Cisco Fabric Manager システム管理 コンフィギュレーション ガイド

Cisco Fabric Manager System Management Configuration Guide

Cisco MDS NX-OS Release 4.1(1b) ～ 4.2(1)
2009 年 8 月

Text Part Number: OL-19583-01-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、米国シスコシステムズ発行ドキュメントの参考和訳です。米国サイト掲載ドキュメントとの差異が生じる場合があるため、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 Fabric Manager システム管理 コンフィギュレーション ガイド

CONTENTS

新しい情報および変更点

Cisco MDS NX-OS Release 4.2(1) では、次の情報に関する新しい機能固有のコンフィギュレーション ガイドで、ソフトウェア コンフィギュレーション情報が利用できるようになりました。

- 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にある情報は、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、現在でも Cisco.com で提供されており、MDS NX-OS Release 4.2(1) 以前のすべてのソフトウェア リリースで使用することをお勧めします。各ガイドでは、特定のリリースで導入された機能や利用できる機能について説明しています。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関する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 Command Line Interface（CLI; コマンドライン インターフェイス）、ファイル システム、および設定情報について説明します。

マニュアル タイトルの完全なリストについては、「はじめに」の関連資料のリスト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、シスコ システムズの Web サイトから入手可能な『*Cisco MDS 9000 Family Release Notes*』を参照してください。

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、MDS NX-OS Release 4.2(1) からのこのガイドの新機能および変更された機能を示します。

表 1　Cisco MDS NX-OS Release 4.2(x) の新機能と変更された機能

機能	新規および変更トピック	対象リリース	参照項目
[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 7 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 9 章「ドメイン パラメータの設定」

はじめに

ここでは、『Cisco Fabric Manager 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。さらに、関連資料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	Fabric Manager 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	SNMP の設定	SNMP を使用して、Fabric Manager で作成したロールを変更する方法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	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 10 章	SPAN によるネットワーク 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 11 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、かぎカッコ（< >）で囲んで示しています。
`[ ]`	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
`!, #`	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

このマニュアルでは、次の表記法を使用しています。

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

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

関連資料

Cisco MDS 9000 ファミリ向けのマニュアル セットには、次のマニュアルが含まれています。マニュアルをオンラインで検索するには、次のサイトにある 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 Storage Services Interface Images*』
- 『*Cisco MDS 9000 Family Release Notes for Cisco MDS 9000 EPLD Images*』
- 『*Release Notes for Cisco MDS 9000 Family Fabric Manager*』

準拠規格および安全情報

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

互換性情報

- 『*Cisco Data Center Interoperability Support Matrix*』
- 『*Cisco MDS 9000 NX-OS Hardware and Software Compatibility Information and Feature Lists*』
- 『*Cisco MDS NX-OS Release Compatibility Matrix for Storage Service Interface Images*』
- 『*Cisco MDS 9000 Family Switch-to-Switch Interoperability Configuration Guide*』
- 『*Cisco MDS NX-OS Release Compatibility Matrix for IBM SAN Volume Controller Software for Cisco MDS 9000*』
- 『*Cisco MDS SAN-OS Release Compatibility Matrix for VERITAS Storage Foundation for Networks Software*』

ハードウェアのインストール

- 『*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 Release 4.1(x) and SAN-OS 3(x) Software Upgrade and Downgrade Guide*』
- 『*Cisco MDS 9000 Family Storage Services Interface Image Install and Upgrade Guide*』
- 『*Cisco MDS 9000 Family Storage Services Module Software Installation and Upgrade 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 Fabric Manager

- 『*Cisco Fabric Manager Fundamentals Configuration Guide*』
- 『*Cisco Fabric Manager Interfaces Configuration Guide*』
- 『*Cisco Fabric Manager Fabric Configuration Guide*』
- 『*Cisco Fabric Manager Quality of Service Configuration Guide*』
- 『*Cisco Fabric Manager Security Configuration Guide*』
- 『*Cisco Fabric Manager IP Services Configuration Guide*』
- 『*Cisco Fabric Manager Intelligent Storage Services Configuration Guide*』
- 『*Cisco Fabric Manager High Availability and Redundancy Configuration Guide*』
- 『*Cisco Fabric Manager Inter-VSAN Routing Configuration Guide*』
- 『*Cisco Fabric Manager Online Help*』
- 『*Cisco Fabric Manager Web Services Online Help*』

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 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*』
- 『*Cisco MDS 9000 Family Secure Erase Configuration Guide*』
- 『*Cisco MDS 9000 Family Cookbook for Cisco MDS SAN-OS*』

トラブルシューティングおよび参照情報

- 『*Cisco NX-OS System Messages Reference*』
- 『*Cisco MDS 9000 Family NX-OS Troubleshooting Guide*』
- 『*Cisco MDS 9000 Family NX-OS MIB Quick Reference*』
- 『*Cisco MDS 9000 Family NX-OS SMI-S Programming Reference*』
- 『*Cisco MDS 9000 Family Fabric Manager Server Database Schema*』

CHAPTER 1

システム管理の概要

システム管理機能を使用し、Fabric Manager を使用してスイッチを監視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、リモートで監視されます。ログ メッセージは、システムをリブートすると消えます。

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。多様なメッセージ形式を使用できるため、ポケットベル サービス、標準 E メール、または XML ベースの自動解析アプリケーションと最適な互換性を保つことができます。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ル」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監視できます。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。

スイッチの状態の監視については、第 6 章「システム プロセスとログの監視」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 レイヤ 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、Fabric Manager 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 Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）標準のモニタリング規格です。RMON を使用すると、さまざまなネットワーク エージェントやコンソール システムが、ネットワーク モニタリング データを交換できます。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 スイッチを監視できます。

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 スイッチではランダムな ID が使用されます。

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。

スイッチド ポート アナライザ（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 トラフィックを監視します。すべてのファイバ チャネル インターフェイスを通過するトラフィックは、SPAN Destination ポート（SD ポート）と呼ぶ特殊なポートに複製されます。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 モードのインターフェイスは、通常のデータ トラフィック用に使用できません。ファイバ チャネル アナライザを SD ポートにアタッチして、SPAN トラフィックを監視できます。

SPAN 機能については、第 10 章「SPAN を使用したネットワーク トラフィックの監視」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 アトリビュートを検出したり、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 Servers 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 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。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分散します。

この章の内容は、次のとおりです。

CFS について

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。

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（NPV）
- FlexAttach 仮想 pWWN
- NTP
- Dynamic Port VSAN Membership
- Distributed Device Alias Services
- 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のプロトコル

- 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。

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 のスコープ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可能なポート 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。一度に 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しないと思われる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、3 つの段階にわかれます。

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 2 種類あります。

- 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、ポート セキュリティ設定などの、複数のスイッチで操作および配信が可能な情報の配信に使用されます。

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。

スイッチの CIFS 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なっています。アプリケーションは、データと設定情報を、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 対応スイッチに配信できます。これは通常の動作モードです。

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化し、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。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。

Fabric 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　[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。

CFS アプリケーション要件

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 には次の要件があります。

- 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、保留データベースによって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なデータベース）が上書きされます。
- 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した 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、アプリケーションによって異なります。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。一時バッファ内の変更はコミット操作を実行しなければ適用されません。

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 アプリケーションは、配信機能をイネーブルまたはディセーブルにすることができます。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。

アプリケーションの配信を明示的にイネーブルにしない限り、CFS はアプリケーションの設定は配信されません。

Fabric 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　CFS をイネーブルにする機能を選択します。たとえば、[Switches] > [Events] の順に展開し、[Physical Attributes] ペインで [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。

Fabric Manager が CFS の変更ステータスを受信すると、[Last Result] カラムが更新されます。

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。

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）別のユーザが設定作業を実行しようとしても、拒否されます。

変更のコミット

コミット動作は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、設定が変更されていない場合は、空のコミットを使用できます。この場合は、コミット動作によりロックを取得し、現在のデータベースを配信するセッションが開始されます。

CFS インフラストラクチャを使用して機能に対する設定変更をコミットした場合は、次のいずれかの応答に関する通知を受信します。

- 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。

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。

Fabric 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　CFS をイネーブルにする機能を選択します。たとえば、[Switches]、[Events] の順に展開し、[Physical Attributes] ペインで [CallHome] を選択します。

[Information] ペインの [CFS] タブに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　任意のスイッチの [Config Action] カラムの値を右クリックして、ドロップダウン メニューからオプション（[Copy]、[Paste]、[Export to File]、[Print Table]、[Detach Table]）を選択します。

ステップ 4　[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。

Fabric Manager は CFS の変更ステータスを取り込んで、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　[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　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。

ステップ 3　（オプション）この情報を必要とする CFS 機能の CFS 配信基準として、[Type] または [VsanID] を指定できます。

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　[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。

注意　変更をコミットしない場合、変更は実行コンフィギュレーションに保存されません。

変更の廃棄

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。

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

設定の保存

（保留データベースにまだ存在していて）適用されていない変更内容は、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なデータベースのコンフィギュレーションを上書きします。

注意　変更をコミットしない場合、変更は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。この機能には Admin 権限が必要です。

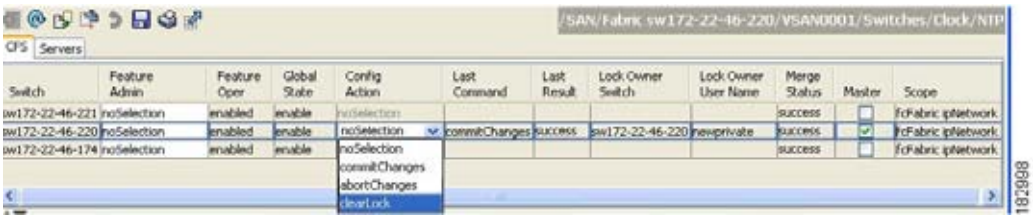
Fabric Manager を使用してロックをクリアするには、次の手順を実行します。

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（図 2-1 を参照）。

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。

図 2-1　ロックのクリア



注意　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。

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構成情報セットが異なっているために、マージ イベント中に調整が必要になることがあります。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 がサポートするプロトコルは、CFS レイヤで複雑なマージを処理することにより、必要なマージ数を 1 に削減します。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動作します。このプロトコルでは、ファブリック内の 1 つのスイッチがそのファブリックのマージ マネージャとして選択されます。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。

2 つのファブリック内のマージ マネージャは、マージ中にコンフィギュレーション データベースを相互に交換します。一方のデータベースのアプリケーションが情報をマージし、マージに成功したかどうかを判別して、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は、マージされたデータベースが結合されたファブリック内のすべてのスイッチに配信され、新規ファブリック全体が一貫したステートになります。マージ障害から回復するには、新規ファブリック内の任意のスイッチから配信を開始します。この配信により、ファブリック内のすべてのピアが同じコンフィギュレーション データベースに復元されます。

CFS 設定情報の表示

Device Manager を使用してスイッチの 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は、CFS を使用する各機能の配信ステータス（現在登録されているアプリケーションが CFS を使用しているかどうか、最後に成功したマージの結果）を表示します。

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。

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 が重複メッセージを送信することはありません。

- 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 2-2 はファイバ 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 2-2　ファイバ チャネル接続と IP 接続を持つネットワーク例 1

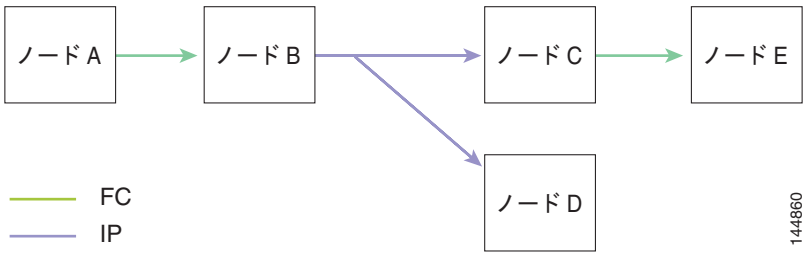


図 2-3 は、ノード D とノード E がファイバ チャネルを使用して接続されていることを除き、図 2-2 と同じです。ノード B にはノード C とノード D の IP 用配布リストがあるため、この例のすべてのプロセスは同じです。ノード D はすでにノード B からの配布リストに入っているため、ノード C はノード D に転送しません。

図 2-3　ファイバ チャネル接続と IP 接続を持つネットワーク例 2

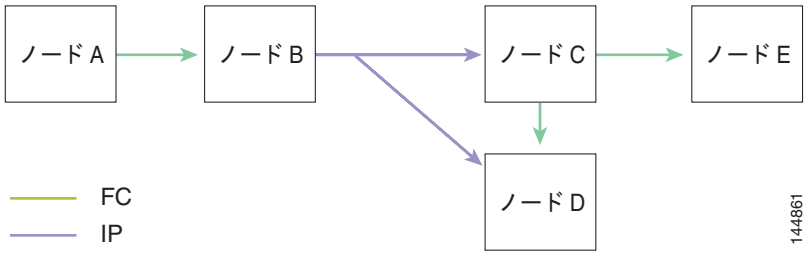
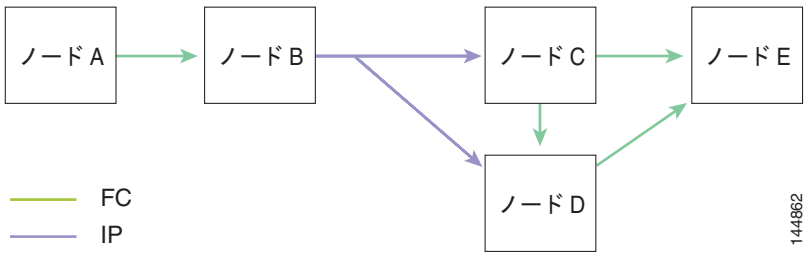


図 2-4 は、ノード D とノード E が IP を使用して接続されていることを除き、図 2-3 と同じです。ノード E はノード B からの配布リストに入っていないため、ノード C およびノード D は両方ともイベントをノード E に転送します。

図 2-4　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 のためのスタティック IP ピアの設定

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。

Cisco MDS Fabric Manager 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。

Fabric Manager 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。

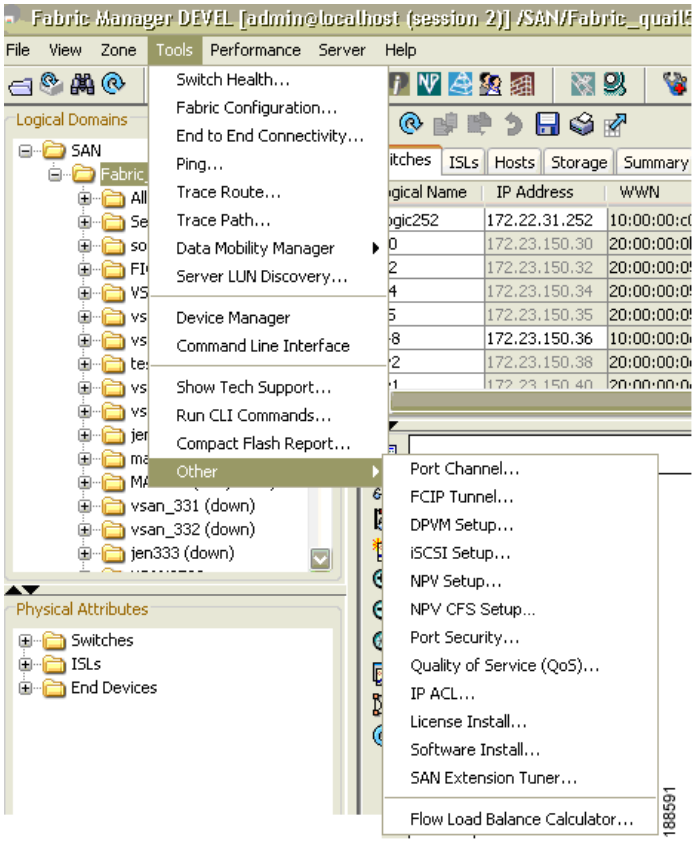
（注）　新しい NPV スイッチがファブリックに追加された場合、NPV CFS セットアップ ウィザードを起動してリストを更新する必要があります。これは、Fabric Manager でリストが自動的に更新されないためです。

リストへのピアの追加

Fabric Manager を使用してスタティック IP ピア リストを設定するには、次の手順を実行します。

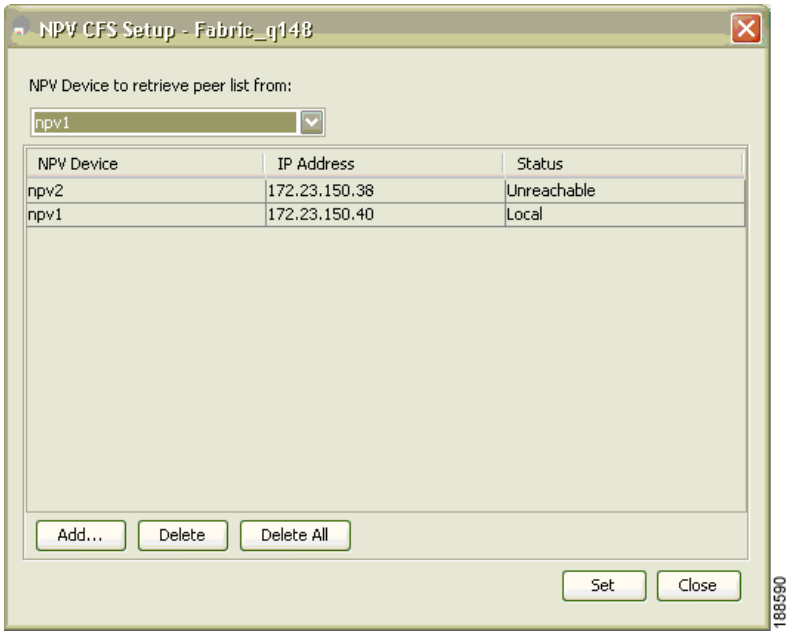
ステップ 1　Fabric Manager のメニューから、[Tools] > [Other] > [NPV CFS Setup] の順に選択します。

図 2-5　[NPV CFS Setup] メニュー



[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。

図 2-6　NPV Device Selection



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

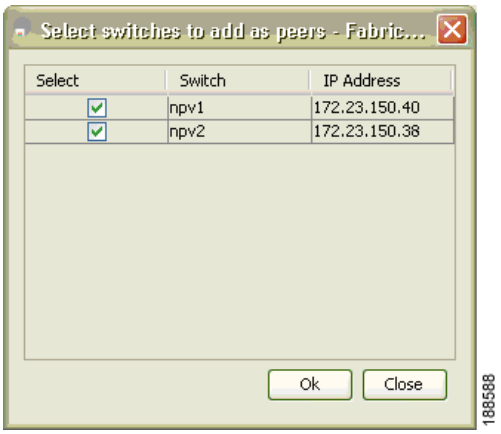
スイッチから取得したリスト内の NPV デバイスがファブリックに存在する場合、ステータスとして、Local、Reachable、Unreachable、Discovery in Progress のいずれかが表示されます。NPV デバイスがファブリック中に存在しない場合、ステータスは Not in Fabric と表示されます。

（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。

次の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。

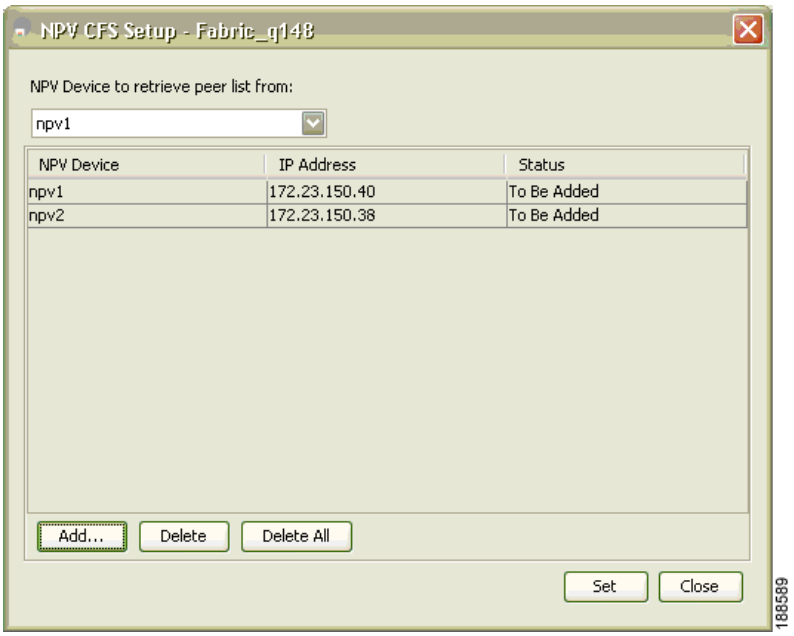
図 2-7　ピア選択



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。

図 2-8　ピア選択の確認



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

Fabric Manager を使用して 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　Fabric Manager のメニューから、[Tools] > [Other] > [NPV CFS Setup] の順に選択します。

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 ボックスから、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。

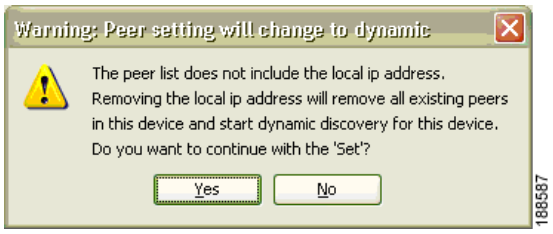
ステップ 3　次のいずれかの作業を行って、ピアまたはローカル ホストを削除済みとしてマークします。

- 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。次のメッセージ ボックスが表示されます。

図 2-9　動的なピア検出の開始



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。

```
-------------------------------------------------------------
 IP address    WWN name                  Status
-------------------------------------------------------------
 1.2.3.4       00:00:00:00:00:00:00:00   Discovery Inprogress
 1.2.3.5       20:00:00:0d:ec:06:55:b9   Reachable
 1.2.3.6       20:00:00:0d:ec:06:55:c0   Local
```

CFS リージョン

ここでは、次の内容について説明します。

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。VSAN 内には CFS リージョンを設定できません。

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 の範囲の番号で識別されます。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。リージョンは 1 ～ 200 まで設定できます。デフォルト リージョンは、下位互換性を維持します。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、新しいリージョンに割り当てられて、そのスコープがそのリージョンに制限される場合、配信またはマージの目的で他のすべてのリージョンを無視します。機能へのリージョンの割り当てには、初期物理スコープの配信に優先順位があります。

CFS リージョンを設定すると、複数の機能に設定を配信できます。ただし、所定のスイッチで所定の機能の設定を配信することができるのは、一度に 1 つの CFS リージョンだけです。一旦機能を割り当てた CFS リージョンは、その設定を別の CFS リージョン内に配信できなくなります。

Fabric Manager を使用した CFS リージョンの管理

ここでは、Fabric Manager 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。Fabric Manager 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。

- 「CFS リージョンの作成」（P.2-17）
- 「CFS リージョンへの機能の割り当て」（P.2-17）
- 「別のリージョンへの機能の移動」（P.2-18）
- 「リージョンからの機能の削除」（P.2-19）

CFS リージョンの作成

Fabric Manager を使用して 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] ペインの [Switches] フォルダを展開し、[CFS] をクリックします。

[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。

図 2-10 に、[Create a Region] ダイアログボックスを示します。

図 2-10　[Create a Region] ダイアログボックス

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

Fabric Manager を使用して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] ペインの [Switches] フォルダを展開し、[CFS] をクリックします。

[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。

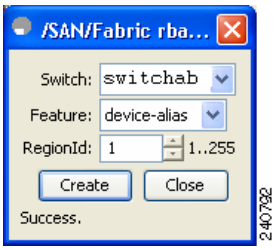
ステップ 2　[Feature by Region] タブをクリックします。

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。

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

図 2-11 に、[Assign a Feature] ダイアログボックスを示します。

図 2-11　[Assign a Feature] ダイアログボックス



ステップ 4　ドロップダウン ボックス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。

[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。

（注）　[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、次のセクションで説明する別のタスクで実行できます。

別のリージョンへの機能の移動

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。

Fabric Manager を使用して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。

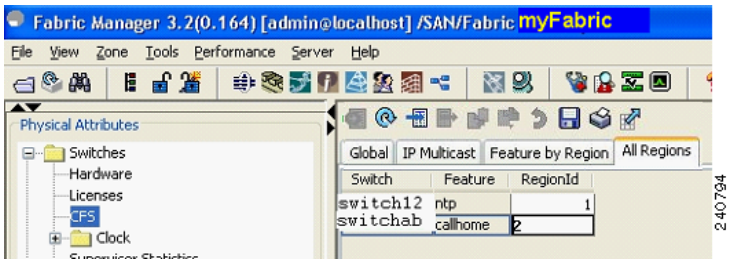
ステップ 1　[Physical Attributes] ペインの [Switches] フォルダを展開し、[CFS] を選択します。

[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。

図 2-12 は、[Feature by Region] タブを表示します。このタブには、すべてのスイッチと、その機能およびリージョンの詳細が表示されます。

図 2-12　[Feature by Region] タブ



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

Fabric Manager を使用して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。

図 2-13 に、確認ダイアログボックスを示します。

図 2-13　リージョンからの機能の削除

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

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。

図 2-14 に、確認ダイアログボックスを示します。

図 2-14　CFS リージョンの削除

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。

Fabric Manager を使用した CFS の例

この手順は、Fabric 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。

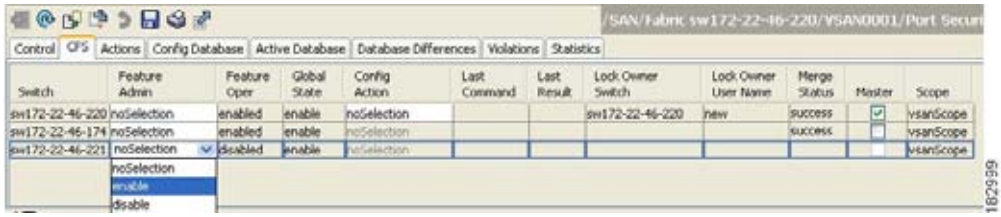
ステップ 1　設定する CFS 対応機能を選択します。たとえば、[Logical Domains] ペインで [VSAN] を展開してから、[Port Security] を選択します。

[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（図 2-15 を参照）。

図 2-15　CFS 設定



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。Fabric Manager 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（図 2-16 を参照）。

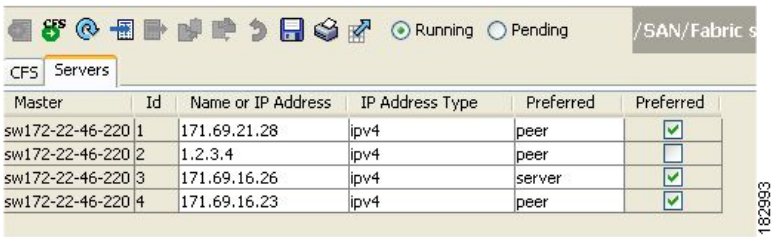
ステップ 8　機能の設定を変更します。たとえば、[Master] カラムの名前を右クリックし、[Create Row] を選択して、NTP 用のサーバを作成します。

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。

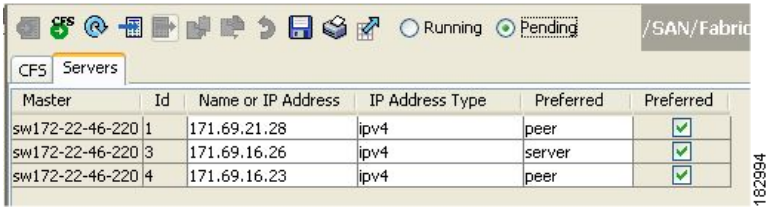
図 2-16　[Servers] タブ



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。

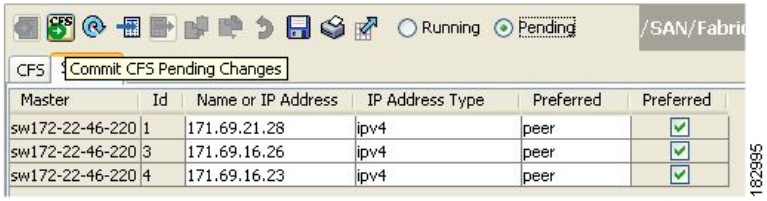
変更を加えると、ステータスが自動的に **Pending** に変わります（図 2-17 を参照）。

図 2-17　Pending へのステータス変更



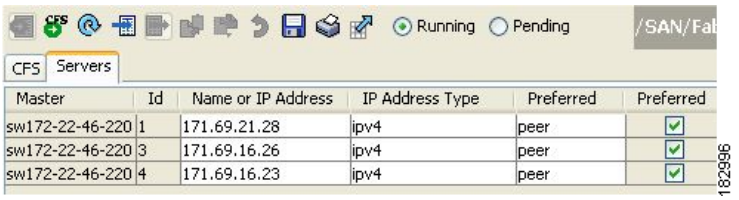
ステップ 10　[Commit CFS Pending Changes] アイコンをクリックして、変更内容を保存します（図 2-18 を参照）。

図 2-18　Commit CFS Pending Changes



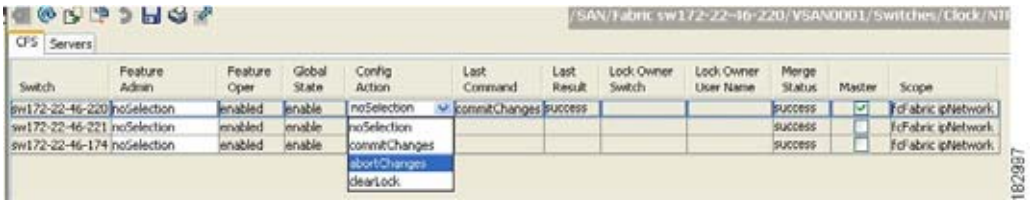
ステップ 11　ステータスが **Running** に変わります（図 2-19 を参照）。

図 2-19　Running へのステータス変更



ステップ 12　CFS をイネーブルにするスイッチごとに、[Config Action] ドロップダウン リストで [abortChanges] を選択します（図 2-20 を参照）。

図 2-20　設定変更のコミット



（注）　[enable] を選択した場合は、Fabric 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。

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。

Fabric Manager を使用して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、[Switches] 、[Events] 、の順に展開し、[Physical Attributes] ペインで [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

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。

Device Manager を使用して 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 がイネーブル化されていて、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。

（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。

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

CHAPTER 3

システム メッセージ ロギングの設定

この章では、Cisco MDS 9000 ファミリ スイッチでシステム 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。この章の内容は、次のとおりです。

システム メッセージ ロギングの概要

システム メッセージを監視するには、Fabric Manager 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、システムをリブートすると消えます。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	認証システム	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

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
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
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

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
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	システムは使用不能	LOG_EMERG
alerts	1	すぐに措置が必要	LOG_ALERT
critical	2	クリティカル状態	LOG_CRIT
errors	3	エラー状態	LOG_ERR
warnings	4	警告状態	LOG_WARNING
notifications	5	正常ではあるが注意を要する状況	LOG_NOTICE
informational	6	情報メッセージ	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 System Messages Reference*』を参照してください。

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。

ここで説明する内容は、次のとおりです。

- 「メッセージ ロギングの開始」（P.3-3）
- 「コンソールの重大度」（P.3-4）
- 「モジュール ロギング」（P.3-5）
- 「ログ ファイル」（P.3-6）
- 「システム メッセージ ロギング サーバ」（P.3-7）
- 「Fabric Manager Web サーバからの syslog サーバの確認」（P.3-9）
- 「Fabric Manager Web サーバからのログの参照」（P.3-10）

メッセージ ロギングの開始

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。

Fabric Manager を使用して 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。

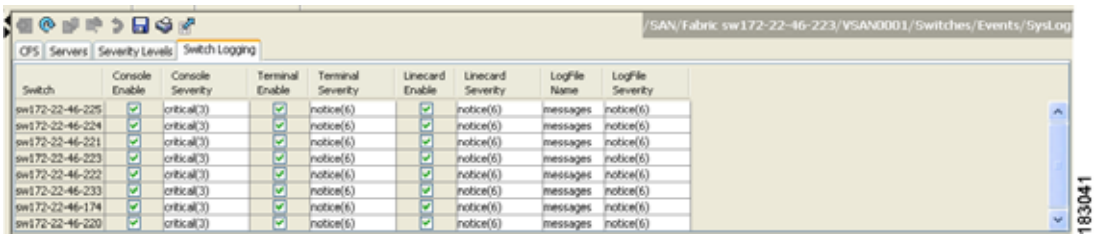
ステップ 2　[Switches]、[Events] の順に展開し、[Physical Attributes] ペインの [SysLog] を選択します。

[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。

図 3-1 に示すスイッチ情報が表示されます。

図 3-1　Fabric Manager の [Switch Logging] タブ



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。

コンソールの重大度

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。

ヒント　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。

Fabric Manager を使用してロギング 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。

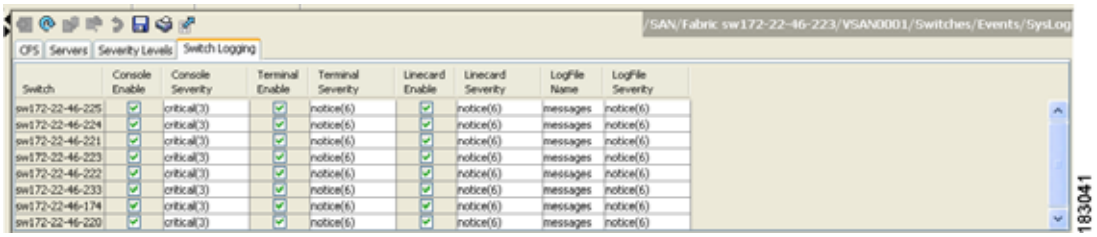
ステップ 2　[Switches]、[Events] の順に展開し、[Physical Attributes] ペインの [SysLog] を選択します。

[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。

図 3-2 に示すスイッチ情報が表示されます。

図 3-2　Fabric Manager の [Switch Logging] タブ



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

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。

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 Manager で、[Switches]、[Events] の順に展開し、[Physical Attributes] ペインの [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。

図 3-3 または図 3-4 に示すスイッチ情報が表示されます。

図 3-3　Fabric Manager の [Switch Logging] タブ

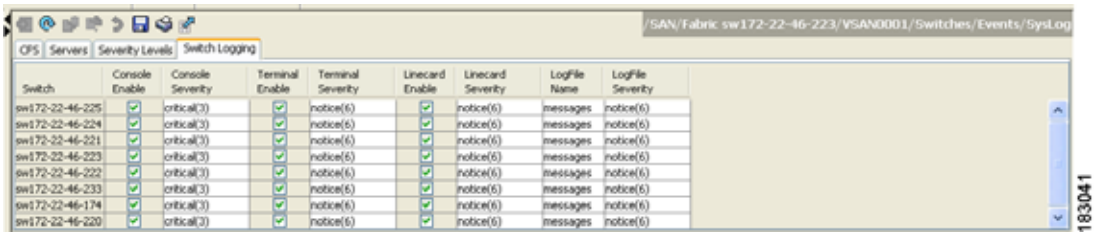
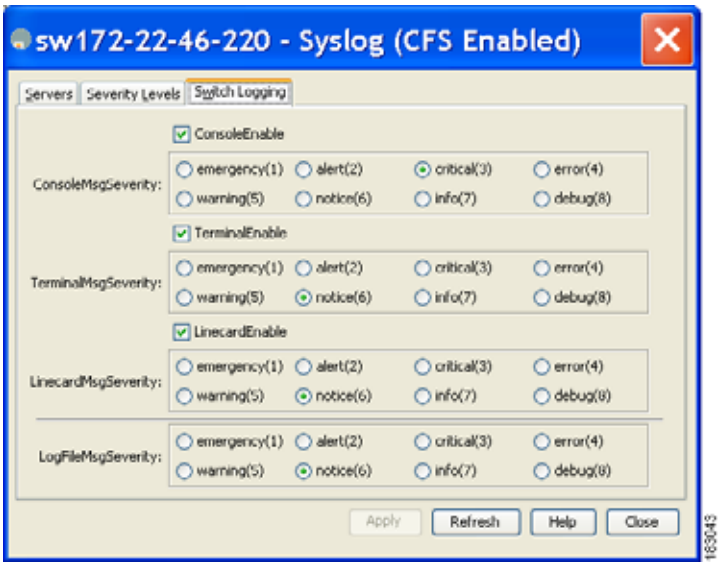


図 3-4　Device Manager の [Switch Logging] タブ



ステップ 2　メッセージ ロギングを実行する場所のチェックボックス（[ConsoleEnable]、[TerminalEnable]、[LineCardEnable]）をオンにします。

ステップ 3　Fabric Manager 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（図 3-3 を参照）。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（図 3-4 を参照）。

ステップ 4　Fabric Manager 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

ロギング メッセージはログ 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。

Fabric Manager を使用してログ 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　[Switches]、[Events] の順に展開し、[Physical Attributes] ペインの [SysLog] を選択します。

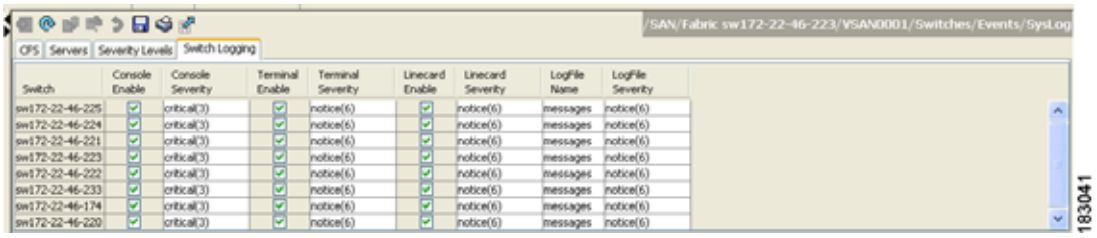
[Information] ペインに、SysLog 情報が表示されます。

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。

図 3-5 の情報が表示されます。

図 3-5　Fabric Manager の [Switch Logging] タブ



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。

（注）　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。

システム メッセージ ロギング サーバ

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。

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

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

ステップ 3　次のコマンドを実行して、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~
```

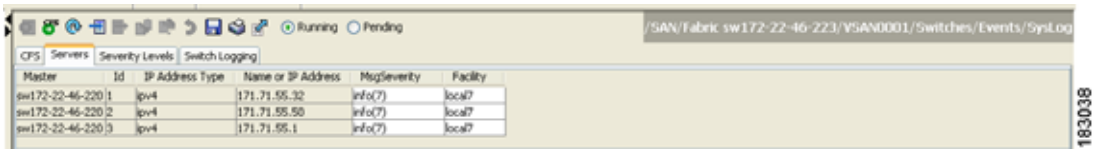
（注）　CFS を使用している機能の [Information] ペインのほとんどのタブは、[CFS] タブをクリックするまで薄く表示されます。[CFS] タブには、CFS がイネーブルになっているスイッチと、この機能のマスター スイッチが表示されます。[CFS] タブをクリックすると、CFS を使用している [Information] ペインの他のタブがアクティブになります。

最大 3 台の syslog サーバを設定できます。Fabric Manager 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 Fabric Manager にする必要があります。

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。

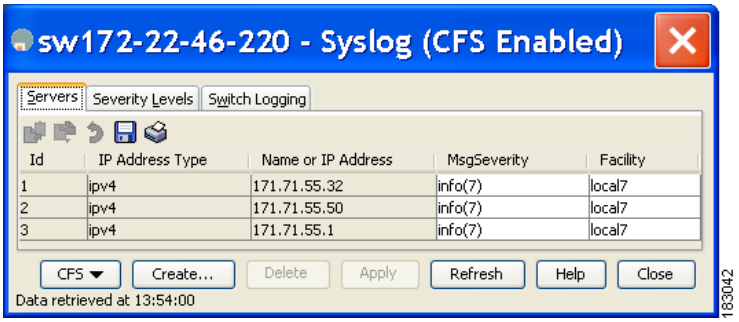
ステップ 1　Fabric Manager で、[Switches] 、[Events] の順に展開し、[Physical Attributes] ペインで [SysLog] を選択して、[Information] ペインで [Servers] タブをクリックします。

図 3-6　Fabric Manager の [Syslog] の [Servers] タブ



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。

図 3-7　Fabric Manager の [Syslog] の [Servers] タブ



ステップ 2　新しい syslog サーバを追加するには、Fabric Manager で [Create Row icon] をクリックするか、Device Manager で [Create] クリックします（図 3-7 を参照）。

ステップ 3　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 4　[MsgSeverity] オプション ボタンをクリックしてメッセージの重大度しきい値を設定し、[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 5　Fabric Manager 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。

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 MDS 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）。

Fabric Manager Web サーバからの syslog サーバの確認

syslog サーバを、Fabric Manager 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　Fabric Manager Web Server で使用するブラウザを指定します。

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。

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	認証システム	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

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
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
user	ユーザ プロセス	標準
uucp	UNIX 間コピー プログラム	標準

Fabric Manager Web サーバからのログの参照

Fabric Manager Web Server 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　Fabric Manager Web Server で使用するブラウザを指定します。

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

Fabric Manager Server 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。

（注）　**show logging** コマンドを使用すると、スイッチで設定されているロギング レベルがデフォルトのレベルと違う場合にだけ出力が表示されます。

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	message（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	未設定
サーバ数	3 台
サーバ ファシリティ	local7

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。多様なメッセージ形式を使用できるため、ポケットベル サービス、標準 E メール、または XML ベースの自動解析アプリケーションと最適な互換性を保つことができます。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。

（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、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 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。

この章の内容は、次のとおりです。

Call Home の機能

Call Home 機能は、Cisco MDS 9000 ファミリを通じて直接利用できます。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。柔軟なメッセージ配信オプションとフォーマット オプションにより、特定のサポート要件を簡単に組み込むことができます。

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されたレポートに適してします。
  - プレーンテキスト：人間が読むのに適した、フォーマット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 フォーマットを使用すると、Cisco Systems Technical Assistance Center とやり取りできるようになります。
- 複数の同時メッセージ宛先。宛先プロファイルごとに、最大 50 件の E 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。

Smart Call Home の概要

Smart Call Home は、Cisco SMARTnet Service のコンポーネントであり、選択したシスコ製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 は次の機能を提供します。

- 継続的なデバイスのヘルス監視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。
- ダウンロード可能な Transport Gateway（TG）集約ポイントを通じた、セキュアなメッセージ転送。TG 集約ポイントは、複数のデバイスに対するサポートが必要な場合や、セキュリティ要件によってデバイスを直接インターネットに接続することが禁止されている場合に使用します。
- すべての Call Home デバイスの Call Home メッセージおよび推奨事項、コンポーネントと設定情報への Web ベースのアクセス。関連する Field Notice、Security Advisory、End-of-Life 情報へのアクセスを提供します。

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。	ありません。
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）	ありません。
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 の入手

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。

登録には次の項目が必要です。

- 使用しているスイッチの SMARTnet 連絡先番号
- E 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 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。次の点に注意してください。

- 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、E メール、Cisco Smart Call Home などの自動化されたサービスのどれなのかによって変わります。
- 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 スイッチは、E メール サーバと IP 接続できることが必要です。
- 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。

Call Home を設定するには、次の手順を実行します。

ステップ 1　連絡先情報を割り当てます。

ステップ 2　宛先プロファイルを設定します。

ステップ 3　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 4　E メール オプションを設定します。

ステップ 5　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 6　Call Home メッセージをテストします。

コンタクト情報の設定

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、コンタクト 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。

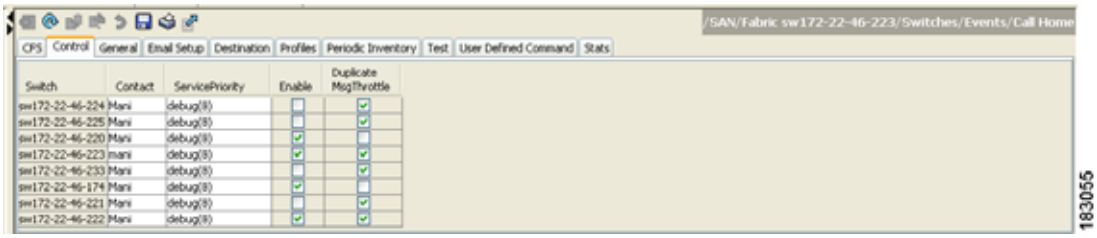
（注）　スイッチ プライオリティは、ファブリック内の各スイッチ固有です。このプライオリティは、運用要員または TAC サポート要員によって、最初に対処すべき Call Home メッセージを決定するために使用されます。各スイッチから送信される重大度が同じ Call Home アラートに優先順位を設定できます。

Fabric Manager を使用して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　Fabric Manager の [Physical Attributes] ペインで、[Switches]、[Events] の順に展開し、[Call Home] を選択します。

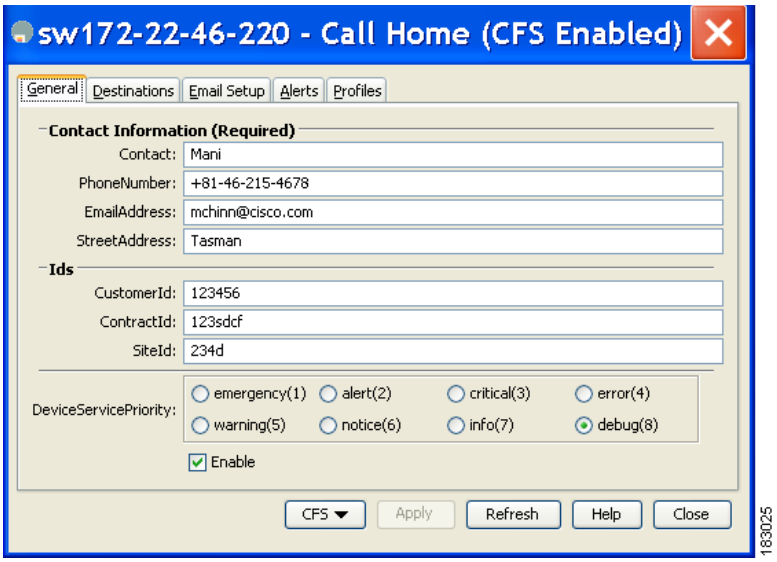
[Information] ペインに [Call Home] タブが表示されます（図 4-1 を参照）。

図 4-1　Fabric Manager の [Call Home]



ステップ 2　Device Manager で、[Admin] > [Events] > [Call Home] の順にクリックします。図 4-2 を参照してください。

図 4-2　Device Manager の [Call Home]



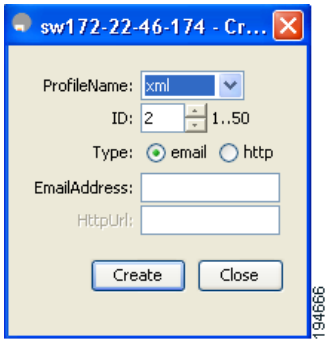
ステップ 3　[General] タブをクリックし、連絡先情報を割り当てて Call Home 機能をイネーブルにします。Call Home はデフォルトではイネーブルになっていません。Call Home 通知の送信元を識別する E メール アドレスを入力する必要があります。

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。図 4-3 に示す宛先作成ウィンドウが表示されます。

図 4-3　宛先作成ウィンドウ



b.　プロファイル名、ID、宛先の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　Fabric Manager 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。

宛先プロファイル

宛先プロファイルには、アラート通知で必要な配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。1 つ以上の宛先プロファイルが必要です。1 つ以上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。

（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）。

宛先プロファイルに対し、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、転送メカニズムに関係する実際のアドレスです。
- メッセージ フォーマット：アラートを送信するために使用するメッセージ フォーマット（フル テキスト、ショート テキスト、XML）。

Fabric Manager を使用して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。

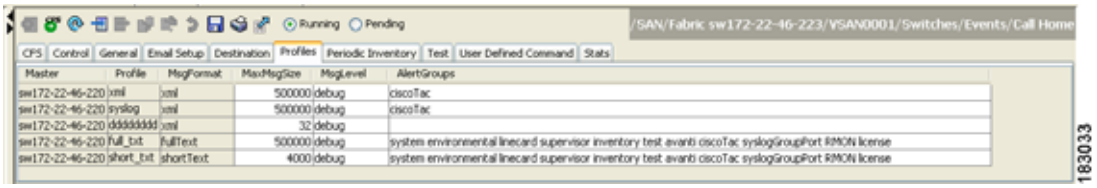
ステップ 1　[Switches]、[Events] の順に展開し、[Physical Attributes] ペインの [Call Home] を選択します。

（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。

図 4-4 に示すように、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。

図 4-4　複数のスイッチに対する Call Home プロファイル



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。

Fabric Manager を使用して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。

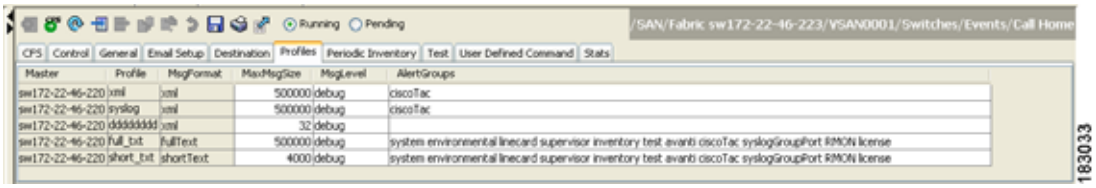
ステップ 1　[Switches]、[Events] の順に展開し、[Physical Attributes] ペインの [Call Home] を選択します。

（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。

図 4-5　　複数のスイッチに対する Call Home プロファイル



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

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 ファミリのすべてのスイッチでサポートされています。さまざまなタイプの Call Home アラートが、そのタイプに従ってさまざまなアラート グループに分類されています。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。

（注）　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。

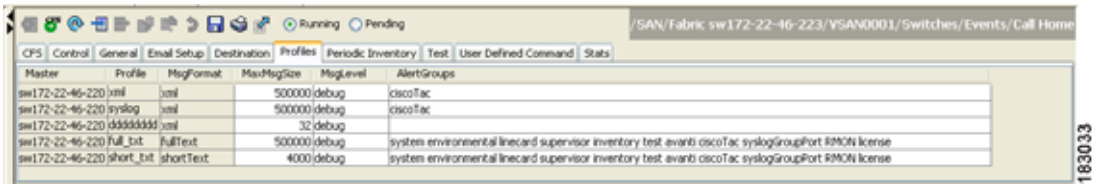
Fabric Manager を使用してアラート グループを宛先プロファイルに関連付けるには、次の手順を実行します。

ステップ 1　[Switches]、[Events] の順に展開し、[Physical Attributes] ペインの [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。

図 4-6 に示すように、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。

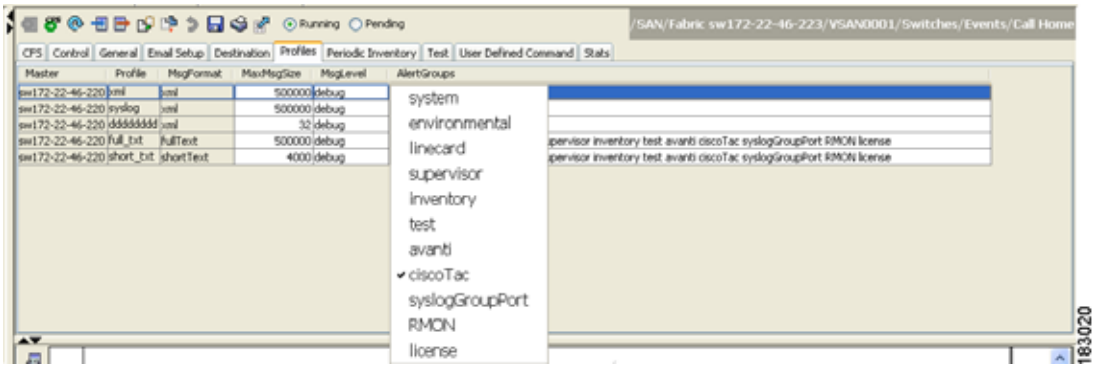
図 4-6　複数のスイッチに対する Call Home プロファイル



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。

図 4-7 に示すアラート グループ ドロップダウン メニューが表示されます。

図 4-7　アラート グループ ドロップダウン メニュー



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。

カスタマイズされたアラート グループ メッセージ

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、有効な **show** コマンドを追加で実行できます。これらの追加の **show** コマンドの出力は、定義済みの **show** コマンドの出力とともに、通知メッセージに格納されます。

（注）　1 つのアラート グループには、最大 5 個のユーザ定義 **show** コマンドを割り当てることができます。アラート グループには **show** コマンドだけを割り当てることができます。

（注）　カスタマイズされた **show** コマンドは、フルテキストおよび XML アラートのグループだけでサポートされます。ショート テキスト アラート グループ（short-txt-destination）では、テキストが 128 バイトに制限されるため、カスタマイズされた **show** コマンドはサポートされません。

アラートを送信するときに実行する **show** コマンドを割り当てるには、コマンドをアラート グループに割り当てる必要があります。アラートを送信する際、Call Home はアラート グループをアラート タイプに関連付け、**show** コマンドの出力をアラート メッセージに添付します。

（注）　**show** コマンドが定義されているシスコ以外の TAC アラート グループに対する宛先プロファイルと、シスコ TAC アラート グループに対する宛先プロファイルが、同じでないことを確認してください。

Fabric Manager を使用したアラート グループ メッセージのカスタマイズ

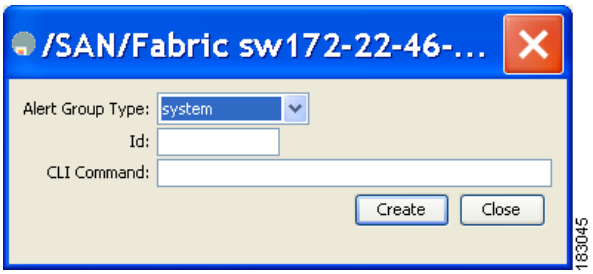
Fabric Manager を使用して Call Home アラート グループ メッセージをカスタマイズするには、次の手順を実行します。

ステップ 1　[Switches]、[Events] の順に展開し、[Physical Attributes] ペインの [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。

図 4-8 に示すユーザ定義コマンド情報が表示されます。

図 4-8　ユーザ定義コマンド ダイアログボックス



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、手順 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 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。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）。

（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。

Fabric Manager を使用した Call Home メッセージ レベルの設定

Fabric Manager を使用して、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　Fabric Manager で、[Physical Attributes] ペインの [Switches] フォルダを展開し、[Events] を展開して、[Call Home] を選択します。

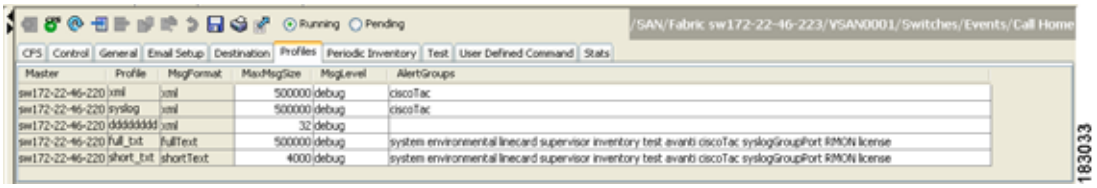
[Information] ペインに、Call Home 情報が表示されます。

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。

図 4-9 に示すように、Call Home プロファイルが表示されます。

図 4-9　Call Home プロファイル



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

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。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.4-30）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

ファイルを syslog アラート グループに関連付け（現在、syslog アラート グループは syslog-group-port しかありません）、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 レベル機能」（P.4-11）を参照）。

（注）　Call Home は、メッセージ テキスト中の 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 System Messages Reference*』の記載どおりに出力されます。

Fabric Manager を使用した syslog ベースのアラートの設定

Fabric Manager を使用して 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。

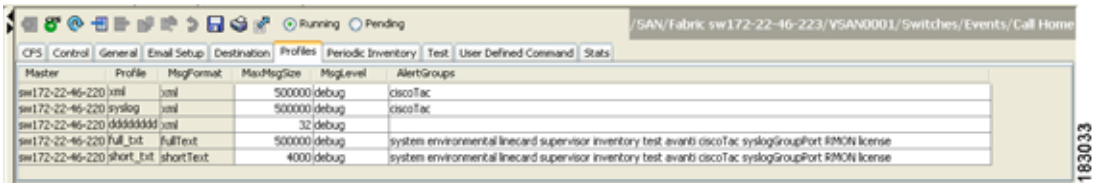
ステップ 2　[Switches]、[Events] の順に展開し、[Physical Attributes] ペインの [Call Home] を選択します。

[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。

図 4-10 に示すように、Call Home プロファイルが表示されます。

図 4-10　Call Home プロファイル



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 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。

Fabric Manager を使用した RMON アラートの設定

Fabric Manager を使用して 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　[Switches]、[Events] の順に展開し、[Physical Attributes] ペインの [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。

図 4-11 に示すように、Call Home プロファイルが表示されます。

図 4-11　Call Home プロファイル

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。

E メール オプション

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。

Fabric Manager を使用した一般的な E メール オプションの設定

Fabric Manager を使用して一般的な E 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　[Switches]、[Events] の順に展開し、[Physical Attributes] ペインの [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。

図 4-12　Call Home の [e-mail Setup] タブ

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。

HTTPS サポート

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。

デフォルトでは、Cisco MDS 9000 ファミリの全スイッチでこの機能がディセーブルに設定されています。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。

Fabric Manager を使用した定期的なコンポーネント通知のイネーブル化

Cisco MDS 9000 ファミリ スイッチで、Fabric Manager を使用して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。

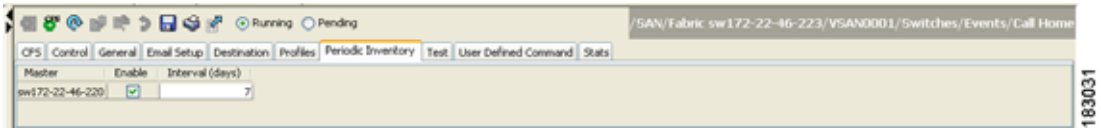
ステップ 2　[Switches]、[Events] の順に展開し、[Physical Attributes] ペインの [Call Home] を選択します。

[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。

図 4-13 に示す、Call Home の定期コンポーネント情報が表示されます。

図 4-13　Call Home の [Periodic Inventory] タブ



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

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。

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。

Fabric Manager を使用したメッセージ スロットリングのイネーブル化

Cisco MDS 9000 ファミリ スイッチで、Fabric Manager を使用してメッセージ 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。

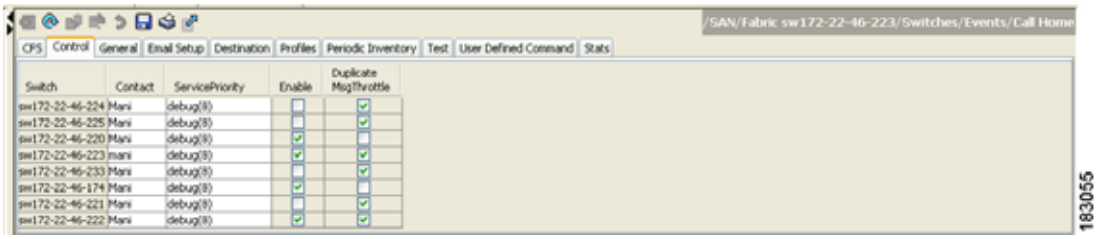
ステップ 2　[Switches]、[Events] の順に展開し、[Physical Attributes] ペインの [Call Home] を選択します。

[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。

図 4-14 に示す情報が表示されます。

図 4-14　Call Home の [Control] タブ



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。

Call Home のイネーブル機能

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。

Fabric Manager を使用した Call Home のイネーブル化

Fabric Manager を使用して 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。

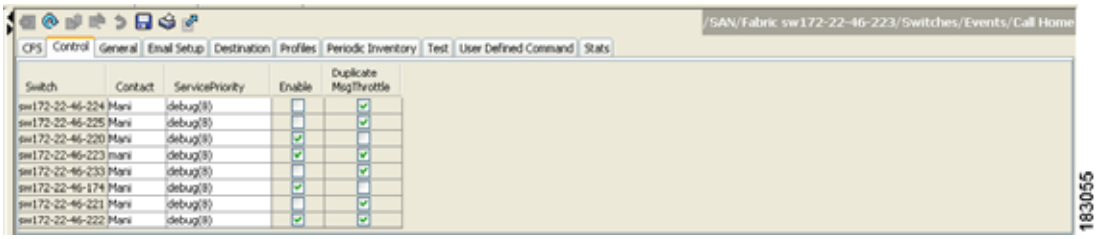
ステップ 2　[Switches]、[Events] の順に展開し、[Physical Attributes] ペインの [Call Home] を選択します。

[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。

図 4-15 に示す情報が表示されます。

図 4-15　Call Home の [Control] タブ



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　[Apply Changes] アイコンをクリックします。

Call Home 設定の配信

ファブリック内のすべての Cisco MDS スイッチで、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。

スイッチの配信をイネーブルにした後で最初の設定操作を実行すると、ファブリック全体のロックが自動的に取得されます。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。どちらの場合に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」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。

Fabric Manager を使用した Call Home ファブリック配信のイネーブル化

Fabric Manager を使用して 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。

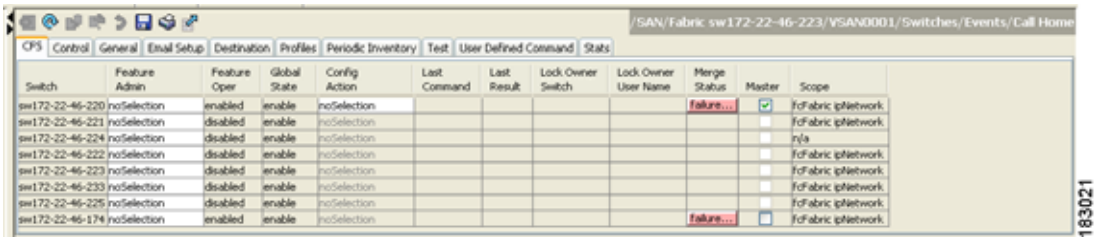
ステップ 2　[Switches]、[Events] の順に展開し、[Physical Attributes] ペインの [Call Home] を選択します。

[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。

図 4-16 に示す、Call Home の CFS 情報が表示されます。

図 4-16　Call Home の [CFS] タブ



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。

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。管理者がこの作業を行うと、保留データベースに対する変更は廃棄され、ファブリックのロックは解除されます。

ヒント　変更は一時的なディレクトリだけで使用可能であり、スイッチが再起動されると廃棄されます。

データベース マージの注意事項

詳細については、「CFS マージのサポート」（P.2-9）を参照してください。

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。

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。

Fabric Manager を使用した Call Home のテスト

Fabric Manager を使用して、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　[Switches]、[Events] の順に展開し、[Physical Attributes] ペインの [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 or 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。

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 遅延トラップの設定

Fabric Manager は、EMC E-mail Home XML E メール メッセージを生成するように設定できます。SAN-OS リリース 3.x およびそれよりも前のリリースでは、Fabric Manager はインターフェイス トラップを受信し、EMC E-mail Home E 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 Fabric Manager が E 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。

Cisco Fabric Manager を使用した遅延トラップの設定

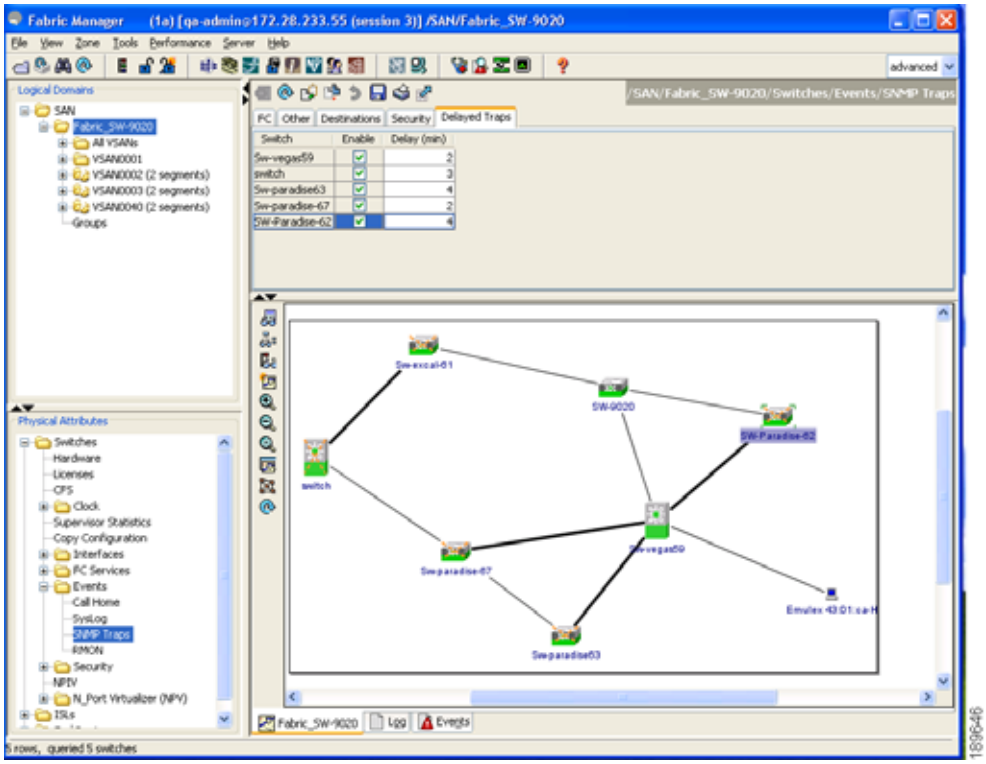
server.callhome.delayedtrap.enable プロパティが、server.properties コンフィギュレーション ファイルのセクション 9 Call Home に追加されています。プロパティ ファイルでは、Fabric Manager サーバが、EMC E-mail Home メッセージに対し、通常の linkDown トラップではなく遅延トラップを使用するように設定できます。この機能をイネーブルにするには、遅延トラップをスイッチ レベルで有効にし、server.properties コンフィギュレーション ファイルで server.callhome.delayedtrap.enable 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。

NX-OS Release 4.1(3) 以降が動作するスイッチ上で、Fabric Manager を使用して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] で、[Switches] > [Events] の順に展開し、[SNMP Traps] を選択します。

Fabric Manager 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。

図 4-17　[Delayed Trap] ダイアログボックス



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。

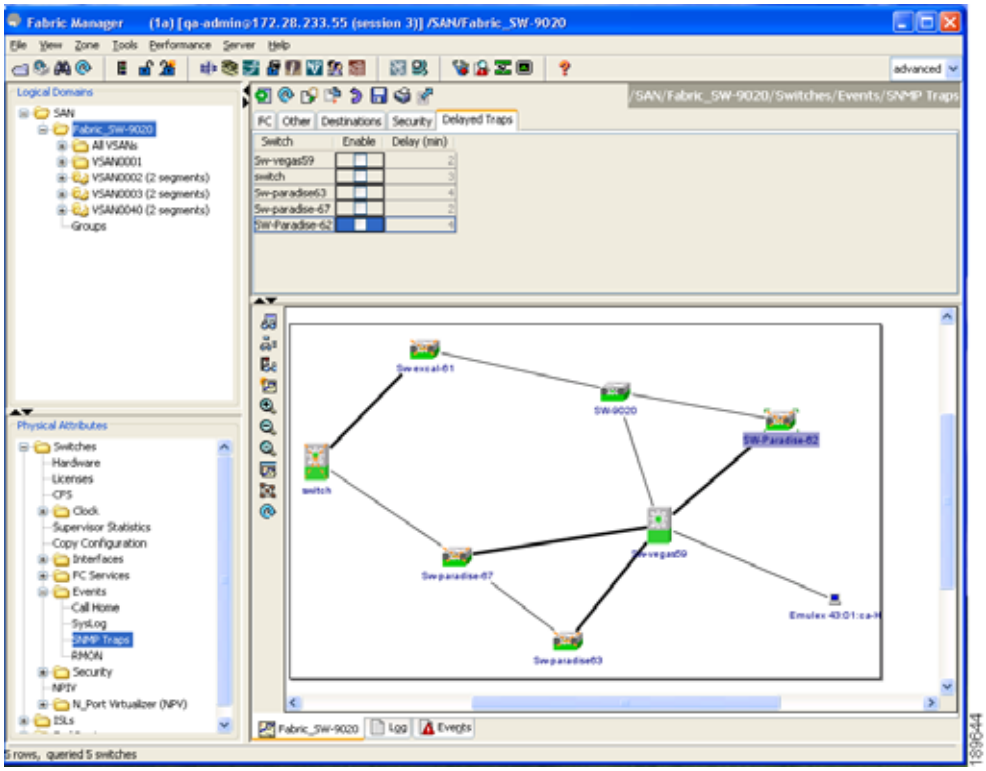
ステップ 4　[Apply] をクリックして変更を保存します。

（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。

図 4-18　[Delayed Trap] ダイアログボックス



ステップ 2　[Apply] をクリックします。

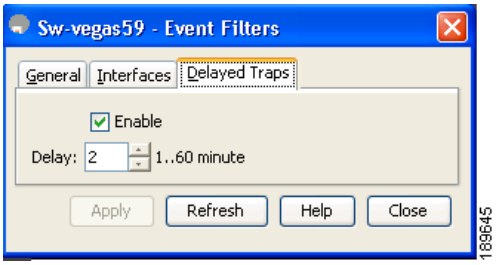
Cisco Device Manager を使用した遅延トラップのイネーブル化

Device Manager を使用して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　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。

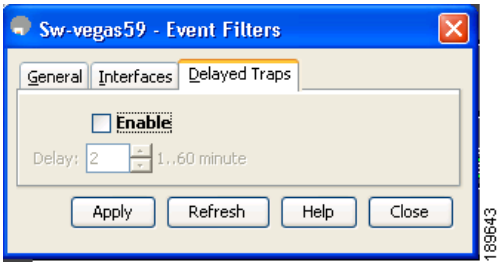
図 4-19　[Delayed Traps] ダイアログボックス



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。

図 4-20　[Disable Traps] ダイアログボックス



フル テキスト フォーマットの 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 フォーマットの 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&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 フォーマットの 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>
```

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。転送されるメッセージにはコマンド出力が含まれます。表 4-2 にトリガー イベントの一覧を示します。

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-port	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

表 4-3 に、イベント カテゴリとコマンド出力の一覧を示します。

表 4-3　イベント カテゴリと実行されるコマンド

イベント カテゴリ	説明	実行されるコマンド
システム show module show version show tech-support platform show tech-support sysmgr show hardware show sprom all	ユニットの動作に不可欠な、障害またはソフトウェア システムによって生成されるイベント。	**show tech-support** **show system redundancy status**
環境 show module show version show environment show logging logfile | tail -n 200	電源、ファン、温度アラームなどの環境センシング要素に関連するイベント。	**show module** **show environment**

表 4-3　イベント カテゴリと実行されるコマンド （続き）

イベント カテゴリ	説明	実行されるコマンド
ラインカード ハードウェア show module show version show tech-support platform show tech-support sysmgr show hardware show sprom all	標準またはインテリジェント ラインカード ハードウェアに関連するイベント。	**show tech-support**
スーパーバイザ ハードウェア show module show version show tech-support platform show tech-support sysmgr show hardware show sprom all	スーパーバイザ モジュールに関連するイベント。	**show tech-support**
コンポーネント show module show version show hardware show inventory show system uptime show sprom all show license usage	コンポーネント ステータスは、ユニットがコールド ブートされる場合や、FRU が挿入または除去されたときに提供されます。これは、クリティカルでないイベントと見なされ、情報はステータスと権利付与のために使用されます。	**show version**
テスト show module show version	ユーザがテスト メッセージを生成しました。	**show version**

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.4-11）を参照）。

ここでは、Cisco MDS 9000 ファミリの 1 つ以上のスイッチを使用する場合の 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 4-4 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 テキスト中の 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 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 System Messages Reference*』を参照）。

表 4-4　重大度と syslog レベルのマッピング

Call Home のレベル	使用されるキーワード	syslog レベル	説明
Catastrophic (9)	**Catastrophic**	なし	ネットワーク全体の破滅的な障害。
Disaster (8)	**Disaster**	なし	ネットワークへの重大な影響。
Fatal (7)	**Fatal**	Emergency (0)	システムは使用不能。
Critical (6)	**Critical**	Alert (1)	クリティカル状態、すぐに注意が必要。
Major (5)	**Major**	Critical (2)	メジャー状態。
Minor (4)	**Minor**	Error (3)	マイナー状態。
Warning (3)	**Warning**	Warning (4)	警告状態。
Notify (2)	**Notification**	Notice (5)	基本的な通知および情報メッセージ。単独では問題ない可能性があります。
Normal (1)	**Normal**	Information (6)	正常状態への復帰を意味する正常イベント。
Debug (0)	**Debugging**	Debug (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 4-5 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 4-5　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
日付/タイムスタンプ	トリガー イベントのタイムスタンプ

表 4-5　ショート テキスト メッセージ （続き）

データ項目	説明
エラー切り分けメッセージ	トリガー イベントの英語による説明
アラーム緊急度	システム メッセージに適用されるレベルなどのエラー レベル

表 4-6、表 4-7、および表 4-8 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 4-6　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 に限る）
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 Ddaylight Savings Iime（DST; 夏時間）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については、「イベント トリガー」（P.4-28）を参照してください。	/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 4-4 を参照）。	/mml/header/level - aml-block:Severity
送信元 ID	ルーティングの製品タイプ。	/mml/header/source - ch:Series
デバイス ID	メッセージを生成したエンド 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」であり、シャーシ シリアル番号としてのシリアル ID を識別します。 • *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、コンタクト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
コンタクト ID	任意のサポート サービスによって、コンタクト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	シスコが提供するサイト 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:SiteId

表 4-6　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 に限る）
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」であり、シャーシ シリアル番号としてのシリアル ID を識別します。 • *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テキスト。	/mml/body/msgDesc - ch:MessageDescription
デバイス名	イベントが発生したノード。デバイスのホスト名です。	/mml/body/sysName - ch:SystemInfo/Name
連絡先名	イベントが発生したノードに関する問題に対する、連絡先担当者の名前。	/mml/body/sysContact - ch:SystemInfo/Contact
連絡先の E メール	このユニットの連絡先として識別された人の E メール アドレス。	/mml/body/sysContacte-mail - ch:SystemInfo/Contacte-mail
連絡先の電話番号	このユニットの連絡先として識別された人の電話番号。	/mml/body/sysContactPhoneNumber - ch:SystemInfo/ContactPhoneNumber
住所	このユニットに関連する RMA パーツを発送するための住所が格納されるオプション フィールド。	/mml/body/sysStreetAddress - ch:SystemInfo/StreetAddress
モデル名	スイッチのモデル名 製品ファミリ名に含まれている特定のモデル。	/mml/body/chassis/name - rme:Chassis/Model
シリアル番号	ユニットのシャーシ シリアル番号。	/mml/body/chassis/serialNo - rme:Chassis/SerialNumber
シャーシのパーツ番号	シャーシのトップ アセンブリ番号。	/mml/body/fru/partNo - rme:chassis/Card/PartNumber
シャーシ 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 名	イベント メッセージを生成している、影響のある FRU の名前。	/mml/body/fru/name - rme:chassis/Card/Model

表 4-6　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 に限る）
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
FRU パーツ番号	影響のある FRU のパーツ番号。	/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 で動作しているソフトウェアのバージョン。	/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	具体的なコマンド出力。	/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 4-7　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 に限る）
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.4-28）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

表 4-7　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 に限る）
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 4-4 を参照）。	/mml/header/level - aml-block:Severity
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	メッセージを生成したエンド 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」であり、シャーシ シリアル番号としてのシリアル ID を識別します。 • *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、コンタクト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
コンタクト ID	任意のサポート サービスによって、コンタクト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」であり、シャーシ シリアル番号としてのシリアル ID を識別します。 • *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テキスト。	/mml/body/msgDesc - ch-inv:MessageDescription
デバイス名	イベントが発生したノード。	/mml/body/sysName - ch-inv:SystemInfo/Name

表 4-7　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 に限る）
連絡先名	イベントが発生したノードに関する問題に対する、連絡先担当者の名前。	/mml/body/sysContact - ch-inv:SystemInfo/Contact
連絡先の E メール	このユニットの連絡先として識別された人の E メール アドレス。	/mml/body/sysContacte-mail - ch-inv:SystemInfo/Contacte-mail
連絡先の電話番号	このユニットの連絡先として識別された人の電話番号。	/mml/body/sysContactPhone Number - ch-inv:SystemInfo/ContactPhoneNumber
住所	このユニットに関連する RMA パーツを発送するための住所が格納されるオプション 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。製品ファミリ名に含まれている特定のモデル。	/mml/body/chassis/name - rme:Chassis/Model
シリアル番号	ユニットのシャーシ シリアル番号。	/mml/body/chassis/serialNo - rme:Chassis/SerialNumber
シャーシのパーツ番号	シャーシのトップ アセンブリ番号。	/mml/body/fru/partNo - rme:chassis/Card/PartNumber
シャーシ 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 メッセージを生成している、影響のある FRU の名前。	/mml/body/fru/name - rme:chassis/Card/Model
FRU シリアル番号	FRU のシリアル番号。	/mml/body/fru/serialNo - rme:chassis/Card/SerialNumber
FRU のパーツ番号	FRU のパーツ番号。	/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 で動作しているソフトウェアのバージョン。	/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

表 4-7　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 に限る）
添付タイプ	具体的なコマンド出力。	/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	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.4-28）を参照）。	/mml/attachments/attachment/atdata - aml-block:Attachment/Data

表 4-8　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 に限る）
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.4-28）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 4-4 を参照）。	/mml/header/level - aml-block:Severity
送信元 ID	ルーティングの製品タイプ。	/mml/header/source - ch:Series
デバイス ID	メッセージを生成したエンド 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は、このフィールドを空にする必要があります。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」であり、シャーシ シリアル番号としてのシリアル ID を識別します。 • *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

表 4-8　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 に限る）
カスタマー ID	任意のサポート サービスによって、コンタクト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
コンタクト ID	任意のサポート サービスによって、コンタクト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	シスコが提供するサイト 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: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」であり、シャーシ シリアル番号としてのシリアル ID を識別します。 • *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テキスト。	/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
連絡先名	イベントが発生したノードに関する問題に対する、連絡先担当者の名前。	/mml/body/sysContact - ch:SystemInfo/Contact
連絡先の E メール	このユニットの連絡先として識別された人の E メール アドレス。	/mml/body/sysContacte-mail - ch:SystemInfo/Contacte-mail
連絡先の電話番号	このユニットの連絡先として識別された人の電話番号。	/mml/body/sysContactPhoneNumber - ch:SystemInfo/ContactPhoneNumber
住所	このユニットに関連する RMA パーツを発送するための住所が格納されるオプション フィールド。	/mml/body/sysStreetAddress - ch:SystemInfo/StreetAddress
モデル名	スイッチのモデル名 製品ファミリ名に含まれている特定のモデル。	/mml/body/chassis/name - rme:Chassis/Model
シリアル番号	ユニットのシャーシ シリアル番号。	/mml/body/chassis/serialNo - rme:Chassis/SerialNumber

表 4-8　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 に限る）
シャーシのパーツ番号	シャーシのトップ 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
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	具体的なコマンド出力。	/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

デフォルト設定

表 4-9 に、Call Home のデフォルト設定の一覧を示します。

表 4-9　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 フォーマット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 フォーマット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 フォーマット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
プロファイルに関連付けられているアラート グループ	All
フォーマット タイプ	XML
Call Home メッセージ レベル	0（ゼロ）

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。

この章の内容は、次のとおりです。

コマンド スケジューラの概要

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。

（注） コマンド スケジューラを使用するために、ライセンスを取得する必要はありません。

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。

スケジューリングに関する注意事項

Cisco MDS スイッチでジョブをスケジューリングする場合、次の点に注意してください。

- 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。

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には、次の手順を実行します。

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。

ここで説明する内容は、次のとおりです。

- 「コマンド スケジューラの実行ステータスの確認」（P.5-9）

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、Cisco MDS 9000 ファミリの全スイッチでこの機能がディセーブルに設定されています。

コマンド スケジューラ機能の設定および確認コマンドを使用できるのは、スイッチ上でコマンド スケジューラがイネーブルに設定されている場合だけです。この機能をディセーブルにすると、関連するすべての設定が自動的に廃棄されます。

コマンド スケジューリング機能をイネーブルにするには次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config t`	コンフィギュレーション モードを開始します。
ステップ 2	`switch(config)# feature scheduler`	コマンド スケジューラをイネーブルにします。
	`switch(config)# no feature scheduler`	スケジューラの設定を廃棄して、コマンド スケジューラをディセーブルにします（デフォルト）。

コマンド スケジューラのステータスを表示するには、**show scheduler config** コマンドを使用します。

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

リモート ユーザ認証の設定

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。

（注）　AAA 認証では、コマンド スケジューラ ジョブを作成および設定する前に、リモート ユーザのクリア テキスト パスワードが必要になります。

リモート ユーザ認証を設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config t`	コンフィギュレーション モードを開始します。
ステップ 2	`switch(config)# scheduler aaa-authentication password X12y34Z56a`	リモート ユーザのクリア テキスト パスワードを設定します。
ステップ 3	`switch(config)# scheduler aaa-authentication password 0 X12y34Z56a`	リモート ユーザのクリア テキスト パスワードを設定します。
ステップ 4	`switch(config)# no scheduler aaa-authentication password`	リモート ユーザのクリア テキスト パスワードを削除します
ステップ 5	`switch(config)#scheduler aaa-authentication user newuser password Z98y76X54b`	リモート ユーザ newuser のクリア テキスト パスワードを設定します
ステップ 6	`switch(config)#scheduler aaa-authentication user newuser password 0 Z98y76X54b`	リモート ユーザ newuser のクリア テキスト パスワードを設定します
ステップ 7	`switch(config)# no scheduler aaa-authentication password user newuser`	リモート ユーザ newuser のクリア テキスト パスワードを削除します

リモート ユーザのスケジューラ パスワード設定を表示するには、**show running-config** コマンドを使用します。

```
switch# show running-config | include "scheduler aaa-authentication"
scheduler aaa-authentication username newuser password 7 "C98d76S54e"
```

（注）　スケジューラ リモート ユーザ パスワードは、**show running-config** コマンドの出力中で、常に暗号化された形式で表示されます。コマンド中の暗号化オプション（**7**）は、ASCII 設定のスイッチへの適用をサポートするためにあります。

ジョブの定義

ジョブを定義するには、ジョブ名を指定する必要があります。この操作を行うと、ジョブ定義（config-job））サブモードが開始されます。このサブモードでは、ジョブが実行する CLI コマンドのシーケンスを定義できます。ジョブの定義を完了するには、必ず config-job サブモードを終了してください。

（注）

- Cisco MDS NX-OS Release 4.1(1b) よりも前の MDS NX-OS または SAN-OS のリリースで作成されたジョブ設定ファイルはサポートされていません。ただし、ジョブ設定ファイルを編集し、ジョブの中のコマンドを、セミコロン（;）を使用して 1 行に結合することはできます。
- ジョブの定義を完了するには、config-job サブモードを終了する必要があります。
- config-job サブモードを終了した後では、コマンドの変更または削除はできません。変更するには、定義済みのジョブ名を明示的に削除し、新しいコマンドを使用してジョブを再設定する必要があります。

コマンド スケジューラのジョブを定義するには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# conf t` `switch(config)#`	コンフィギュレーション モードを開始します。
ステップ 2	`switch(config)# scheduler job name addMemVsan99` `switch(config-job)#`	ジョブ名を定義して、ジョブ定義サブモードを開始します。

ステップ 3	`switch(config-job)# command1;[command2;command3;...]`
	`switch(config-job-submode)# end`
	`switch#`
	
	例 1：
	`switch(config-job)# config terminal;vsan database;vsan 99 interface fc1/1 - 4`
	`switch(config-job-config-vsan-db)# end`
	`switch#`
		指定されたジョブの処理シーケンスを指定します。定義済みのコマンドは有効性が確認されて、今後使用するために保管されます。
		（注） config-job サブモードは必ず終了してください。

	例 2： `switch(config)# scheduler job name offpeakQOS` `switch(config-job)# conf t ; qos class-map offpeakbackupcmap match-all ; match source-wwn 23:15:00:05:30:00:2a:1f ; match destination-wwn 20:01:00:05:30:00:28:df ;exit ; qos policy-map offpeakbackuppolicy ; class offpeakbackupcmap ; priority high ; exit ; exit ; qos service policy offpeakbackuppolicy vsan 1` `switch(config-job)# end` `switch#`	一連の設定コマンドをスケジューリングする例を示します。

ステップ 4	**exit**
	
	例：
	`switch(config-job)# exit`
	`switch(config)#`
		ジョブ設定モードを終了し、ジョブを保存します。

ステップ 5	**show scheduler job** [*name*] 例： `switch(config)# show scheduler job`	（オプション）ジョブ情報を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（オプション）この設定変更を保存します。

ジョブ定義の確認

ジョブ定義を確認するには、**show scheduler job** コマンドを使用します。

```
switch# show scheduler job addMemVsan99
Job Name: addMemVsan99
----------------------
  config terminal
   vsan database
    vsan 99 interface fc1/1
    vsan 99 interface fc1/2
    vsan 99 interface fc1/3
```

```
vsan 99 interface fc1/4
```

ジョブの削除

コマンド スケジューラのジョブを削除するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# **conf t** switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **no scheduler job name addMemVsan99**	定義済みジョブおよびジョブ内で定義されたすべてのコマンドを削除します。

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。

定期的スケジュールの指定

定期ジョブの実行を指定すると、ジョブは指定された間隔（毎日、毎週、毎月、または差分）で定期的に実行されます。

コマンド スケジューラの定期ジョブを指定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# **conf t** switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **scheduler schedule name weekendbackupqos** switch(config-schedule)#	ジョブ スケジュール（weekendbackup）を定義して、そのスケジュールのサブモードを開始します。
	switch(config)# **no scheduler schedule name weekendbackup**	定義したスケジュールを削除します。
ステップ 3	switch(config-schedule)# **job name offpeakZoning** switch(config-schedule)# **job name offpeakQOS**	このスケジュールに 2 つのジョブ offpeakZoning および offpeakQOS を割り当てます。
ステップ 4	switch(config-schedule)# **no job name addMem99**	このスケジュールに割り当てられたジョブを削除します。

次に示す設定は参考例です。

switch(config-schedule)# **time daily 23:00**	指定されたジョブを、毎日午後 11 時に 実行します。
switch(config-schedule)# **time weekly Sun:23:00**	毎週日曜日の午後 11 時に実行するように指定します。
switch(config-schedule)# **time monthly 28:23:00**	毎月 28 日の午後 11 時に実行するように指定します。日にちを 29、30、または 31 日に指定した場合、コマンドは各月の最終日に自動的に実行されます。

`switch(config-schedule)# time start now repeat 48:00`	現在（*now*）の 2 分後から 48 時間ごとにジョブを実行するように指定します。今日が 2004 年 9 月 24 日で、現在の時刻が午後 2 時であれば、コマンドは 2004 年 9 月 24 日の午後 2 時 2 分に実行が開始され、その後は 48 時間ごとに継続的に実行されます。
`switch(config-schedule)# time start 14:00 repeat 14:00:00`	今日が 2004 年 9 月 24 日（金曜日）であれば、隔週金曜日の午後 2 時（14 日ごと）にジョブが 実行されます。

time パラメータの主なフィールドは大半がオプションです。これらのフィールドを省略すると、現在時刻と同じ値が指定されたと見なされます。たとえば、現在時刻が 2004 年 9 月 24 日の 22:00 の場合、コマンドは次のように実行されます。

- **time start 23:00 repeat 4:00:00** コマンドの場合、開始時刻は 2004 年 9 月 24 日の 23:00 時です。
- **time daily 55** コマンドの場合、毎日 22 時 55 分に実行されます。
- **time weekly 23:00** コマンドの場合、毎週金曜日の 23:00 時に実行されます。
- **time monthly 23:00** コマンドの場合、毎月 24 日の 23:00 時に実行されます。

（注） スケジュールに対して設定された時間間隔が、割り当てられたジョブの実行に必要な時間よりも短い場合、直前のスケジュール実行完了時刻から設定された時間間隔が経過しないと後続のスケジュールは実行されません。たとえば、スケジュールが 1 分間隔で実行され、スケジュールに割り当てられたジョブが完了するのに 2 分かかる場合です。最初のスケジュールが 22:00 に実行され、ジョブが 22:02 に完了する場合、次の処理は 1 分間隔に従って 22:03 に実行されて 22:05 に完了します。

一時的スケジュールの指定

一時ジョブの実行を指定すると、そのジョブは一度だけ実行されます。

コマンド スケジューラの一時ジョブを指定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# conf t` `switch(config)#`	コンフィギュレーション モードを開始します。
ステップ 2	`switch(config)# scheduler schedule name configureVsan99` `switch(config-schedule)#`	ジョブ スケジュール（configureVsan99）を定義して、そのスケジュールのサブモードを開始します。
ステップ 3	`switch(config-schedule)# job name addMemVsan99`	このスケジュールに定義済みジョブ名（addMemVsan99）を割り当てます。
ステップ 4	`switch(config-schedule)# time start 2004:12:14:23:00`	2004 年 12 月 14 日の午後 11 時に 1 回だけ実行するように指定します。
	`switch(config-schedule)# no time`	このスケジュールに割り当てられた時刻を削除します。

スケジューラ設定の確認

スケジューラ設定を表示するには、**show scheduler config** コマンドを使用します。

```
switch# show scheduler config
config terminal
  feature scheduler
  scheduler logfile size 512
end

config terminal
   scheduler job name addMemVsan99
     config terminal
       vsan database
       vsan 99 interface fc1/1
       vsan 99 interface fc1/2
       vsan 99 interface fc1/3
       vsan 99 interface fc1/4
end

config terminal
  scheduler schedule name configureVsan99
    time start 2004:8:10:9:52
    job name addMemVsan99
end
```

スケジュールの削除

スケジュールを削除するには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# conf t` `switch(config)#`	コンフィギュレーション モードを開始します。
ステップ 2	`switch(config)# no scheduler schedule name weekendbackup`	定義したスケジュールを削除します。

割り当てられたジョブの削除

割り当てられたジョブを削除するには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# conf t` `switch(config)#`	コンフィギュレーション モードを開始します。
ステップ 2	`switch(config)# scheduler schedule name weekendbackupqos` `switch(config-schedule)#`	ジョブ スケジュール（weekendbackupqos）を指定して、そのスケジュールのサブモードを開始します。
ステップ 3	`switch(config-schedule)# no job name addMem99`	このスケジュールに割り当てられたジョブ（addMem99）を削除します。

スケジュール時刻の削除

スケジュール時刻を削除するには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# conf t` `switch(config)#`	コンフィギュレーション モードを開始します。
ステップ 2	`switch(config)# scheduler schedule name weekendbackupqos` `switch(config-schedule)#`	ジョブ スケジュール（weekendbackup）を定義して、そのスケジュールのサブモードを開始します。
ステップ 3	`switch(config-schedule)# no time`	スケジュール時刻の設定を削除します。このスケジュールは時刻を再度設定するまで実行されません。

コマンド スケジューラの実行ステータスの確認

コマンド スケジューラの実行ステータスを確認するには、**show scheduler schedule** コマンドを使用します。

```
switch# show scheduler schedule configureVsan99
Schedule Name       : configureVsan99
----------------------------------
User Name           : admin
Schedule Type       : Run once on Tue Aug 10 09:48:00 2004
Last Execution Time: Tue Aug 10 09:48:00 2004
----------------------------------------------
          Job Name                  Status
----------------------------------------------
addMemVsan99                        Success (0)
```

実行ログ

ここではコマンド スケジューラの実行ログについて説明します。内容は次のとおりです。

実行ログの概要

コマンド スケジューラはログ ファイルを管理しています。このファイルの内容は変更できませんが、ファイル サイズは変更できます。このログファイルは循環ログで、実行されたジョブの出力が格納されます。ジョブの出力がログ ファイルよりも大きい場合、このファイルに格納される出力は一部が切り捨てられます。

設定できるログ ファイルの最大サイズは 1024 KB です 実行ログ ファイルのデフォルト サイズは 16 KB です。

実行ログの設定

実行ログ ファイルのサイズを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# **conf t** switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **scheduler logfile size 1024**	ログファイルを最大 1024 KB に設定します。
	switch(config)# **no scheduler logfile size**	ログのサイズをデフォルトの 16 KB に設定します。

実行ログ ファイルの設定を表示するには、**show scheduler config** コマンドを使用します。

```
switch# show scheduler config
config terminal
  feature scheduler
  scheduler logfile size 1024
end
```

実行ログ ファイルの内容の表示

システムで実行されるすべてのジョブの実行ログを表示するには、**show scheduler logfile** コマンドを使用します。

```
switch# show scheduler logfile
Job Name       : addMemVsan99              Job Status: Success (0)
Schedule Name  : configureVsan99           User Name : admin
Completion time: Tue Aug 10 09:48:00 2004
-------------------------- Job Output --------------------------
`config terminal`
`vsan database`
`vsan 99 interface fc1/1`
`vsan 99 interface fc1/2`
`vsan 99 interface fc1/3`
`vsan 99 interface fc1/4`
```

実行ログ ファイルの内容のクリア

スケジューラ実行ログ ファイルの内容をクリアするには、EXEC モードで **clear scheduler logfile** コマンドを実行します。

```
switch# clear scheduler logfile
```

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

CHAPTER 6

システム プロセスおよびログのモニタ

この章では、スイッチ状態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。

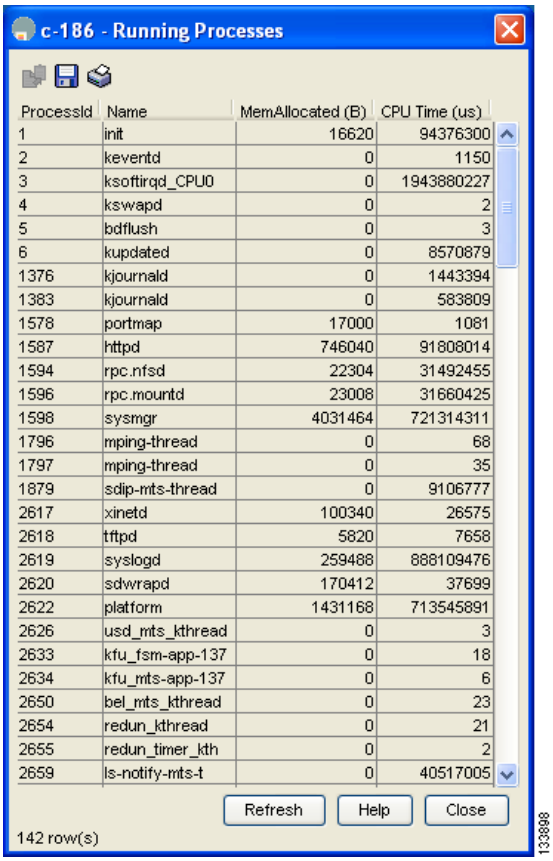
システム プロセスの表示

Device Manager を使用して、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。

図 6-1 のように、[Running Processes] ダイアログボックスが表示されます。

図 6-1　[Running Processes] ダイアログボックス



各項目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。

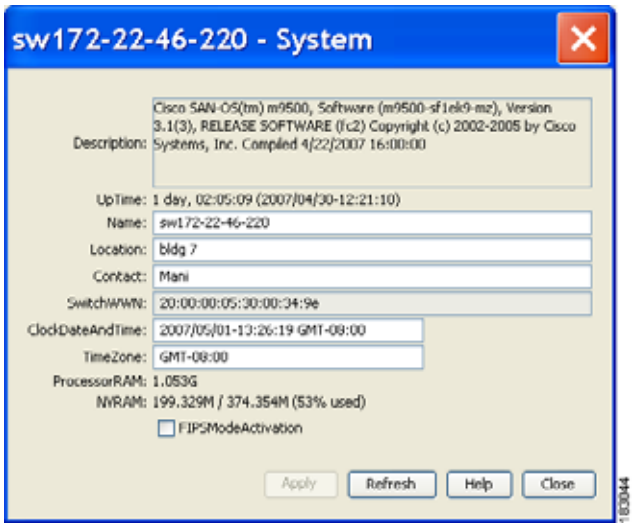
システム ステータスの表示

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。

図 6-2 のような [System] ダイアログボックスが表示されます。

図 6-2　[System] ダイアログボックス



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 ファイルおよびログ ファイル

ここでは、次の内容について説明します。

コア ステータスの表示

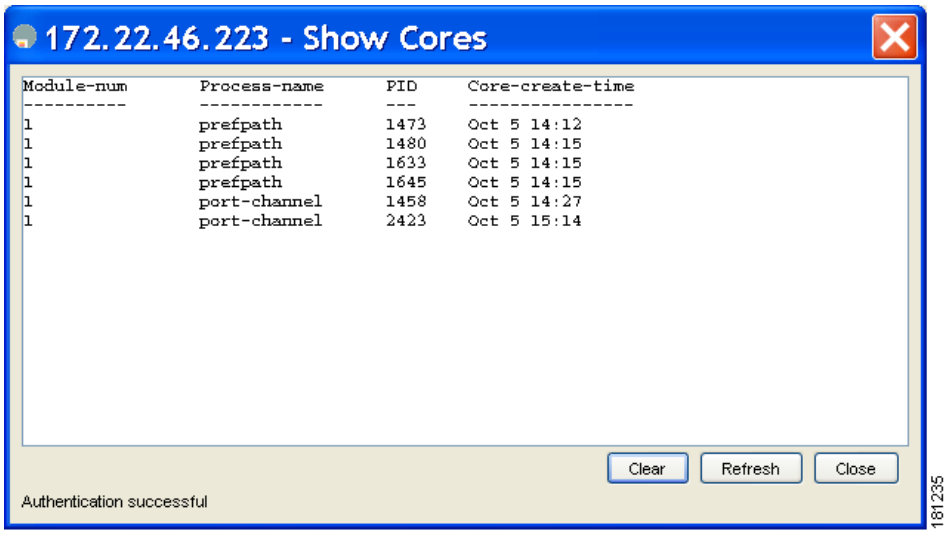
（注）　このスイッチで SSH2 がイネーブルになっていることを確認してください。

Device Manager を使用して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。

ステップ 1　[Admin] > [Show Cores] を選択します。

図 6-3 のように、[Show Cores] ダイアログボックスが表示されます。

図 6-3　[Show Cores] ダイアログボックス



Module-num は、コアが生成されたスロット番号を示します。この例で、fspf core がアクティブ スーパーバイザ モジュール（スロット 5）で生成され、fcc がスタンバイ スーパーバイザ モジュール（スロット 6）で生成され、acltcam および fib が、スイッチング モジュール（スロット 8）で生成されています。

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 ディレクトリのクリア

（注）　このスイッチで SSH2 がイネーブルになっていることを確認してください。

Device Manager を使用して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。

ソフトウェアはサービスごと、およびスロットごとに直前のコアをいくつか保管し、アクティブ スーパーバイザ モジュール上のその他のすべて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。

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。

最初と最後のコア ステータスの確認

保存したコア ファイルに関する詳細な情報を表示できます。コア ファイルの保存についての詳細を例 6-1 に示します。

例 6-1　アクティブ スーパーバイザ モジュール上の vdc 2 上の通常のサービス

アクティブ スーパーバイザ モジュール上の vdc2 から出力された 5 つの radius コア ファイルがあります。2 番目と 3 番目に古いファイルが、service.conf ファイルで定義されているコア ファイルの数に従うために削除されます。

```
switch# show cores vdc vdc2

VDC No Module-num       Process-name      PID     Core-create-time
------ ----------       ------------      ---     ----------------
2      5                radius            6100    Jan 29 01:47
2      5                radius            6101    Jan 29 01:55
2      5                radius            6102    Jan 29 01:55
2      5                radius            6103    Jan 29 01:55
2      5                radius            6104    Jan 29 01:57

switch# show cores vdc vdc2

VDC No Module-num       Process-name      PID     Core-create-time
------ ----------       ------------      ---     ----------------
2      5                radius            6100    Jan 29 01:47
2      5                radius            6103    Jan 29 01:55
2      5                radius            6104    Jan 29 01:57
```

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。

ここで説明する内容は、次のとおりです。

OHMS の概要

OHMS は、システム ハードウェアを次の方法で監視します。

- 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。テストは事前に設定された間隔で実行され、すべての主要な障害ポイントを対象とし、MDS スイッチで障害の発生した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復旧処置を行います。

- 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。
- 障害を検出するとすぐに、コール ホーム、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。
- 詳細なテストを行うために、障害ポートを隔離します。
- 適切なソフトウェア コンポーネントに障害を通知します。
- 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）。
- スイッチ上で CLI をサポートし、表示、テスト、およびテスト統計情報の取得、またはシステム ヘルス テストの設定変更を行うことができるようにします。
- 障害エリアに重点を置いたテストを行います。

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。

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。このテストは、ファイバ チャネル インターフェイスだけで使用できます。

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。

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 ヘルスとログのデフォルト設定

パラメータ	デフォルト
カーネル コア生成	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
障害動作	イネーブル

CHAPTER 7

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。

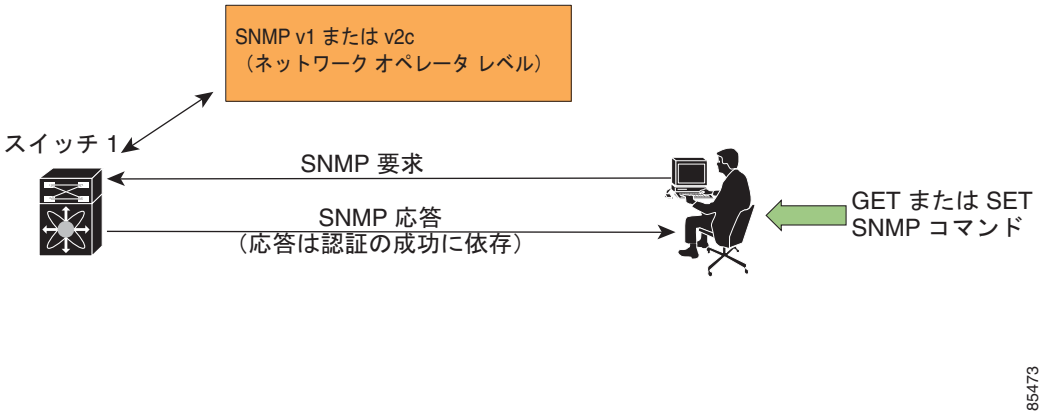
CLI ユーザと SNMP ユーザのユーザ、パスワード、ロールは、すべて同じです。CLI を通じて設定されたユーザは SNMP（たとえば、Fabric Manager や Device Manager）を使用してスイッチにアクセスでき、その逆も可能です。

この章の内容は、次のとおりです。

SNMP セキュリティの概要

SNMP 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 レイヤ 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 7-1 を参照）。

図 7-1　　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制御方式です。SNMPv3 は、強力な認証を使用することによってアクセス制御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。ネットワーク上でのフレームの認証および暗号化を組み合わせることによって、デバイスへの安全なアクセスを提供します。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：有効な送信元からのメッセージであるかどうかを判別します。
- 暗号化：パケット内容をスクランブルし、不当に読み取られないようにします。

SNMPv3 は、セキュリティ モデルとセキュリティ レベルの両方を提供します。セキュリティ モデルは、ユーザおよびユーザが所属するロールに対して設定する認証ストラテジです。セキュリティ レベルは、セキュリティ モデルの中で許容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って、SNMP パケットの取り扱いに適用されるセキュリティ メカニズムが決まります。

SNMP スイッチの連絡先情報と場所情報の割り当て

32 文字以内（スペースを除く）のスイッチの連絡先情報と、スイッチの場所を割り当てることができます。

Fabric Manager を使用して、連絡先情報と場所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 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 ベースのアクセス制御が含まれています。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。ユーザ認証が確認されると、SNMP PDU は次の段階へと処理されます。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/ロール ポリシーを適用します。

ここで説明する内容は、次のとおりです。

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、Fabric Manager 用に作成された一時的な SNMP ログインを使用できるのは、24 時間ではなく、1 時間になりました。

- 既存の SNMP ユーザは、auth および priv パスフレーズを現状どおり継続して使用します。
- 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 Access Control List（IP-ACL; IP アクセス コントロール リスト）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*は業界全体で使用されている標準的な SNMP 用語であるため、SNMP に関するこの項では、「ロール」のことを「グループ」で表します。

SNMP アクセス権限は、グループ単位で編成します。SNMP の各グループは、CLI におけるロールと類似しています。各グループは、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の 3 つのアクセスで定義されます。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、Fabric Manager、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、クローンの秘密鍵を変更してから、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。
- Fabric Manager。
- 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（Fabric Manager 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、Fabric Manager 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 Fabric Manager 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。

ここで説明する内容は、次のとおりです。

AES 暗号化ベースのプライバシ

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 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 暗号化を選択できます。**priv** オプションを **aes-128** トークンと併用すると、プライバシ 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 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 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。

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。

Fabric Manager を使用して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　[Switches] > [Security] の順に展開し、[Physical Attributes] ペインの [Users and Roles] を選択します。

ステップ 2　[Information] ペインの [Users] タブをクリックし、図 7-2 に示すようなユーザのリストを表示します。

図 7-2　[Users] タブのユーザ情報

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（図 7-3 を参照）。

図 7-3　[Privacy] タブ

ステップ 8　[Enforce SNMP Privacy Encryption] チェックボックスをオンにし、管理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。

Fabric Manager を使用し、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　[Switches] > [Security] の順に展開し、[Physical Attributes] ペインの [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。

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

Fabric Manager を使用して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。

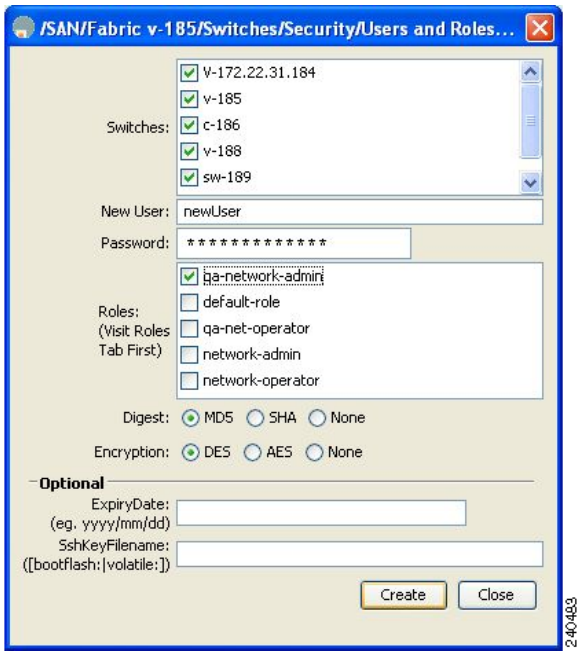
ステップ 1　[Switches] > [Security] の順に展開し、[Physical Attributes] ペインの [Users and Roles] を選択します。

ステップ 2　[Information] ペインの [Users] タブをクリックし、図 7-2 に示すような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（図 7-4 を参照）。

図 7-4　[Create Users] ダイアログボックス



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

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。

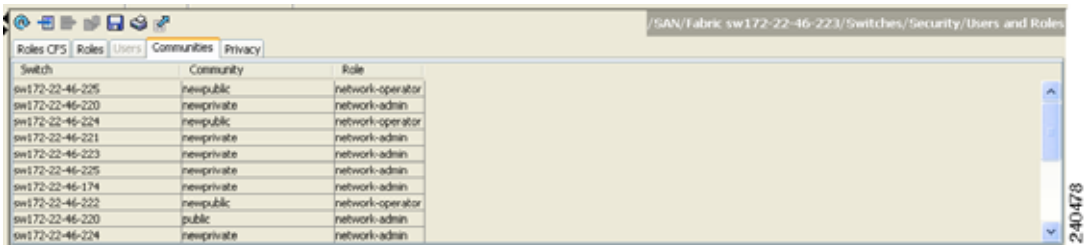
Fabric Manager を使用して SNMPv1 または SNMPv2c のコミュニティ ストリングを作成するには、次の手順を実行します。

ステップ 1　[Switches] > [Security] の順に展開し、[Physical Attributes] ペインの [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（図 7-5 を参照）。

図 7-5　[Users and Roles] の [Communities] タブ



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

Fabric Manager を使用してコミュニティ 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　[Switches] > [Security] の順に展開し、[Physical Attributes] ペインの [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

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）　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。

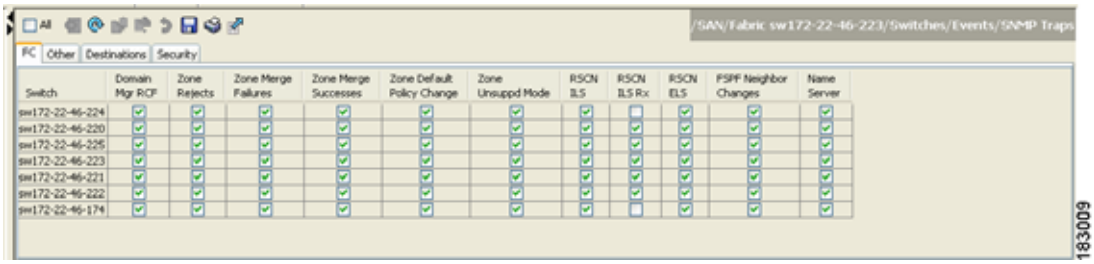
- 「SNMPv2c 通知の設定」（P.7-9）

SNMPv2c 通知の設定

Fabric Manager を使用して 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　[Switches] > [Events] の順に展開し、[Physical Attributes] ペインで [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（図 7-6 を参照）。

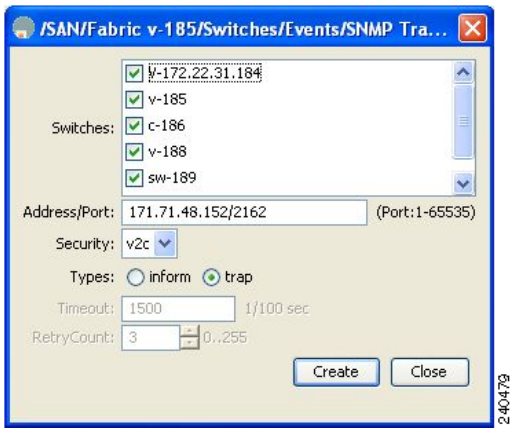
図 7-6　SNMP 通知



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 Destination] ダイアログボックスが表示されます（図 7-7 を参照）。

図 7-7　[Create Destinations] ダイアログボックス



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

（注）　Fabric Manager を使用して、IPv4 を使用した SNMPv3 通知を設定するには、[Create Destinations] ダイアログボックスの [Security] ドロップダウン リストから [v3] を選択します（図 7-7 を参照）。必要に応じて、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。[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

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。通知は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。

表 7-1 に、4.2(1) よりも前のバージョンの Cisco NX-OS MIB に対して通知をイネーブルにするための、Fabric Manager での手順を示します。[Switches] > [Events] > [SNMP Traps] の順に選択し、この表に示すチェックボックスを表示します。

（注）　[Switches] > [Events] > [SNMP Traps] を選択すると、SNMP 通知の設定方法に応じて、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.7-10）で表示される通知を参照してください。

表 7-1　SNMP 通知のイネーブル化

MIB	Fabric Manager のチェックボックス
CISCO-ENTITY-FRU-CONTROL-MIB	[Other] タブを選択し、[FRU Changes] をオンにします。
CISCO-FCC-MIB	[Other] タブを選択し、[FCC] をオンにします。

表 7-1　SNMP 通知のイネーブル化 （続き）

MIB	Fabric Manager のチェックボックス
CISCO-DM-MIB	[FC] タブを選択し、[Domain Mgr RCF] をオンにします。
CISCO-NS-MIB	[FC] タブを選択し、[Name Server] をオンにします。
CISCO-FCS-MIB	[Other] タブを選択し、[FCS Rejects] をオンにします。
CISCO-FDMI-MIB	[Other] タブを選択し、[FDMI] をオンにします。
CISCO-FSPF-MIB	[FC] タブを選択し、[FSPF Neighbor Change] をオンにします。
CISCO-LICENSE-MGR-MIB	[Other] タブを選択し、[License Manager] をオンにします。
CISCO-IPSEC-SIGNALLING-MIB	[Other] タブを選択し、[IPSEC] をオンにします。
CISCO-PSM-MIB	[Other] タブを選択し、[Port Security] をオンにします。
CISCO-RSCN-MIB	[FC] タブを選択し、[RSCN ILS] および [RCSN ELS] をオンにします。
SNMPv2-MIB	[Other] タブを選択し、[SNMP AuthFailure] をオンにします。
VRRP-MIB, CISCO-IETF-VRRP-MIB	[Other] タブを選択し、[VRRP] をオンにします。
CISCO-ZS-MIB	[FC] タブを選択し、[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

その他の通知はすべてデフォルトでディセーブルになっています。

Fabric Manager Release 4.3(1b) およびそれ以前を使用した個々の通知のイネーブル化

4.2(1) よりも前のバージョンに対し Fabric 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　[Switches] > [Events] の順に展開し、[Physical Attributes] ペインで [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、Fibre Channel 関連の通知をイネーブルにします。

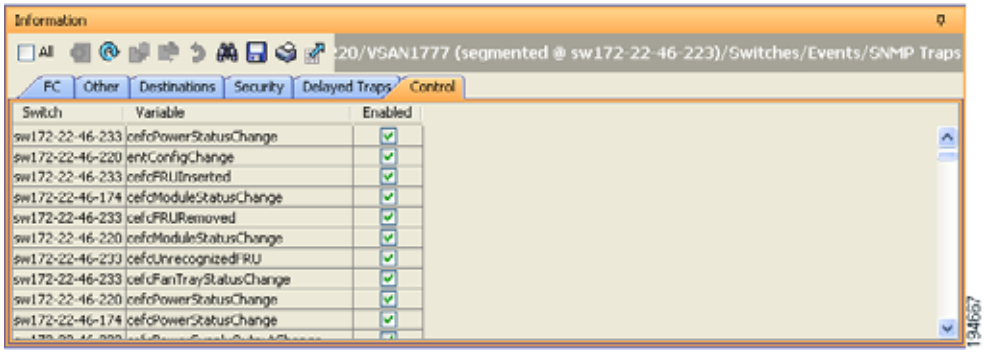
ステップ 3　イネーブルにする各通知のチェックボックスをオンにします。

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。

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（図 7-8 を参照）。

図 7-8　SNMP トラップ ウィンドウ



（注） [Control] タブは、NX-OS Release 4.2(1) 以降でだけ使用できます。Fabric Manager Release 4.2(1) 以降を使用して個別の通知をイネーブルにするには、[Control] タブをクリックします。

ステップ 6　[Apply Changes] アイコンをクリックして、エントリを作成します。

Device Manager を使用した個々の通知のイネーブル化

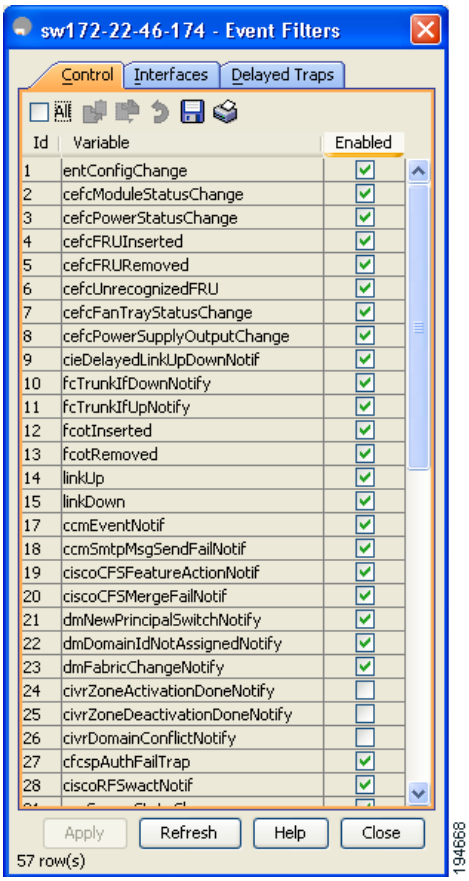
Device Manager を使用して個々の通知をイネーブルにするには、次の手順を実行します。

（注） Device Manager で、コマンド **no snmp-server enable traps link** 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。

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（図 7-9 を参照）。

図 7-9　[Event Filters] ウィンドウ



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。

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。

通知対象ユーザの資格情報は、SNMPv3 インフォーム通知メッセージを設定された SNMP に暗号化するために使用されます。

（注）　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。

イベント セキュリティの設定

注意　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。

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。Fabric Manager 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。

Fabric Manager を使用して 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　[Switches] > [Events] の順に展開し、[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。

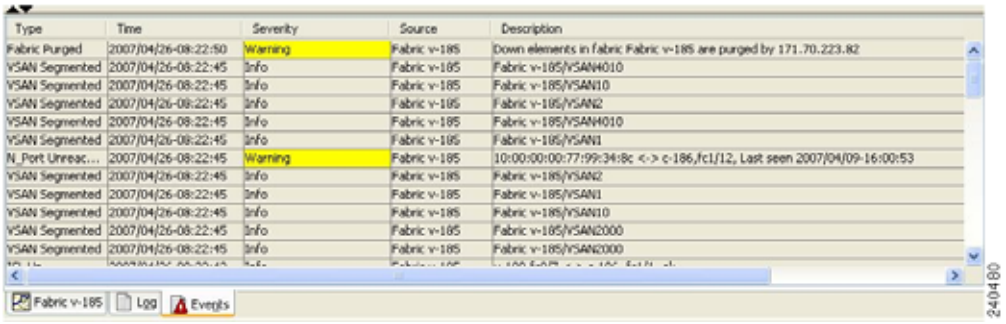
ステップ 3　メッセージ プロトコル モデル（MPModel）、セキュリティ モデル、セキュリティ名、およびセキュリティ レベルを設定します。

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

SNMP イベント ログを Fabric Manager で表示するには、[Events] タブをクリックします（図 7-10 を参照）。[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 7-10　イベント情報



（注）　イベント ログを表示するには、MDS syslog マネージャを設定しておく必要があります。

注意　これらの値を別の Fabric Manager 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恐れがあります。

デフォルト設定

表 7-2 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 7-2　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

CHAPTER 8

RMON の設定

RMON は Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）標準のモニタリング規格です。RMON を使用すると、さまざまなネットワーク エージェントやコンソール システムが、ネットワーク モニタリング データを交換できます。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 の概要

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 セキュリティに関連する Command Line Interface（CLI; コマンドライン インターフェイス）の設定については、「SNMP セキュリティの概要」（P.7-1）を参照してください。

Threshold Manager を使用した 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。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 Fabric Manager 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） また、RMON MIB オブジェクトにアクセスするには、スイッチ上で SNMP を設定することも必要です。

RMON アラームの設定

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。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.16 の場合、1.3.6.1.2.1.2.2.1.14.16）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。

オプションで指定できるパラメータは、次のとおりです。

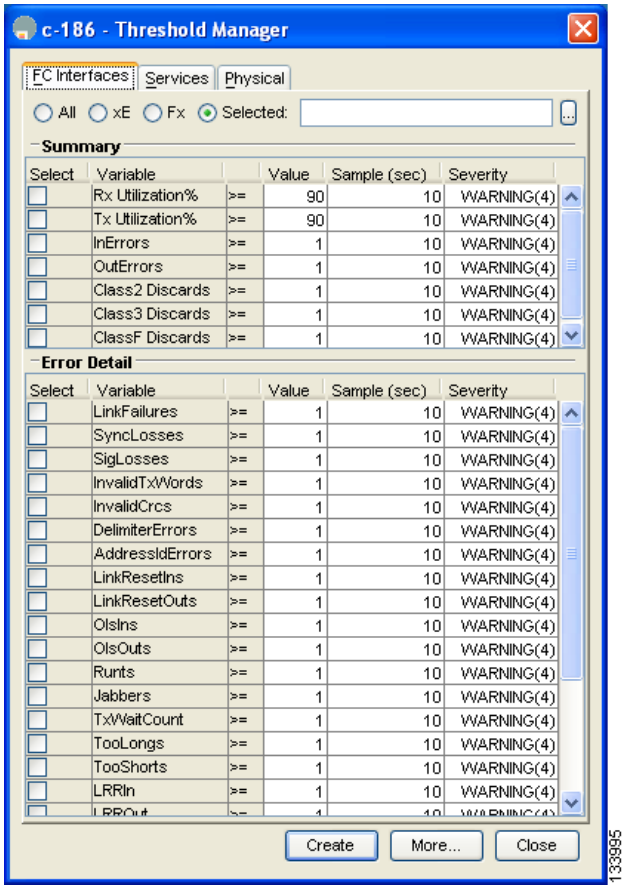
- 上昇しきい値および下限しきい値が指定値を超えた場合に発生させるイベント番号
- アラームの所有者

ポートごとの RMON アラームのイネーブル化

Device Manager を使用し、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（図 8-1 を参照）。

図 8-1　[Threshold Manager] ダイアログボックス



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、[Fatal]、[Warning]、[Critical]、[Error]、[Information] の中から選択します。

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。

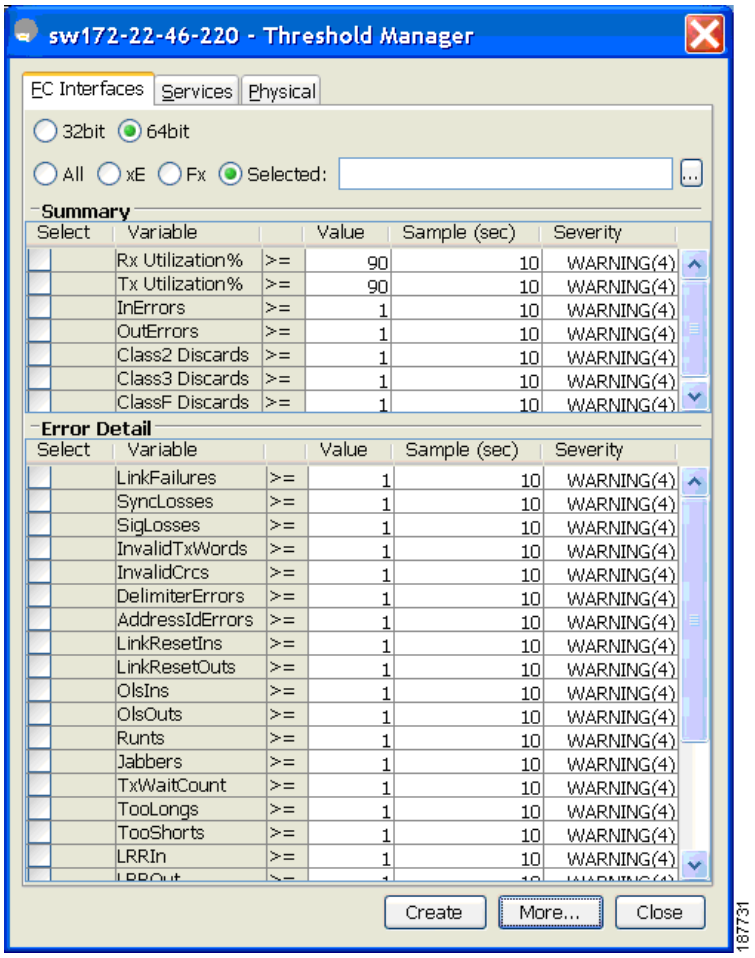
32 ビット アラームと 64 ビット アラームのイネーブル化

Device Manager を使用し、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（図 8-2 を参照）。

図 8-2　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



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。

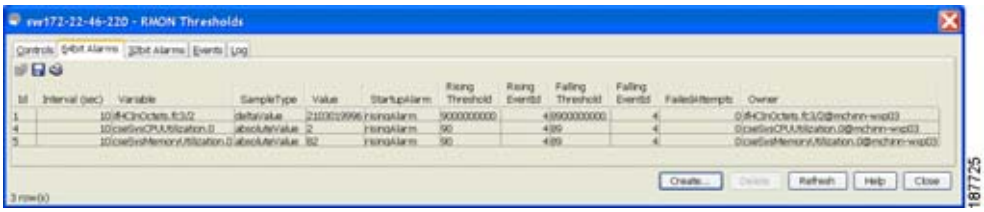
ステップ 6　アラームに割り当てる重大度を、[Fatal]、[Warning]、[Critical]、[Error]、[Information] の中から選択します。

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。

図 8-3　[RMON Thresholds] ダイアログボックス



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。

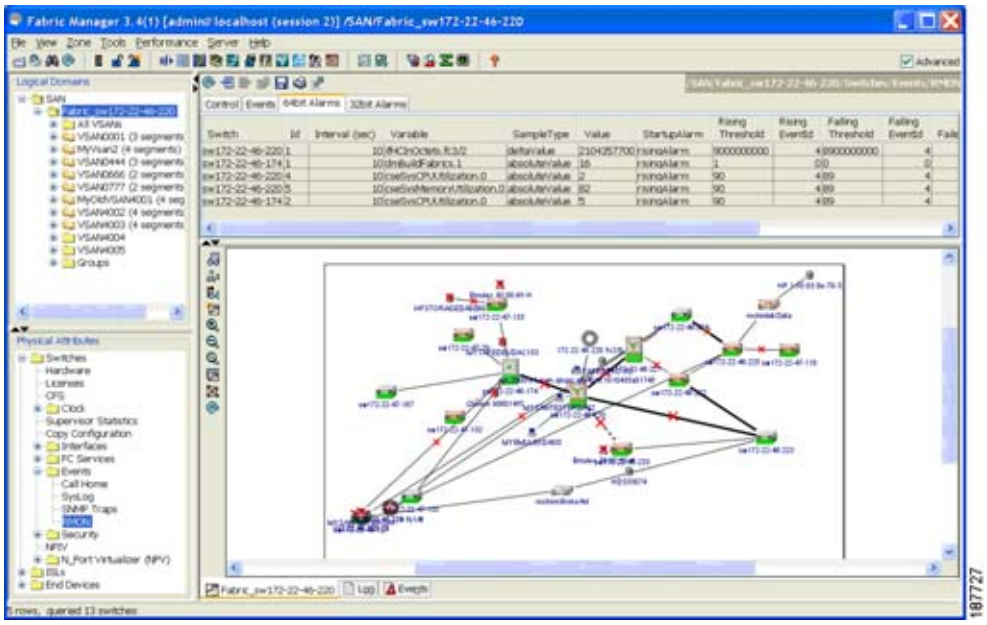
Fabric Manager での RMON アラームの作成

Fabric Manager を使用して 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] > [Events] > [RMON] タブを選択します。

64 ビット アラーム ダイアログボックスが表示されます（図 8-4 を参照）。

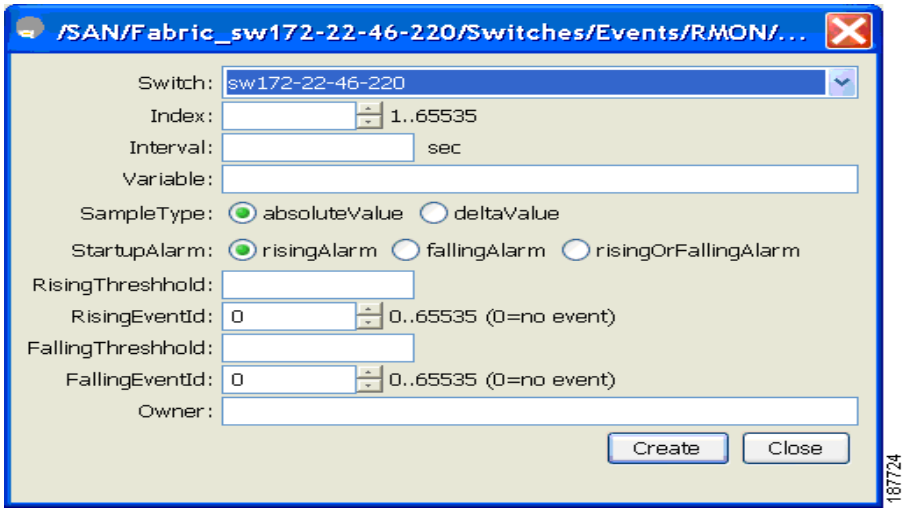
図 8-4　64 ビット アラーム ダイアログボックス



ステップ 2　[64-bit alarms] タブをクリックします。

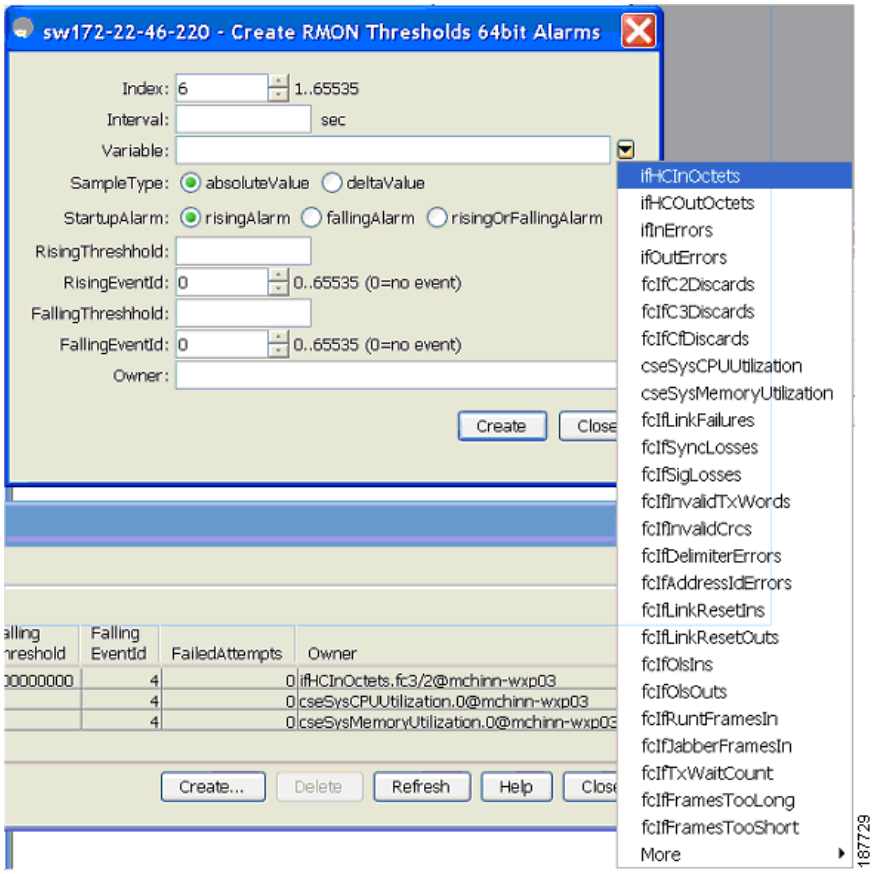
ステップ 3　[Create Row] タブをクリックします。[Create Row] ウィンドウが表示されます（図 8-5 を参照）。

図 8-5　64 ビット アラームの [Create Row] タブ



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 （図 8-6 を参照してください）。

図 8-6　64 ビット アラームの MIB 変数フィールド ダイアログボックス



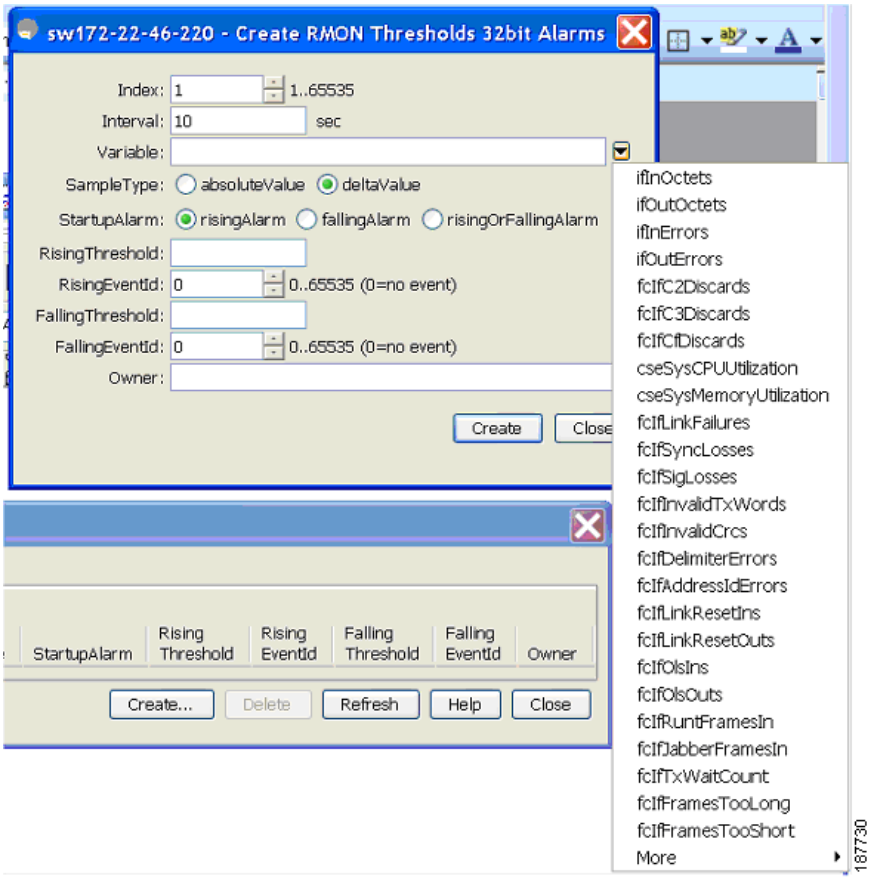
（注）　[Variable] フィールドの入力を完了するには、ドロップダウン リストから選択した変数に加え、ifHCInOctets のように、インターフェイスの詳細を入力する必要があります。

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 （図 8-7 を参照してください）。

図 8-7　32 ビット アラームの MIB 変数フィールド ダイアログボックス



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

Device Manager を使用し、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。

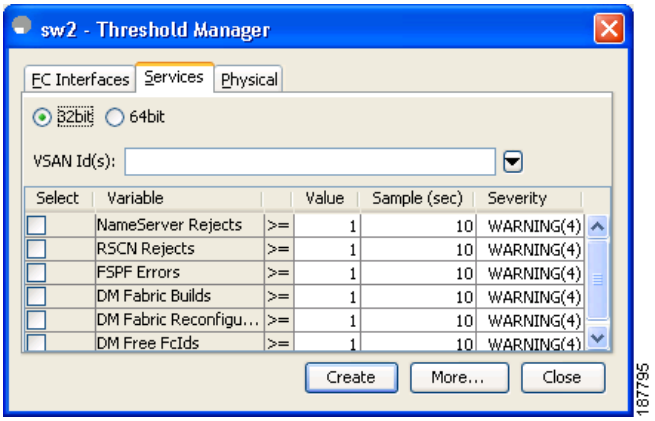
ステップ 1　[Admin] > [Events] > [Threshold Manager] を選択し、[Services] タブをクリックします。

[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（図 8-8 を参照）。

図 8-8　32 ビット アラーム ダイアログボックスの [Services] タブ



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)] フィールドで、監視対象の VSAN を 1 つ以上入力します（複数の VSAN を指定する場合は、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　監視する各変数の [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、[Fatal]、[Critical]、[Error]、[Warning]、[Information] から選択します。

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。

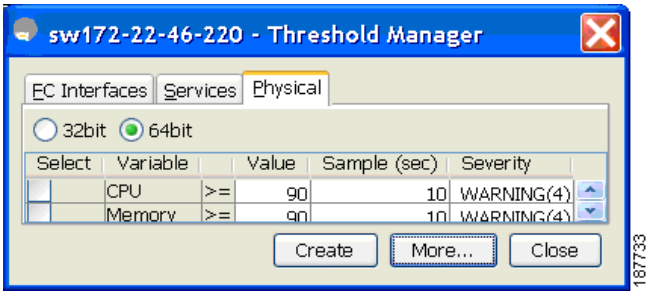
物理コンポーネントに対する 32 ビットおよび 64 ビット RMON アラームのイネーブル化

Device Manager を使用して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（図 8-9 を参照）。

図 8-9　64 ビット アラームの [Physical] タブ



ステップ 2　監視する各変数の [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、[Fatal(1)]、[Warning(2)]、[Critical(3)]、[Error(4)]、[Information(5)] の中から選択します。

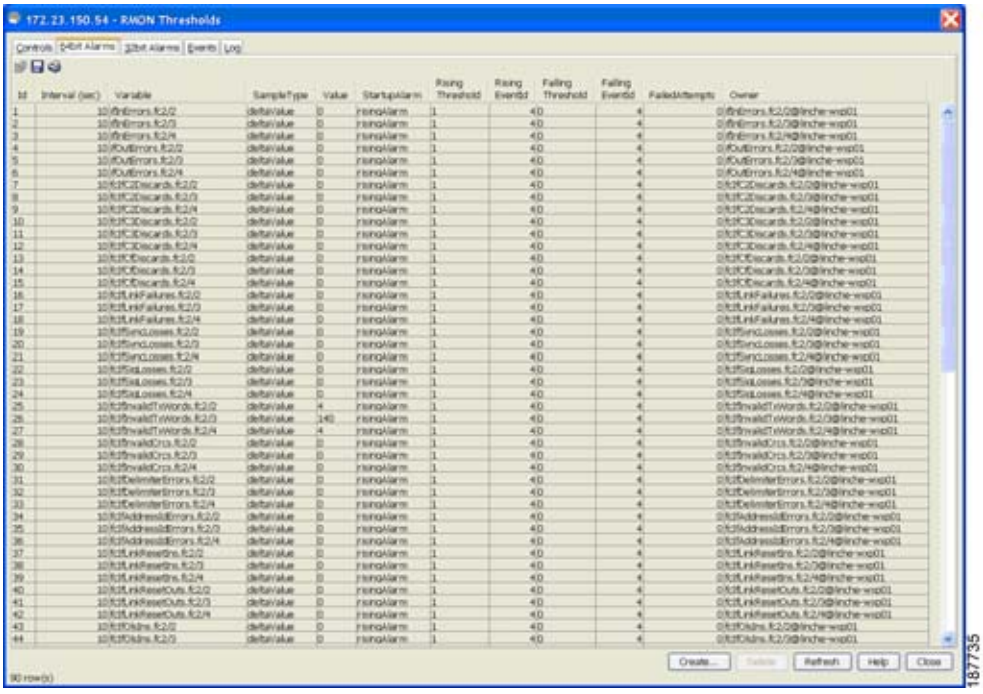
ステップ 6　[Create] をクリックします。

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（図 8-10 を参照）。

図 8-10　[64-Bit Alarms] タブ



（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

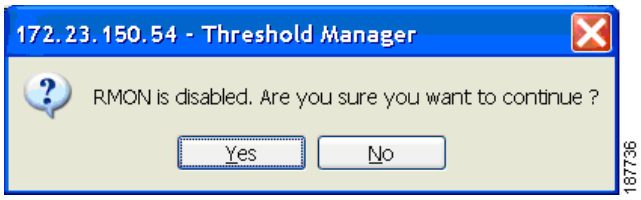
RMON は、スイッチを設定する前に RMON アラームの設定を確認しません。

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　[Physical Attributes] > [Events] > [RMON] を選択し、[Control] タブをクリックします。

Threshold Manager の RMON アラーム作成ダイアログボックスが表示されます（図 8-11 を参照）。

図 8-11　Threshold Manager の RMON アラーム作成ダイアログボックス



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。

図 8-12　[RMON Threshold] の [Control] タブ

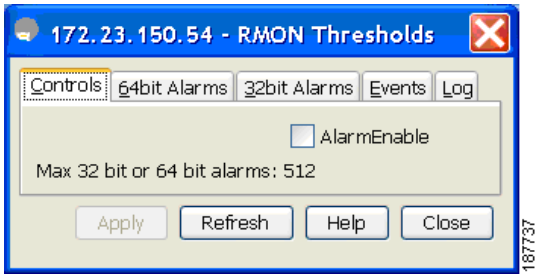
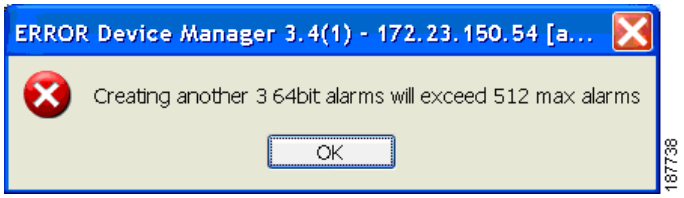


図 8-13　Device Manager のエラー タブ



RMON イベントの管理

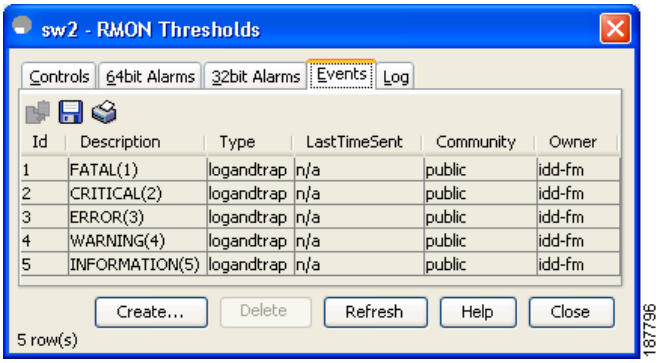
Device Manager を使用してカスタマイズされた RMON イベントを定義するには、次の手順を実行します。

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] の [Events] タブが表示されます（図 8-14 を参照）。

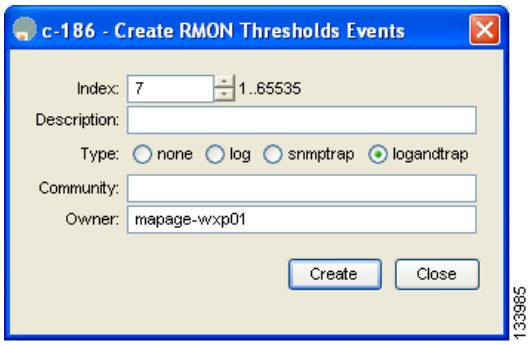
図 8-14　[RMON Thresholds] の [Events] タブ



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（図 8-15 を参照）。

図 8-15　[Create RMON Thresholds Events] ダイアログボックス



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

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、この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

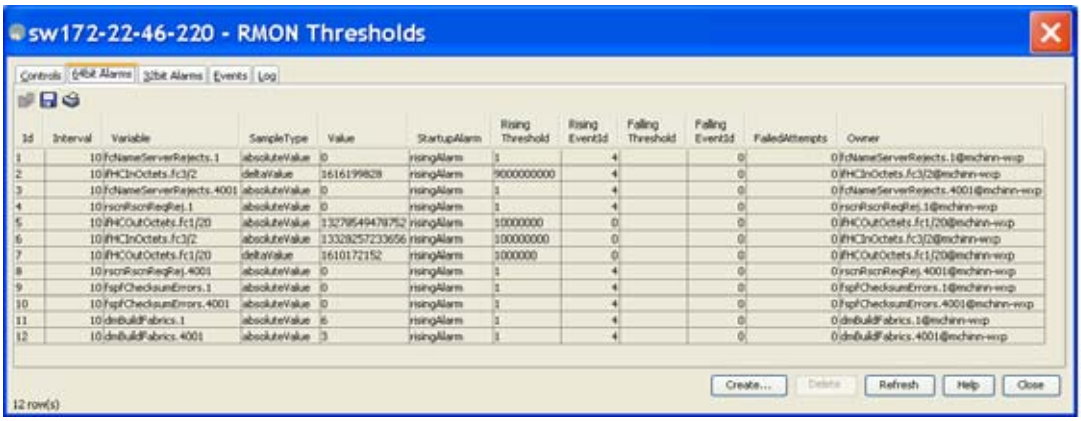
Device Manager を使用して、すでにイネーブルになっているアラームを表示するには、次の手順を実行します。

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（図 8-16 を参照）。

図 8-16　[RMON Thresholds] ダイアログボックス



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

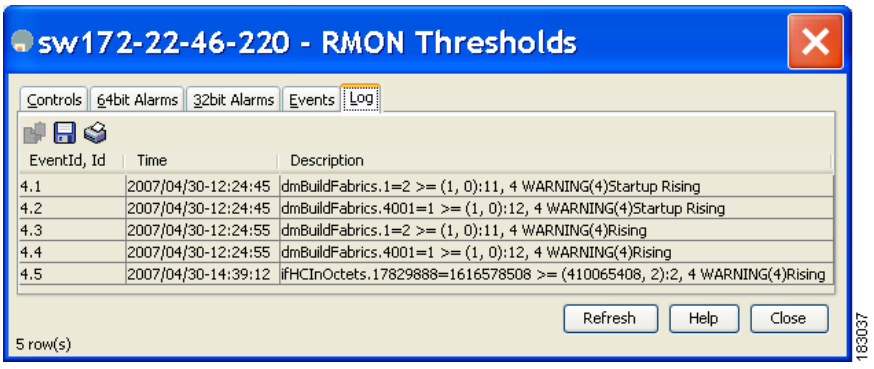
Device Manager を使用して RMON ログを表示するには、次の手順を実行します。

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（図 8-17 を参照）。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。

図 8-17　[RMON Thresholds] の [Log] タブ



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

CHAPTER 9

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。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 スイッチではランダムな ID が使用されます。

注意 fcdomain パラメータを毎日変更しないでください。このような変更は、管理者や、スイッチの動作に精通した担当者が実行してください。

ヒント 設定の変更時には、実行コンフィギュレーションを保存してください。次回スイッチをリブートすると、保存したコンフィギュレーションが使用されます。コンフィギュレーションを保存しないと、以前保存したスタートアップ コンフィギュレーションが使用されます。

この章の内容は、次のとおりです。

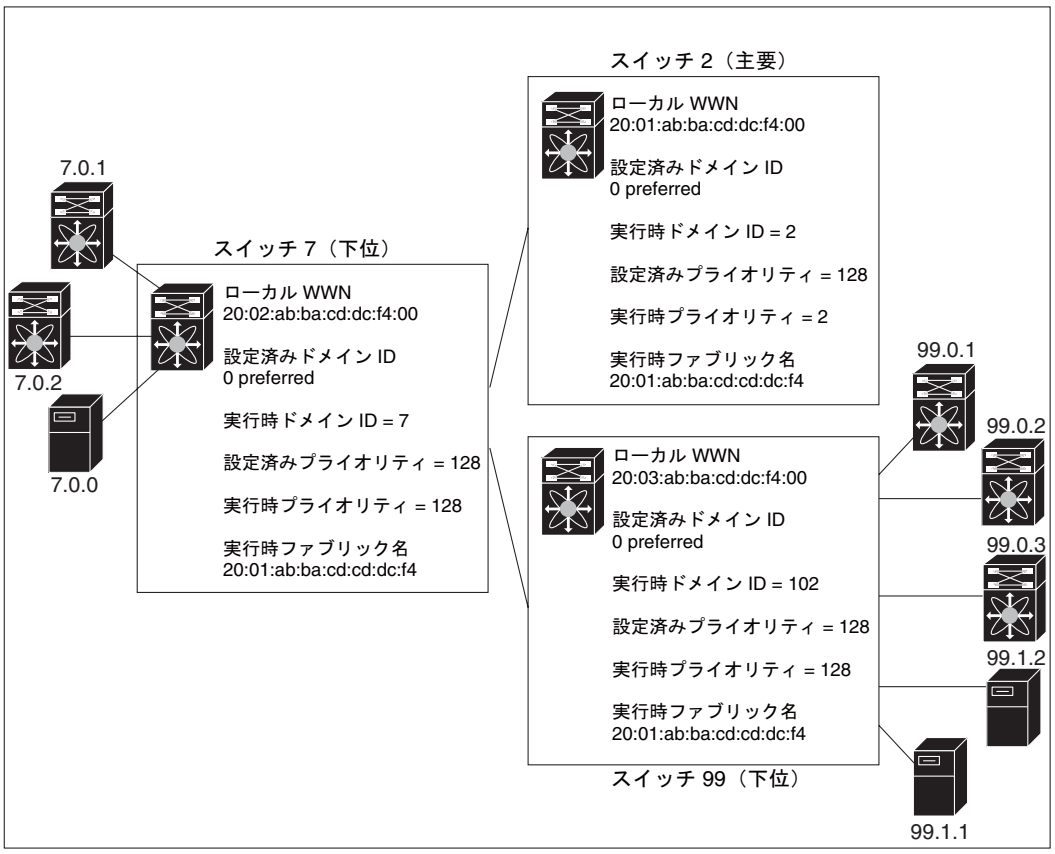
ファイバ チャネル ドメイン

ここでは、fcdomain の各フェーズについて説明します。

- 主要スイッチ選択：このフェーズでは、ファブリックで一意の主要スイッチが選択されます。
- ドメイン ID 配信：このフェーズでは、ファブリックの各スイッチが一意のドメイン ID を取得します。
- FC ID 割り当て：このフェーズでは、ファブリックで対応するスイッチに接続されている各デバイスに、一意の FC ID が割り当てられます。
- ファブリック再設定：このフェーズでは、ファブリックのすべてのスイッチが再同期され、すべてのスイッチが新しいスイッチ選択フェーズを同時に再開します。

図 9-1 に fcdomain の設定例を示します。

図 9-1　fcdomain の設定例



（注）　すべての手順で使用するドメイン ID および VSAN の値は例にすぎません。設定に合った ID および値を使用してください。

ここでは、fcdomain の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。

- 「ドメインの再起動の概要」（P.9-3）
- 「Domain Manager のターボ モードの設定」（P.9-3）
- 「ドメインの再起動」（P.9-5）
- 「スイッチ プライオリティの概要」（P.9-6）
- 「スイッチ プライオリティの設定」（P.9-7）
- 「fcdomain の初期化の概要」（P.9-7）
- 「fcdomain のイネーブル化またはディセーブル化」（P.9-7）
- 「ファブリック名の設定」（P.9-8）
- 「着信 RCF の概要」（P.9-8）
- 「着信 RCF の拒否」（P.9-8）
- 「結合ファブリックの自動再構成の概要」（P.9-9）

- 「自動再構成のイネーブル化」（P.9-9）

ドメインの再起動の概要

fcdomain では、中断を伴う起動または中断を伴わない起動ができます。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 の矛盾を解決するためには、ドメイン ID を手動で割り当てる必要があります。手動で割り当てたドメイン ID など、多くの設定変更を適用するには、中断を伴う再起動が必要です。中断を伴わないドメインの再起動は、優先ドメイン ID をスタティック ID に変更する（実際のドメイン ID は変更されない）ときに限って許容されます。

（注） ユーザがスタティック ドメインを具体的に設定しますが、スタティック ドメインはランタイム 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、次の中断を伴う再起動または中断を伴わない再起動の後で、ランタイム ドメイン ID がスタティック ドメイン ID に変更されます。

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。

対応するランタイム値に設定の多くを適用できます。後続の各セクションで、fcdomain パラメータをランタイム値に適用する方法について詳しく説明します。

Domain Manager のターボ モードの設定

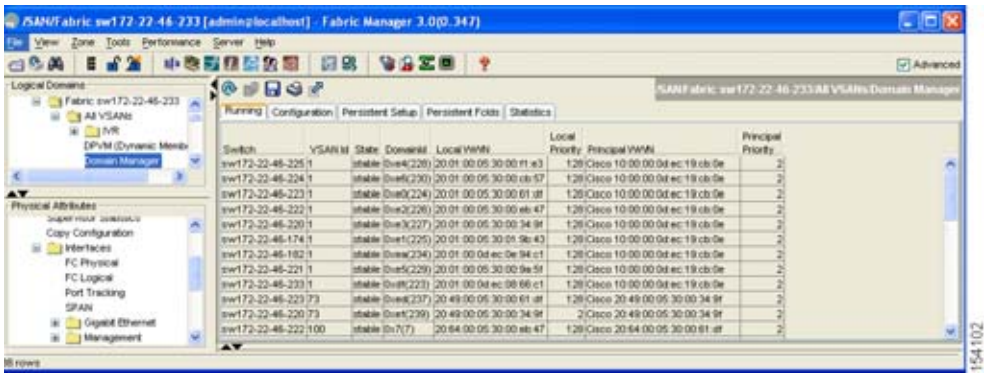
Domain Manager のターボ モード機能を使用すると、最適化を使用して Domain Manager を再起動できます。Domain Manager の再起動では、高速再起動モードと選択再起動モードを選択できます。再起動モードを空白のままにすると、最適化はディセーブルになります。

Fabric 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　[Fabricxx] > [VSANxx] の順に展開し、ターボ モードを設定するファブリックと VSAN の [Logical Domains] ペインで [Domain Manager] を選択します。

[Information] ペインに、図 9-2 に示す、ドメインの [Running] タブの設定が表示されます。

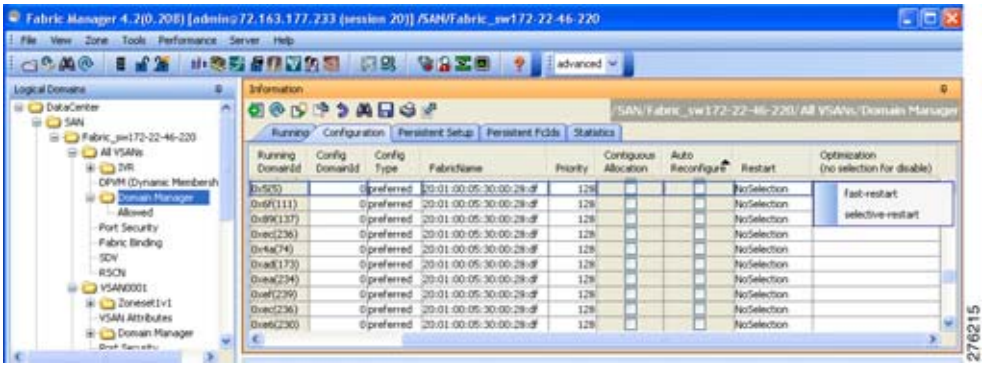
図 9-2　実行中ドメインの設定



ステップ 2　[Configuration] タブをクリックします。

図 9-3 に示すスイッチ設定が表示されます。

図 9-3　ドメインの設定



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。

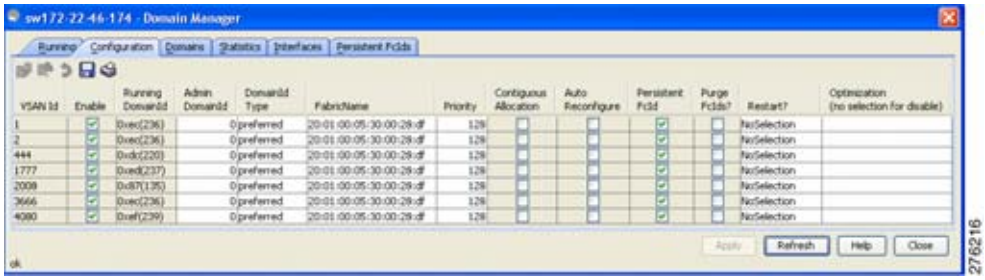
ステップ 4　[Apply Changes] アイコンをクリックし、この再起動を開始します。

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。

図 9-4 に示すスイッチ設定が表示されます。

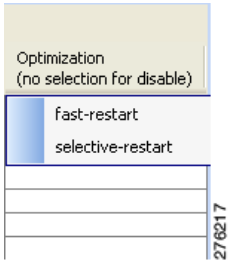
図 9-4　ドメインの設定



（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。図 9-5 に示すように、[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。

図 9-5　[Optimization] フィールド



ステップ 3　[Apply] をクリックしてこの再起動を開始します。

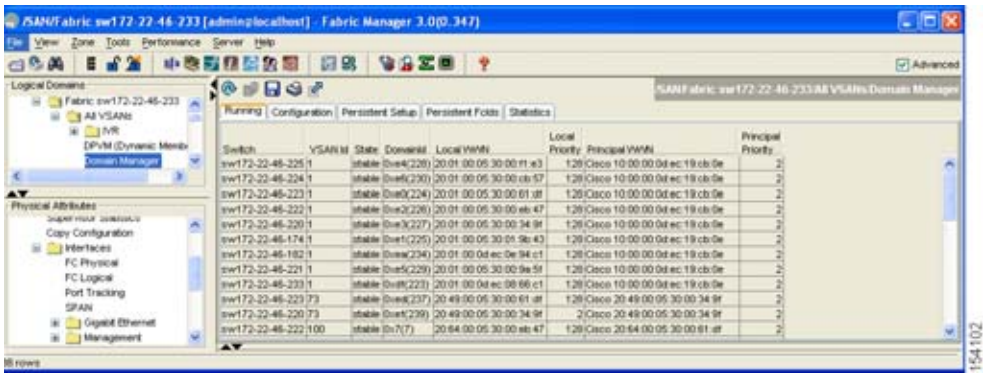
ドメインの再起動

Fabric Manager を使用して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　[Fabricxx] > [VSANxx] の順に展開し、再起動するファブリックおよび VSAN の [Logical Domains] ペインで [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 （図 9-6 を参照してください）。

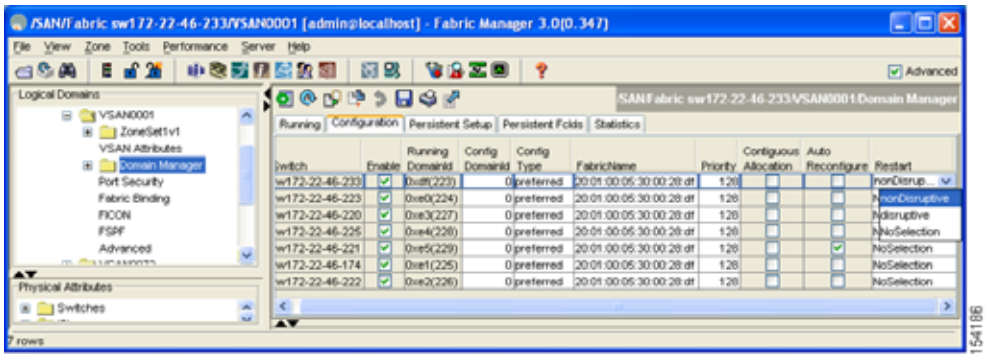
図 9-6　実行中ドメインの設定



ステップ 2　[Configuration] タブをクリックします。

図 9-7 に示すスイッチ設定が表示されます。

図 9-7　ドメインの設定



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 プライオリティの概要

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範囲は 1 ～ 254 です。プライオリティ 1 が最も高いプライオリティになります。値 255 は別のスイッチから受け入れられますが、ローカルに設定できません。

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、プライオリティが最高の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 の再起動時にランタイムに適用されます（「ドメインの再起動の概要」（P.9-3）を参照）。この設定は、中断を伴う再起動および中断を伴わない再起動の両方に適用可能です。

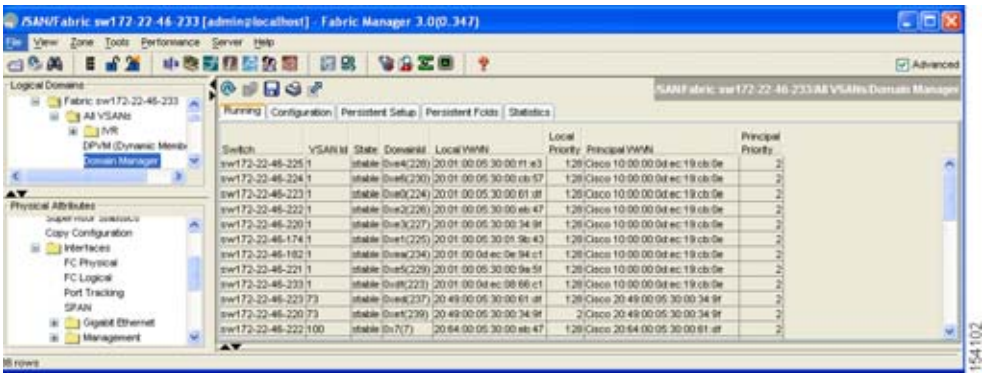
スイッチ プライオリティの設定

Fabric Manager を使用して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　[Fabricxx] > [VSANxx] の順に展開し、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および VSAN の [Logical Domains] ペインで [Domain Manager] を選択します。

図 9-8 のように、[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。

図 9-8　実行中ドメインの設定



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 の初期化の概要

fcdomain 機能はデフォルトで各スイッチでイネーブルになっています。あるスイッチで 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のその他のスイッチに加わらなくなります。fcdomain 設定は、中断を伴う再起動でランタイムに適用されます。

fcdomain のイネーブル化またはディセーブル化

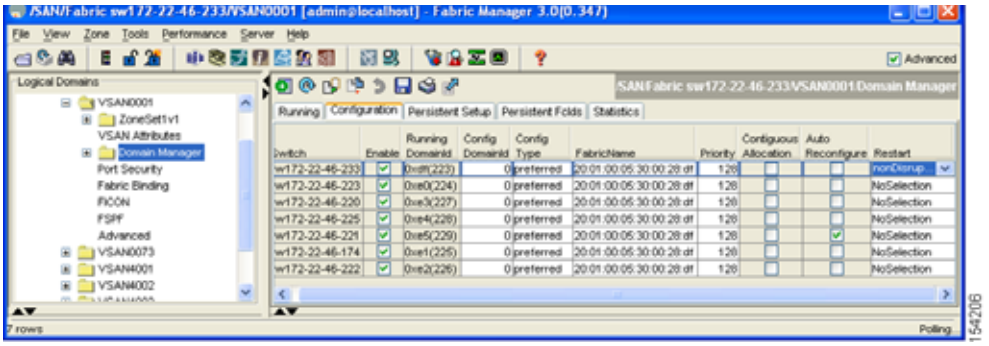
Fabric Manager を使用して、単一の VSAN またはある範囲の VSAN で fcdomain をディセーブルにするには、次の手順を実行します。

ステップ 1　[Fabricxx] > [VSANxx] の順に展開し、fcdomain をディセーブルにするファブリックおよび VSAN の [Logical Domains] ペインで、[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（図 9-9 を参照）。

図 9-9　ドメインの設定



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

Fabric Manager を使用して、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　[Fabric*xx*] > [VSAN*xx*] と展開し、ファブリック名を設定するファブリックおよび VSAN の [Logical Domains] ペインで [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 の概要

インターフェイスや VSAN ごとに、RCF 要求フレームの拒否を選択できます。RCF 拒否オプションはデフォルトでディセーブルです（つまり、RCF 要求フレームは自動的には拒否されません）。

RCF 拒否オプションは、中断を伴う再起動を通じて、実行時にすぐに有効になります（「ドメインの再起動の概要」（P.9-3）を参照）。

着信 RCF の拒否

Fabric Manager を使用して着信 RCF 要求フレームを拒否するには、次の手順を実行します。

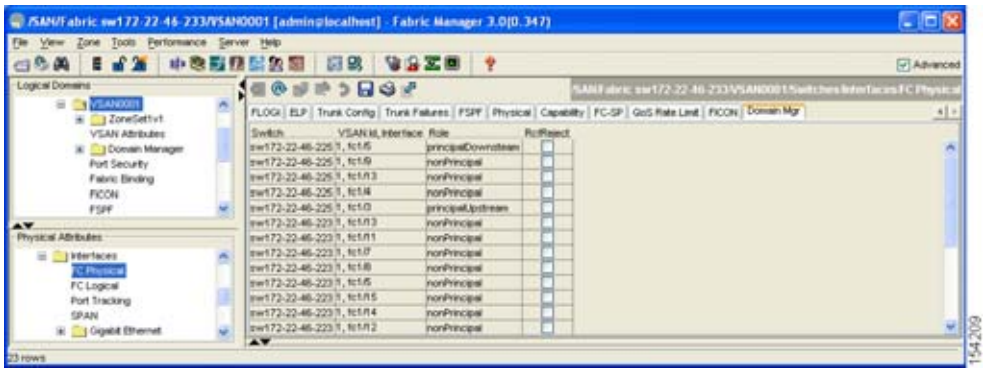
ステップ 1　[Switches] > [Interfaces] の順に展開し、[Physical Attributes] ペインで [FC Physical] を選択します。

[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。

図 9-10 の情報が表示されます。

図 9-10　着信 RCF 要求フレームの拒否



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。

結合ファブリックの自動再構成の概要

自動再構成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。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。

- 自動再構成が両方のスイッチでイネーブルである場合は、中断を伴う再構成フェーズが始まります。
- 片方のスイッチまたは両方のスイッチで自動再構成がディセーブルである場合、2 つのスイッチ間のリンクは分離されます。

自動再構成オプションは実行時にすぐに有効になります。fcdomain を再起動する必要はありません。ドメインのオーバーラップのためにドメインが現在分離されており、後で両方のスイッチで自動再構成オプションをイネーブルにすると、ファブリックは引き続き分離されます。両方のスイッチで自動再構成オプションをイネーブルにしてからファブリックを接続すると、中断を伴う再構成（RCF）が行われます。中断を伴う再構成では、データ トラフィックが影響されることがあります。重複リンクで構成されているドメインを変更して、ドメインのオーバーラップを解消することにより、中断を伴わない fcdomain の再構成を実行できます。

自動再構成のイネーブル化

Fabric Manager を使用して特定の VSAN（またはある範囲の VSAN）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　[Fabric*xx*] > [VSAN*xx*] の順に展開し、自動再構成をイネーブルにするファブリックおよび VSAN の Logical Domains ペインで [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

ドメイン ID により、VSAN でスイッチが一意に識別されます。スイッチには、さまざまな VSAN で異なるドメイン ID が付いていることがあります。ドメイン ID は FC ID 全体の一部分です。

ここでは、ドメイン ID の設定方法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。

ドメイン ID の概要

設定したドメイン ID は、優先またはスタティックにすることができます。デフォルトでは、設定されているドメイン ID は 0（ゼロ）であり、設定タイプは優先です。

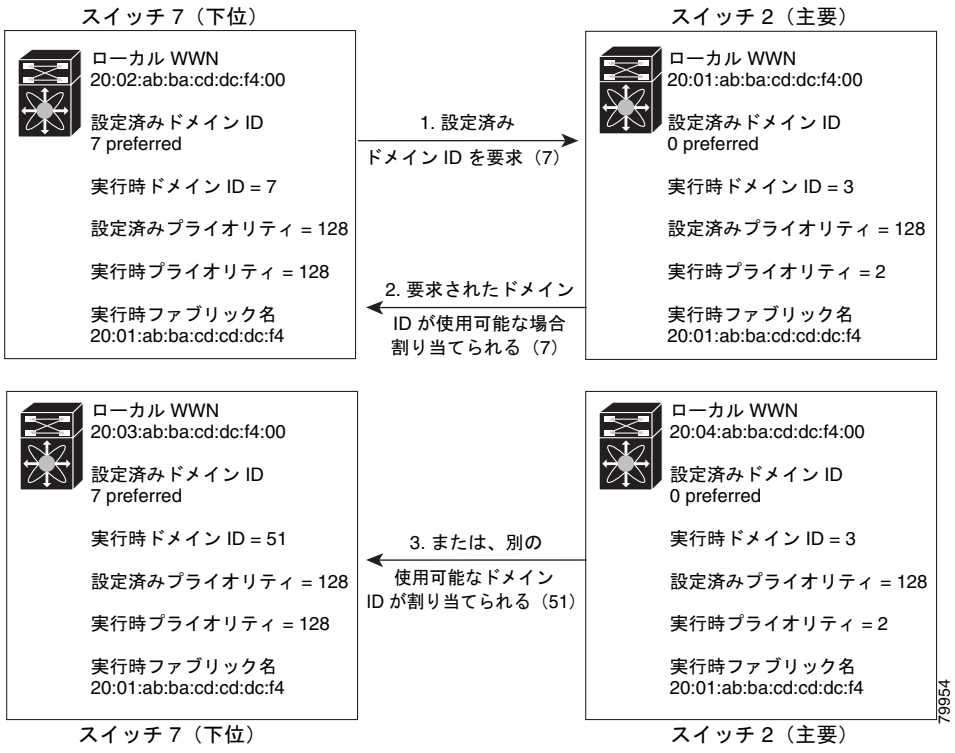
（注）　値 0（ゼロ）は、優先オプションを使用している場合に限り設定できます。

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 を要求で送信します。スタティックなドメイン ID を使用してください。

下位スイッチがドメインを要求すると、次のプロセスが行われます（図 9-11 を参照）。

1. ローカル スイッチが、設定済みドメイン ID 要求を主要スイッチに送信します。
2. 要求されたドメイン ID が使用可能である場合、主要スイッチはそのドメイン ID を割り当てます。要求されたドメイン ID が使用可能でない場合は、別の使用可能なドメイン ID を割り当てます。

図 9-11　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。

- 許可されているドメイン ID リスト
- 設定されているドメイン ID
- 主要スイッチが要求スイッチに割り当てたドメイン ID

特定の状況では次のように変化します。

- 受信したドメイン ID が許可リスト内に収まっていない場合は、要求ドメイン ID がランタイム ドメイン ID になり、その VSAN のインターフェイスはすべて分離されます。
- 割り当てられたドメイン ID および要求したドメイン ID が同一である場合、優先オプションとスタティック オプションは関係なく、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。
- 割り当てられたドメイン ID および要求したドメイン ID が異なる場合は、次のケースが当てはまります。
  - 設定されているタイプがスタティックである場合、割り当てられたドメイン ID は廃棄され、すべてのローカル インターフェイスは分離されて、ローカル スイッチが設定済みドメイン ID を自分自身に割り当て、そのドメイン ID がランタイム 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。

設定されたドメイン ID を変更すると、VSAN で現在設定されているすべての許可ドメイン ID リストに新しいドメイン ID が含まれる場合に限り、変更内容は受け入れられます。ゼロ優先ドメイン ID を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 構成では、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、その VSAN にエクスポートされる可能性がある IVR ドメインにもスタティック ドメインが割り当てられている必要があります。

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 リストの概要」（P.9-13）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ということは、特定のドメイン ID を要求するということです。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 を指定するということも、特定のドメイン ID を要求するということですが、要求したドメイン ID が使用不可である場合、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、中断を伴う再起動または中断を伴わない再起動の後で実行時に適用できますが、優先オプションが実行時に適用されるのは中断を伴う再起動の後だけです（「ドメインの再起動の概要」（P.9-3）を参照）。

（注）　VSAN 内では、すべてのスイッチでドメイン ID タイプが同一である必要があります（スタティックまたは優先）。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。

Fabric Manager を使用して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　[Fabricxx] > [VSANxx] の順に展開し、ドメイン ID を設定するファブリックおよび VSAN の [Logical Domains] ペインで [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 リストの概要

デフォルトでは、割り当てるドメイン ID リストの有効範囲は 1 から 239 までです。許可ドメイン ID リストに含める範囲のリストを指定し、それぞれの範囲をカンマで区切ることができます。主要スイッチは、ローカルに設定されている許可ドメイン 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。今後、NAT 機能がない IVR を実装する必要がある場合は、これが役立ちます。

ヒント　ファブリックの 1 つのスイッチで許可リストを設定する場合は、ファブリックの他の全スイッチで同じリストを設定して一貫性を保つか、Cisco Fabric Service（CFS）を使用して設定を配信することを推奨します。

許可ドメイン ID リストでは、次の条件を満たす必要があります。

- この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 を許可リストに含める必要があります。
- このスイッチが下位スイッチである場合は、ローカル ランタイム ドメイン ID を許可リストに含める必要があります。
- スイッチのローカルで設定されているドメイン ID を許可リストに含める必要があります。
- 割り当てられているドメイン ID、およびその他のすでに設定されているドメイン ID リストの共通部分は空にできません。

許可ドメイン ID リストの設定

Fabric Manager を使用して許可ドメイン 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　[Fabricxx] > [VSANxx] > [Domain Manager] の順に展開し、許可ドメイン ID リストを設定するファブリックおよび VSAN の [Logical Domains] ペインで [Allowed] を選択します。

[Information] ペインに CFS 設定が表示されます（図 9-12 を参照）。

図 9-12　許可 CFS 設定情報

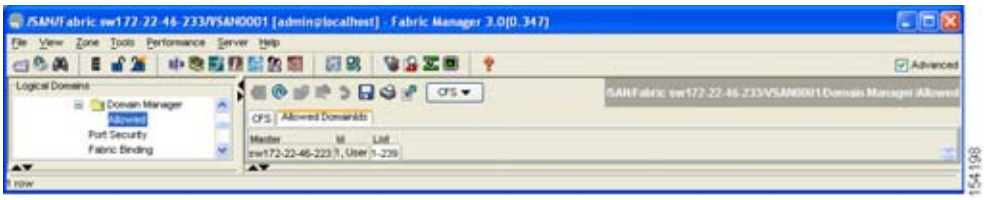
ステップ 2　[Admin] ドロップダウン メニューを [enable] に設定し、[Global] ドロップダウン メニューを [enable] に設定します。

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。

図 9-13 に示す [Allowed Domain ID] 画面が表示されます。

図 9-13　許可ドメイン ID リスト



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 リストの CFS 配信の概要

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。

（注）　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。

VSAN のすべてのスイッチで許可ドメイン ID リストの一貫性を保つには、CFS を使用して許可ドメイン ID リストを配信します。

（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。

配信のイネーブル化

許可ドメイン ID リストの CFS 配信は、デフォルトでディセーブルです。許可ドメイン ID リストの配信先とな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。

Fabric Manager を使用して許可ドメイン ID リスト設定の配信をイネーブルにする（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　[Fabricxx] > [VSANxx] > [Domain Manager] の順に展開し、許可ドメイン ID リストを設定するファブリックおよび VSAN の [Logical Domains] ペインで [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。

ファブリックのロック

既存の設定を変更する最初の処理により、保留設定が作成されてファブリックの機能がロックされます。ファブリックをロックすると、次の条件が成立します。

- 他のユーザは、この機能の設定を変更できなくなります。
- 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。

Fabric Manager を使用して保留中のドメイン設定変更を確定し、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　[Fabricxx] > [VSANxx] > [Domain Manager] の順に展開し、許可ドメイン ID リストを設定するファブリックおよび VSAN の [Logical Domains] ペインで [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

ドメイン設定に対する保留中の変更をいつでも廃棄し、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する（打ち切る）と、設定は影響されずにロックが解除されます。

Fabric Manager を使用して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　[Fabricxx] > [VSANxx] > [Domain Manager] の順に展開し、許可ドメイン ID リストを設定するファブリックおよび VSAN の [Logical Domains] ペインで [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。

ファブリックのロックのクリア

ドメイン設定タスクを実行し、変更の確定か廃棄を行ってロックを解除していない場合、管理者はファブリック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、ファブリックのロックは解除されます。

ヒント　保留中の変更は一時的なディレクトリだけで使用可能であり、スイッチが再起動されると廃棄されます。

Fabric Manager を使用して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　[Fabricxx] > [VSANxx] > [Domain Manager] の順に展開し、許可ドメイン ID リストが必要なファブリックおよび VSAN の [Logical Domains] ペインで [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。

保留中の変更の表示

Fabric Manager を使用して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および VSAN の [Logical Domains] ペインで、[Fabricxx] > [VSANxx] > [Domain Manager] > [Allowed] の順に展開します。

[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

Fabric Manager を使用して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　[Fabricxx] > [VSANxx] > [Domain Manager] の順に展開し、許可ドメイン ID リストを設定するファブリックおよび VSAN の [Logical Domains] ペインで [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。

連続ドメイン ID 割り当ての概要

連続ドメイン割り当てはデフォルトで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。

- 連続ドメイン割り当てが主要スイッチでイネーブルになっている場合、主要スイッチは連続ドメインを特定して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。
- 連続ドメイン割り当てが主要スイッチでディセーブルになっている場合、主要スイッチは使用可能ドメインを下位スイッチに割り当てます。

連続ドメイン ID 割り当てのイネーブル化

Fabric Manager を使用して特定の VSAN（またはある範囲の VSAN）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　[Fabric***xx***] > [VSAN***xx***] と展開し、連続ドメインをイネーブルにするファブリックおよび VSAN の [Logical Domains] ペインで [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

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 機能はイネーブルになっています。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、リブートすると失われます。
- スイッチは、最善の方法でバインディング FC ID を WWN に保持するように設計されています。たとえば 1 つの N ポートがスイッチから切断し、別のデバイスがその FC ID を要求した場合、この要求は許可され、最初に FC ID に関連していた WWN が解放されます。

- 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が 4000 個まで保存されます。このキャッシュがフルになると、新しい（最新）エントリによってキャッシュの最も古いエントリが上書きされます。この場合、最も古いエントリに対応する WWN と FC ID の関連は失われます。
- スイッチ接続動作は、N ポートと NL ポートで異なります。
  - スイッチが同一 VSAN に属する限り、切断してから同一スイッチ内の任意のポートに再接続した場合、N ポートに同一の 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。

ここでは、FC ID の設定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。

固定的 FC ID の概要

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）がポート インターフェイスに接続された後でスイッチが学習したダイナミック エントリをデータベースに自動的に入力します。

（注）　AIX または HP-UX ホストからスイッチに接続している場合は、これらのホストを接続している VSAN 内で固定的な FC ID 機能をイネーブルにしてください。

（注）　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。

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で移動でき、引き続き同一の固定的 FC ID を維持できます。

（注）　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。

（注）　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。

固定的 FC ID 機能のイネーブル化

Fabric Manager を使用して固定的 FC ID 機能をイネーブルするには、次の手順を実行します。

ステップ 1　[Fabricxx] > [VSANxx] の順に展開し、固定的 FC ID 機能をイネーブルにするファブリックおよび VSAN の [Logical Domains] ペインで [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 設定の概要

固定的 FC ID 機能をイネーブルにしたら、固定的 FC ID サブモードを開始し、スタティック エントリまたはダイナミック エントリを FC ID データベースに追加できます。デフォルトの場合、すべての追加エントリはスタティックになります。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 で固定的 FC ID 機能をイネーブルにしてください。
- 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 のランタイム ドメイン ID と同じであることを確認してください。ソフトウェアがドメインの不一致を検出すると、コマンドは拒否されます。
- 領域の設定時には、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。

固定的 FC ID の設定

Fabric Manager を使用して固定的 FC ID を設定するには、次の手順を実行します。

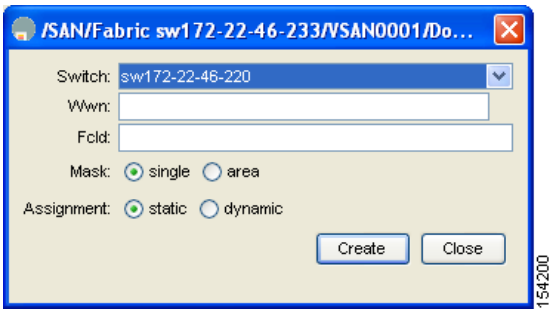
ステップ 1　[Fabric***xx***] > [VSAN***xx***] の順に展開し、固定的 FC ID リストを設定するファブリックおよび VSAN の [Logical Domains] ペインで [Domain Manager] を選択します。

[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。

図 9-14 に示す [Create Persistent FC ID] ダイアログボックスが表示されます。

図 9-14　[Create Persistent FC ID] ダイアログボックス



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 の概要

（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、このセクションを読んでください。

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 ポートの FC ID が 0x6f7704 である場合、このポートのエリアは 77 です。この場合、HBA ポートのエリアは 77 以外にすることができます。HBA ポートの FC ID は手動で設定し、ストレージ ポートの FC ID とは別にする必要があります。

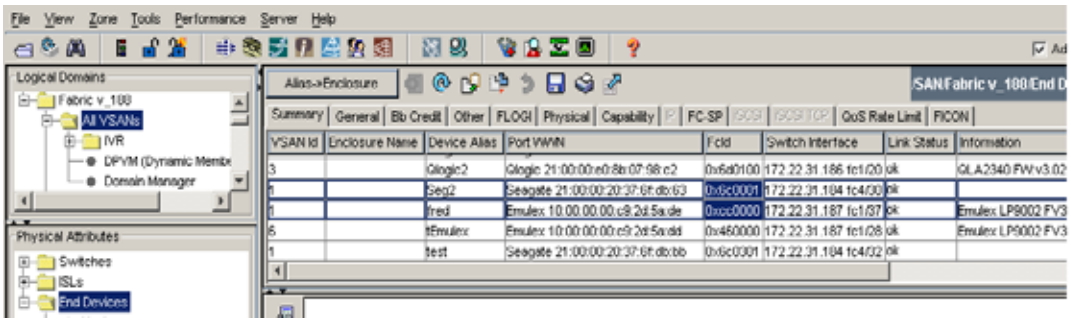
Cisco MDS 9000 ファミリのスイッチでは、FC ID の固定化機能により、この要件への準拠が容易になります。この機能を使用し、ストレージ ポートまたは HBA ポートのいずれかに、エリアが異なる FC ID を事前に割り当てることができます。この例の手順では、スイッチ ドメイン 111（16 進法では 6f）を使用しています。HBA ポートはインターフェイス fc1/9 に、ストレージ ポートは同じスイッチのインターフェイス 1/10 に接続します。

HBA の固有エリア FC ID の設定

Fabric Manager を使用して 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] ペインの [End Device] を展開し、[Information] ペインの [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（図 9-15 を参照）。

図 9-15　Fabric Manager の FLOGI データベース情報



（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　[Switches] > [Interfaces] の順に展開し、[Physical Attributes] ペインで [FC Physical] を選択します。

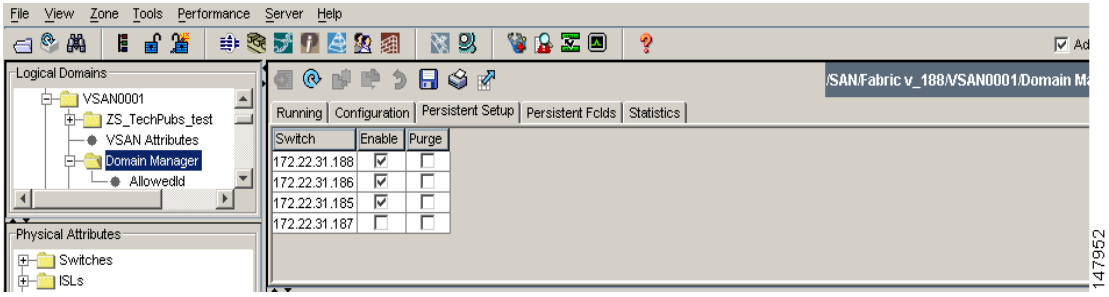
ステップ 3　HBA が接続されているインターフェイスで、[Status Admin] ドロップダウン メニューを [down] に設定します。

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　[Fabricxx] > [VSANxx] の順に展開し、[Domain Manager] を選択します。

ステップ 5　[Information] ペインの [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（図 9-16 を参照）。

図 9-16　Fabric Manager の固定的 FC ID 情報



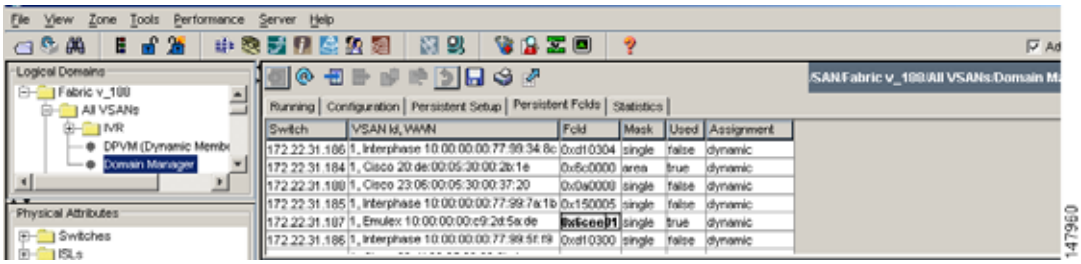
この機能がディセーブルである場合は、この手順を続けて固定的 FC ID をイネーブルにします。

この機能がすでにイネーブルになっている場合は、ステップ 7 に進みます。

ステップ 6　Cisco MDS スイッチで固定的 FC ID 機能をイネーブルにするには、[Enable] チェックボックスをオンにします（図 9-17 を参照）。

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 に置き換えました（図 9-17 を参照）。

図 9-17　Fabric Manager での FC ID の設定



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）　両方の FC ID でエリア割り当てが異なっています。

ステップ 10　[Switches] > [Interfaces] の順に展開し、[Physical Attributes] ペインで [FC 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 の選択消去の概要

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 エントリと FC ID は削除できません。表 9-1 は、固定的 FC ID の消去時に削除される FC ID エントリと維持される FC ID エントリを示しています。

表 9-1　消去される FC ID

固定的 FC ID の状態	固定使用状態	処理
スタティック	使用中	削除されない
スタティック	未使用	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	未使用	削除される

固定的 FC ID の消去

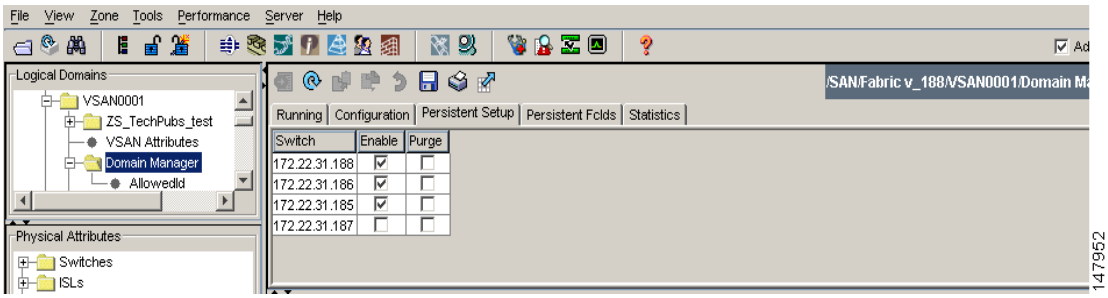
Fabric Manager を使用して固定的 FC ID を削除するには、次の手順を実行します。

ステップ 1　固定的 FC ID を消去するファブリックの [Logical Domains] ペインで、[Fabricxx] > [All VSANs] > [Domain Manager] の順に展開します。[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。

図 9-18 のように、[Information] ペインに固定的 FC ID 設定が表示されます。

図 9-18　Fabric Manager の固定的 FC ID 情報



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（図 9-18 を参照）。

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。

fcdomain の統計情報の表示

Fabric Manager は fcdomain の統計情報を収集し、[Information] ペインに表示します。

Fabric Manager を使用して fcdomain 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　[Fabricxx] > [All VSANs] の順に展開し、統計情報を表示するファブリックの [Logical Domains] ペインで [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。

デフォルト設定

表 9-2 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 9-2　デフォルトの 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
自動再構成オプション	ディセーブル
連続割り当てオプション	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 拒否	ディセーブル

表 9-2　デフォルトの fcdomain パラメータ （続き）

パラメータ	デフォルト
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

CHAPTER 10

SPAN によるネットワーク トラフィックのモニタリング

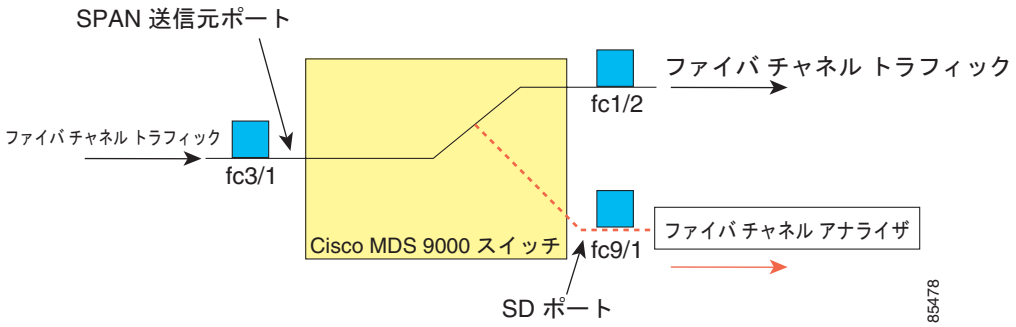
この章では、Cisco MDS 9000 ファミリ スイッチに提供される Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）機能について説明します。この章の内容は、次のとおりです。

SPAN の概要

SPAN 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 トラフィックを監視します。すべてのファイバ チャネル インターフェイスを通過するトラフィックは、SPAN Destination ポート（SD ポート）と呼ぶ特殊なポートに複製されます。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 モードのインターフェイスは、通常のデータ トラフィック用に使用できません。ファイバ チャネル アナライザを SD ポートにアタッチして、SPAN トラフィックを監視できます。

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がなく、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も影響しません（図 10-1 を参照）。

図 10-1　SPAN の伝送

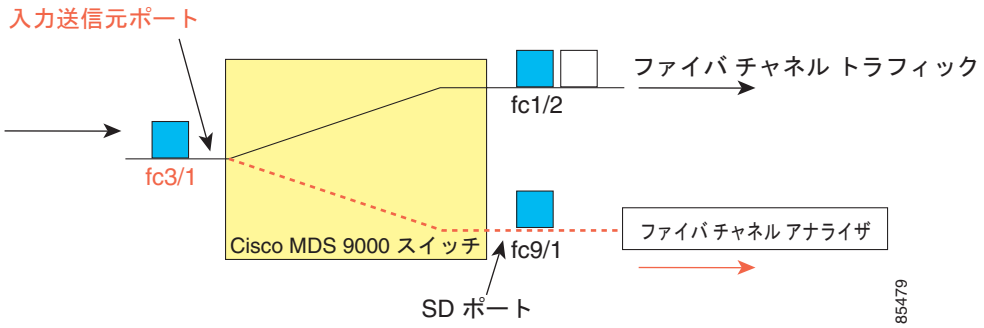


SPAN 送信元

SPAN 送信元とは、トラフィックの監視を開始するインターフェイスです。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。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。

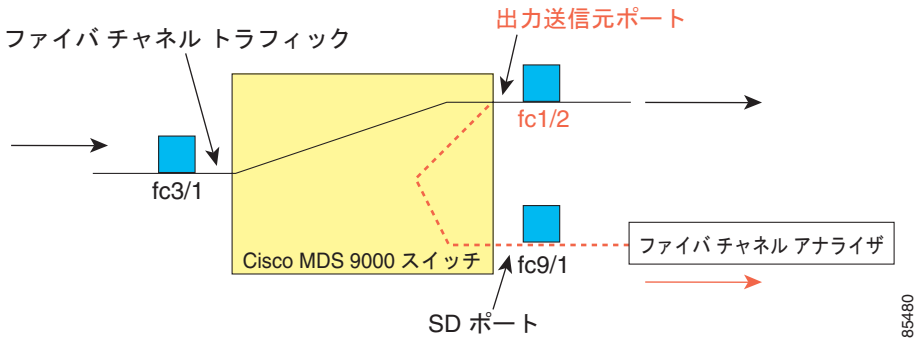
- 入力送信元（Rx）：この送信元インターフェイスを介してスイッチ ファブリックに入るトラフィックは、SD ポートにスパン（コピー）されます（図 10-2 を参照）。

図 10-2　入力方向からの SPAN トラフィック



- 入力送信元（Tx）：この送信元インターフェイスを介してスイッチ ファブリックから送信されるトラフィックは、SD ポートにスパン（コピー）されます（図 10-3 を参照）。

図 10-3　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。
- PortChannel
  - 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

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。

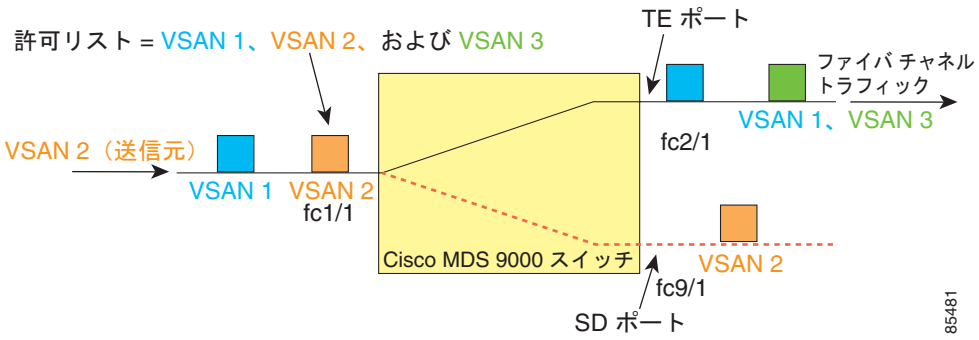
同じ SPAN セッション内では、送信元インターフェイス（物理インターフェイス、PortChannel、または sup-fc インターフェイス）と送信元 VSAN を設定できません。

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 10-4 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 10-4　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。

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監視できます。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 10-4 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。

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、トラフィックを監視できるのは、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。

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。

SPAN を設定する場合の注意事項

SPAN を設定する場合は、次の注意事項が適用されます。

- 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 の設定

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 トラフィックを監視します。

SPAN の設定

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。

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。

（注）　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。

（注）　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 コピーは廃棄されます。SPAN 廃棄を避けるため、max-queued-packets を、100 などの大きい値に設定します。

SPAN セッションの作成

Device Manager を使用して SPAN 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。

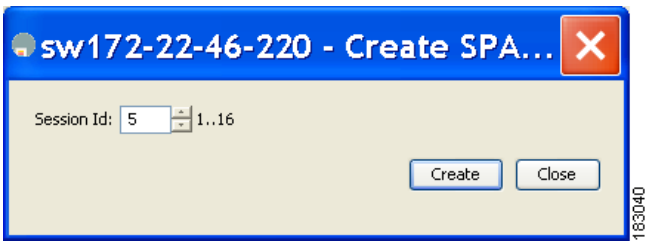
ステップ 1　[Interface] > [SPAN] を選択します。[SPAN] ダイアログボックスが表示されます。

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（図 10-5 を参照）。

図 10-5　[Create SPAN Sessions] ダイアログボックス



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。

SPAN 送信元の編集

Device Manager を使用して SPAN 送信元を編集するには、次の手順を実行します。

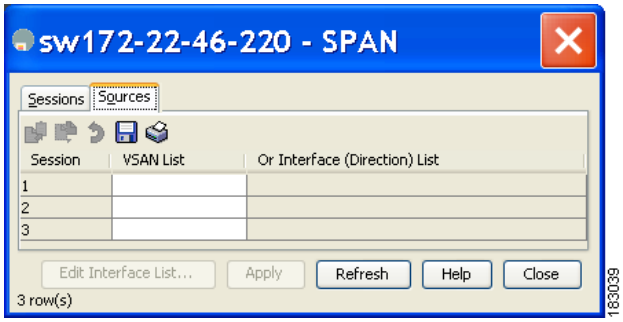
ステップ 1　[Interface] > [SPAN] を選択します。

[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。

図 10-6 のようなダイアログボックスが表示されます。

図 10-6　[SPAN Sources] タブ



ステップ 3　[VSAN List] フィールドに VSAN リスト名を入力します。

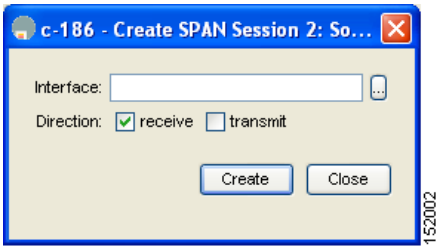
ステップ 4　[Edit Interface List] をクリックします。

[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（図 10-7 を参照）。

図 10-7　[Source Interfaces Interface Sources] ダイアログボックス



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

Device Manager を使用して 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 変換動作

（古い任意のリリースで設定された）SPAN 機能は次のように変換されます。

- 指定されたセッションにおいて送信元インターフェイスおよび送信元 VSAN が設定されている場合は、このセッションからすべての送信元 VSAN が削除されます。

  例：Cisco MDS SAN-OS Release 1.0(4) よりも古いリリース

```
Session 1 (active)
   Destination is fc1/9
   No session filters configured
   Ingress (rx) sources are
      vsans 10-11
     fc1/3,
   Egress (tx) sources are
     fc1/3,
```

  Cisco MDS SAN-OS Release 1.1(1) にアップグレードした後

```
Session 1 (active)
   Destination is fc1/9
   No session filters configured
   Ingress (rx) sources are
     fc1/3,
   Egress (tx) sources are
     fc1/3,
```

アップグレード前は、セッション 1 に送信元インターフェイスと送信元 VSAN が両方とも設定されていました。アップグレード後は、送信元 VSAN が削除されました（法則 1）。

- 送信元インターフェイスにインターフェイス レベルの VSAN フィルタが設定されている場合、送信元インターフェイスもセッションから削除されます。このインターフェイスが双方向に設定されている場合、このインターフェイスは双方向で削除されます。

  例：Cisco MDS SAN-OS Release 1.0(4) よりも古いリリース

```
Session 2 (active)
   Destination is fc1/9
   No session filters configured
   Ingress (rx) sources are
      vsans 12
     fc1/6 (vsan 1-20),
   Egress (tx) sources are
     fc1/6 (vsan 1-20),
```

  Cisco MDS SAN-OS Release 1.1(1) にアップグレードした後

```
Session 2 (inactive as no active sources)
   Destination is fc1/9
   No session filters configured
   No ingress (rx) sources
   No egress (tx) sources
```

（注）　スイッチオーバーまたは新しいスタートアップ コンフィギュレーションを実装すると、推奨されない設定が固定メモリから削除されます。

  セッション 2 には、送信元 VSAN 12 と送信元インターフェイス fc1/6、および Cisco MDS SAN-OS Release 1.0(4) で指定された VSAN フィルタが設定されていました。Cisco MDS SAN-OS Release 1.1(1) にアップグレードすると、次のように変更されます。

  - 送信元 VSAN（VSAN 12）が削除されます（法則 1）。
  - 送信元インターフェイス fc1/6 には VSAN フィルタが指定されていましたが、これも削除されます（法則 2）。

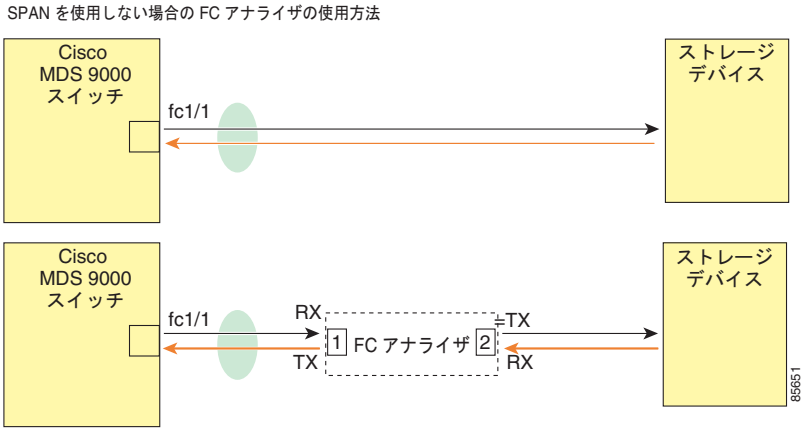
ファイバ チャネル アナライザによるトラフィックのモニタリング

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監視できます。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。

SPAN を使用しない場合

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、トラフィックを監視できます。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 10-8 を参照）。

図 10-8　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。

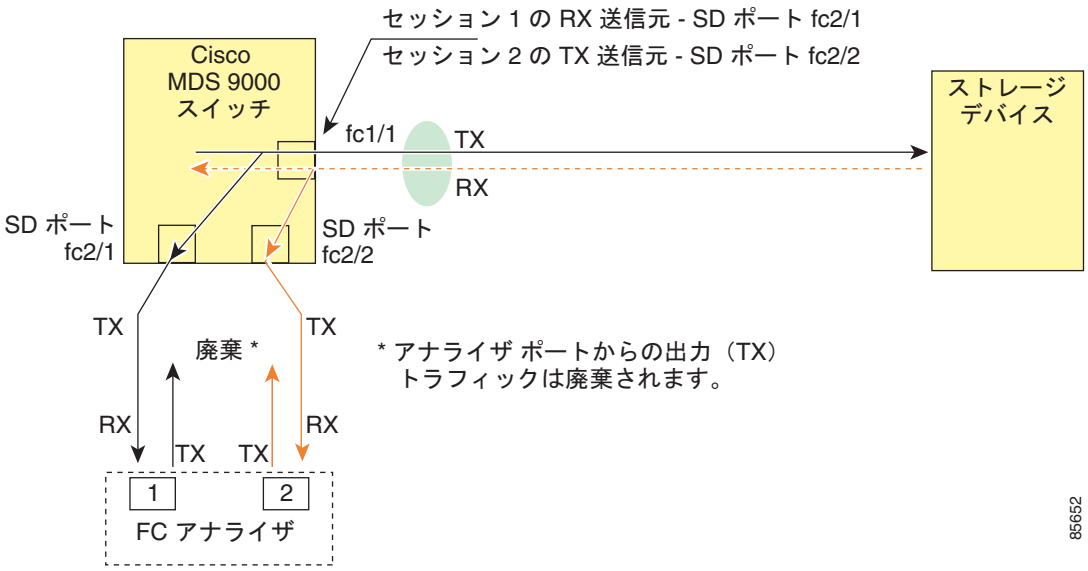
- 2 つのネットワーク デバイス間にファイバ チャネル アナライザを物理的に挿入する必要があります。
- ファイバ チャネル アナライザが物理的に接続されている場合は、トラフィックが中断されます。
- アナライザはポート 1 およびポート 2 の Rx リンクのデータだけをキャプチャします。ポート 1 はインターフェイス fc1/1 からの出力トラフィックを、ポート 2 はインターフェイス fc1/1 への入力トラフィックをキャプチャします。

SPAN を使用する場合

SPAN を使用すると、トラフィックを中断しなくても、図 10-8 と同じトラフィックをキャプチャすることができます。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監視したり、SD ポート fc2/1 の出力トラフィックを監視することができます。このトラフィックは、ファイバ チャネル アナライザでシームレスにキャプチャされます（図 10-9 を参照）。

図 10-9　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



SPAN を使用したファイバ チャネル アナライザの設定

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 10-9 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。

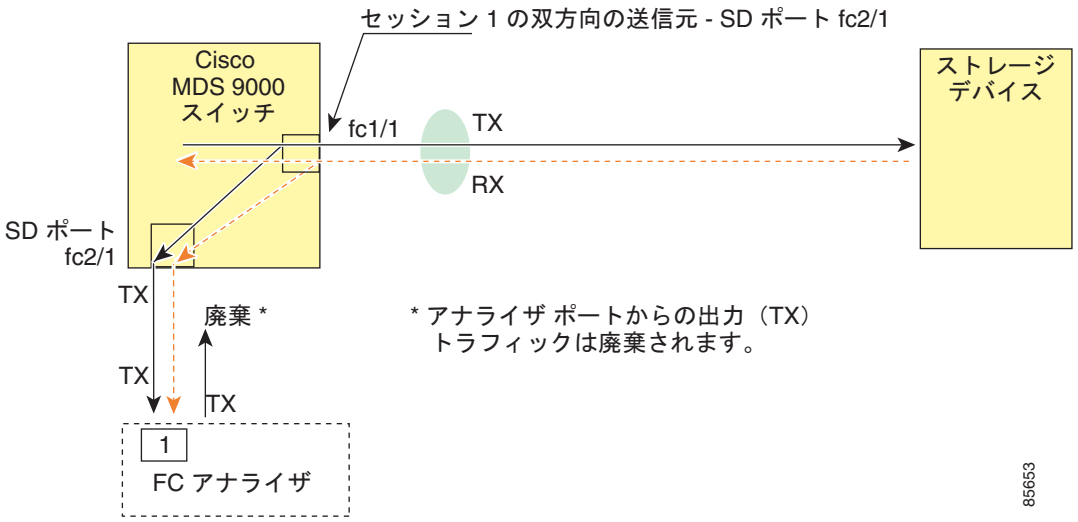
ステップ 4　ファイバ チャネル アナライザのポート 2 に fc2/2 を物理的に接続します。

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監視する場合、SD ポートを 2 つ使用する必要はありません（図 10-9 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監視することにより、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 10-10 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。この設定では 2 ポートアナライザのポートをすべて使用せずに、SD ポートおよびアナライザのポートを 1 つずつ使用するため、図 10-9 の設定よりも便利かつ低コストです。

図 10-10　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。

SPAN のデフォルト設定値

表 10-1 に、SPAN パラメータのデフォルト設定値を示します。

表 10-1　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。

CHAPTER 11

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。この章の内容は、次のとおりです。

FCS の概要

Fabric Configuration Server（FCS）を使用すると、トポロジ アトリビュートを検出したり、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 つ以上の 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することができます。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、それぞれ独自の一連のアトリビュートと値があります。一部のアトリビュートにはヌル値も定義できます。

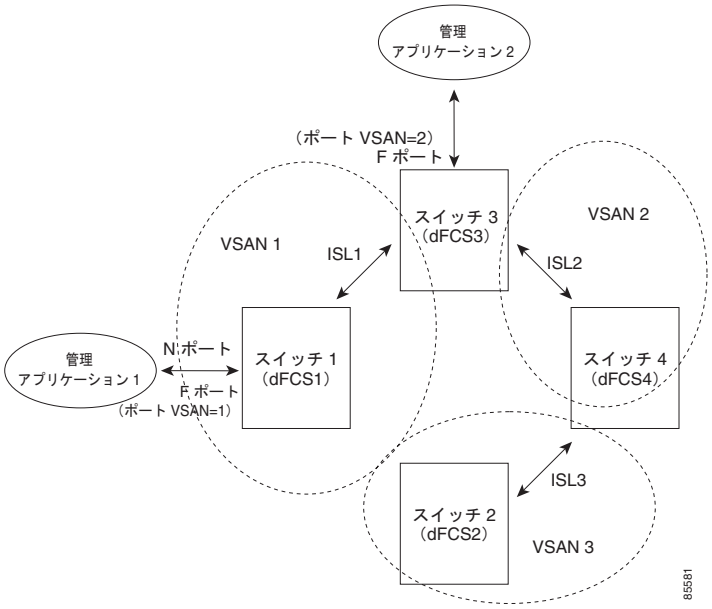
Cisco MDS 9000 ファミリ スイッチ環境では、複数の VSAN がファブリックを構成し、VSAN ごとに 1 つの FCS インスタンスが存在します。

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、Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）または Command Line Interface（CLI; コマンドライン インターフェイス）を使用して取得できます。

図 11-1 で、Management Application 1（M1）はポート VSAN ID が 1 の F ポートを介して接続され、Management Application 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だけで動作します。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 11-1　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することができます。
  - SNMP Manager は FCS MIB（管理情報ベース）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、取得することができます。
- 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。

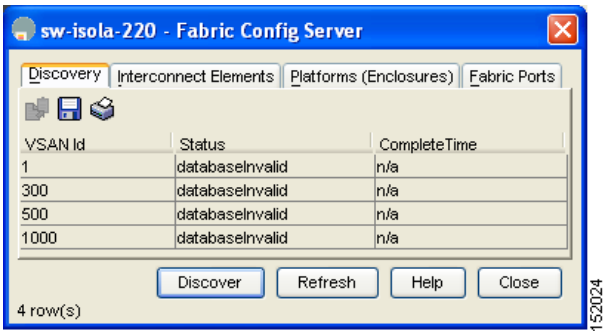
FCS 検出情報の表示

Device Manager を使用して 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（図 11-2 を参照）。

図 11-2　[Fabric Config Server] ダイアログボックス



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

Device Manager を使用して FCS Interconnect Element 情報を表示するには、次の手順を実行します。

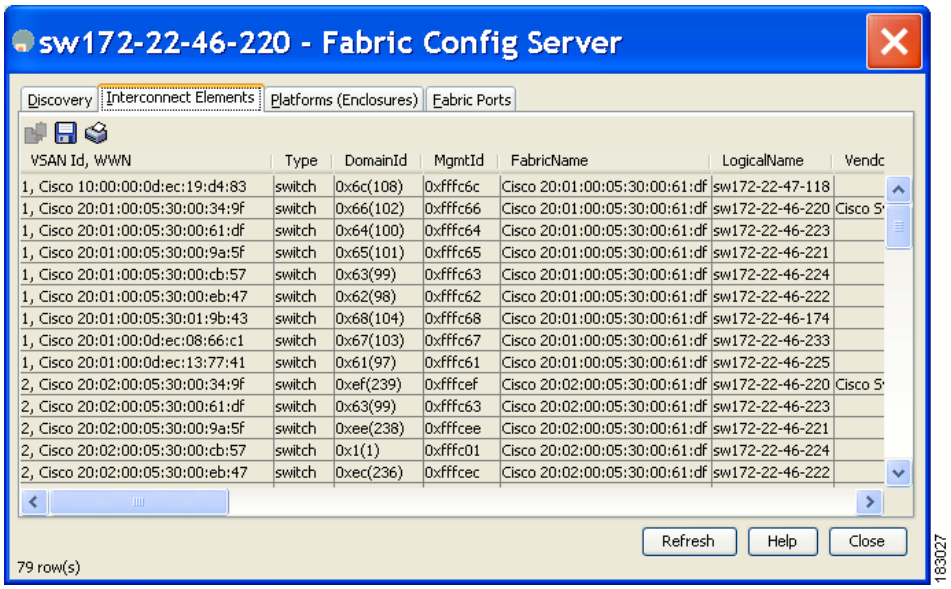
ステップ 1　[FC] > [Advanced] > [Fabric Config Server] を選択します。

[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。

図 11-3 のようなダイアログボックスが表示されます。

図 11-3　FCS の [Interconnect Elements] タブ



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 プラットフォームの作成

Device Manager を使用して 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。

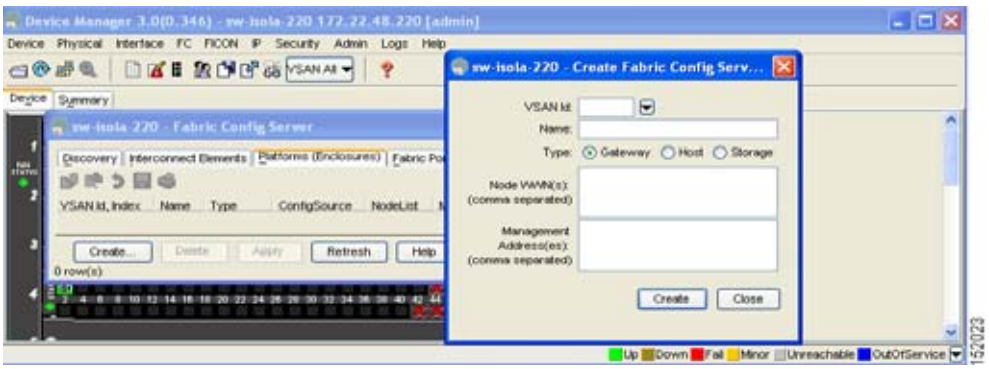
[Fabric Config Server] ダイアログボックスが表示されます。

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（図 11-4 を参照）。

図 11-4　[Create Fabric Config Server] ダイアログボックス



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 Fabric Port の表示

Device Manager を使用して FCS 検出情報を表示するには、次の手順を実行します。

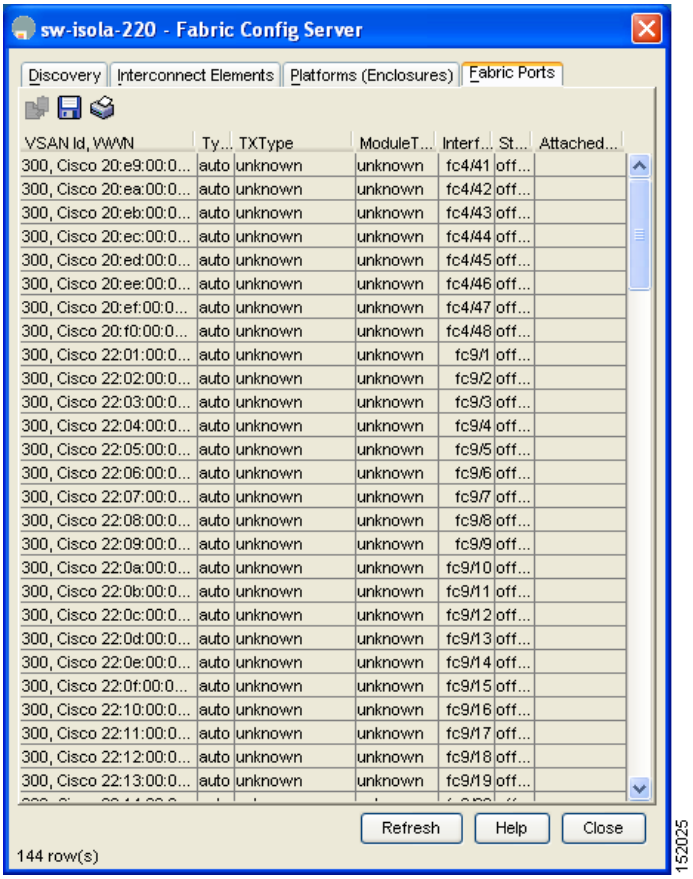
ステップ 1　[FC] > [Advanced] > [Fabric Config Server] を選択します。

[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（図 11-5 を参照）。

図 11-5　FCS の [Fabric Ports] タブ



ステップ 3　[Refresh] をクリックして表示内容を更新します。

デフォルト設定

表 11-1 に FCS のデフォルト設定値を示します。

表 11-1　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の種類	不明

INDEX

数字

A

C

D

E

F

H

I

N

O

P

Q

R

S

T

V

か

け

こ

さ

し

す

そ

て

と

な

ふ

ほ

ま

も

ゆ

る

れ

ろ