにできます。デフォルトでは、通知は 1 つも定義されておらず、通知が生成されることはありません。通知名を指定しないと、すべての通知が無効または有効になります。

SNMP 中央インフラ機能では、イネーブルまたはディセーブルにする必要のあるトラップを追加できます。MIB ブラウザを使用して通知の生成を制御できるようにするために、MIB CISCO-NOTIFICATION-CONTROL-MIB がサポートされています。

スイッチの LinkUp/LinkDown 通知

スイッチに対して、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：インターフェイスに対して ifLinkUpDownTrapEnable（IF-MIB で定義）がイネーブルになっている場合、そのインターフェイスについて CISCO-IF-EXTENSION-MIB.my で定義された通知（cieLinkUp、cieLinkDown）のみが送信されます。
- IETF：インターフェイスに対して ifLinkUpDownTrapEnable（IF-MIB で定義）がイネーブルになっている場合、そのインターフェイスについて IF-MIB で定義された通知（LinkUp、LinkDown）のみが送信されます。通知定義で定義された変数バインドのみが、それらの通知とともに送信されます。
- IEFT extended：インターフェイスに対して ifLinkUpDownTrapEnable（IF-MIB で定義）がイネーブルになっている場合、そのインターフェイスについて IF-MIB で定義された通知（LinkUp、LinkDown）のみが送信されます。通知定義で定義された変数バインドに加え、シスコの実装に固有の IF-MIB で定義された変数バインドも送信されます。これがデフォルト設定です。
- IEFT Cisco：インターフェイスに対して ifLinkUpDownTrapEnable（IF-MIB で定義）がイネーブルになっている場合、そのインターフェイスについて IF-MIB で定義された通知（LinkUp、LinkDown）および CISCO-IF-EXTENSION-MIB.my で定義された通知（cieLinkUp、cieLinkDown）のみが送信されます。通知定義で定義された変数バインドのみが、linkUp 通知や linkDown 通知とともに送信されます。
- IEFT extended Cisco：インターフェイスに対して ifLinkUpDownTrapEnable（IF-MIB で定義）がイネーブルになっている場合、そのインターフェイスについて IF-MIB で定義された通知（LinkUp、LinkDown）および CISCO-IF-EXTENSION-MIB.my で定義された通知（cieLinkUp、cieLinkDown）のみが送信されます。linkUp と linkDown の通知定義で定義された変数バインドに加え、シスコの実装に固有の IF-MIB で定義された変数バインドも LinkUp 通知や LinkDown 通知とともに送信されます。

（注）　シスコの実装に固有の IF-MIB で定義される変数バインドの詳細については、『*Cisco MDS 9000 Family MIB Quick Reference*』を参照してください。

LinkUp および LinkDown トラップ設定の範囲

インターフェイスに対する LinkUp および LinkDown トラップ設定は、次の範囲に基づいてトラップを生成します。

スイッチレベルのトラップ設定	インターフェイスレベルのトラップ設定	インターフェイス リンクについて生成されるトラップか？
イネーブル（デフォルト）	イネーブル（デフォルト）	Yes
イネーブル	ディセーブル	No
ディセーブル	イネーブル	No
ディセーブル	ディセーブル	No

デフォルト設定

表 9-1 に、すべてのスイッチの SNMP 機能のデフォルト設定を示します。

表 9-1　SNMP のデフォルト設定

パラメータ	デフォルト
ユーザ アカウント	有効期限なし（設定されていない場合）
パスワード	なし

SNMP の設定

SNMP は、ネットワーク デバイス間での管理情報の交換を容易にするアプリケーション層プロトコルです。

ここで説明する内容は、次のとおりです。

- 「SNMPv3 ユーザの複数のロールへの割り当て」（P.9-8）
- 「SNMPv3 メッセージ暗号化の適用」（P.9-7）
- 「SNMPv3 ユーザの複数のロールへの割り当て」（P.9-8）
- 「コミュニティの追加または削除」（P.9-8）
- 「コミュニティ ストリングの削除」（P.9-9）

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。

手順の詳細

連絡先および場所の情報を設定するには、次の手順を実行します。

ステップ 1　[Physical Attributes] ペインの [Switches] を展開します。

[Information] ペインにスイッチの設定が表示されます。

ステップ 2　各スイッチの [Location] フィールドと [Contact] フィールドに値を設定します。

ステップ 3　これらの変更を保存する場合は、[Apply Changes] をクリックします。保存されていない変更を廃棄する場合は、[Undo Changes] をクリックします。

SNMPv3 メッセージ暗号化の適用

デフォルトでは、SNMP エージェントは、auth キーと priv キーを使用したユーザ設定の SNMPv3 メッセージ暗号化を使用する。SNMPv3 メッセージの authNoPriv および authPriv の securityLevel パラメータを許可します。

手順の詳細

ユーザのメッセージ暗号化を適用するには、次の手順を実行します。

ステップ 1　[Physical Attributes] ペインから [Switches] を展開し、[Security] を展開し、[Users and Roles] を選択します。

ステップ 2　[Information] ペインで [Users] タブをクリックしてユーザのリストを表示します。

ステップ 3　[Create Row] をクリックします。

[Create Users] ダイアログボックスが表示されます。

ステップ 4　[New User] フィールドにユーザ名を入力します。

ステップ 5　[Role] ドロップダウン メニューからロールを選択します。ドロップダウン メニューから選択しない場合は、フィールドに新しいロール名を入力できます。その場合、前に戻ってこのロールを適切に設定する必要があります。

ステップ 6　[Password] フィールドにユーザのパスワードを入力します。

ステップ 7　[Privacy] タブをクリックします。

ステップ 8　[Enforce SNMP Privacy Encryption] チェックボックスにチェックを入れて、管理用トラフィックを暗号化します。

ステップ 9　[Create] をクリックして新しいエントリを作成します。

SNMPv3 メッセージ暗号化をすべてのユーザに対してグローバルに適用するには、次の手順を実行します。

ステップ 1　[Logical Domains] ペインで [VSAN] を選択します。この操作は、[All VSANS] を選択する場合は実行できません。

ステップ 2　[Physical Attributes] ペインで [Switches] を展開し、[Security] を展開し、[Users and Roles] を選択します。[Information] ペインで [Global] タブをクリックします。

ステップ 3　[GlobalEnforcePriv] チェックボックスをオンにします。

ステップ 4　[Apply Changes] アイコンをクリックして、これらの変更を保存します。

SNMPv3 ユーザの複数のロールへの割り当て

SNMP サーバのユーザ設定が強化され、SNMPv3 ユーザに複数のロール（グループ）を割り当てることが可能になっています。最初に SNMPv3 ユーザを作成した後で、そのユーザにロールを追加できます。

制約事項

- 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。

手順の詳細

複数のロールを新しいユーザに追加するには、次の手順を実行します。

ステップ 1　[Physical Attributes] ペインから [Switches] を展開し、[Security] を展開し、[Users and Roles] を選択します。

ステップ 2　[Information] ペインで [Users] タブをクリックしてユーザのリストを表示します。

ステップ 3　[Create Row] をクリックします。

[Create Users] ダイアログボックスが表示されます。

ステップ 4　チェックボックスを使用してロールを選択します。

ステップ 5　[Digest] と [Encryption] のそれぞれのオプションを選択します。

ステップ 6　（オプション）ユーザの有効期限と、SSH キーのファイル名を入力します。

ステップ 7　[Create] をクリックして新しいロールを作成します。

コミュニティの追加または削除

SNMPv1 および SNMPv2 のユーザの場合は、読み取り専用または読み取り / 書き込みアクセスを設定できます。RFC 2576 を参照してください。

手順の詳細

SNMPv1 または SNMPv2c のコミュニティ ストリングを作成するには、次の手順を実行します。

ステップ 1　[Physical Attributes] ペインから [Switches] を展開し、[Security] を展開し、[Users and Roles] を選択します。

ステップ 2　[Information] ペインで [Communities] タブをクリックします。

既存のコミュニティが表示されます。

ステップ 3　[Create Row] をクリックします。

[Create Community String] ダイアログボックスが表示されます。

ステップ 4　[Switch] のチェックボックスをオンにし、1 つ以上のスイッチを指定します。

ステップ 5　[Community] フィールドにコミュニティ名を入力します。

ステップ 6　[Role] ドロップダウン リストからロールを選択します。

（注）　ドロップダウン リストから選択しない場合は、フィールドに新しいロール名を入力できます。その場合、前に戻ってこのロールを適切に設定する必要があります。

ステップ 7　[Create] をクリックして新しいエントリを作成します。

コミュニティ ストリングの削除

手順の詳細

コミュニティ ストリングを削除するには、次の手順を実行します。

ステップ 1　[Physical Attributes] ペインから [Switches] を展開し、[Security] を展開し、[Users and Roles] を選択します。

ステップ 2　[Information] ペインで [Communities] タブをクリックします。

ステップ 3　削除するコミュニティの名前をクリックします。

ステップ 4　[Delete Row] をクリックしてこのコミュニティを削除します。

SNMP トラップとインフォーム通知の設定

特定のイベントが発生したときに SNMP マネージャに通知を送信するように Cisco MDS スイッチを設定できます。

（注）　SNMP 設定で RMON トラップをイネーブルにする必要があります。詳細については、「RMON の設定」（P.8-1）を参照してください。

（注）　通知をトラップまたはインフォームとして送信する宛先の詳細情報を入手するには、SNMP-TARGET-MIB を使用します。詳細については、『*Cisco MDS 9000 Family MIB Quick Reference*』を参照してください。

ここで説明する内容は、次のとおりです。

SNMPv2c 通知の設定

手順の詳細

SNMPv2c 通知を設定するには、次の手順を実行します。

ステップ 1　[Physical Attributes] ペインで [Events] を展開し、[SNMP Traps] を選択します。
[Information] ペインに SNMP 通知の設定が表示されます。

ステップ 2　[Destinations] タブをクリックして、SNMP 通知の宛先を追加または変更します。

ステップ 3　[Create Row] をクリックして、新しい通知先を作成します。
[Create Destinations] ダイアログボックスが表示されます。

ステップ 4　新しい宛先を設定するスイッチをオンにします。

ステップ 5　宛先の IP アドレスと UDP ポートを設定します。

ステップ 6　[trap] または [inform] オプション ボタンを選択します。

ステップ 7　（オプション）タイムアウトまたはリトライ回数の値を設定します。

ステップ 8　[Create] をクリックして、選択したスイッチにこの宛先を追加します。

ステップ 9　（オプション）[Other] タブをクリックして、特定の通知タイプをスイッチごとにイネーブルにします。

ステップ 10　[Apply Changes] アイコンをクリックして、エントリを作成します。

（注）　スイッチは、イベント（SNMP トラップおよびインフォーム）を、最大 10 件の宛先に転送できます。

SNMPv3 通知の設定

手順の詳細

SNMPv3 通知を設定するには、次の手順を実行します。

ステップ 1　[Create Destinations] ダイアログボックスで [Security] ドロップダウン リストから [v3] を選択します。

ステップ 2　（オプション）インフォームのタイムアウトとリトライの値を設定します。

ステップ 3　[Create] をクリックして、選択したスイッチにこの宛先を追加します。

（注）　SNMPv3 通知の場合、SNMP マネージャは、SNMP メッセージを認証および復号化するために、スイッチの engineID に基づくユーザ資格情報（authKey/PrivKey）を知っていることが期待されます。

SNMP 通知のイネーブル化

表 9-2 に、DCNM-SAN で Cisco NX-OS MIB の通知をイネーブルにする手順を示します。

[Events] > [SNMP Traps] を展開して、この表に一覧されているチェックボックスを表示します。

（注）　[Events] > [SNMP Traps] を選択すると、SNMP 通知をどのように設定したかに応じて、トラップとインフォームの両方がイネーブルになります。「SNMPv3 通知の設定」（P.9-10）で表示される通知を参照してください。

表 9-2　SNMP 通知のイネーブル化

MIB	DCNM-SAN チェックボックス
CISCO-ENTITY-FRU-CONTROL-MIB	[Other] タブをクリックし、[FRU Changes] をオンにします。
CISCO-FCC-MIB	[Other] タブをクリックし、[FCC] をオンにします。
CISCO-DM-MIB	[FC] タブをクリックし、[Domain Mgr RCF] をオンにします。
CISCO-NS-MIB	[FC] タブをクリックし、[Name Server] をオンにします。
CISCO-FCS-MIB	[Other] タブをクリックし、[FCS Rejects] をオンにします。
CISCO-FDMI-MIB	[Other] タブをクリックし、[FDMI] をオンにします。
CISCO-FSPF-MIB	[FC] タブをクリックし、[FSPF Neighbor Change] をオンにします。
CISCO-LICENSE-MGR-MIB	[Other] タブをクリックし、[License Manager] をオンにします。
CISCO-IPSEC-SIGNALLING-MIB	[Other] タブをクリックし、[IPSEC] をオンにします。
CISCO-PSM-MIB	[Other] タブをクリックし、[Port Security] をオンにします。
CISCO-RSCN-MIB	[FC] タブをクリックし、[RSCN ILS] と [RCSN ELS] をオンにします。
SNMPv2-MIB	[Other] タブをクリックし、[SNMP AuthFailure] をオンにします。
VRRP-MIB, CISCO-IETF-VRRP-MIB	[Other] タブをクリックし、[VRRP] をオンにします。
CISCO-ZS-MIB	[FC] タブをクリックし、[Zone Rejects]、[Zone Merge Failures]、[Zone Merge Successes]、[Zone Default Policy Change]、および [Zone Unsuppd Mode] をオンにします。

次の通知はデフォルトでイネーブルになっています。

- entity fru
- license
- link ietf-extended

他の通知はすべて、デフォルトではディセーブルです。

手順の詳細

個々の通知をイネーブルにするには、次の手順を実行します。

ステップ 1　[Physical Attributes] ペインで [Events] を展開し、[SNMP Traps] を選択します。

[Information] ペインに SNMP 通知の設定が表示されます。

ステップ 2　[FC] タブをクリックして、ファイバ チャネル関連の通知をイネーブルにします。

ステップ 3　イネーブルにする各通知のチェックボックスをオンにします。

ステップ 4　[Other] タブをクリックしてその他の通知をイネーブルにします。

ステップ 5　イネーブルにする各通知のチェックボックスをオンにします。

ステップ 6　[Control] タブをクリックし、通知に該当する変数をイネーブルにします。

NX-OS Release 4.2(1) から、通知制御機能のための [Control] タブが利用できるようになりました。この機能を使用すると、通知に該当するすべての変数を、SNMP を通じてイネーブルまたはディセーブルにできます。

[Control] タブは、NX-OS Release 4.2(1) 以降でだけ使用できます。

ステップ 7　イネーブルにする各通知のチェックボックスをオンにします。

ステップ 8　[Apply Changes] アイコンをクリックして、エントリを作成します。

（注）　Device Manager で、**no snmp-server enable traps link** コマンドを実行すると、スイッチでリンク トラップの生成がディセーブルになりますが、個々のインターフェイスでリンク トラップがイネーブルになっている可能性があります。

Device Manager を使用して個々の通知をイネーブルにするには、次の手順を実行します。

ステップ 1　[Admin] > [Events] の順に展開し、[Filters] を選択します。

スイッチによってデータが設定されたテーブルがイベント フィルタ ウィンドウに表示されます。

ステップ 2　[Control] タブをクリックし、通知に該当する変数をイネーブルにします。

NX-OS Release 4.2(1) から、通知制御機能のための [Control] タブが利用できるようになりました。この機能を使用すると、通知に該当するすべての変数を、SNMP を通じてイネーブルまたはディセーブルにできます。

（注）　[Control] タブは、NX-OS Release 4.2(1) 以降でだけ使用できます。

ステップ 3　イネーブルにする各通知のチェックボックスをオンにします。

ステップ 4　[Apply Changes] アイコンをクリックして、エントリを作成します。

通知対象ユーザの設定

SNMPv3 インフォーム通知を SNMP マネージャに送信するには、スイッチ上で通知対象ユーザを設定する必要があります。

SNMP マネージャは、受信した INFORM PDU を認証および復号化するために、同じユーザ資格情報をユーザのローカル設定データ ストアに持っている必要があります。

通知対象ユーザの設定については『*Cisco MDS 9000 Family NX-OS System Management Configuration Guide*』を参照してください。

インターフェイスの Up/Down SNMP リンクステート トラップの設定

デフォルトでは、SNMP リンクステート トラップがすべてのインターフェイスに対してイネーブルになっています。リンクの状態が Up と Down の間で切り替わるたびに、SNMP トラップが生成されます。

何百ものインターフェイスを装備したスイッチが多数存在し、それらの多くでリンクの状態をモニタする必要がない場合があります。そのような場合には、リンクステート トラップをディセーブルにすることも選択できます。

イベント セキュリティの設定

SNMP イベントは、SNMP メッセージと同じ方法で傍受や盗聴から保護できます。DCNM-SAN または Device Manager では、スイッチが生成する SNMP イベントのメッセージ処理モデル、セキュリティ モデル、セキュリティ レベルを設定できます。

制約事項

- これは高度な機能であるため、SNMPv3 の経験が豊富な管理者だけが使用することをお勧めします。

手順の詳細

SNMP イベント セキュリティを設定するには、次の手順を実行します。

ステップ 1　[Events] を展開し、[SNMP Traps] を選択します。

ステップ 2　[Information] ペインで [Security] タブをクリックします。

SNMP 通知のセキュリティ情報が表示されます。

ステップ 3　メッセージ プロトコル モデル（MPModel）、セキュリティ モデル、セキュリティ名、およびセキュリティ レベルを設定します。

ステップ 4　[Apply Changes] アイコンをクリックし、変更を保存して適用します。

SNMP イベント ログの表示

前提条件

- イベント ログを表示する前に、MDS Syslog マネージャをセットアップする必要があります。

制約事項

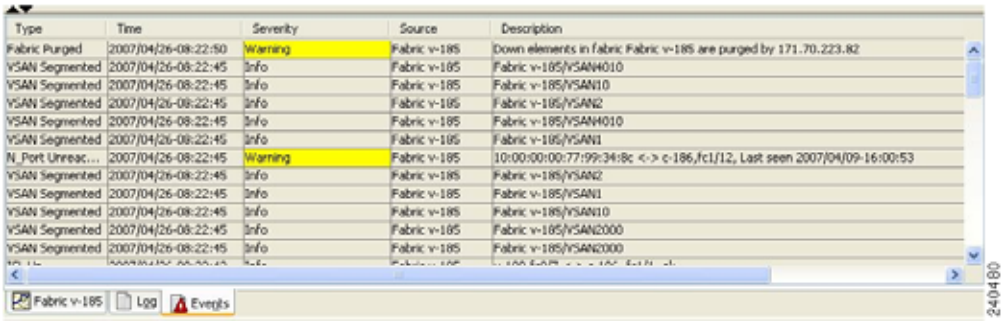
- これらの値を別の DCNM-SAN ワークステーションから同時に変更すると、予測できない結果が生じるおそれがあります。

手順の詳細

DCNM-SAN から SNMP イベント ログを表示するには、[Events] タブをクリックします。

[Events] に、単一のスイッチのイベント ログの一覧が表示されます（図 9-2 を参照）。

図 9-2　　イベント情報



SNMP のフィールドの説明

ここでは、SNMP のフィールドの説明を示します。

IP 統計情報 SNMP

フィールド	説明
BadVersions	SNMP プロトコル エンティティに配信され、未サポートの SNMP バージョン用だった SNMP メッセージの合計数。
BadCommunityNames	認識されない SNMP コミュニティ名を使用している SNMP エンティティに配信された SNMP メッセージの合計数。
BadCommunityUses	SNMP エンティティに配信され、指定された名前の SNMP コミュニティで許可されていない SNMP 処理を示していた SNMP メッセージの合計数。
ASNParseErrs	受信した SNMP メッセージをデコードするときに、SNMP エンティティで発生した ASN.1 エラーまたは BER エラーの合計数。

フィールド	説明
TooBigs	SNMP プロトコル エンティティに配信され、エラーステータス フィールドの値が tooBig だった SNMP PDU の合計数。
SilentDrops	SNMP エンティティに配信され、空の変数バインディング フィールドを持つ別の Response-PDU を格納した応答のサイズがローカルな制約または要求の送信元に関連付けられた最大メッセージ サイズよりも大きかったため自動的にドロップされた、GetRequest-PDU、GetNextRequest-PDU、GetBulkRequest-PDU、SetRequest-PDU、および InformRequest-PDU の合計数。
ProxyDrops	SNMP エンティティに配信され、返信できた Response-PDU がなかった状態（タイムアウトを除く）でプロキシ ターゲットへのメッセージ（変換されたものを含む）の送信に失敗したため自動的にドロップされた、GetRequest-PDU、GetNextRequest-PDU、GetBulkRequest-PDU、SetRequest-PDU、および InformRequest-PDU の合計数。
NoSuchNames	SNMP プロトコル エンティティに配信され、エラーステータス フィールドの値が noSuchName だった SNMP PDU の合計数。
BadValues	SNMP プロトコル エンティティに配信され、エラーステータス フィールドの値が badValue だった SNMP PDU の合計数。
ReadOnlys	SNMP プロトコル エンティティに配信され、エラーステータス フィールドの値が readOnly だった有効な SNMP PDU の合計数。エラーステータス フィールドに値 readOnly が格納された SNMP PDU を生成することは、SNMP の誤った実装を検出する手段として提供されているので、これはプロトコル エラーであることを意味します。
GenErrs	SNMP プロトコル エンティティに配信され、エラーステータス フィールドの値が genErr だった SNMP PDU の合計数。
Pkts	転送サービスから SNMP エンティティに配信されたメッセージの合計数。
GetRequests	SNMP プロトコル エンティティによって受け入れられ、処理された SNMP Get-Request PDU の合計数。
GetNexts	SNMP プロトコル エンティティによって受け入れられ、処理された SNMP Get-Next PDU の合計数。
SetRequests	SNMP プロトコル エンティティによって受け入れられ、処理された SNMP Set-Request PDU の合計数。
OutTraps	SNMP プロトコル エンティティによって生成された SNMP Trap PDU の合計数。
OutGetResponses	SNMP プロトコル エンティティによって生成された SNMP Get-Response PDU の合計数。
OutPkts	SNMP プロトコル エンティティから転送サービスに渡された SNMP メッセージの合計数。
TotalReqVars	有効な SNMP Get-Request PDU と Get-Next PDU を受信した結果として、SNMP プロトコル エンティティによって正常に取得された MIB オブジェクトの合計数。
TotalSetVars	有効な SNMP Set-Request PDU を受信した結果として、SNMP プロトコル エンティティによって正常に変更された MIB オブジェクトの合計数。

SNMP セキュリティ ユーザ

フィールド	説明
Role	セキュリティ モデルに依存しない形式でのユーザ。
Password	一般ユーザのパスワード。SNMP の場合、このパスワードは、認証と機密保全の両方に使用されます。CLI と XML の場合、認証のみに使用されます。
Digest	使用されるダイジェスト認証プロトコルのタイプ。
Encryption	使用される暗号化認証プロトコルのタイプ。
ExpiryDate	このユーザの有効期限が切れる日付。
SSH Key File Configured	ユーザが SSH 公開キーで設定されているかどうかを指定します。
SSH Key File	SSH 公開キーを保管しているファイルの名前。SSH 公開キーは、このユーザの SSH セッションを認証するために使用されます。これは、CLI ユーザに対してのみ適用されます。形式は次のいずれかになります。 • OpenSSH 形式の SSH 公開キー • IETF SECSH（商用の SSH 公開キー形式）の SSH 公開キー • 公開キーの抽出元となる PEM（Privacy-Enhanced Mail 形式）の SSH クライアント証明書 • 証明書ベースの認証用の SSH クライアント証明書 DN（識別名）
Creation Type	ユーザのクレデンシャル ストアのタイプ。ユーザによってこのテーブルに行が作成されると、デバイスに対してローカルなクレデンシャル ストアにユーザ エントリが作成されます。AAA サーバ ベースの認証などのリモート認証メカニズムの場合、資格情報は他の（リモートの）システムまたはデバイスに保管されます。
Expiry Date	このユーザの有効期限が切れる日付。

関連トピック

SNMP の設定

SNMP セキュリティ コミュニティ

フィールド	説明
Community	コミュニティ ストリング。
Role	セキュリティ モデル名。

関連トピック

コミュニティの追加または削除

コミュニティ ストリングの削除

セキュリティ ユーザ グローバル

フィールド	説明
Enforce SNMP Privacy Encryption	SNMP エージェントにより、SNMPv3 メッセージに対する暗号化の使用がシステム内のすべてのユーザに対してグローバルに適用されるかどうかを指定します。
Cache Timeout	これにより、ローカル システム内でユーザ資格情報をキャッシュするための最大タイムアウト値が指定されます。

（注）　管理者が Device Manager で新しいユーザを作成する場合または既存のユーザを削除する場合、プライバシー パスワードと認証パスワードが必要です。ただし、新しいユーザの作成時に管理者がこれらの資格情報を入力しなくても、Device Manager は、管理者の認証パスワードをプライバシー パスワードとして使用します。ユーザに対して定義されたプライバシー プロトコルが DES（デフォルト）ではない場合、MDS 内の SNMP エージェントはパケットを復号化できなくなり、SNMP エージェントはタイムアウトします。ユーザに対して定義されたプライバシー プロトコルが DES ではない場合、ユーザがログイン時にプライバシー パスワードとプロトコルの両方を入力する必要があります。

その他の参考資料

SNMP の実装に関する詳細情報については、次の各項を参照してください。

- 「MIB」（P.9-17）

MIB

MIB	MIB のリンク
• CISCO-SNMP-TARGET-EXT-MIB • CISCO-SNMP-VACM-EXT-MIB	MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 http://www.cisco.com/en/US/products/ps5989/prod_technical_reference_list.html

SNMP の機能履歴

表 9-3 に、この機能のリリース履歴を示します。Release 3.x 以降のリリースで導入または変更された機能のみが表に記載されています。

表 9-3　SNMP の機能履歴

機能名	リリース	機能情報
[SNMP Trap] の [Control] タブ	4.2(1)	NX-OS Release 4.2(1) で追加された新しい [Control] タブの詳細を追加。

CHAPTER 10

ドメイン パラメータの設定

Fibre Channel domain（fcdomain; ファイバ チャネル ドメイン）機能では、FC-SW-2 標準で記述されているように、主要スイッチ選択、ドメイン ID 配信、FC ID 割り当て、ファブリック再設定機能が実行されます。

この章の内容は、次のとおりです。

ファイバ チャネル ドメインについて

Fibre Channel domain（fcdomain; ファイバ チャネル ドメイン）機能では、FC-SW-2 標準で記述されているように、主要スイッチ選択、ドメイン ID 配信、FC ID 割り当て、ファブリック再設定機能が実行されます。ドメインは VSAN 単位で設定されます。ドメイン ID を設定しない場合、ローカル スイッチはランダムな ID を使用します。

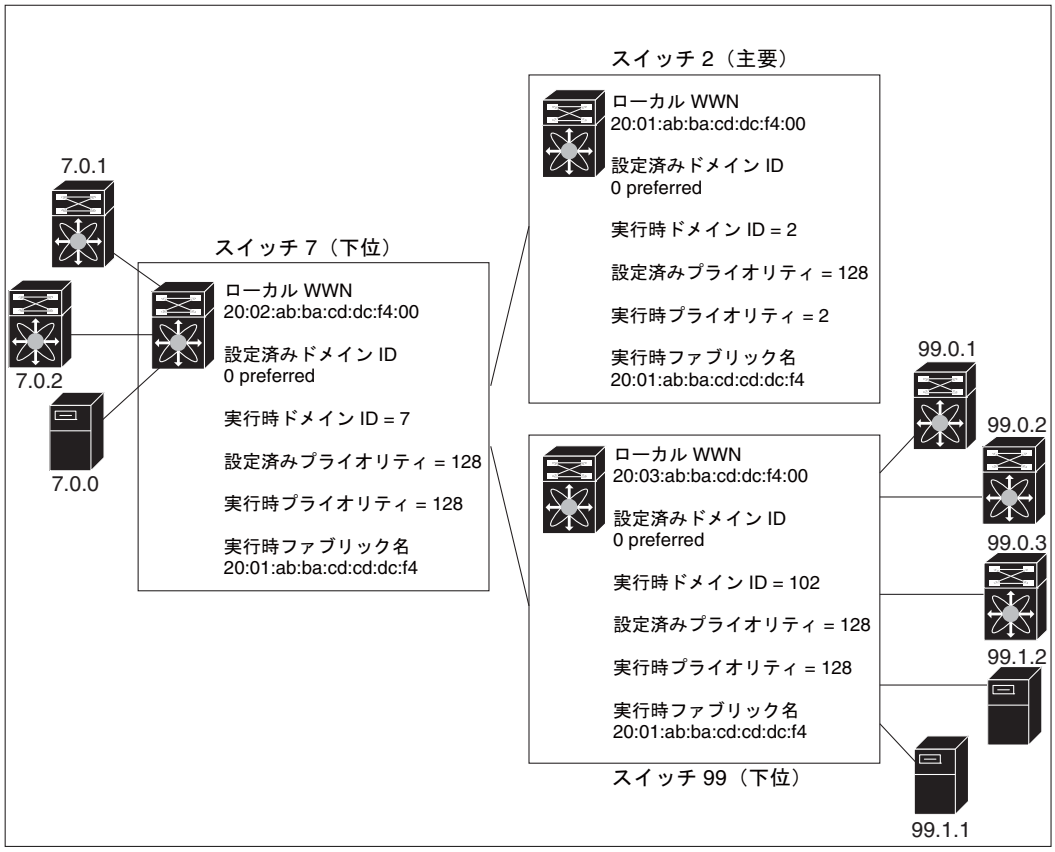
ここでは、fcdomain の各フェーズについて説明します。

- 主要スイッチの選択：このフェーズでは、ファブリック内で一意の主要スイッチを選択できます。
- ドメイン ID の配信：このフェーズでは、ファブリック内のスイッチごとに、一意のドメイン ID を取得できます。
- FC ID の割り当て：このフェーズでは、ファブリック内の対応するスイッチに接続された各デバイスに、一意の FC ID を割り当てることができます。
- ファブリックの再設定：このフェーズでは、ファブリック内のすべてのスイッチを再同期化して、新しい主要スイッチ選択フェーズを同時に再開できるようにします。

注意　fcdomain パラメータは、通常変更しないでください。これらの変更は、管理者が行うか、スイッチ操作を熟知している人が行ってください。

図 10-1 に fcdomain の設定例を示します。

図 10-1　fcdomain の設定例



ここで説明する内容は、次のとおりです。

- 「ドメインの再起動」（P.10-3）
- 「ドメイン マネージャの高速再起動」（P.10-3）
- 「スイッチ プライオリティ」（P.10-4）
- 「fcdomain の開始」（P.10-4）
- 「着信 RCF」（P.10-4）
- 「マージされたファブリックの自動再構成」（P.10-4）
- 「ドメイン ID」（P.10-4）
- 「ファブリックのロック」（P.10-7）
- 「変更のコミット」（P.10-7）
- 「ファブリックのロックのクリア」（P.10-7）
- 「FC ID」（P.10-8）

ドメインの再起動

ファイバ チャネル ドメインは、中断を伴う方法または中断を伴わない方法で起動できます。中断を伴う再起動を実行すると、Reconfigure Fabric（RCF）フレームがファブリックのその他のスイッチに送信され、VSAN のすべてのスイッチでデータ トラフィックが中断されます（リモートでセグメント化されている ISL を含む）。中断を伴わない再起動を実行すると、Build Fabric（BF）フレームがファブリックのその他のスイッチに送信され、そのスイッチだけでデータ トラフィックが中断されます。

ドメイン ID の競合を解消するには、手動でドメイン ID を割り当てる必要があります。ドメイン ID を手動で割り当てるなど、ほとんどの設定変更では中断再起動が必要になります。ドメインの非中断再起動は、優先ドメイン ID をスタティック ドメイン ID（実ドメイン ID は変更なし）に変更する場合にかぎり実行できます。

（注） スタティック ドメインはユーザによって固有に設定されるため、実行時のドメインと異なることがあります。ドメイン ID が異なる場合は、次回の中断または非中断再起動後にスタティック ドメイン ID を使用するように、実行時のドメイン ID が変更されます。

ヒント VSAN が INTEROP モードである場合は、その VSAN の fcdomain で中断を伴う再起動を実行できません。

ほとんどの設定は、対応する実行時の値に適用できます。ここでは、実行時の値に fcdomain パラメータを適用する方法について詳細に説明します。

ドメイン マネージャの高速再起動

Cisco MDS SAN-OS Release 3.0(2) からは、主要リンクに障害が発生したときに、ドメイン マネージャが新しい主要リンクを選択する必要があります。デフォルトでは、ドメイン マネージャは Build Fabric（BF）フェーズを開始し、その後主要スイッチ選択フェーズが続きます。これらのフェーズは両方とも VSAN 内のすべてのスイッチに影響を及ぼし、完了するまで合計 15 秒以上かかります。ドメイン マネージャが新しい主要リンクの選択に必要な時間を短縮するために、ドメイン マネージャの高速再起動機能をイネーブルにできます。

高速再起動がイネーブルで、バックアップ リンクを利用できる場合、ドメイン マネージャはわずか数ミリ秒で新しい主要リンクを選択し、障害が発生したリンクを交換します。また、新しい主要リンクの選択に必要な再設定は、VSAN 全体ではなく、障害が発生したリンクに直接接続した 2 つのスイッチにだけ影響します。バックアップ リンクが利用できない場合、ドメイン マネージャはデフォルトの動作に戻り、BF フェーズを開始します。その後、主要スイッチ選択フェーズが続きます。高速再起動機能はどのインターオペラビリティ モードでも使用できます。

ヒント 大部分のファブリックでは、特に多数の論理ポート（3200 以上）を使用する場合、高速再起動を使用することを推奨します。論理ポートは VSAN の物理ポートのインスタンスであるためです。

スイッチ プライオリティ

新しいスイッチは、安定したファブリックに参加する場合、主要スイッチになることがあります。主要スイッチ選択フェーズ中に、最高のプライオリティを持つスイッチが主要スイッチになります。2 つのスイッチに同じプライオリティが設定されている場合は、WWN が小さいスイッチが主要スイッチになります。

プライオリティ設定は、fcdomain の再起動の実行時に適用されます（「ドメインの再起動」（P.10-3）を参照）。この設定は、中断再起動および非中断再起動のどちらにも適用できます。

fcdomain の開始

デフォルトでは、fcdomain 機能は各スイッチ上でイネーブルになっています。スイッチ内で fcdomain 機能をディセーブルにすると、そのスイッチはファブリック内のその他のスイッチと共存できなくなります。fcdomain 設定は中断再起動の実行時に適用されます。

着信 RCF

インターフェイス単位、VSAN 単位で RCF 要求フレームを拒否するように選択できます。RCF 拒否オプションはデフォルトでディセーブルになっています（つまり、RCF 要求フレームは自動的に拒否されません）。

RCF 拒否オプションは、中断を伴う再起動によって、実行時にすぐに有効になります（「ドメインの再起動」（P.10-3）を参照）。

マージされたファブリックの自動再構成

デフォルトでは、autoreconfigure オプションはディセーブルです。ドメインが重なる別々の安定ファブリックに属する 2 つのスイッチを結合する場合は、次のような状況になる可能性があります。

- 両方のスイッチで autoreconfigure オプションがイネーブルの場合、中断再設定フェーズが開始します。
- いずれかまたは両方のスイッチで autoreconfigure オプションがディセーブルの場合は、2 つのスイッチ間のリンクが隔離されます。

autoreconfigure オプションは実行時に即座に有効になります。fcdomain を再起動する必要はありません。ドメインが重複によって現在隔離されており、後で両方のスイッチの autoreconfigure オプションをイネーブルにする場合は、ファブリックは隔離状態のままです。ファブリックを接続する前に両方のスイッチで autoreconfigure オプションをイネーブルにした場合、中断再設定（RCF）が発生します。中断再設定が発生すると、データ トラフィックが影響を受けることがあります。fcdomain に非中断再設定を行うには、重複リンク上の設定済みドメインを変更し、ドメインの重複を排除します。

ドメイン ID

ドメイン ID は VSAN 内のスイッチを一意に識別します。スイッチは異なる VSAN に異なるドメイン ID を持つことがあります。ドメイン ID は FC ID 全体の一部です。

設定済みドメイン ID のタイプは優先またはスタティックになります。デフォルトで、設定済みドメイン ID は 0（ゼロ）、設定タイプは優先です。

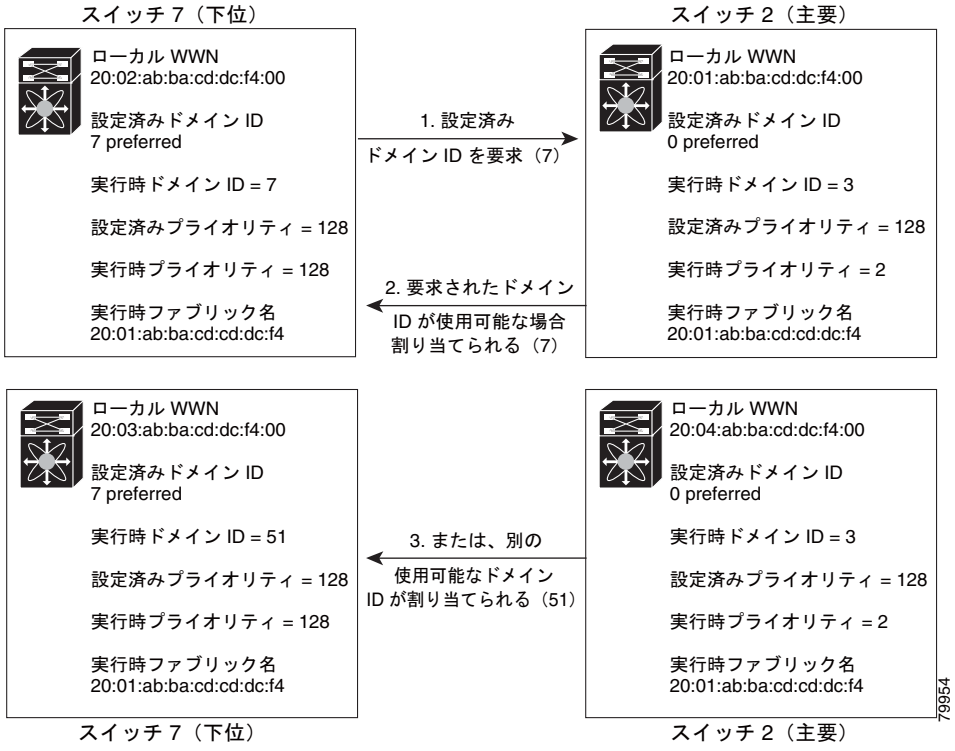
（注）　値 0（ゼロ）を設定できるのは、優先オプションを使用した場合だけです。

ドメイン ID を設定しない場合、ローカル スイッチは要求内でランダムな ID を送信します。スタティック ドメイン ID を使用することを推奨します。

下位スイッチがドメインを要求する場合は、次のプロセスが実行されます（図 10-2 を参照）。

1. ローカル スイッチは主要スイッチに設定済みドメイン ID 要求を送信します。
2. 要求されたドメイン ID が使用可能な場合、主要スイッチはこの ID を割り当てます。使用不可能な場合は、使用可能な別のドメイン ID を割り当てます。

図 10-2　　優先オプションを使用した設定プロセス



下位スイッチの動作は、次の要因によって変化します。

- 許可ドメイン ID リスト。
- 設定済みドメイン ID。
- 主要スイッチが要求元スイッチに割り当てたドメイン ID。

状況に応じて、次のように変更されます。

- 受信されたドメイン ID が許可リストに含まれない場合は、要求されたドメイン ID が実行時ドメイン ID になり、該当する VSAN のすべてのインターフェイスが隔離されます。
- 割り当てられたドメイン ID と要求されたドメイン ID が同じである場合は、優先およびスタティック オプションは関係せず、割り当てられたドメイン ID が実行時ドメイン ID になります。
- 割り当てられたドメイン ID と要求されたドメイン ID が異なる場合は、次のようになります。

- 設定タイプがスタティックの場合は、割り当てられたドメイン ID が廃棄され、すべてのローカル インターフェイスは隔離され、ローカル スイッチには設定済みのドメイン ID が自動的に割り当てられます（この ID が実行時ドメイン ID になります）。
- 設定されているタイプが優先の場合、ローカル スイッチは主要スイッチによって割り当てられたドメイン ID を受け入れて、割り当てられたドメイン ID がランタイム ドメイン ID になります。

設定済みドメイン ID を変更したときに、変更が受け入れられるのは、新しいドメイン ID が、VSAN 内に現在設定されているすべての許可ドメイン ID リストに含まれている場合だけです。または、ドメイン ID を 0 の優先に設定することもできます。

ヒント　特定の VSAN で FICON 機能がイネーブルになっている場合、その VSAN のドメイン ID はスタティックな状態のままになります。スタティック ID 値は変更できますが、優先オプションには変更できません。

（注）　NAT 構成のない IVR では、IVR トポロジ内の 1 つの VSAN でスタティック ドメイン ID が設定されている場合、トポロジ内の他の VSAN（エッジまたは中継）にもスタティック ドメイン ID を設定する必要があります。
IVR NAT 設定で、IVR トポロジ内の 1 つの VSAN に静的ドメイン ID が設定されている場合は、その VSAN にエクスポート可能な IVR ドメインにも静的ドメインを割り当てる必要があります。

注意　設定したドメインの変更をランタイム ドメインに適用する場合は、**fcdomain** を再起動する必要があります。

（注）　許可ドメイン ID リストを設定した場合、追加するドメイン ID は VSAN でその範囲に収まっている必要があります。「許可ドメイン ID リストの設定」（P.10-14）を参照してください。

スタティック ドメイン ID または優先ドメイン ID の指定

スタティック ドメイン ID タイプを割り当てる場合、特定のドメイン ID を要求します。スイッチは、要求したアドレスを取得できなかった場合、自分自身をファブリックから分離します。優先ドメイン ID を指定した場合も特定のドメイン ID を要求しますが、要求したドメイン ID を取得できない場合スイッチは、別のドメイン ID を受け入れます。

スタティック オプションは、中断再起動または非中断再起動後の実行時に適用できますが、優先オプションは中断再起動後の実行時にだけ適用できます（「ドメインの再起動」（P.10-3）を参照）。

許可ドメイン ID リスト

デフォルトでは、割り当て済みのドメイン ID リストの有効範囲は 1 ～ 239 です。許可ドメイン ID リストに複数の範囲を指定し、各範囲をカンマで区切れます。主要スイッチは、ローカルに設定された許可ドメイン リストで使用可能なドメイン ID を割り当てます。

重複しないドメイン ID で VSAN を設計するには、許可ドメイン ID リストを使用します。このリストは将来 NAT 機能を使用しない IVR を実装する必要がある場合に役立ちます。

許可ドメイン ID リストの CFS 配信

Cisco Fabric Service（CFS）インフラストラクチャを使用し、ファブリックのすべての Cisco MDS スイッチに許可ドメイン ID リストの設定情報を配信することをイネーブルにすることができます。この機能により、1 つの MDS スイッチのコンソールからファブリック全体の設定を同期できます。同じ設定が VSAN 全体に配信されるため、発生する可能性がある設定ミスや、同一 VSAN の 2 つのスイッチで互換性がない許可ドメインを設定する可能性を回避できます。

CFS を使用して許可ドメイン ID リストを配信し、VSAN 内のすべてのスイッチで許可ドメイン ID リストの整合性をとるようにします。

（注）　許可ドメイン ID リストを設定し、主要スイッチで確定することを推奨します。

CFS の詳細については、第 2 章「CFS インフラストラクチャの使用」を参照してください。

連続ドメイン ID 割り当て

デフォルトでは、連続ドメイン割り当てはディセーブルです。下位スイッチが複数のドメインを主要スイッチに要求し、ドメインが連続していない場合は、次のような状況になる可能性があります。

- 主要スイッチで連続ドメイン割り当てがイネーブルの場合、主要スイッチは連続ドメインを特定し、それらを下位スイッチに割り当てます。連続ドメインが使用できない場合、NX-OS ソフトウェアはこの要求を却下します。
- 主要スイッチで連続ドメイン割り当てがディセーブルの場合、主要スイッチは使用可能なドメインを下位スイッチに割り当てます。

ファブリックのロック

既存の設定を変更するときの最初のアクションによって、保留中の設定が作成され、ファブリック内の機能がロックされます。ファブリックをロックすると、次の条件が適用されます。

- 他のユーザがこの機能の設定に変更を加えることができなくなります。
- アクティブな設定をコピーすると保留中の設定が作成されます。これ以後の変更は保留設定に対して行われ、アクティブな設定（およびファブリック内の他のスイッチ）に変更をコミットするか、または変更を廃棄するまで、保留設定にとどまります。

変更のコミット

保留されているドメイン設定の変更を VSAN のその他の MDS スイッチに適用するには、変更を確定する必要があります。保留中の設定変更が配信され、正常に確定された時点で、設定変更は VSAN 全体の MDS スイッチでアクティブな設定に適用されて、ファブリックのロックが解除されます。

ファブリックのロックのクリア

ドメイン設定作業を実行し、変更をコミットまたは廃棄してロックを解除していない場合、管理者はファブリック内の任意のスイッチからロックを解除できます。管理者がこのタスクを実行すると、保留中の変更は廃棄され、ファブリック ロックが解除されます。

保留中の変更は volatile ディレクトリだけで使用でき、スイッチを再起動すると廃棄されます。

FC ID

Cisco MDS 9000 ファミリ スイッチに N または NL ポートがログインする場合、FC ID が割り当てられます。デフォルトでは、固定的 FC ID 機能はイネーブルです。この機能をディセーブルにした場合、次の結果になります。

- N ポートまたは NL ポートが Cisco MDS 9000 ファミリ スイッチにログインします。要求側の N ポートまたは NL ポートの WWN、および割り当てられた FC ID は保持され、揮発性キャッシュに保存されます。この揮発性キャッシュの内容は、再起動時に保存されません。
- スイッチは、FC ID と WWN のバインディングをベストエフォート方式で保持するように設計されています。たとえば、スイッチから 1 つの N ポートを切断したあとに、別のデバイスから FC ID が要求されると、この要求が許可されて、WWN と初期 FC ID の関連付けが解除されます。
- 揮発性キャッシュには、WWN と FC ID のバインディングのエントリを 4000 まで格納できます。このキャッシュが満杯になると、新しい（より最近の）エントリによって、キャッシュ内の最も古いエントリが上書きされます。この場合、最も古いエントリの対応する WWN と FC ID の関連付けが失われます。
- スイッチ接続動作は、N ポートと NL ポートで異なります。
  - N ポートを取り外し、同じスイッチの任意のポートに接続すると、（このポートが同じ VSAN に属するかぎり）この N ポートには同じ FC ID が割り当てられます。
  - NL ポートが同じ FC ID になるのは、スイッチ上の以前接続されていたポートと同じポートに再度接続された場合だけです。

固定的 FC ID

固定的 FC ID がイネーブルである場合は、次のようになります。

- fcdomain 内の現在*使用中の* FC ID は、リブートしても保持されます。
- fcdomain は、デバイス（ホストまたはディスク）をポート インターフェイスに接続したあとに学習されたダイナミック エントリを、自動的にデータベースに入力します。

固定的 FC ID 設定

固定的 FC ID 機能をイネーブルにすると、固定的 FC ID サブモードを開始して、FC ID データベースにスタティックまたはダイナミック エントリを追加できるようになります。デフォルトでは、追加されたすべてのエントリはスタティックです。固定的 FC ID は VSAN 単位で設定します。固定的 FC ID を手動で設定するには、次の要件に従ってください。

- 必要な VSAN 内で固定的 FC ID 機能がイネーブルになっていることを確認します。
- 必要な VSAN がアクティブ VSAN であることを確認してください。固定的 FC ID は、アクティブな VSAN に対してだけ設定できます。
- FC ID のドメイン部分が必要な VSAN 内の実行時ドメイン ID と同じであることを確認します。ソフトウェアがドメインの不一致を検出した場合、コマンドは拒否されます。
- エリアを設定するときに、FC ID のポート フィールドが 0（ゼロ）であることを確認します。

（注） FICON は、前面パネルのポート番号に基づき、異なる方式を使用して FC ID を割り当てます。この方式は、FICON VSAN における FC ID の固定化よりも優先されます。

HBA の固有エリア FC ID について

（注）　HBA ポートおよびストレージ ポートを同一スイッチに接続している場合に限り、この項を読んでください。

HBA ポートとストレージ ポートを両方とも同一スイッチに接続している場合、一部の HBA ポートにはストレージ ポートとは別のエリア ID が必要となります。たとえば、ストレージ ポート FC ID が 0x6f7704 の場合、このポートのエリアは 77 です。この場合、HBA ポートのエリアには 77 以外の値を設定できます。HBA ポートの FC ID は、ストレージ ポートの FC ID と異なる値に手動で設定する必要があります。

Cisco MDS 9000 ファミリのスイッチでは、FC ID の固定化機能により、この要件への準拠が容易になります。この機能を使用すると、ストレージ ポートまたは HBA ポートに異なるエリアを持つ FC ID を事前に割り当てることができます。

固定的 FC ID の選択消去

固定的 FC ID は、選択的に消去できます。現在使用中のスタティック エントリおよび FC ID は、削除できません。表 10-1 に、固定的 FC ID の消去時に削除または保持される FC ID エントリを示します。

表 10-1　消去される FC ID

固定的 FC ID の状態	固定的 FC ID の使用状態	アクション
スタティック	使用中	削除されない
スタティック	使用中でない	削除されない
ダイナミック	使用中	削除されない
ダイナミック	使用中でない	削除される

注意事項と制限

- 設定を変更した場合は、必ず実行コンフィギュレーションを保存してください。次回にスイッチを再起動したときに、保存された設定が使用されます。設定を保存しない場合は、前回保存されたスタートアップ コンフィギュレーションが使用されます。
- すべての手順で使用されるドメイン ID および VSAN 値は、単なる例です。必ずご使用の設定に適用される ID および値を使用してください。

デフォルト設定

表 10-2 に、すべての fcdomain パラメータのデフォルト設定の一覧を示します。

表 10-2　デフォルト fcdomain パラメータ

パラメータ	デフォルト
fcdomain 機能	イネーブル。
設定済みドメイン ID	0（ゼロ）。
設定済みドメイン	優先。

表 10-2　デフォルト fcdomain パラメータ （続き）

パラメータ	デフォルト
autoreconfigure オプション	ディセーブル。
contiguous-allocation オプション	ディセーブル。
プライオリティ	128。
許可リスト	1 ～ 239。
ファブリック名	20:01:00:05:30:00:28:df。
rcf-reject	ディセーブル。
固定的 FC ID	イネーブル。
許可ドメイン ID リスト設定の配信	ディセーブル。

ファイバ チャネル ドメインの設定

ここでは、fcdomain 機能について説明します。ここで説明する内容は、次のとおりです。

Domain Manager のターボ モードの設定

Domain Manager のターボ モード機能を使用すると、最適化を使用して Domain Manager を再起動できます。Domain Manager の再起動には fast-restart モードか selective-restart モードを選択できます。再起動モードの設定を空のままにして、最適化をディセーブルにすることもできます。

手順の詳細

Domain Manager のターボ モードを設定するには、次の手順を実行します。

ステップ 1　ターボ モードを設定するファブリックと VSAN について、[Logical Domains] ペインで [Fabric] > [All VSANs] を展開し、[Domain Manager] を選択します。
[Information] ペインにドメインの [Running] タブの設定が表示されます

ステップ 2　[Configuration] タブをクリックします。

ステップ 3　ファブリック内の最適化するスイッチに対し、[Optimization] ドロップダウン メニューを [fast-restart] または [selective-restart] に設定します。[Optimization] フィールドで何も選択しないと、最適化はディセーブルになります。

ステップ 4　[Apply Changes] アイコンをクリックし、この再起動を開始します。

Device Manager を使用して Domain Manager のターボ モードを設定するには、次の手順を実行します。

ステップ 1　[FC] > [Domain Manager] の順に展開し、[Configuration] タブを選択します。

（注）　[Optimization] フィールドは、NX-OS Release 4.2(1) よりも前のリリースにはありません。

ステップ 2　ファブリック内の最適化するスイッチに対し、[Optimization] ドロップダウン メニューを [fast-restart] または [selective-restart] に設定します。[Optimization] フィールドで何も選択しないと、最適化はディセーブルになります。

ステップ 3　[Apply] をクリックしてこの再起動を開始します。

ドメインの再起動

手順の詳細

中断を伴うファブリックの再起動、または中断を伴わない再起動を行うには、次の手順を実行します。

ステップ 1　再起動するファブリックと VSAN について、[Logical Domains] ペインで [Fabric] > [All VSANs] を展開し、[Domain Manager] を選択します。

ステップ 2　[Configuration] タブをクリックします。

ステップ 3　ファブリック内の fcdomain を再起動するすべてのスイッチに対し、[Restart] ドロップダウン メニューを [disruptive] または [nonDisruptive] に設定します。

ステップ 4　[Apply Changes] アイコンをクリックし、この fcdomain の再起動を開始します。

スイッチ プライオリティの設定

制約事項

- デフォルトでプライオリティ 128 が設定されています。プライオリティの有効設定範囲は 1 ～ 254 です。プライオリティ 1 が最高のプライオリティです。値 255 は、他のスイッチからは受け入れられますが、ローカルには設定できません。

手順の詳細

主要スイッチのプライオリティを設定するには、次の手順を実行します。

ステップ 1　主要スイッチのプライオリティを設定するファブリックと VSAN について、[Logical Domains] ペインで [Fabric] > [All VSANs] を展開し、[Domain Manager] を選択します。

ステップ 2　ファブリック内で主要スイッチにするスイッチの [Priority] を高い値に設定します。

ステップ 3　[Apply Changes] アイコンをクリックして、これらの変更を保存します。

fcdomain のイネーブル化またはディセーブル化

手順の詳細

単一の VSAN または VSAN 範囲で fcdomain をディセーブルまたは再度イネーブルにするには、次の手順を実行します。

ステップ 1　fcdomain をディセーブルにするファブリックと VSAN について、[Logical Domains] ペインで [Fabric] > [All VSANs] を展開し、[Domain Manager] を選択します。

[Information] ペインにドメインの実行コンフィギュレーションが表示されます。

ステップ 2　[Configuration] タブをクリックし、fcdomain をディセーブルにするファブリックのスイッチごとに、[Enable] チェックボックスをオフにします。

ステップ 3　[Apply Changes] アイコンをクリックして、これらの変更を保存します。

ファブリック名の設定

手順の詳細

ディセーブルになっている fcdomain のファブリック名の値を設定するには、次の手順を実行します。

ステップ 1　ファブリック名を設定するファブリックと VSAN について、[Logical Domains] ペインで [Fabric] > [All VSANs] を展開し、[Domain Manager] を選択します。

[Information] ペインにドメインの実行コンフィギュレーションが表示されます。

ステップ 2　[Configuration] タブをクリックし、ファブリックのスイッチごとにファブリック名を設定します。

ステップ 3　[Apply Changes] アイコンをクリックして、これらの変更を保存します。

着信 RCF の拒否

手順の詳細

着信 RCF 要求フレームを拒否するには、次の手順を実行します。

ステップ 1　[Physical Attributes] ペインで [Switches] > [FC Interfaces] を展開し、[Physical] を選択します。

[Information] ペインにファイバ チャネル設定が表示されます。

ステップ 2　[Domain Mgr] タブをクリックします。

ステップ 3　RCF 要求フレームを拒否するインターフェイスごとに、[RcfReject] チェックボックスをオンにします。

ステップ 4　[Apply Changes] アイコンをクリックして、これらの変更を保存します。

自動再構成のイネーブル化

手順の詳細

特定の VSAN（または VSAN 範囲）で自動再構成をイネーブルにするには、次の手順を実行します。

ステップ 1　自動再構成をイネーブルにするファブリックと VSAN について、[Logical Domains] ペインで [Fabric] > [All VSANs] を展開し、[Domain Manager] を選択します。

[Information] ペインにドメインの実行コンフィギュレーションが表示されます。

ステップ 2　[Configuration] タブをクリックし、自動的に再構成するファブリックのスイッチごとに [Auto Reconfigure] チェックボックスをオンにします。

ステップ 3　[Apply Changes] アイコンをクリックして、これらの変更を保存します。

ドメイン ID の設定

ドメイン ID は VSAN 内のスイッチを一意に識別します。スイッチは異なる VSAN に異なるドメイン ID を持つことがあります。ドメイン ID は FC ID 全体の一部です。

設定済みドメイン ID のタイプは優先またはスタティックになります。デフォルトで、設定済みドメイン ID は 0（ゼロ）、設定タイプは優先です。

ここで説明する内容は、次のとおりです。

- 「スタティック ドメイン ID または優先ドメイン ID の指定」（P.10-13）
- 「許可ドメイン ID リストの設定」（P.10-14）
- 「許可ドメイン ID 配信のイネーブル化」（P.10-15）
- 「連続ドメイン ID 割り当てのイネーブル化」（P.10-16）

スタティック ドメイン ID または優先ドメイン ID の指定

制約事項

- 1 つの VSAN 内のスイッチは、すべて同じドメイン ID タイプ（スタティックまたは優先）を持っている必要があります。あるスイッチがスタティック ドメイン タイプで、別のスイッチが優先ドメイン タイプであるというように、設定が混在している場合は、リンクが分離されることがあります。

手順の詳細

スタティックまたは優先のドメイン ID を指定するには、次の手順を実行します。

ステップ 1　ドメイン ID を設定するファブリックと VSAN について、[Logical Domains] ペインで [Fabric] > [All VSANs] を展開し、[Domain Manager] を選択します。

[Information] ペインにドメインの実行コンフィギュレーションが表示されます。

ステップ 2　[Config DomainID] に値を入力し、[Config Type] ドロップダウン メニューから [static] または [preferred] をクリックし、ファブリックのスイッチにドメイン ID を設定します。

ステップ 3　[Apply Changes] アイコンをクリックして、これらの変更を保存します。

許可ドメイン ID リストの設定

前提条件

許可ドメイン ID リストは、次の条件を満たす必要があります。

- スイッチが主要スイッチである場合は、現在割り当てられているすべてのドメイン ID が許可リストに含まれている必要があります。
- このスイッチが下位スイッチである場合は、ローカル実行時ドメイン ID が許可リストに含まれている必要があります。
- ローカルに設定されたスイッチのドメイン ID が許可リスト内に含まれている必要があります。
- 割り当てられたドメイン ID の一部が、その他の設定済みドメイン ID のリストのいずれかに含まれている必要があります。

ファブリック内の 1 つのスイッチに許可リストを設定する場合は、整合性を保つために、ファブリック内のその他のすべてのスイッチに同じリストを設定するか、CFS を使用して設定を配信することを推奨します。

手順の詳細

許可ドメイン ID リストを設定するには、次の手順を実行します。

ステップ 1　許可ドメイン ID リストを設定するファブリックと VSAN について、[Logical Domains] ペインで [Fabric] > [All VSANs] > [Domain Manager] を展開し、[Allowed] を選択します。

[Information] ペインに CFS 設定が表示されます。

ステップ 2　[Admin] ドロップダウン メニューを [enable] に設定し、[Global] ドロップダウン メニューを [enable] に設定します。

ステップ 3　[Apply Changes] をクリックし、CFS による許可ドメイン ID リストの配信をイネーブルにします。

ステップ 4　[Allowed DomainIds] タブを選択します。

ステップ 5　このドメインの許可ドメイン ID リストに list を設定します。

ステップ 6　[CFS] タブを選択し、[Config Action] を [commit] に設定します。

ステップ 7　[Apply Changes] アイコンをクリックしてこの許可ドメイン ID リストを確定し、VSAN で配信します。

許可ドメイン ID 配信のイネーブル化

許可ドメイン ID リストの CFS 配信はデフォルトではディセーブルになっています。許可ドメイン ID リストを配信するすべてのスイッチで配信をイネーブルにする必要があります。

前提条件

- CFS を使用して許可ドメイン ID リストを配信するには、ファブリック内のすべてのスイッチは Cisco SAN-OS Release 3.0(1) 以降を実行している必要があります。

手順の詳細

許可ドメイン ID リスト設定の配信をイネーブル（またはディセーブル）にするには、次の手順を実行します。

ステップ 1　許可ドメイン ID リストを設定するファブリックと VSAN について、[Logical Domains] ペインで [Fabric] > [All VSANs] > [Domain Manager] を展開し、[Allowed] を選択します。

[Information] ペインに CFS 設定が表示されます。

ステップ 2　許可ドメイン ID リストの CFS 配信をイネーブルにするには、[Admin] ドロップダウン メニューを [enable] に、[Global] ドロップダウン メニューを [enable] に設定します。

ステップ 3　[Apply Changes] アイコンをクリックし、CFS による許可ドメイン ID リストの配信をイネーブルにします。

変更のコミット

手順の詳細

保留中のドメイン設定変更をコミットし、ロックを解除するには、次の手順を実行します。

ステップ 1　許可ドメイン ID リストを設定するファブリックと VSAN について、[Logical Domains] ペインで [Fabric] > [All VSANs] > [Domain Manager] を展開し、[Allowed] を選択します。

[Information] ペインに CFS 設定が表示されます。

ステップ 2　[Config Action] ドロップダウン メニューを [commit] に設定します。

ステップ 3　[Apply Changes] アイコンをクリックしてこの許可ドメイン ID リストを確定し、VSAN で配信します。

変更の廃棄

いつでもドメイン設定への保留変更を廃棄して、ファブリックのロックを解除できます。保留中の変更を廃棄（中断）する場合、設定には影響せずに、ロックが解除されます。

手順の詳細

保留中のドメイン設定変更を廃棄し、ロックを解除するには、次の手順を実行します。

ステップ 1　許可ドメイン ID リストを設定するファブリックと VSAN について、[Logical Domains] ペインで [Fabric] > [All VSANs] > [Domain Manager] を展開し、[Allowed] を選択します。

[Information] ペインに CFS 設定が表示されます。

ステップ 2　[Config Action] ドロップダウン メニューを [abort] に設定します。

ステップ 3　[Apply Changes] アイコンをクリックし、許可ドメイン ID リストに対する保留中の変更を廃棄します。

連続ドメイン ID 割り当てのイネーブル化

手順の詳細

特定の VSAN（または VSAN 範囲）で連続ドメインをイネーブルにするには、次の手順を実行します。

ステップ 1　連続ドメインをイネーブルにするファブリックと VSAN について、[Logical Domains] ペインで [Fabric] > [All VSANs] を展開し、[Domain Manager] を選択します。

[Information] ペインにドメインの実行コンフィギュレーションが表示されます。

ステップ 2　[Configuration] タブをクリックし、連続割り当てをイネーブルにするファブリックのスイッチごとに [Contiguous Allocation] チェックボックスをオンにします。

ステップ 3　[Apply Changes] アイコンをクリックして、これらの変更を保存します。

FC ID の設定

Cisco MDS 9000 ファミリ スイッチに N または NL ポートがログインする場合、FC ID が割り当てられます。

ここで説明する内容は、次のとおりです。

固定的 FC ID 機能のイネーブル化

AIX または HP-UX ホストからスイッチに接続する場合は、それらのホストに接続する VSAN で固定的 FC ID 機能をイネーブルにする必要があります。

F ポートに割り当てられた固定的 FC ID は、インターフェイス間を移動させることができ、同じ固定的 FC ID をそのまま維持することができます。

制約事項

- FC ID はデフォルトでイネーブルになっています。このデフォルト動作は、Cisco MDS SAN-OS Release 2.0(1b) よりも前のリリースから変更されており、リブートした後で FC ID が変更されなくなります。このオプションは、VSAN ごとにディセーブルにできます。
- ループ接続デバイス（FL ポート）を使用した固定的 FC ID は、設定されたポートと同じポートに接続され続ける必要があります。
- デバイス上の Arbitrated Loop Physical Address（ALPA）のサポートの違いにより、ループ接続デバイスの FC ID の固定化は保証されません。

手順の詳細

固定的 FC ID 機能をイネーブルにするには、次の手順を実行します。

ステップ 1　固定的 FC ID 機能をイネーブルにするファブリックと VSAN について、[Logical Domains] ペインで [Fabric] > [All VSANs] を展開し、[Domain Manager] を選択します。

[Information] ペインにドメインの実行コンフィギュレーションが表示されます。

ステップ 2　[Persistent Setup] タブを選択し、固定的 FC ID をイネーブルにするファブリックのスイッチごとに [enable] チェックボックスをオンにします。

ステップ 3　[Apply Changes] アイコンをクリックして、これらの変更を保存します。

固定的 FC ID の設定

手順の詳細

固定的 FC ID を設定するには、次の手順を実行します。

ステップ 1　固定的 FC ID リストを設定するファブリックと VSAN について、[Logical Domains] ペインで [Fabric] > [All VSANs] を展開し、[Domain Manager] を選択します。

[Information] ペインにドメインの実行コンフィギュレーションが表示されます。

ステップ 2　[Persistent FcIds] タブをクリックし、[Create Row] をクリックします。

ステップ 3　スイッチ、WWN、固定にする FC ID を選択します。

ステップ 4　[Mask] オプション ボタンを [single] または [area] に設定します。

ステップ 5　[Assignment] オプション ボタンを [static] または [dynamic] に設定します。

ステップ 6　[Apply Changes] アイコンをクリックして、これらの変更を保存します。

HBA の固有エリア FC ID の設定

手順の詳細

HBA ポートに別のエリア ID を設定するには、次の手順を実行します。

ステップ 1　[Physical Attributes] ペインで [End Device] を展開し、[Information] ペインで [FLOGI] タブを選択して、HBA のポート WWN（[Port Name] フィールド）を取得します。

（注）　この設定では、両方の FC ID に同じエリア 00 が割り当てられています。

ステップ 2　[Physical Attributes] ペインから [Switches] > [FC Interfaces] を展開し、[Physical] を選択します。

ステップ 3　HBA が接続されているインターフェイスで、[Status Admin] ドロップダウン メニューを [down] に設定します。

MDS スイッチで HBA インターフェイスがシャットダウンされます。

ステップ 4　[Fabric] > [All VSANs] を展開し、[Domain Manager] を選択します。

ステップ 5　[Information] ペインで [Persistent Setup] タブをクリックし、FC ID 機能がイネーブルであることを確認します。

この機能がディセーブルの場合は、この手順を継続して、固定的 FC ID をイネーブルにします。

この機能がすでにイネーブルの場合は、ステップ 7 に進みます。

ステップ 6　[Enable] チェックボックスをオンにして、Cisco MDS スイッチで固定的 FC ID 機能をイネーブルにします。

ステップ 7　[Persistent FcIds] タブを選択し、エリア割り当てが異なる新しい FC ID を [FcId] フィールドで割り当てます。この例では、00 を ee に置き換えます。

ステップ 8　[Apply Changes] をクリックし、新しい FC ID を保存します。

ステップ 9　FC ID の値を比較し、HBA の FC ID を確認します。

（注）　これで、両方の FC ID にそれぞれ異なるエリアが割り当てられました。

ステップ 10　[Physical Attributes] ペインから [Switches] > [FC Interfaces] を展開し、[Physical] を選択します。HBA が接続されているインターフェイスで、[Status Admin] ドロップダウン メニューを [up] に設定します。MDS スイッチで HBA インターフェイスがイネーブルになります。

固定的 FC ID の消去

手順の詳細

固定的 FC ID を消去するには、次の手順を実行します。

ステップ 1　固定的 FC ID を消去するファブリックについて、[Logical Domains] ペインで [Fabric] > [All VSANs] > [Domain Manager] を展開します。[Information] ペインにドメインの実行コンフィギュレーションが表示されます。

ステップ 2　[Persistent Setup] タブをクリックします。

ステップ 3　固定的 FC ID を消去するスイッチの [Purge] チェックボックスをオンにします。

ステップ 4　[Apply Changes] アイコンをクリックして、これらの変更を保存します。

ファブリックのロックのクリア

ファブリックのロックを解除するには、次の手順を実行します。

ステップ 1　許可ドメイン ID リストが必要なファブリックと VSAN について、[Logical Domains] ペインで [Fabric] > [All VSANs] > [Domain Manager] を展開し、[AllowedId] を選択します。

[Information] ペインに CFS 設定が表示されます。

ステップ 2　[Config Action] ドロップダウン メニューを [clear] に設定します。

ステップ 3　[Apply Changes] アイコンをクリックし、ファブリックのロックをクリアします。

FC ドメイン設定の確認

ドメイン ID の設定情報を表示するには、次の作業を行います。

- 「保留中の変更の表示」（P.10-19）
- 「セッション ステータスの表示」（P.10-20）

保留中の変更の表示

保留中の設定変更を表示するには、次の手順を実行します。

ステップ 1　許可ドメイン ID リストを設定するファブリックと VSAN について、[Logical Domains] ペインで [Fabric] > [All VSANs] > [Domain Manager] > [Allowed] を展開します。

[Information] ペインに CFS 設定が表示されます。

ステップ 2　[Config View As] ドロップダウン メニューを [pending] に設定します。

ステップ 3　[Apply Changes] アイコンをクリックし、ファブリックのロックをクリアします。

ステップ 4　[AllowedDomainIds] タブをクリックします。

許可ドメイン ID リストの保留中の設定が表示されます。

セッション ステータスの表示

配信セッションのステータスを表示するには、次の手順を実行します。

ステップ 1　許可ドメイン ID リストを設定するファブリックと VSAN について、[Logical Domains] ペインで [Fabric] > [All VSANs] > [Domain Manager] を展開し、[Allowed] を選択します。

ステップ 2　CFS 設定およびセッション ステータスが [Information] ペインに表示されます。

FC ドメインのモニタリング

ここでは、次の内容について説明します。

- 「fcdomain の統計情報の表示」（P.10-20）

fcdomain の統計情報の表示

DCNM-SAN は fcdomain の統計情報を収集し、[Information] ペインに表示します。

fcdomain の統計情報を表示するには、次の手順を実行します。

ステップ 1　統計情報を表示するファブリックについて、[Logical Domains] ペインで [Fabric] > [All VSANs] を展開し、[Domain Manager] を選択します。

[Information] ペインにドメインの実行コンフィギュレーションが表示されます。

ステップ 2　[Statistics] タブをクリックします。[Information] ペインに FC ID の統計情報が表示されます。

FC ドメインのフィールドの説明

ここでは、FC ドメインのフィールドの説明を示します。

IVR ドメイン

フィールド	説明
Domain Id	VSAN を表すために使用される FC ドメイン ID。

ドメイン パラメータの機能履歴

表 10-3 に、この機能のリリース履歴を示します。Release 3.x 以降のリリースで導入または変更された機能のみが表に記載されています。

表 10-3　ドメイン パラメータの機能履歴

機能名	リリース	機能情報
Domain Manager のターボ モード	4.2(1)	Domain Manager のターボ モードの設定手順を追加。
許可ドメイン ID リストの CFS サポート	3.0(1)	CFS インフラストラクチャを使用して許可ドメイン ID リストをファブリック内で配信できます。

CHAPTER 11

SPAN を使用したネットワーク トラフィックのモニタリング

この章では、Cisco MDS 9000 ファミリ スイッチに提供される Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）機能について説明します。

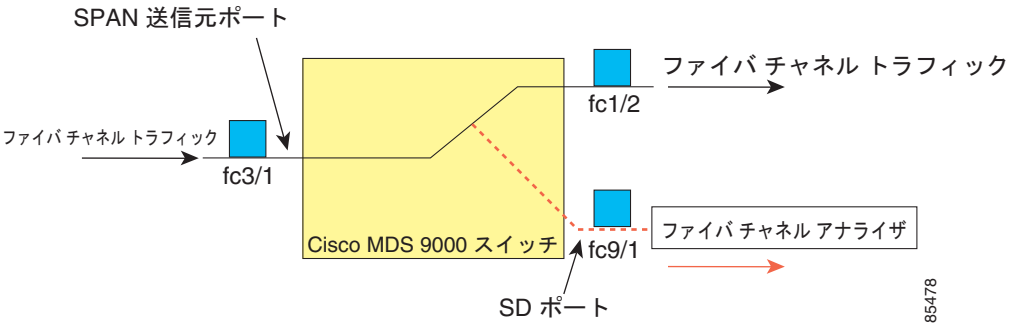
この章の内容は、次のとおりです。

SPAN について

Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）機能は、Cisco MDS 9000 ファミリ スイッチ特有のものです。SPAN は、ファイバ チャネル インターフェイスを通じてネットワーク トラフィックをモニタします。任意のファイバ チャネル インターフェイスを通るトラフィックは、SPAN 宛先ポート（SD ポート）という専用ポートに複製することができます。スイッチの任意のファイバ チャネル ポートを SD ポートとして設定できます。SD ポート モードに設定したインターフェイスは、標準データ トラフィックには使用できません。ファイバ チャネル アナライザを SD ポートに接続して、SPAN トラフィックをモニタできます。

SD ポートはフレームを受信しませんが、SPAN 送信元トラフィックのコピーを送信します。SPAN 機能は他の機能に割り込むことなく、SPAN 送信元ポートのネットワーク トラフィックのスイッチングに影響しません（図 11-1 を参照）。

図 11-1　SPAN の送信



この項では、次の項目について説明します。

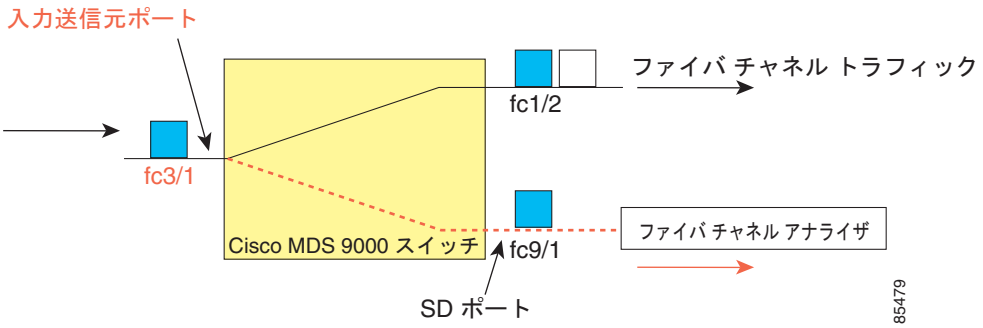
- 「SPAN 送信元」（P.11-2）
- 「IPS 送信元ポート」（P.11-3）
- 「使用可能な送信元インターフェイス タイプ」（P.11-4）
- 「送信元としての VSAN」（P.11-4）
- 「SPAN セッション」（P.11-4）
- 「フィルタの指定」（P.11-5）
- 「SD ポートの特性」（P.11-5）
- 「ファイバ チャネル アナライザによるトラフィックのモニタリング」（P.11-5）
- 「SPAN を使用しないモニタリング」（P.11-6）
- 「SPAN を使用するモニタリング」（P.11-6）
- 「単一 SD ポートによるトラフィックのモニタ」（P.11-7）
- 「SD ポート設定」（P.11-8）
- 「FC トンネルのマッピング」（P.11-8）
- 「VSAN インターフェイスの作成」（P.11-9）
- 「リモート SPAN」（P.11-9）
- 「RSPAN の使用の利点」（P.11-10）
- 「FC トンネルと RSPAN トンネル」（P.11-10）
- 「ST ポート設定」（P.11-11）
- 「ST ポートの特性」（P.11-11）
- 「明示的なパスの作成」（P.11-12）

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。VSAN を SPAN 送信元として指定することもできます。この場合は、指定された 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 送信元に含まれます。送信元として VSAN が指定されている場合は、この VSAN 内のすべての物理ポートおよび PortChannel が SPAN 送信元として含まれます。任意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。

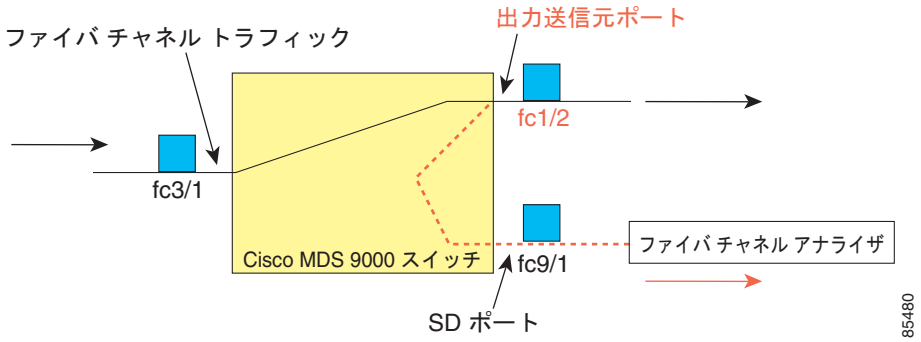
- 入力送信元（Rx）：この送信元インターフェイスを介してスイッチ ファブリックに入るトラフィックは、SD ポートにスパン（コピー）されます（図 11-2 を参照）。

図 11-2　入力方向からの SPAN トラフィック



- 出力送信元（Tx）：この送信元インターフェイスを介してスイッチ ファブリックから出ていくトラフィックは、SD ポートにスパン（コピー）されます（図 11-3 を参照）。

図 11-3　出力方向からの SPAN トラフィック



IPS 送信元ポート

SPAN 機能は、IP Storage Service（IPS）モジュールで利用できます。この SPAN 機能を実装できるのは、物理ギガビット イーサネット ポートでなく、FCIP および iSCSI 仮想ファイバ チャネル ポート インターフェイス上だけです。IPS モジュールで使用可能なすべてのインターフェイス（8 個の iSCSI インターフェイスおよび 24 個の FCIP インターフェイス）では、入力トラフィック、出力トラフィック、または両方向のトラフィックに SPAN を設定できます。

（注） イーサネット トラフィックに SPAN を設定するには、Cisco MDS 9000 ファミリ IPS モジュールに接続されたシスコ製スイッチまたはルータを使用します。

使用可能な送信元インターフェイス タイプ

SPAN 機能を使用できるインターフェイス タイプは、次のとおりです。

- 物理ポート（F ポート、FL ポート、TE ポート、E ポート、および TL ポート）。
- インターフェイス sup-fc0（スーパーバイザに対するトラフィック）
  - sup-fc0 インターフェイスを介してスーパーバイザ モジュールからスイッチ ファブリックに送信されるファイバ チャネル トラフィックを、入力トラフィックと言います。入力送信元ポートとして sup-fc0 が選択されている場合は、このトラフィックがスパンされます。
  - sup-fc0 インターフェイスを介してスイッチ ファブリックからスーパーバイザ モジュールに送信されるファイバ チャネルトラフィックを、出力トラフィックと言います。出力送信元ポートとして sup-fc0 が選択されている場合は、このトラフィックがスパンされます。
- ポートチャネル
  - PortChannel 内のすべてのポートが含まれ、送信元としてスパンされます。
  - PortChannel 内のポートを SPAN 送信元として個別に指定できません。設定済みの SPAN 固有のインターフェイス情報は廃棄されます。
- IPS モジュール固有のファイバ チャネル インターフェイス
  - iSCSI インターフェイス
  - FCIP インターフェイス

送信元としての VSAN

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。送信元として VSAN が指定されている場合は、この VSAN 内のすべての物理ポートおよび PortChannel が SPAN 送信元として含まれます。TE ポートが含まれるのは、TE ポートのポート VSAN が送信元 VSAN と一致する場合だけです。設定済みの許可 VSAN リストに送信元 VSAN が含まれている場合でも、ポート VSAN が異なっていれば、TE ポートは除外されます。

同じ SPAN セッション内では、送信元インターフェイス（物理インターフェイス、PortChannel、または sup-fc インターフェイス）と送信元 VSAN を設定できません。

SPAN セッション

各 SPAN セッションは、1 つの宛先と複数の送信元の対応関係、およびネットワーク トラフィックをモニタするために指定されたその他のパラメータを表します。1 つの宛先を 1 つ以上の SPAN セッションで使用することができます。スイッチには最大 16 個の SPAN セッションを設定できます。各セッションには複数の送信元ポートおよび 1 つの宛先ポートを設定できます。

SPAN セッションをアクティブにするには、少なくとも 1 つの送信元および SD ポートを起動して、機能させる必要があります。このようにしないと、トラフィックが SD ポートに転送されません。

ヒント　1 つの送信元を 2 つのセッションで共有することは可能です。ただし、各セッションはそれぞれ異なる方向（1 つは入力、1 つは出力）でなければなりません。

SPAN セッションを一時的に非アクティブ（一時停止）にできます。この期間中、トラフィック モニタリングは停止します。

フィルタの指定

VSAN ベースのフィルタリングを実行すると、指定された VSAN 上でネットワーク トラフィックを選択的にモニタできます。この VSAN フィルタは、セッション内のすべての送信元に適用できます（図 11-14 を参照）。スパンされるのは、このフィルタ内の VSAN だけです。

指定されたセッション内のすべての送信元に適用されるセッション VSAN フィルタを指定できます。これらのフィルタは双方向であり、セッションに設定されたすべての送信元に適用されます。各 SPAN セッションは、1 つの宛先と複数の送信元の対応関係、およびネットワーク トラフィックをモニタするために指定されたその他のパラメータを表します。

SD ポートの特性

SD ポートには、次の特性があります。

- BB_credits を無視します。
- 出力（Tx）方向のデータ トラフィックだけを許可します。
- デバイスまたはアナライザを物理的に接続する必要はありません。
- 1 Gbps または 2 Gbps の速度だけをサポートします。自動速度オプションは使用できません。
- 複数のセッションで同じ宛先ポートを共有できます。
- SD ポートがシャットダウンされると、共有されたすべてのセッションが SPAN トラフィックの生成を停止します。
- 発信フレームは、Extended Inter-Switch Link（EISL）フォーマットでカプセル化することができます。
- SD ポートにはポート VSAN がありません。
- Storage Services Module（SSM）を使用した SD ポートの設定はできません。
- SPAN セッションで使用中のポート モードは、変更できません。

（注）　SD ポート モードを別のポート モードに変更する必要がある場合は、まずすべてのセッションから SD ポートを削除し、次にポート モードを変更する必要があります。

ファイバ チャネル アナライザによるトラフィックのモニタリング

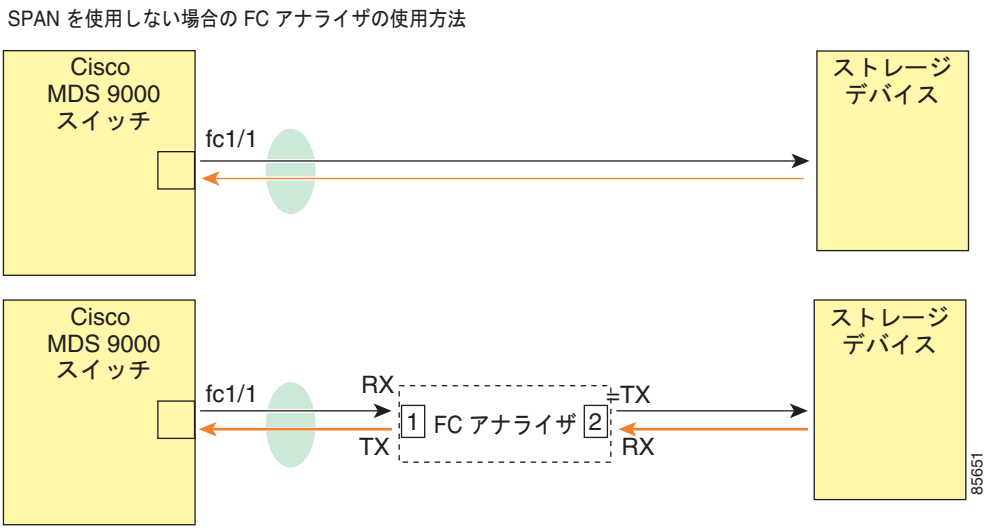
SPAN を使用すると、トラフィックを中断することなく、インターフェイス上でトラフィックをモニタできます。トラブルシューティング時においてトラフィックを中断することによって問題の環境が変更され、問題の再現が困難になる場合には、この機能が特に役立ちます。次の 2 つの方法のいずれかでトラフィックをモニタできます。

- SPAN を使用しない場合
- SPAN を使用する場合

SPAN を使用しないモニタリング

別のスイッチまたはホストに接続された Cisco MDS 9000 ファミリ スイッチのインターフェイス fc1/1 を使用して、トラフィックをモニタできます。インターフェイス fc1/1 を通るトラフィックを分析するには、スイッチとストレージ デバイスをファイバ チャネル アナライザで物理的に接続する必要があります（図 11-4 を参照）。

図 11-4　SPAN を使用しない場合のファイバ チャネル アナライザの使用方法



この接続タイプには、次のような制約があります。

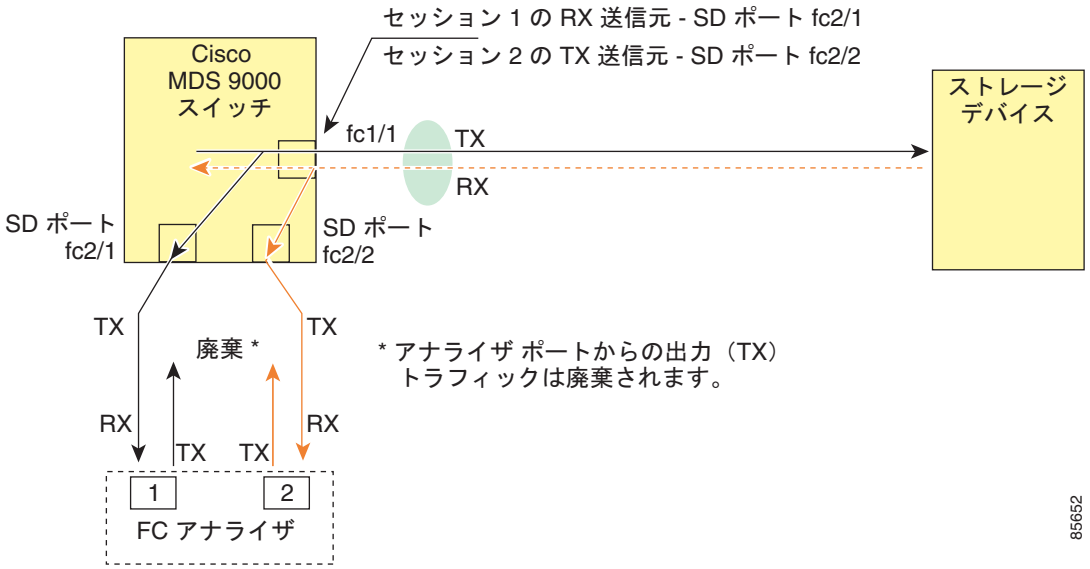
- 2 つのネットワーク デバイス間にファイバ チャネル アナライザを物理的に挿入する必要があります。
- ファイバ チャネル アナライザが物理的に接続されている場合は、トラフィックが中断されます。
- アナライザはポート 1 およびポート 2 の Rx リンクのデータだけをキャプチャします。ポート 1 はインターフェイス fc1/1 からの出力トラフィックを、ポート 2 はインターフェイス fc1/1 への入力トラフィックをキャプチャします。

SPAN を使用するモニタリング

SPAN を使用すると、前述のトラフィック（図 11-4 を参照）をトラフィックの中断なしでキャプチャできます。ファイバ チャネルアナライザはポート 1 の入力（Rx）リンクを使用して、インターフェイス fc1/1 から送信されるすべてのフレームをキャプチャします。また、ポート 2 の入力リンクを使用して、インターフェイス fc1/1 へのすべての入力トラフィックをキャプチャします。

SPAN を使用すると、SD ポート fc2/2 で fc1/1 の入力トラフィックをモニタしたり、SD ポート fc2/1 の出力トラフィックをモニタすることができます。このトラフィックは、FC アナライザでシームレスにキャプチャされます（図 11-5 を参照）。

図 11-5　SPAN を使用した場合のファイバ チャネル アナライザの使用方法

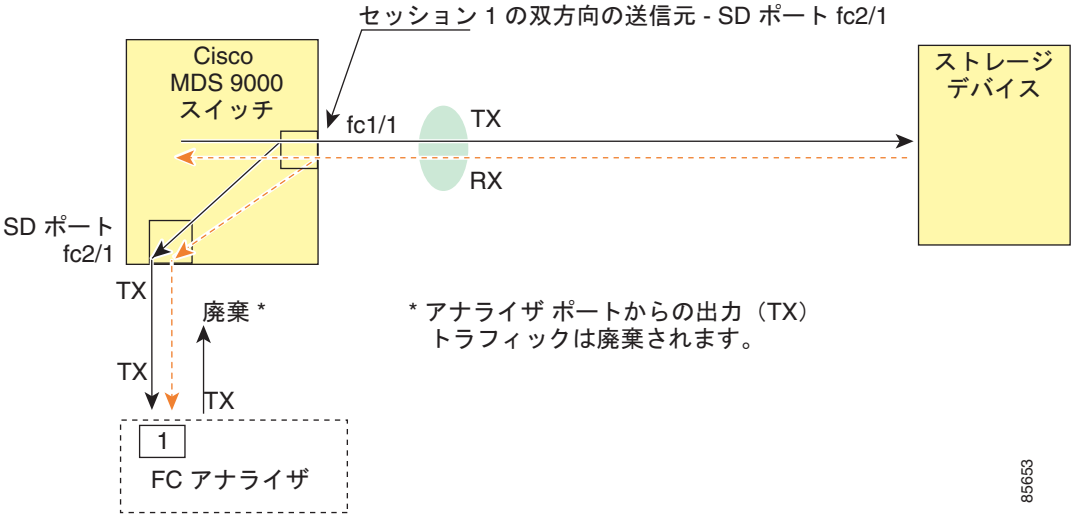


単一 SD ポートによるトラフィックのモニタ

任意のインターフェイス上で双方向トラフィックをモニタする場合、SD ポートを 2 つ使用する必要はありません（図 11-5 を参照）。同じ SD ポート fc2/1 でこのインターフェイスのトラフィックをモニタすることにより、SD ポートおよびファイバ チャネル アナライザ ポートを 1 つずつ使用することができます。

図 11-6 に、宛先ポート fc2/1 および送信元インターフェイス fc1/1 を含む 1 つのセッションを使用して、入力および出力方向のトラフィックをキャプチャする SPAN 設定を示します。この設定には、図 11-5 に示された設定よりも多くの利点があり、費用対効果に優れています。完全な 2 ポート アナライザを使用する代わりに、1 つの SD ポートとアナライザ上の 1 つのポートが使用されます。

図 11-6　単一 SD ポートを使用した場合のファイバ チャネル アナライザ

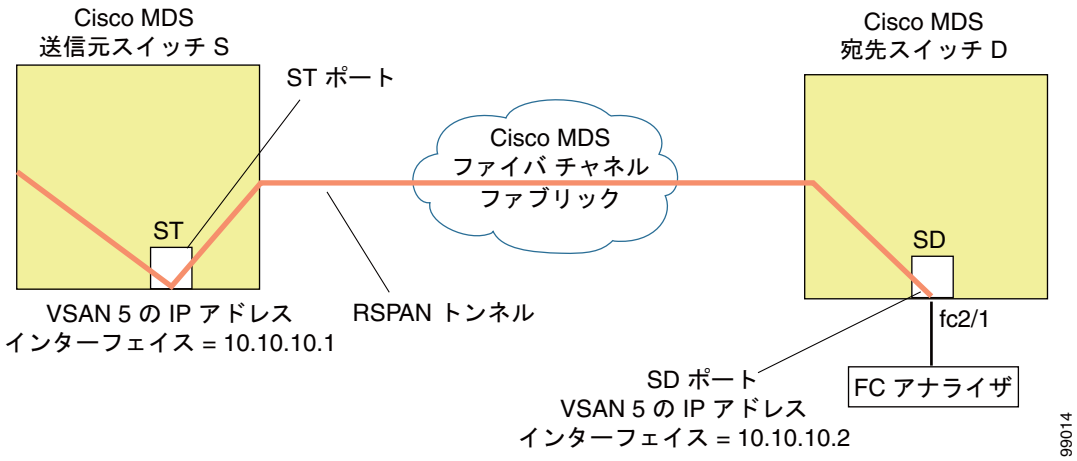


この設定を使用するには、キャプチャされたすべてのフレームの入出力トラフィックを区別する機能がアナライザに必要です。

SD ポート設定

宛先スイッチ内の SD ポートにより、FC アナライザは、ファイバ チャネル トンネルからの RSPAN トラフィックを受信できるようになります。図 11-7 に、RSPAN トンネル設定を示します。トンネル宛先もすでに設定されています。

図 11-7　RSPAN トンネル設定

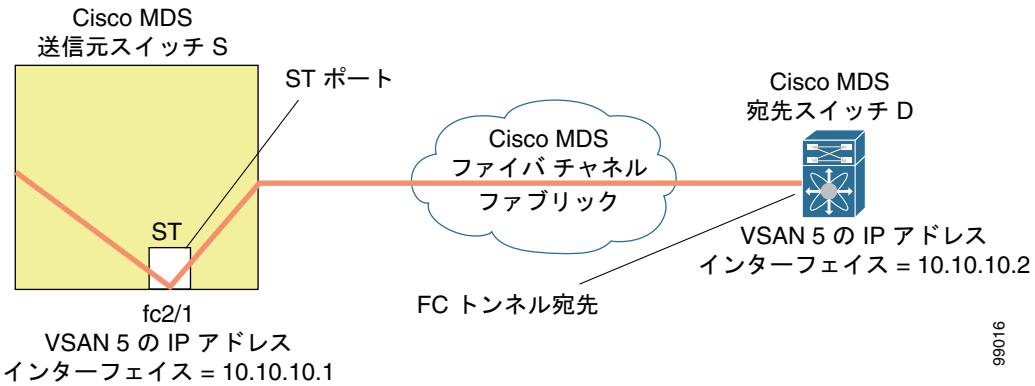


（注）　Storage Services Module（SSM）を使用した SD ポートの設定はできません。

FC トンネルのマッピング

tunnel-id-map オプションにより、宛先スイッチでのトンネルの出力インターフェイスが指定されます（図 11-8 を参照）。

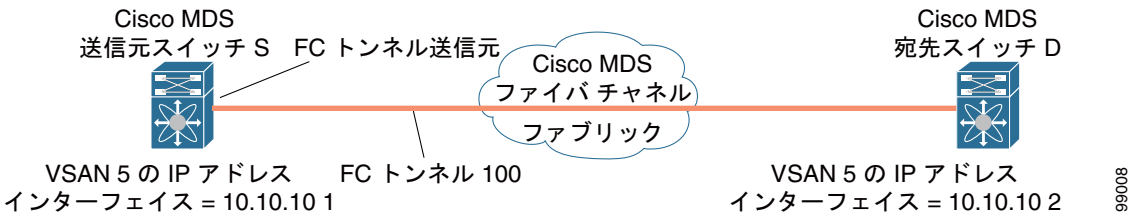
図 11-8　FC トンネル設定



VSAN インターフェイスの作成

図 11-9 に、基本的な FC トンネル設定を示します。

図 11-9　　FC トンネル設定



（注）　この例では、VSAN 5 が VSAN データベースですでに設定されているものとします。

リモート SPAN

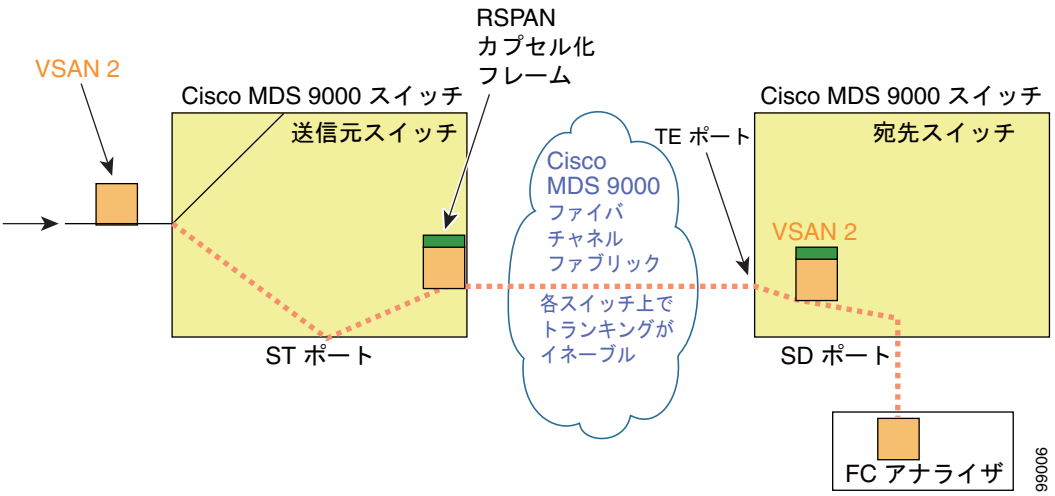
（注）　HP c-Class BladeSystem 対応 Cisco Fabric Switch および IBM BladeSystem 対応 Cisco Fabric Switch は、リモート SPAN をサポートしていません。

リモート SPAN（RSPAN）機能により、ファイバ チャネル ファブリック内の 1 台以上の送信元スイッチで配信される 1 つ以上の SPAN 送信元のトラフィックをリモートでモニタできるようになります。SPAN 宛先（SD）ポートは、宛先スイッチ内でリモート モニタリング用に使用されます。宛先スイッチは、一般に送信元スイッチとは別に用意されますが、同じファイバ チャネル ファブリックに接続されます。Cisco MDS 送信元スイッチでトラフィックをモニタするのと同様に、任意のリモートの Cisco MDS 9000 ファミリ スイッチまたはディレクタでトラフィックを複製し、モニタすることができます。

RSPAN 機能は他の機能に割り込むことなく、SPAN 送信元ポートのネットワーク トラフィックのスイッチングに影響しません。リモート スイッチ上でキャプチャされたトラフィックは、送信元スイッチから宛先スイッチに至るまでの経路上にあるすべてのスイッチ上でトランキングがイネーブルにされているファイバ チャネル ファブリック上をトンネリングされます。ファイバ チャネル トンネルは、トランク化された ISL（TE）ポートを使用して構造化されます。TE ポート以外にも、RSPAN 機能では他に 2 つのインターフェイス タイプが使用されます（図 11-10 を参照）。

- SD ポート：FC アナライザがリモート SPAN トラフィックを取得するために使用できるパッシブ ポート。
- ST ポート：SPAN トンネル（ST）ポートは、RSPAN ファイバ チャネル トンネル用の送信元スイッチ内の入口ポートです。ST ポートは、特別な RSPAN ポートであり、通常のファイバ チャネル トラフィックに使用することはできません。

図 11-10　RSPAN の送信



RSPAN の使用の利点

RSPAN 機能には、次の利点があります。

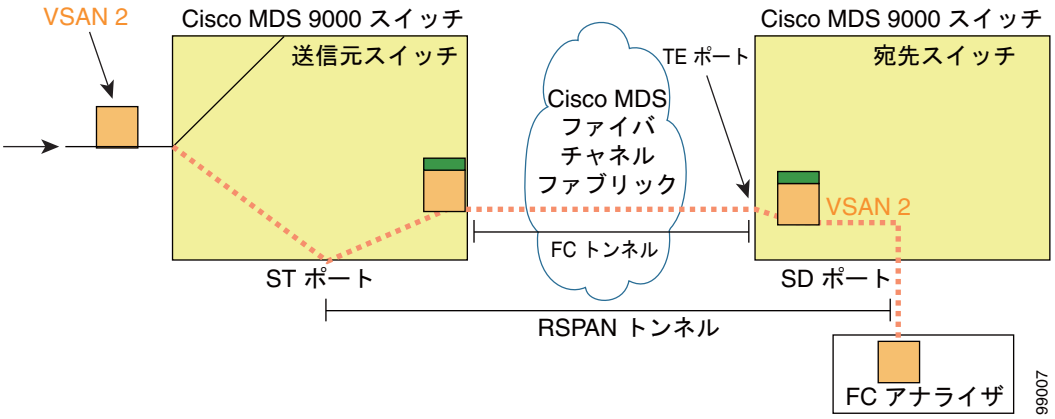
- 遠隔地での中断のないトラフィック モニタリングが可能になります。
- 複数のスイッチ上でリモート トラフィックをモニタするために 1 つの SD ポートを使用することにより、費用対効果に優れたソリューションを提供します。
- 任意のファイバ チャネル アナライザで動作します。
- Cisco MDS 9000 ポート アナライザ アダプタと互換性があります。
- 送信元スイッチ内のトラフィックに影響を与えません。ただし、ファブリック内の他のポートと ISL 帯域幅を共有します。

FC トンネルと RSPAN トンネル

FC トンネルは、送信元スイッチと宛先スイッチの間の論理的なデータ パスです。FC トンネルは、送信元スイッチから開始し、離れた場所にある宛先スイッチで終端します。

RSPAN では、送信元スイッチ内の ST ポートから開始し、宛先スイッチ内の SD ポートで終端する特別なファイバ チャネル トンネル（FC トンネル）が使用されます。FC トンネルを送信元スイッチ内の ST ポートにバインドし、それと同じ FC トンネルを宛先スイッチ内の SD ポートにマッピングする必要があります。マッピングとバインディングが設定されると、その FC トンネルは RSPAN トンネルと呼ばれます（図 11-11 を参照）。

図 11-11　FC トンネルと RSPAN トンネル

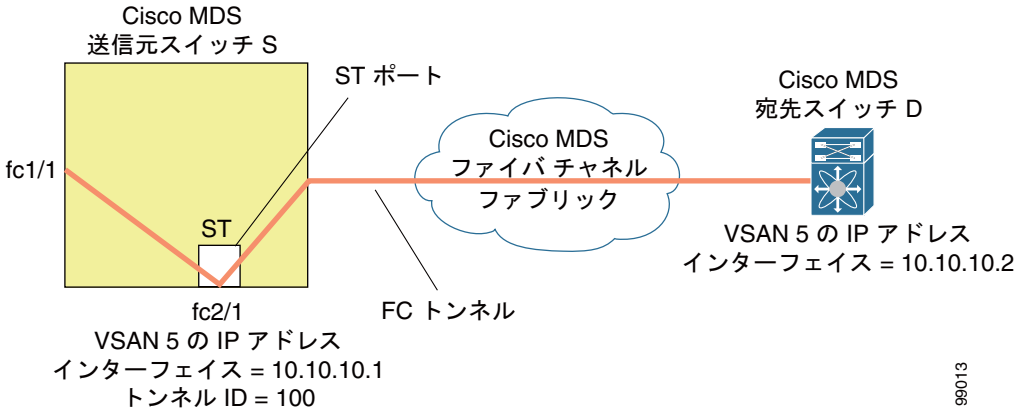


ST ポート設定

FC トンネルを作成した後、送信元スイッチにおいて、その FC トンネルにバインドされるように ST ポートを設定する必要があります。バインディングとマッピングが完了すると、その FC トンネルは RSPAN トンネルになります。

図 11-12 に、基本的な FC トンネル設定を示します。

図 11-12　FC トンネルのバインディング



ST ポートの特性

ST ポートには、次の特性があります。

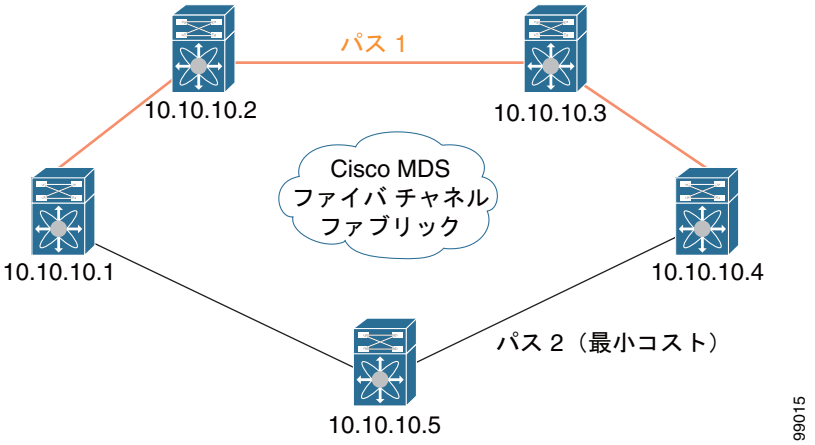
- ST ポートは、FC フレームの RSPAN カプセル化を実行します。
- ST ポートは、BB_credit を使用しません。
- 1 つの ST ポートは、1 つの FC トンネルにしかバインドできません。
- ST ポートは、RSPAN トラフィックの伝送以外には使用できません。
- ST ポートは、Storage Services Module（SSM）を使用して設定することはできません。

明示的なパスの作成

explicit-path オプションを使用して、Cisco MDS ファイバ チャネル ファブリックを通過する明示的なパスを指定できます（送信元ベース ルーティング）。たとえば、トンネル宛先に対して複数のパスがある場合、このオプションを使用して、FC トンネルが宛先スイッチまで常に 1 つのパスを使用するように指定できます。この場合、ソフトウェアは、他のパスが使用可能であっても、この指定されたパスを使用します。

このオプションが特に役立つのは、使用可能なパスが他にあるときでも特定のパスにトラフィックを誘導したい場合です。RSPAN の場合、RSPAN トラフィックが既存のユーザ トラフィックの妨げにならないように、明示的なパスを指定できます。1 台のスイッチ内で作成できる明示的なパスの数に制限はありません（図 11-13 を参照）。

図 11-13　明示的なパスの設定



注意事項と制限

SPAN 設定時の注意事項

SPAN を設定する場合は、次の注意事項と制限が適用されます。

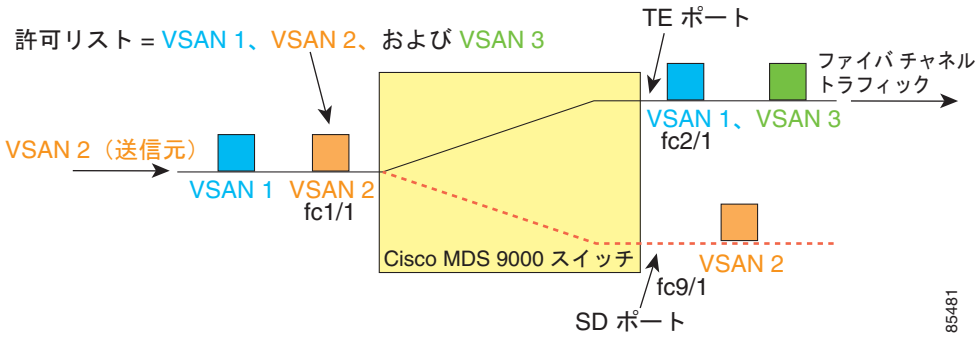
- 複数の入力（Rx）送信元には、最大 16 個の SPAN セッションを設定できます。
- 1 つの出力（Tx）ポートには、最大 3 個の SPAN セッションを設定できます。
- 32 ポート スイッチング モジュールでは、1 つのポート グループ（ユニット）内の 4 つのすべてのポートに、同じセッションを設定する必要があります。必要に応じて、このユニット内の 2 つまたは 3 つのポートだけを設定することもできます。
- 送信元の合計帯域幅が宛先ポートの速度を超えると、SPAN フレームは廃棄されます。
- 送信元ポートで廃棄されたフレームは、スパンされません。
- SPAN は、Fibre Channel over Ethernet（FCoE）ネットワーク内のポーズ フレームをキャプチャしません。仮想拡張（VE）ポートから送信されるポーズ フレームは、最も外側の MAC レイヤで生成および終端が行われるためです。FCoE の詳細については、『*Cisco NX-OS FCoE Configuration Guide for Cisco Nexus 7000 and Cisco MDS 9500*』を参照してください。

VSAN を送信元として設定する場合の注意事項

VSAN を送信元として設定する場合は、次の注意事項に従ってください。

- 送信元 VSAN に含まれるすべてのインターフェイスのトラフィックは、入力方向の場合にだけスパンされます。
- VSAN が送信元として指定されている場合は、VSAN に含まれるインターフェイス上でインターフェイスレベルの SPAN 設定を実行することができません。設定済みの SPAN 固有のインターフェイス情報は廃棄されます。
- VSAN 内のインターフェイスが送信元として設定されている場合は、この VSAN を送信元として設定できません。VSAN を送信元として設定する前に、まずこのようなインターフェイス上の既存の SPAN 設定を削除する必要があります。
- インターフェイスが送信元として含まれるのは、ポート VSAN が送信元 VSAN と一致する場合だけです。図 11-14 に、VSAN 2 を送信元として使用した場合の設定を示します。
  - スイッチ内のすべてのポートは、fc1/1 を除いて、VSAN 1 内にあります。
  - インターフェイス fc1/1 は、ポート VSAN 2 を含む TE ポートです。VSAN 1、2、および 3 は許可リスト内で設定されます。
  - VSAN 1 および VSAN 2 は、SPAN 送信元として設定されています。

図 11-14　送信元としての VSAN



この設定では、次のようになります。

  - 送信元としての VSAN 2 には、ポート VSAN 2 を持つ TE ポート fc1/1 だけが含まれます。
- ポート VSAN が VSAN 1 と一致しないため、送信元としての VSAN 1 には TE ポート fc1/1 が含まれません。

フィルタを指定する場合の注意事項

SPAN フィルタには、次の注意事項が適用されます。

- PortChannel 設定は、PortChannel 内にあるすべてのポートに適用されます。
- フィルタが指定されていない場合は、該当するインターフェイスのすべてのアクティブ VSAN からのトラフィックがデフォルトでスパンされます。
- セッションでは任意の VSAN フィルタを指定できますが、トラフィックをモニタできるのは、該当するポート VSAN 上、または該当するインターフェイスで許可されているアクティブ VSAN 上だけです。

RSPAN 設定時の注意事項

SPAN を設定する場合は、次の注意事項が適用されます。

- RSPAN トンネルのエンドツーエンドのパス上にあるすべてのスイッチは、Cisco MDS 9000 ファミリに属している必要があります。
- RSPAN トラフィックが含まれるすべての VSAN がイネーブルになっている必要があります。RSPAN トラフィックが含まれる VSAN がイネーブルになっていないと、そのトラフィックはドロップされます。
- RSPAN が実装されるファイバ チャネル トンネルのエンドツーエンドのパス内にある各スイッチ上で次の設定を実行する必要があります。
  - トランキングをイネーブルにし（デフォルトではイネーブル）、トランク対応リンクをパス内の最低コスト リンクにする必要があります。
  - VSAN インターフェイスを設定する必要があります。
  - ファイバ チャネル トンネル機能をイネーブルにする必要があります（デフォルトではディセーブル）。
  - IP ルーティングをイネーブルにする必要があります（デフォルトではディセーブル）。

（注） IP アドレスが VSAN と同じサブネット内である場合は、トラフィックがスパンされるすべての VSAN に対して VSAN インターフェイスを設定する必要はありません。

- 単一のファイバ チャネル スイッチ ポートを ST ポート機能専用にする必要があります。
- モニタ対象のポートを ST ポートとして設定してはなりません。
- FC トンネルの IP アドレスは、VSAN インターフェイスと同じサブネット内に存在する必要があります。

SPAN および RSPAN のデフォルト設定

表 11-1 に、SPAN パラメータのデフォルト設定値を示します。

表 11-1　SPAN パラメータのデフォルト設定値

パラメータ	デフォルト
SPAN セッション	アクティブ
フィルタが指定されていない場合	SPAN トラフィックには、すべてのアクティブ VSAN から特定のインターフェイスを経由するトラフィックが含まれます。
カプセル化	ディセーブル。
SD ポート	出力フレーム形式はファイバ チャネルです。

表 11-2 に、RSPAN パラメータのデフォルト設定を示します。

表 11-2　RSPAN パラメータのデフォルト設定値

パラメータ	デフォルト
FC トンネル	ディセーブル。
明示パス	設定されていません。
最小コスト パス	明示パスが設定されていない場合に使用されます。

SPAN の設定

Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）機能は、Cisco MDS 9000 ファミリ スイッチ特有のものです。SPAN は、ファイバ チャネル インターフェイスを通じてネットワーク トラフィックをモニタします。

この項では、次の項目について説明します。

SPAN の SD ポートの設定

手順の詳細

SD ポートを使用してネットワーク トラフィックをモニタするには、次の手順を実行します。

ステップ 1　SD ポートを設定します。

ステップ 2　指定した SPAN セッションに SD ポートを接続します。

ステップ 3　セッションに送信元インターフェイスを追加して、ネットワーク トラフィックをモニタします。

Device Manager を使用して SPAN モニタリングの SD ポートを設定するには、次の手順を実行します。

ステップ 1　設定するポートを右クリックして [Configure] を選択します。

通常のポート設定ダイアログボックスが表示されます。

ステップ 2　[Mode] で [SD] を選択します。

ステップ 3　[Apply] をクリックして変更を適用します。

ステップ 4　ダイアログボックスを閉じます。

SPAN の max-queued-packets の設定

SPAN 宛先ポートがオーバーサブスクライブ状態の場合や、送信元トラフィックが宛先ポートの速度を超えている場合、SPAN セッションの送信元ポートはそのスループットを下げます。影響の程度は、受け取る送信元トラフィックの量に比例します。max-queued-packets の値をデフォルト値の 15 から 1 に減らすと、送信元ポートに対する影響を防ぐことができます。送信元インターフェイスのスループットに影響を与える可能性があるため、この設定のデフォルト値を再考する必要があります。

制約事項

- SPAN の max-queued-packets は、スイッチで現在 SPAN セッションがアクティブでない場合にだけ変更できます。
- FCIP インターフェイスを通過するトラフィックをスパンしている場合、SD インターフェイスの帯域幅が、複製されるトラフィックの量を上回っている場合でも、SPAN コピーはドロップされます。SPAN ドロップを避けるため、max-queued-packets を、100 などの大きい値に設定します。

デフォルトでは、送信元インターフェイスの帯域幅の合計が宛先ポートの帯域幅を超えると、SPAN フレームは廃棄されます。値が大きいほど、SPAN トラフィックがデータ トラフィック スループットと引き換えに廃棄されるのではなく、SPAN 宛先に到達する可能性が高くなります。

SPAN セッションの作成

手順の詳細

SPAN セッションを作成するには、次の手順を実行します。

ステップ 1　[Interface] > [SPAN] を選択します。[SPAN] ダイアログボックスが表示されます。

ステップ 2　[Sessions] タブをクリックします。

ステップ 3　[Create] をクリックします。

[Create SPAN Sessions] ダイアログボックスが表示されます。

ステップ 4　上向きまたは下向き矢印キーを使用して 1 ～ 16 のセッション ID を選択し、[Create] をクリックします。

ステップ 5　作成するセッションごとにステップ 4 を繰り返します。

ステップ 6　該当するセッションの [Dest Interface] フィールドに宛先インターフェイスを入力します。

ステップ 7　該当するセッションの [Filter VSAN List] フィールドにフィルタ VSAN リストを入力します。

ステップ 8　[Admin] ドロップダウン リストで [active] を選択するか、アクティブな管理ステータスを選択します。

ステップ 9　[Apply] をクリックして変更を保存します。

ステップ 10　2 つのダイアログボックスを閉じます。

第 2 世代ファブリック スイッチ用の SPAN の設定

シスコの第 2 世代ファブリック スイッチ（MDS 9124 など）では、SPAN セッションが両方向（Rx と Tx）でサポートされます。

（注）　第 2 世代ファブリック スイッチを使用する場合、アクティブな SPAN セッションは 1 つしか作成できません。

制約事項

- 複数の SPAN 送信元インターフェイスを Rx 方向と Tx 方向で指定できます。
- 同じ SPAN セッション内に入力インターフェイスと出力インターフェイスを混在させることはできません。SPAN は、Rx 方向と Tx 方向が混在する設定をすべて拒否します。一方、単一方向で複数の SPAN 送信元インターフェイスを指定することはできます。

第 2 世代ファブリック スイッチでは、出力方向において 1 つの VSAN に対してのみ VSAN フィルタがサポートされます。この制限は、入力方向には適用されません。たとえば、TE ポートのインターフェイスで 1 ～ 5 のアクティブな VSAN が存在する場合、VSAN 2 に対して VSAN フィルタを指定すると、VSAN 2 上のトラフィックのみがフィルタリングされます。

SPAN 送信元の編集

手順の詳細

SPAN 送信元を編集するには、次の手順を実行します。

ステップ 1　[Interface] > [SPAN] を選択します。
[SPAN] ダイアログボックスが表示されます。

ステップ 2　[Sources] タブをクリックします。

ステップ 3　[VSAN List] フィールドに VSAN リスト名を入力します。

ステップ 4　[Edit Interface List] をクリックします。
[Source Interfaces] ダイアログボックスが表示されます。

ステップ 5　[Create] をクリックします。
[Source Interfaces Interface Sources] ダイアログボックスが表示されます。

ステップ 6　[browse] ボタンをクリックして、使用できる FC ポートのリストを表示します。

ステップ 7　ポートを選択し、[OK] をクリックします。

ステップ 8　指定する方向（[receive] または [transmit]）をクリックします。

ステップ 9　[Create] をクリックして FC インターフェイス送信元を作成します。

ステップ 10　開いている 3 つのダイアログボックスの [Close] をクリックし、それぞれのダイアログボックスを閉じます。

SPAN セッションの削除

手順の詳細

SPAN セッションを削除するには、次の手順を実行します。

ステップ 1　[Interface] > [SPAN] を選択します。

[SPAN] ダイアログボックスが表示されます。

ステップ 2　[Sessions] タブをクリックします。

ステップ 3　削除する SPAN セッションをクリックします。

ステップ 4　[Delete] をクリックします。

SPAN セッションが削除されます。

ステップ 5　ダイアログボックスを閉じます。

SPAN を使用したファイバ チャネル アナライザの設定

手順の詳細

SPAN を使用してファイバ チャネル アナライザを設定するには（図 11-5 の例を使用）、次の手順を実行します。

ステップ 1　セッション 1 を使用して SD ポート fc2/1 上でトラフィックを送信するように、インターフェイス fc1/1 の入力（Rx）方向に SPAN を設定します。

ステップ 2　セッション 2 を使用して SD ポート fc2/2 上でトラフィックを送信するように、インターフェイス fc1/1 の出力（Tx）方向に SPAN を設定します。

ステップ 3　ファイバ チャネル アナライザのポート 1 に fc2/1 を物理的に接続します。

ステップ 4　ファイバ チャネル アナライザのポート 2 に fc2/2 を物理的に接続します。

RSPAN の設定

RSPAN トンネルは、送信元スイッチ内で開始し、宛先スイッチ内で終端します。ここでは、スイッチ S が送信元となり、スイッチ D が宛先になると仮定しています。

前提条件

- 送信元スイッチと宛先スイッチに加え、ファイバ チャネル ファブリック内に Cisco MDS スイッチが存在する場合はそれらにも VSAN を設定する必要があります。

手順の詳細

RSPAN 機能を使用してネットワーク トラフィックをモニタするには、次の手順を実行します。

ステップ 1　ファイバ チャネル トンネル（FC トンネル）の作成に利用する VSAN インターフェイスを宛先スイッチ（スイッチ D）と送信元スイッチ（スイッチ S）に作成します。

ステップ 2　トンネルのエンドツーエンドのパス内にある各スイッチで FC トンネルをイネーブルにします。

ステップ 3　FC トンネルを開始し（スイッチ S）、そのトンネルを VSAN インターフェイスの IP アドレスにマッピングします（スイッチ D）。それにより、トンネルからのすべての RSPAN トラフィックが SD ポートに誘導されるようにします。

ステップ 4　宛先スイッチ（スイッチ D）で SPAN モニタリング用の SD ポートを設定します。

ステップ 5　送信元スイッチ（スイッチ S）で ST ポートを設定し、その ST ポートを FC トンネルにバインドします。

ステップ 6　送信元スイッチ（スイッチ S）でネットワーク トラフィックをモニタする RSPAN セッションを作成します。

送信元スイッチの設定

ここでは、送信元スイッチ（スイッチ S）で実行する必要のある作業を示します。

- 「VSAN インターフェイスの作成」（P.11-9）
- 「すべての中間スイッチの設定」（P.11-19）

すべての中間スイッチの設定

ここでは、RSPAN トンネルのエンドツーエンドのパス内にあるすべての中間スイッチで実行する必要のある作業を示します。

- 「VSAN インターフェイスの設定」（P.11-19）
- 「IP ルーティングのイネーブル化」（P.11-19）

VSAN インターフェイスの設定

図 11-7（P.11-8）に、宛先スイッチ（スイッチ D）で終端している RSPAN トンネル設定を示します。

（注）　この例では、VSAN 5 が VSAN データベースですでに設定されているものとします。

IP ルーティングのイネーブル化

IP ルーティング機能は、デフォルトではディセーブルになっています。ファブリック内のエンドツーエンドのパス内にある各スイッチ（送信元スイッチと宛先スイッチを含む）において IP ルーティングをイネーブルにする必要があります。この手順は、FC トンネルをセットアップするために必要です。

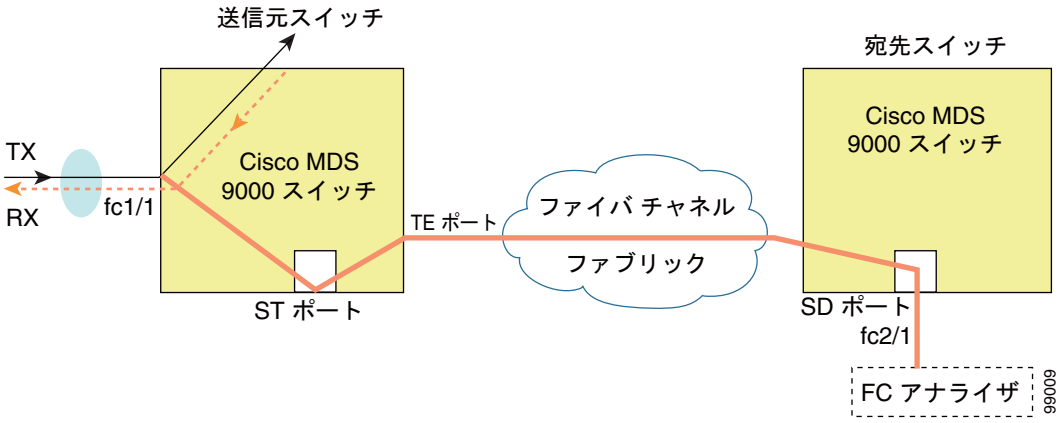
宛先スイッチの設定

ここでは、宛先スイッチ（スイッチ D）で実行する必要のある作業を示します。

RSPAN トラフィックのモニタリング

セッションを設定した後、必要に応じてこのセッションに対する他の SPAN 送信元を設定することもできます。図 11-15 に、宛先ポート fc2/1 および送信元インターフェイス fc1/1 を含む 1 つのセッションを使用して、入力および出力方向のトラフィックをキャプチャする RSPAN 設定を示します。

図 11-15　単一の SD ポートを使用して RSPAN トラフィックをモニタするファイバ チャネル アナライザ



この設定を使用するには、キャプチャされたすべてのフレームの入出力トラフィックを区別する機能がアナライザに必要です。

RSPAN の設定例

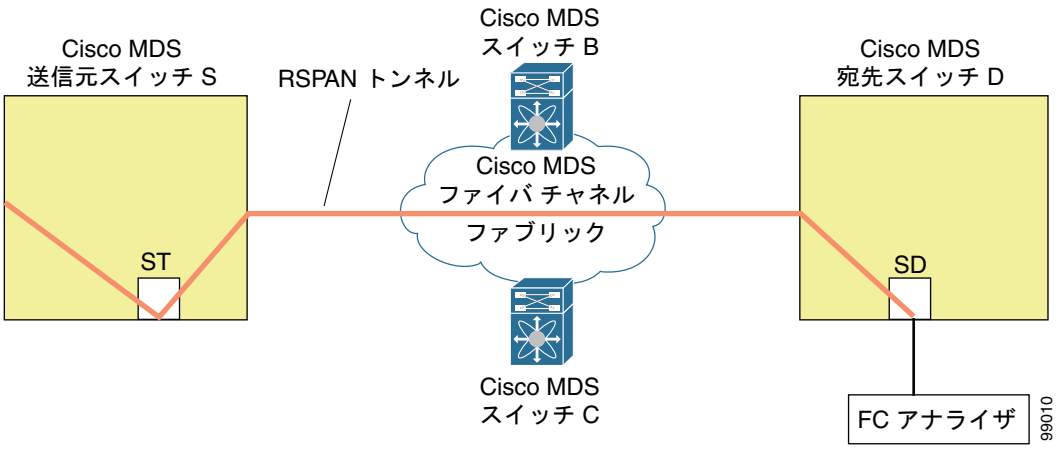
この項では、次の項目について説明します。

（注）　RSPAN は、SD ポートがローカル SPAN トラフィックをリモート SPAN トラフィックと一緒に転送するように、ローカル SPAN 機能と組み合わせることができます。ここでは、さまざまな SPAN 送信元とトンネルのシナリオが説明されます。

単一の送信元と 1 本の RSPAN トンネル

送信元のスイッチ S と宛先のスイッチ D がファイバ チャネル ファブリックを介して相互接続されます。RSPAN トンネルは SPAN セッションの宛先インターフェイスとして設定され、ST ポートは SPAN トラフィックを RSPAN トンネル経由で転送します（図 11-16 を参照）。

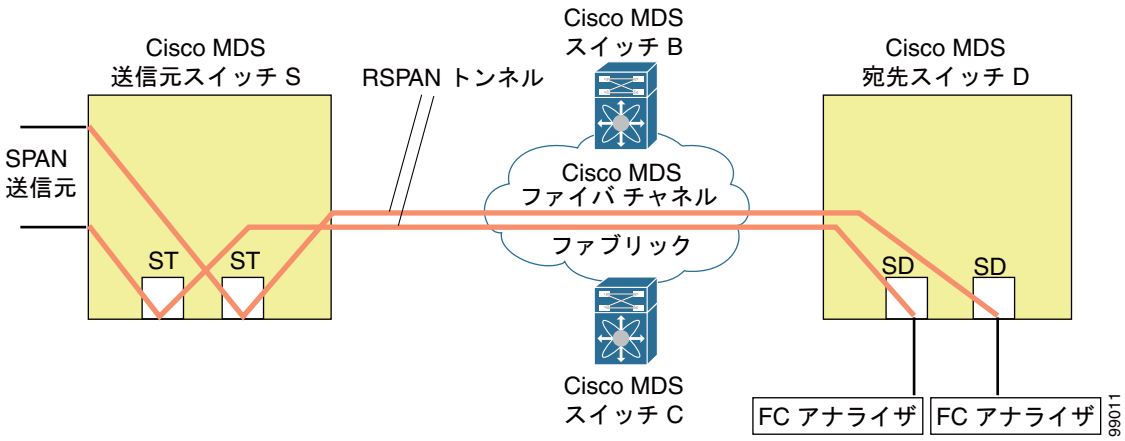
図 11-16　送信元スイッチが 1 台、宛先スイッチが 1 台、トンネルが 1 本の場合の RSPAN シナリオ



単一の送信元と複数の RSPAN トンネル

図 11-17 に、スイッチ S とスイッチ N の間に設定された 2 本の独立した RSPAN トンネルを示します。各トンネルの関連 ST ポートは送信元スイッチ内に存在し、独立 SD ポートは宛先スイッチ内に存在します。この設定は、トラブルシューティングの場合に役立ちます。

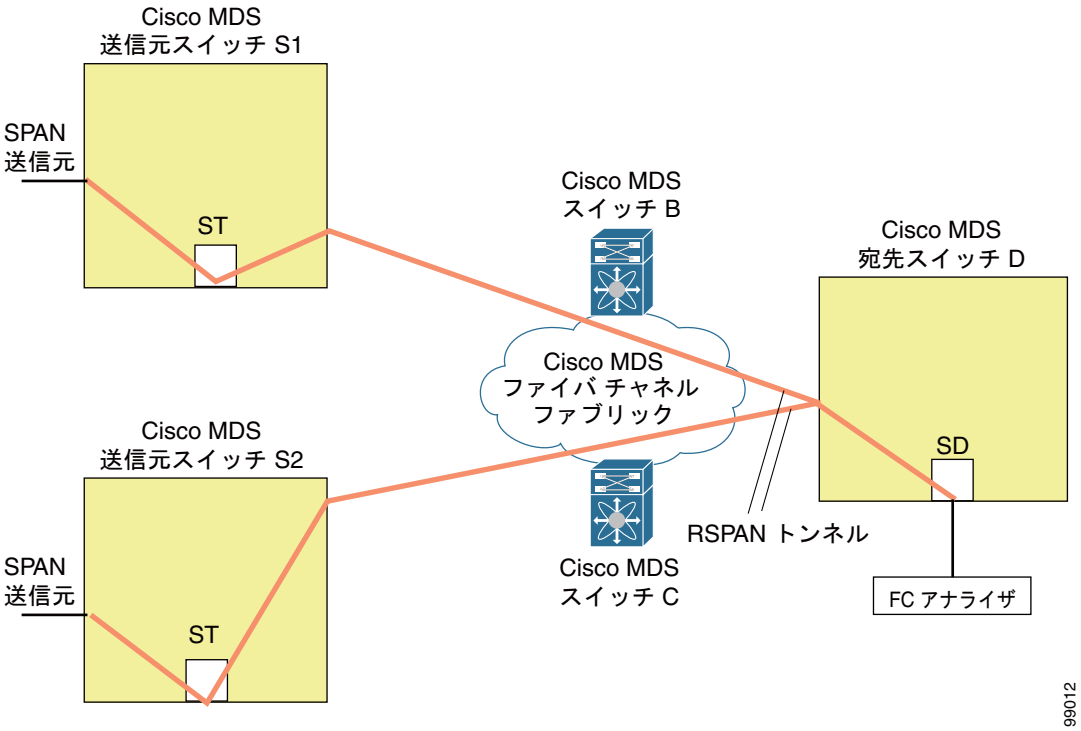
図 11-17　送信元スイッチが 1 台、宛先スイッチが 1 台、トンネルが複数の場合の RSPAN シナリオ



複数の送信元と複数の RSPAN トンネル

図 11-18 に、スイッチ S1 とスイッチ S2 の間に設定された 2 本の独立した RSPAN トンネルを示します。これらのトンネルは、関連 ST ポートがそれぞれ別々の送信元スイッチ内に存在し、両方とも宛先スイッチ内にある同じ SD ポートで終端します。

図 11-18　送信元スイッチが 2 台、宛先スイッチが 1 台、トンネルが複数の場合の RSPAN シナリオ



この設定は、リモート モニタリングの場合に役立ちます。たとえば、管理者は宛先スイッチからリモートで 2 台の送信元スイッチをモニタできます。

SPAN のフィールドの説明

ここでは、SPAN のフィールドの説明を示します。

SPAN セッション

フィールド	説明
Dest Interface	SPAN 宛先ポート インターフェイス。
Filter VSAN List	このセッションに割り当てられる VSAN。
Status Admin	アクティブなセッションを一時停止にするか、非アクティブのセッションをアクティブにします。
Status Oper	セッションの現在の状態。
Description	セッション ステータスの説明。
VSAN List	このセッションに割り当てられる VSAN。
Or Interface (Direction)	セッション用に設定される宛先ポート ID。
Inactive Reason	このセッションがアクティブになっていない理由の説明。

関連トピック

SPAN セッション

SPAN セッションの作成

SPAN セッションの削除

SPAN について

SPAN 送信元の編集

SPAN グローバル

フィールド	説明
MaxQueuedSpanPackets	このフィールドは、すべての SPAN セッションに対するドロップしきい値パケット数を指定します。[MaxQueuedSpanPackets] フィールドは、アクティブなセッションが存在しないときにのみ使用できます。

SPAN 送信元インターフェイス

フィールド	説明
[Interface]、[Direction]	セッション用に設定される宛先ポート ID、およびトラフィックの方向。

CHAPTER 12

Fabric Configuration Server の設定

この章では、Cisco MDS 9000 ファミリのディレクタとスイッチで提供されている Fabric Configuration Server（FCS）機能について説明します。内容は次のとおりです。

FCS について

Fabric Configuration Server（FCS）を使用すると、トポロジ属性を検出したり、ファブリック要素の設定情報リポジトリを維持したりすることができます。通常、管理アプリケーションは N ポートを通してスイッチの FCS に接続されます。FCS は次のオブジェクトに基づいて、ファブリック全体を表示します。

- Interconnect Element（IE）オブジェクト：ファブリック内の各スイッチは IE オブジェクトに対応しています。ファブリックは 1 つまたは複数の IE オブジェクトで構成されます。
- ポート オブジェクト：IE の各物理ポートはポート オブジェクトに対応しています。ポート オブジェクトにはスイッチ ポート（xE、Fx、および TL ポート）および接続された Nx ポートが含まれます。
- プラットフォーム オブジェクト：一連のノードをプラットフォーム オブジェクトとして定義して、管理可能な単一のエンティティにできます。これらのノードはファブリックに接続されたエンドデバイス（ホスト システム、ストレージ サブシステム）です。プラットフォーム オブジェクトは、ファブリックのエッジ スイッチ上にあります。

各オブジェクトには、それぞれ独自の属性および値のセットがあります。一部の属性にはヌル値も定義できます。

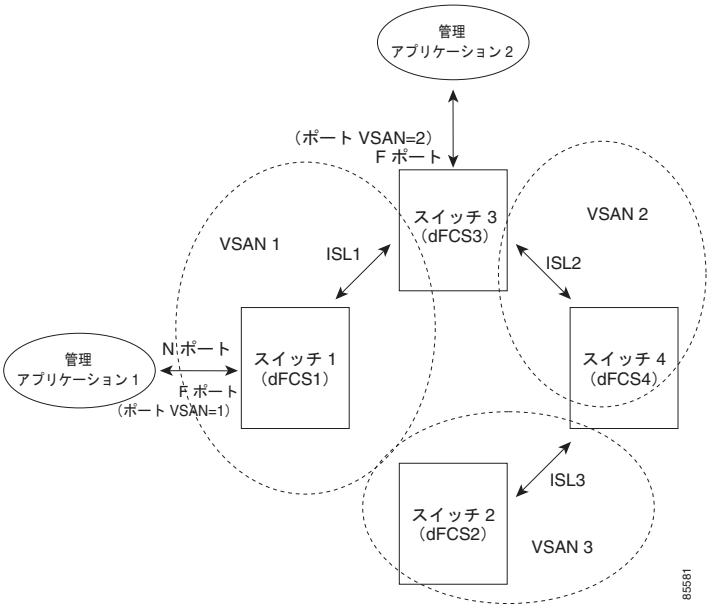
Cisco MDS 9000 ファミリ スイッチ環境では、複数の VSAN がファブリックを構成し、VSAN ごとに 1 つの FCS インスタンスが存在します。

Cisco NX-OS Release 4.1(1) から、FCS は仮想デバイスの検出をサポートしています。FCS コンフィギュレーション サブモードで **fcs virtual-device-add** コマンドを実行すると、特定の VSAN またはすべての VSAN で仮想デバイスを検出できます。IVR 用にゾーン分割されたデバイスは、IVR ゾーン セットをアクティブ化する前に、このコマンドで検出し、Request Domain ID（RDI）をイネーブルにする必要があります。

スイッチに管理アプリケーションが接続されている場合、スイッチの FCS に転送されるすべてのフレームは、スイッチ ポート（Fx ポート）のポート VSAN に属します。管理アプリケーションの表示対象はこの VSAN に限定されます。ただし、このスイッチが属する他の VSAN に関する情報は、SNMP または CLI を使用して取得できます。

図 12-1 では、管理アプリケーション 1（M1）は、ポート VSAN ID が 1 の F ポートを介して接続され、管理アプリケーション 2（M2）はポート VSAN ID が 2 の F ポートを介して接続されています。M1 はスイッチ S1 および S3 の FCS 情報を、M2 はスイッチ S3 および S4 の FCS 情報をそれぞれ問い合せることができます。スイッチ S2 の情報はどちらにも提供されません。FCS は、VSAN で表示可能なこれらのスイッチ上でだけ動作します。なお、S3 は VSAN 1 にも属していますが、M2 は VSAN 2 にだけ FCS 要求を送信できます。

図 12-1　　VSAN 環境における FCS



FCS の重要性

ここでは、FCS の重要性について説明します。

- FCS は次のようなネットワーク管理をサポートします。
  - N ポート管理アプリケーションはファブリック要素に関する情報を問い合せて、取得できます。
  - SNMP マネージャは FCS 管理情報ベース（MIB）を使用して、ファブリック トポロジ情報の検出を開始して、取得できます。
- FCS は、標準の F ポートおよび E ポートだけでなく、TE ポートと TL ポートもサポートします。
- FCS は、プラットフォームに登録された論理名および管理アドレスを使用して、一連のモードを維持することができます。FCS はすべての登録情報のバックアップをセカンダリ ストレージに維持し、変更があるたびに更新します。再起動またはスイッチオーバーが発生すると、FCS はセカンダリ ストレージ情報を取得し、データベースを再構築します。
- SNMP マネージャは FCS に、ファブリック内のすべての IE、ポート、およびプラットフォームについて問い合せることができます。

デフォルト設定

表 12-1 に FCS のデフォルト設定値を示します。

表 12-1　FCS のデフォルト設定値

パラメータ	デフォルト
プラットフォーム名のグローバル チェック	ディセーブル。
プラットフォームのノード タイプ	不明。

FCS の設定

Fabric Configuration Server（FCS）を使用すると、トポロジ属性を検出したり、ファブリック要素の設定情報リポジトリを維持したりすることができます。

ここでは、次の内容について説明します。

- 「FCS プラットフォームの作成」（P.12-3）

FCS プラットフォームの作成

手順の詳細

FCS プラットフォームを作成するには、次の手順を実行します。

ステップ 1　[FC] > [Advanced] > [Fabric Config Server] を選択します。

[Fabric Config Server] ダイアログボックスが表示されます。

ステップ 2　[Platforms (Enclosures)] タブをクリックします。

ステップ 3　[Create] をクリックします。

[Create Fabric Config Server] ダイアログボックスが表示されます。

ステップ 4　VSAN ID を入力します。または利用可能な VSAN ID のドロップダウン リストから ID を選択します。

ステップ 5　[Name] フィールドに、Fabric Configuration Server の名前を入力します。

ステップ 6　サーバの種類を選択します（**Gateway**、**Host**、**Storage**）。

ステップ 7　サーバの WWN を入力します。

ステップ 8　サーバの管理アドレスを入力します。

ステップ 9　[Create] をクリックしてサーバを作成します。または、[Close] をクリックし、変更を廃棄して [Fabric Config Server] ダイアログボックスに戻ります。

FCS 設定の確認

FCS 設定情報を表示するには、この項に記載された作業のいずれかを実行します。

ここで説明する内容は、次のとおりです。

FCS 検出情報の表示

手順の詳細

FCS 検出情報を表示するには、次の手順を実行します。

ステップ 1　[FC] > [Advanced] > [Fabric Config Server] を選択します。
[Fabric Config Server] ダイアログボックスが表示されます。

ステップ 2　[Discovery] タブをクリックします。

ステップ 3　[Discover] をクリックしてファブリックを再検出し、[Refresh] をクリックして表示内容を更新します。

FCS 要素の表示

手順の詳細

FCS Interconnect Element 情報を表示するには、次の手順を実行します。

ステップ 1　[FC] > [Advanced] > [Fabric Config Server] を選択します。
[Fabric Config Server] ダイアログボックスが表示されます。

ステップ 2　[Interconnect Elements] タブをクリックします。

ステップ 3　[Close] をクリックして、ダイアログボックスを閉じます。

FCS Fabric Port の表示

手順の詳細

FCS 検出情報を表示するには、次の手順を実行します。

ステップ 1　[FC] > [Advanced] > [Fabric Config Server] を選択します。
[Fabric Config Server] ダイアログボックスが表示されます。

ステップ 2　[Fabric Ports] タブをクリックします。

ファブリック ポートの一覧が表示されます。

ステップ 3　[Refresh] をクリックして表示内容を更新します。

FCS のフィールドの説明

ここでは、FCS のフィールドの説明を示します。

フィールド	説明
FabricConfigServer - Request Rejects	ファブリック コンフィギュレーション サーバが拒否時に通知を発行するかどうかを指定します。

その他の参考資料

FCS の実装に関する詳細情報については、次の項を参照してください。

- 「MIB」（P.12-5）

MIB

MIB	MIB のリンク
• CISCO-FCS-MIB	MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 http://www.cisco.com/en/US/products/ps5989/prod_technical_reference_list.html

INDEX

数字

A

B

C

D

E

F

H

I

N

O

Q

R

S

T

V

あ

い

え

お

か

け

こ

さ

し

す

そ

た

て

と