# Cisco MDS 9000 シリーズ NX-OS システム管理設定ガイド

**初版**：2017 年 5 月 5 日

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

# 目 次

# はじめに

ここでは、『Cisco MDS 9000 Series Configuration Guideを使用している対象読者、構成、および表記法について説明します。また、関連資料の入手方法の情報を説明し、次の章にも続きます。



## 対象読者

このインストレーション ガイドは、電子回路および配線手順に関する知識を持つ電子または電気機器の技術者を対象にしています。

## 表記法

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に記載されていない参照資料を紹介しています。

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。

警告は、次のように表しています。

警告 「危険」の意味です。人身事故を予防するための注意事項が記述されています。機器の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止対策に留意してください。Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. ステートメント 1071。

# 関連資料

Cisco MDS 9000 シリーズ スイッチのドキュメンテーションには、次のマニュアルが含まれます。

**Release Notes**

http://www.cisco.com/c/en/us/support/storage-networking/mds-9000-nx-os-san-os-software/products-release-notes-list.html

**『Regulatory Compliance and Safety Information』**

http://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/hw/regulatory/compliance/RCSI.html

**互換性に関する情報**

http://www.cisco.com/c/en/us/support/storage-networking/mds-9000-nx-os-san-os-software/products-device-support-tables-list.html

**インストールおよびアップグレード**

http://www.cisco.com/c/en/us/support/storage-networking/mds-9000-nx-os-san-os-software/products-installation-guides-list.html

**Configuration**

http://www.cisco.com/c/en/us/support/storage-networking/mds-9000-nx-os-san-os-software/products-installation-and-configuration-guides-list.html

**CLI**

http://www.cisco.com/c/en/us/support/storage-networking/mds-9000-nx-os-san-os-software/products-command-reference-list.html

**トラブルシューティングおよび参考資料**

http://www.cisco.com/c/en/us/support/storage-networking/mds-9000-nx-os-san-os-software/tsd-products-support-troubleshoot-and-alerts.html

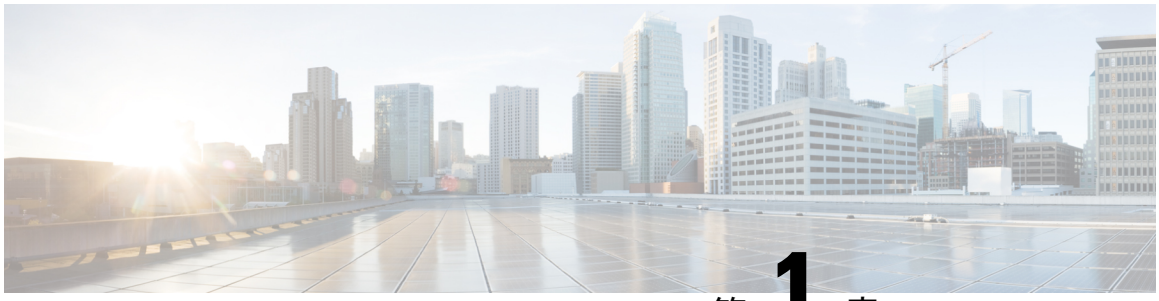
オンラインでドキュメントを検索するには、次の Web サイトにある Cisco MDS NX-OS Documentation Locator を使用してください。

http://www.cisco.com/c/en/us/td/docs/storage/san_switches/mds9000/roadmaps/doclocater.html

# マニュアルの入手方法およびテクニカル サポート

ドキュメントの入手、Cisco Bug Search Tool（BST）の使用、サービス要求の送信、追加情報の収集の詳細については、『What's New in Cisco Product Documentation』を参照してください。

新しく作成された、または改訂されたシスコのテクニカル コンテンツをお手元で直接受け取るには、『What's New in Cisco Product Documentation』RSS フィードをご購読ください。RSS フィードは無料のサービスです。



第 1 章

# システム管理の概要

You can use the system management features to monitor and manage a switch using Cisco MDS NX-OS software. 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。



## Cisco Fabric Services

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。

For information on configuring CFS, see CFS インフラストラクチャの使用 （5 ページ）.

## システム メッセージ

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

For information about configuring system messages, see システム メッセージ ロギングの設定 （29 ページ）.

# Call Home

Call Home は、重要なシステム イベントを E メールで通知します。ポケットベル サービス、通常の電子メール、または XML ベースの自動解析アプリケーションとの適切な互換性のために、さまざまなメッセージの形式が使用できます。この機能の一般的な用途としては、ネットワーク サポート技術者を直接ポケットベルで呼び出したり、ネットワーク オペレーション センター（NOC）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 設定の詳細については、 を参照してください。

# Scheduler

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については、「メンテナンス ジョブのスケジューリング （123 ページ）」を参照してください。

# システム プロセスとログ

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

スイッチの健全性のモニタリングに関する詳細は、システム プロセスとログのモニタリング （137 ページ） を参照してください。

# 組み込まれている Event Manager

Embedded Event Manager（EEM）はデバイス上で発生するイベントをモニタし、設定に基づいて各イベントの回復またはトラブルシューティングのためのアクションを実行します。EEM は次の 3 種類の主要コンポーネントからなります。

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

EEM の設定に関する詳細は、Embedded Event Manager の設定 （173 ページ） を参照してください。

# SNMP

簡易ネットワーク管理プロトコル（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層プロトコルです。すべての Cisco MDS 9000 ファミリ スイッチで、SNMPv1、SNMPv2c、および SNMPv3 の 3 つの SNMP バージョンが使用できます。CLI と SNMP は、Cisco MDS 9000 ファミリのすべてのスイッチで共通のロールを使用します。SNMP を使用して CLI で作成したロールを変更したり、その逆を行うことができます。

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

SNMP の設定については、SNMP の設定 （249 ページ） を参照してください。

# RMON

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

RMON の設定の詳細についRMON の設定 （195 ページ）ては、を参照してください。

# ドメイン パラメータ

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

ファイバ チャネル ドメイン機能の設定に関する詳細については、ドメイン パラメータの設定 （277 ページ） を参照してください。

# SPAN

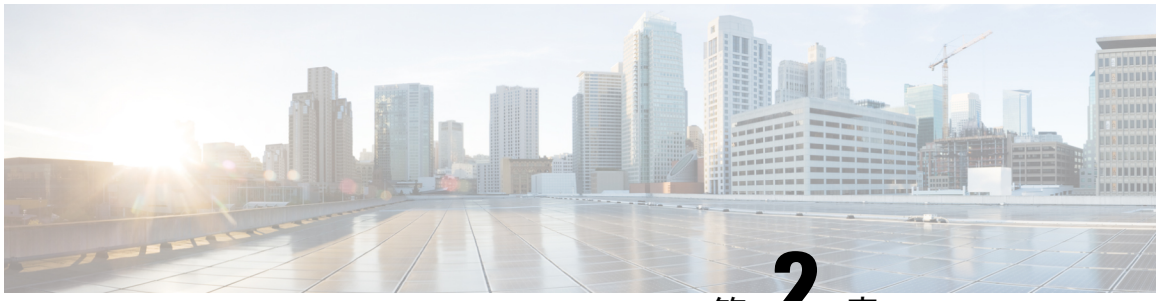
スイッチドポート アナライザ（SPAN）機能は、Cisco MDS 9000 ファミリのスイッチ専用の機能です。SPAN は、ファイバ チャネル インターフェイスを通じてネットワーク トラフィックをモニタします。任意のファイバ チャネル インターフェイスを通るトラフィックは、SPAN 宛先ポート（SD ポート）という専用ポートに複製することができます。スイッチの任意のファイバ チャネル ポートを SD ポートとして設定できます。SD ポート モードに設定したインターフェイスは、標準データ トラフィックには使用できません。ファイバ チャネル アナライザを SD ポートに接続して、SPAN トラフ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

SPAN 機能に関する詳細は、SPAN を使用したネットワーク トラフィックのモニタリング （309 ページ） を参照してください。

# Fabric Configuration Server

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

FCS の設定の詳細については、Fabric Configuration Server の設定 （351 ページ）を参照してください。



第 2 章

# CFS インフラストラクチャの使用

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



## CFS について

Cisco MDS NX-OS ソフトウェアは Cisco Fabric Services（CFS）インフラストラクチャを使用して、効率的なデータベース配信を実現し、デバイスの柔軟性を高めます。ファブリック内のすべてのスイッチに設定情報を自動的に配信できるため、SAN プロビジョニングが簡単になります。

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

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

# CFS を使用した Cisco MDS NX-OS 機能

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

- N ポート バーチャライゼーション
- FlexAttach 仮想 pWWN
- NTP
- ダイナミック ポート VLAN メンバーシップ
- 分散デバイス エイリアス サービス
- 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
- 使用可能なドメイン ID リスト
- RSCN タイマー
- iSLB

# CFS の機能

CFS には次の機能があります。

- CFS レイヤでクライアント/サーバ関係を持たないピアツーピア プロトコル
- 3 つの配信スコープ
  - 論理スコープ：配信は、VSAN のスコープ内で発生します。
  - 物理スコープ：配信は、物理トポロジ全体におよびます。
  - 選択した VSAN セットを超える場合：Inter-VSAN Routing（IVR）などの一部のアプリケーションは、一部の特定の VSAN を超えた設定の配信を必要とします。これらのアプリケーションは、配信を制限する VSAN セットを CFS に指定できます。
- 3 つの配信モード
  - 協調型配信：ファブリック内で同時に 1 つの配信だけが許可されます。
  - 非協調型配信：協調型配信が進行中である場合を除いて、ファブリック内で複数の同時配信を実行できます。

- 無制限の非協調型配信：既存の協調型配信がある場合でも、ファブリック内で複数の同時配信が許可されます。無制限の非協調型配信は、他のすべての配信タイプの配信と同時に実行できます。

- ファブリック マージ イベント中（2 つの独立したファブリックのマージ中）に、アプリケーション設定のマージを実行するマージ プロトコルをサポートします。

# アプリケーションの CFS のイネーブル化

すべての CFS ベースのアプリケーションでは、配信機能をイネーブルまたはディセーブルにできます。Cisco SAN-OS Release 2.0(1b) よりも前に存在していた機能では、配信機能がデフォルトでディセーブルになっており、配信機能を明示的にイネーブルにする必要がありました。

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

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

# CFS プロトコル

CFS 機能は、下位層の転送には依存しません。現在、Cisco MDS スイッチでは、CFS プロトコル レイヤはファイバ チャネル 2（FC2）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 配信の範囲

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

- VSAN レベル（論理スコープ）

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

- 物理トポロジ レベル（物理スコープ）

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

- 選択されたスイッチ間

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

# CFS の配信モード

CFS は、さまざまなアプリケーション要件をサポートするため、協調型配信と非協調型配信の、2 種類の配信モードをサポートしています。2 つのモードは相互に排他的です。常に 1 つのモードだけを適用できます。

## 非協調型配信

非協調型配信は、ピアからの情報と競合させたくない情報を配信する場合に使用されます。例としては、iSNS などのローカル デバイス登録が挙げられます。1 つのアプリケーションで、複数の非協調型配信が可能です。

## 協調型配信

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

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

協調型配信には、次の 2 種類があります。

- CFS によるもの：アプリケーションが介在することなく、アプリケーション要求に応じて CFS が各段階を実行します。
- アプリケーションによるもの：各段階がアプリケーションによって完全に管理されます。

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

## 無制限の非協調型配信

無制限の非協調型配信では、既存の協調型配信がある場合でも、ファブリック内で複数の同時配信が許可されます。無制限の非協調型配信は、他のすべての配信タイプの配信と同時に実行できます。

# 混合ファブリック内での CFS の接続性

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

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

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

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

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

# ファブリックのロック

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

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

ステータスをロック CFS の確認のについてを参照してください CFS ロック ステータスの確認（25 ページ）。

# 変更のコミット

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

一般に、コミット機能はセッションを開始しません。セッションを開始するのは、ロック機能だけです。ただし、設定変更がこれまでに行われていなければ、空のコミットが可能です。この場合、コミット操作の結果として、ロックを取得し、現在のデータベースを配信するセッションが行われます。

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

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

（注） Once the **feature commit** is done the running configuration has been modified on all switches participating in the feature's distribution. You can then use the **copy running-config startup-config fabric** command to save the running-config to the startup-config on all the switches in the fabric.

# CFS 結合のサポート

アプリケーションは CFS を通して、設定をファブリック内で継続的に同期します。このような 2 つのファブリック間で ISL を起動すると、これらのファブリックがマージされることがあります。これらの 2 つのファブリック内の設定情報セットが異なっている時は、マージイベント中に調停する必要があります。CFS は、アプリケーション ピアがオンラインになるたびに通知を送信します。M 個のアプリケーション ピアがあるファブリックが N 個アプリケーション ピアがある別のファブリックとマージし、アプリケーションが通知のたびにマージ動作を行う場合は、リンク アップ イベントによりファブリック内で M*N 回のマージがトリガーされます。

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

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

マージに成功した場合、マージしたデータベースは結合ファブリック内のすべてのスイッチに配信され、新規ファブリック全体が一貫したステートになります。

# IP を介した CFS 配信

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

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

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

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

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

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

図 1 : ファイバ チャネル接続と IP 接続を使用するネットワーク例 1 （12 ページ） に、ファイバ チャネル接続と IP 接続の両方を持つネットワークを示します。ノード A はファイバ チャネルを介してノード B にイベントを転送します。ノード B はユニキャスト IP を使用してノード C とノード D にイベントを転送します。ノード C はファイバ チャネルを介してノード E にイベントを転送します。

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

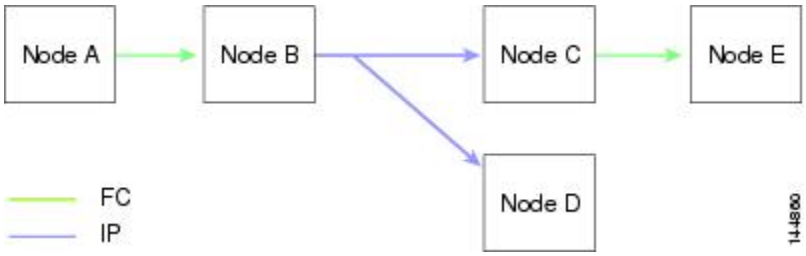



図 2 : ファイバ チャネル接続と IP 接続を使用するネットワーク例 2 （12 ページ） は、ノード D とノード E がファイバ チャネルを使用して接続されていることを除き、図 1 : ファイバ チャネル接続と IP 接続を使用するネットワーク例 1 （12 ページ） と同じです。ノード B にはノード C とノード D の IP 用配信リストがあるので、この例のすべてのプロセスは同じです。ノード D はすでにノード B からの配信リストに入っているため、ノード C はノード D に転送しません。

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

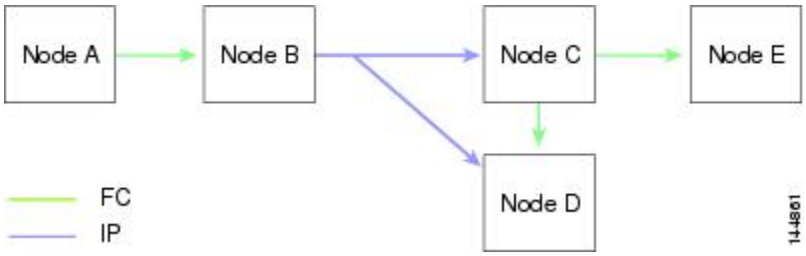
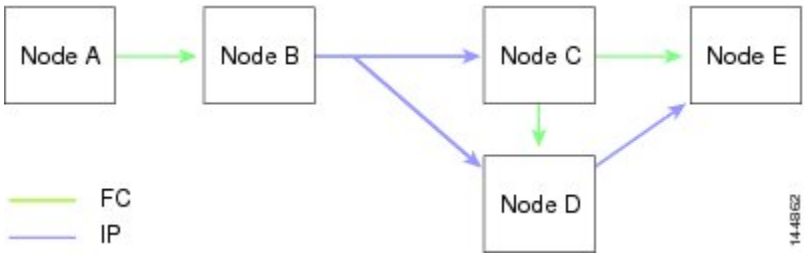



図 3 : ファイバ チャネル接続と IP 接続を使用するネットワーク例 3 （12 ページ） は、ノード D とノード E が IP を使用して接続されていることを除き、図 2 : ファイバ チャネル接続と IP 接続を使用するネットワーク例 2 （12 ページ） と同じです。ノード E はノード B からの配信リストに入っていないため、ノード C とノード D はイベントをノード E に転送します。

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




# CFS 向けスタティック IP ピア

IP を介した CFS は、スタティック IP のピアでも使用できます。この場合、IP マルチキャストを使用したダイナミック検索は無効で、CFS 配信が静的に設定されたピアでのみ実行されます。

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。

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。このようなデバイスは、CFS 向けにピアのスタティック IP を使用する利点があります。

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

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

# CFS リージョンの概要

CFS リージョンは、物理配信スコープにおける所定の機能またはアプリケーションに対するスイッチのユーザ定義のサブセットです。SAN が広い範囲におよぶ場合、物理プロキシミティに基づいてスイッチ セット間で特定のプロファイルの配信をローカライズまたは制限しなければならない場合があります。MDS SAN-OS Release 3.2.(1) よりも前のバージョンでは、SAN 内のアプリケーションの配信スコープは、物理ファブリック全体におよんでおり、ファブリック内の特定のスイッチのセットに配信を制限する機能はありませんでした。CFS リージョンの機能では、CFS リージョンを作成することでこの制限を克服できます。CFS リージョンは、CFS 機能またはアプリケーションに対する、ファブリック内の複数の配信アイランドです。CFS regions are designed to restrict the distribution of a feature's configuration to a specific set or grouping of switches in a fabric.

（注） CFS リージョンは、SAN 内の物理スイッチに対してだけ設定できます。CFS リージョンの設定は、VSAN では行えません。

**Example CFS Scenario**: Call Home is an application that triggers alerts to Network Administrators when a situation arises or something abnormal occurs. ファブリックが広い範囲におよび、ファブリック内のスイッチのサブセットを担当するネットワーク管理者が複数存在する場合、Call Home アプリケーションは、管理者のいる場所にかかわらずすべてのネットワーク管理者にアラートを送信します。Call Home アプリケーションは、メッセージ アラートを選択してネットワーク管理者に送信するために、CFS リージョンを実装してアプリケーションの物理スコープを調整するか絞り込む必要があります。

CFS リージョンは、0 ～ 200 の数字で識別されます。リージョン 0 はデフォルトのリージョンとして予約されており、ファブリック内のすべてのスイッチを含みます。1 ～ 200 のリージョ

ンを設定できます。デフォルト リージョンでは下位互換性を維持しています。リリース 3.2(1) よりも前の SAN-OS が動作するスイッチが同じファブリック上にある場合、これらのスイッチを同期化する際に、リージョン 0 の機能だけがサポートされます。これらのスイッチを同期化する際、他のリージョンの機能は無視されます。

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

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

# 注意事項と制約事項

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

CFS には、次の注意事項と制限事項があります。

- 暗黙的な CFS の使用：CFS 対応アプリケーションに CFS タスクを初めて発行した場合は、設定変更プロセスが開始し、アプリケーションによってファブリックがロックされます。
- 保留データベース：保留データベースはコミットされていない情報を保持する一時的なバッファです。データベースがファブリック内の他のスイッチのデータベースと同期するように、コミットされていない変更はすぐに適用されません。変更をコミットすると、保留データベースはコンフィギュレーション データベース（別名、アクティブ データベースまたは有効データベース）を上書きします。
- アプリケーション単位でイネーブル化またはディセーブル化される CFS 配信：CFS 配信ステートのデフォルト（イネーブルまたはディセーブル）は、アプリケーション間で異なります。CFS 配信がディセーブル化されたアプリケーションは、設定を配信せず、ファブリック内の他のスイッチからの配信も受信しません。
- 明示的な CFS コミット：大半のアプリケーションでは、新しいデータベースをファブリックに配信したりファブリック ロックを解放したりするために一時的なバッファ内の変更をアプリケーションデータベースにコピーする明示的なコミット動作が必要です。コミット操作を実行しないと、一時的バッファ内の変更は適用されません。

# デフォルト設定

表 1 : デフォルトの CFS パラメータ （15 ページ） に、CFS 設定のデフォルト設定値を示します。

表 *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 |
| CFS 向けスタティック IP ピア | ディセーブル |
| IPv4 マルチキャストアドレス | 239.255.70.83 |
| IPv6 マルチキャストアドレス | ff15:efff:4653 |

# CFS の設定

このセクションでは設定プロセスについて説明します。

## スイッチの CFS 配信のディセーブル化

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

物理接続を維持したまま、スイッチで IP を介した CFS を含む CFS をグローバルに無効化し、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。

（注） 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。

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

**手順**

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **no cfs distribute**

IP を介した CFS を含む、スイッチ上のすべてのアプリケーションの CFS 配信をグローバルにディセーブルにします。

**ステップ 3** switch(config)# **cfs distribute**

スイッチの CFS 配信をイネーブルにします（デフォルト）。

# 変更のコミット

You can commit changes for a specified feature by entering the **commit** command for that feature.

## 変更の破棄

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

You can discard changes for a specified feature by using the **abort** command for that feature.

## 設定の保存

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

⚠

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

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。

CFS のロックを消去するには、次の手順に従います。

**手順**

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **dpvm abort**

以前に設定ロックが取得されたスイッチから設定を中止します。このメソッドにより、ファブリック全体で CFS ロックを消去します。

ファブリック全体で DPVM アプリケーションの CFS ロックを消去します。

**ステップ 3** switch(config)# **clear dpvm session**

ファブリック内のすべてのスイッチからセッションを消去します。

DPVM アプリケーションの CFS ロックを消去します。

# IP を介した CFS のイネーブル化

## 有効化または ipv4 CFS を無効化

IPv4 を介した CFS 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。

**手順**

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **cfs ipv4 distribute**

スイッチのすべてのアプリケーションに対して IPv4 を介した CFS をグローバルでイネーブルにします。

**ステップ 3** switch(config)# **no cfs ipv4 distribute**

```
This will prevent CFS from distributing over IPv4 network.
Are you sure? (y/n) [n] y
```

スイッチの IPv4 を介した CFS をディセーブルにします（デフォルト）。

## 有効化または IPv6 Over CFS を無効化

IPv6 を介した CFS 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。

手順

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **cfs ipv6 distribute**

スイッチのすべてのアプリケーションに対して IPv6 を介した CFS をグローバルでイネーブルにします。

**ステップ 3** switch(config)# **no cfs ipv6 distribute**

スイッチの IPv6 を介した CFS をディセーブルにします（デフォルト）。

# IP を介した CFS の IP マルチキャスト アドレスの設定

同様のマルチキャスト アドレスを持つすべての CFS over IP 対応スイッチにより、1 つの CFS over IP ファブリックが構成されます。ネットワーク トポロジ変更を検出するためのキープアライブ メカニズムのような CFS プロトコル特有の配信は、IP マルチキャスト アドレスを使用して情報を送受信します。

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

IP を介した CFS の IPv4 または IPv6 どちらかのマルチキャスト アドレス値を設定できます。デフォルトの IPv4 マルチキャスト アドレスは 239.255.70.83 で、デフォルトの IPv6 マルチキャスト アドレスは ff15:efff:4653 です。

## IPv4 を介した CFS の IP マルチキャスト アドレスの設定

IPv4 を介した CFS の IP マルチキャスト アドレスを設定するには、次の手順を実行します。

手順

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **cfs ipv4 mcast-address 239.255.1.1**

```
Distribution over this IP type will be affected
Change multicast address for CFS-IP ?
```

IPv4 を介した CFS 配信の IPv4 マルチキャスト アドレスを設定します。有効な IPv4 アドレスの範囲は 239.255.0.0 ～ 239.255.255.255 および 239.192/16 ～ 239.251/16 です。

**ステップ 3** switch(config)# **no cfs ipv4 mcast-address 239.255.1.1**

**例**：

```
Distribution over this IP type will be affected
Change multicast address for CFS-IP ?Are you sure? (y/n)  [n] y
```

IPv4 を介した CFS 配信の デフォルトの IPv4 マルチキャスト アドレスに戻します。CFS のデフォルトの IPv4 マルチキャスト アドレスは 239.255.70.83 です。

## IPv6 を介した CFS の IP マルチキャスト アドレスの設定

To configure an IP multicast address for CFS over IPv6, follow these steps:

**手順**

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **cfs ipv6 mcast-address ff15::e244:4754**

```
Distribution over this IP type will be affected
Change multicast address for CFS-IP ?
Are you sure? (y/n)  [n] y
```

IPv6 を介した CFS 配信の IPv6 マルチキャスト アドレスを設定します。有効な IPv6 アドレスの範囲は ff15::/16（ff15::0000:0000 ～ ff15::ffff:ffff）および ff18::/16（ff18::0000:0000 ～ ff18::ffff:ffff）です。

**ステップ 3** switch(config)# **no cfs ipv6 mcast-address ff15::e244:4754**

```
Distribution over this IP type will be affected
Change multicast address for CFS-IP ?
Are you sure? (y/n)  [n] y
```

IPv6 を介した CFS 配信のデフォルトの IPv6 マルチキャスト アドレスに戻します。IP を介した CFS のデフォルトの IPv6 マルチキャスト アドレスは ff15::efff:4653 です。

# CFS 用静的 IP ピアの設定

IP を介した CFS のスタティック IP ピア アドレスを設定するには、これらの手順に従います。

### 手順

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **cfs static-peers**

```
WARNING: This mode will stop dynamic discovery and rely only on the static peers. For
this mode to be in effect, at least one static peer will need to be configured.
Do you wish to continue? (y/n)  [n] y
```

switch(config-cfs-static)#

CFS スタティック ピア モードを開始して、マルチキャスト転送を使用してピアのダイナミック検索を無効にします。これを有効にするには、少なくとも 1 個のスタティック ピアを手順 3 で設定する必要があります。

**ステップ 3** switch(config)# **no cfs static-peers**

```
WARNING: This will remove all existing peers and start dynamic discovery.
Do you wish to continue? (y/n)  [n] y
```

すべてのスイッチでマルチキャスト転送を使用して、CFS スタティック ピアの検索を無効にしダイナミック ピア検索を有効にします。

**ステップ 4** switch(config-cfs-static)# **ip address 1.2.3.4**

switch(config-cfs-static)#**ip address 1.2.3.5**

switch(config-cfs-static)# **end**

switch#

スタティック ピア リストに IP アドレスを追加し、CFS 対応としてスイッチをマークします。To display the static IP peers list, use the **show cfs static peers** command.

**ステップ 5** switch(config-cfs-static)# **no ip address 1.2.3.3**

switch(config-cfs-static)# **end**

スタティック ピア リストから IP アドレスを削除し、マルチキャスト転送を使用してスイッチをダイナミック ピア検索に移動します。

**ステップ 6** switch# **show cfs static peers**

必要な CFS スタティック ピアの IP アドレス、WWN、ステータスを表示します。

- 検索進行中
- ローカル
- Reachable
- Unreachable
- ローカル IP が存在しません

- 再検索および配信が無効です

（注） IP アドレスおよび WWW はローカル スイッチで設定される必要があります。CFS がローカル スイッチ情報を受信しない場合、CFS はピア スイッチでに対して検索を開始できません。

# CFS リージョンの設定

## CFS リージョンの作成

CFS リージョンを作成する手順は、次のとおりです。

### 手順

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **cfs region 4**

例えば 4 など領域を作成します。

## CFS リージョンへのアプリケーションの割り当て

スイッチでリージョンにアプリケーションを割り当てる手順は、次のとおりです。

### 手順

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **cfs region 4**

領域、たとえば、4 の番号を作成します。

**ステップ 3** switch(config-cfs-region)# **ntp**

switch(config-cfs-region)# **callhome**

アプリケーションを追加します。

# 別の CFS リージョンへのアプリケーションの移動

地域 2 (ターゲット地域) に NTP と Call Home のアプリケーションと地域 1 (元の領域) からの例には、別の CFS 領域にアプリケーションを移動することができます。

アプリケーションを移動するには、このタスクを実行します。

**手順**

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **cfs region 2**

2 の領域を開始します。

**ステップ 3** switch(config-cfs-region)# **ntp**

switch(config-cfs-region)# **callhome**

元々リージョン 1 に属していたアプリケーションをリージョン 2 に移動するよう指定します。たとえば、ここでは、NTP および Call Home アプリケーションをリージョン 2 に移動します。

（注） 同じリージョンにアプリケーションを複数回追加しようとすると、「Application already present in the same region.」というエラー メッセージが表示されます。

# リージョンからのアプリケーションの削除

リージョンからのアプリケーションの削除は、アプリケーションをデフォルト リージョンのリージョン 0 に戻す場合と同じです。したがって、ファブリック全体がアプリケーションの配信の範囲になります。

地域 1 からアプリケーションを削除する手順は、次のとおりです。

**手順**

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **cfs region 1**

地域 1 を入力します。

**ステップ 3** switch(config-cfs-region)# **no ntp**

switch(config-cfs-region)# **no callhome**

移動する、リージョン 1 に属するアプリケーションを削除します。

# CFS リージョンの削除

リージョンの削除とは、リージョン定義を取り消すことです。リージョンを削除すると、リージョンによってバインドされているすべてのアプリケーションが解除されてデフォルト リージョンに戻ります。

リージョンを削除する手順は（例：リージョン番号 4）次のとおりです。

**手順**

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **no cfs region 4**

**例**：

```
WARNING: All applications in the region wiil be  moved to default region.
Are you sure? (y/n)  [n]
```

リージョン 4 を削除します。

（注） 手順 2 のあとに、「All the applications in the region will be moved to the default region.」という警告が表示されます。

# CFS 設定の確認

CFS のコンフィギュレーション情報を表示するには、次の作業のいずれかを行います。

| コマンド | 目的 |
|---|---|
| **show cfs status** | スイッチの CFS 配信のステータスを表示します。 |
| **show cfs application** | 現在 CFS に登録されているアプリケーションを表示します。 |
| **show cfs lock** | 現在、アプリケーションによって取得されるすべてのロックを表示します。 |
| **show cfs status** | IP を介した CFS 設定を確認します。. |
| **show cfs region brief** | CFS リージョンに関する簡単な情報を表示します。 |

| コマンド | 目的 |
|---|---|
| **show cfs region** | CFS リージョンに関する詳細な情報を表示します。 |

For detailed information about the fields in the output from these commands, refer to the *Cisco MDS 9000 Family Command Reference* .

# CFS 配信ステータスの確認

The **show cfs status** command displays the status of CFS distribution on the switch.

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

# アプリケーション登録スターテスの確認

The **show cfs application** command displays the applications that are currently registered with CFS. 最初のカラムには、アプリケーション名が表示されます。2 番めのカラムは、アプリケーションの配信がイネーブルであるかディセーブルであるかを示します（enabled または disabled）。最後のカラムは、アプリケーションの配信範囲を示します（論理、物理、またはその両方）。

（注） The **show cfs application** command only displays applications registered with CFS. CFS を使用するコンディショナルサービスは、これらのサービスが稼働していなければ出力には示されません。

```
switch# show cfs application
-----------------------------------------------
 Application    Enabled   Scope
-----------------------------------------------
 ntp            No        Physical-fc-ip
 fscm           Yes       Physical-fc
 role           No        Physical-fc-ip
 rscn           No        Logical
 radius         No        Physical-fc-ip
 fctimer        No        Physical-fc
 syslogd        No        Physical-fc-ip
 callhome       No        Physical-fc-ip
 fcdomain       No        Logical
 fc-redirect    Yes       Physical-fc
 device-alias   Yes       Physical-fc
Total number of entries = 11
```

The **show cfs application name** command displays the details for a particular application. 表示されるのは、イネーブル/ディセーブル ステート、CFS に登録されているタイムアウト、結合可能であるか（結合のサポートに対して CFS に登録されているか）、および配信範囲です。

```
switch# show cfs application name ntp
```

```
 Enabled        : Yes
 Timeout        : 5s
 Merge Capable  : Yes
 Scope          : Physical
 Region     : Default
```

# CFS ロック ステータスの確認

The **show cfs lock** command displays all the locks that are currently acquired by any application. このコマンドにより、アプリケーションごとにアプリケーション名とロックの取得範囲が表示されます。アプリケーション ロックが物理範囲で取得されている場合、このコマンドはスイッチ WWN、IP アドレス、ユーザ名、およびロック所有者のユーザ タイプを表示します。アプリケーションが論理範囲で取得されている場合、このコマンドはロックが取得された VSAN、ドメイン、IP アドレス、ユーザ名、およびロック所持者のユーザ タイプを表示します。

```
switch# show cfs lock
Application: ntp
Scope      : Physical
--------------------------------------------------------------------------
 Switch WWN               IP Address       User Name    User Type
--------------------------------------------------------------------------
 20:00:00:05:30:00:6b:9e  10.76.100.167    admin        CLI/SNMP v3
 Total number of entries = 1
Application: port-security
Scope      : Logical
-----------------------------------------------------------
 VSAN   Domain   IP Address       User Name    User Type
-----------------------------------------------------------
 1      238      10.76.100.167    admin        CLI/SNMP v3
 2      211      10.76.100.167    admin        CLI/SNMP v3
 Total number of entries = 2
```

The **show cfs lock name** command displays the lock details similar for the specified application.

### 指定したアプリケーションのロック情報

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

# IP を介した CFS 設定の確認

To verify the CFS over IP configuration, use the **show cfs status** command.

```
switch# show cfs status
Distribution : Enabled
Distribution over IP : Disabled
```

```
IPv4 multicast address : 239.255.70.83
IPv6 multicast address : ff15::efff:4653
```

# IP を介した CFS の IP マルチキャスト アドレス設定の確認

To verify the IP multicast address configuration for CFS over IP, use the **show cfs status** command.

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

# スタティック IP ピア設定の確認

To verify the IP peer configuration, use the **show cfs status** command.

```
switch# show cfs status
Distribution: Enabled
Distribution over IP: Enabled - mode IPv4 (static)
IPv4 multicast address : 239:255:70:83
IPv6 multicast address : ff15::efff:4563
```

To display the status of static IP peers discovery, use the **show cfs static peers** command.

```
switch# show cfs static peers
-------------------------------------------------------------
IP Address     WWN                          Status
-------------------------------------------------------------
192.0.2.4     00:00:00:00:00:00:00:00      Discovery in progress
192.0.2.5     20:00:00:0d:ec:06:55:b9      Reachable
192.0.2.6     20:00:00:0d:ec:06:55:c0      Local
```

# CFS 地域の検査

CFS 地域を表示する手順は、次のとおりです。

**手順**

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **show cfs region brief**

CFS 地域に関する要約情報を表示します。

**ステップ 3** switch(config)# **show cfs region**

CFS 地域に関する詳細情報を表示します。

（注） 正常に CFS ピアを形成するには、2 つの異なる管理スイッチに接続されている 2 つの異なるスイッチで、一般的な mcast IP を設定できます。

# その他の参考資料

CFS の実装に関する詳細情報については、次の項を参照してください。

### MIB

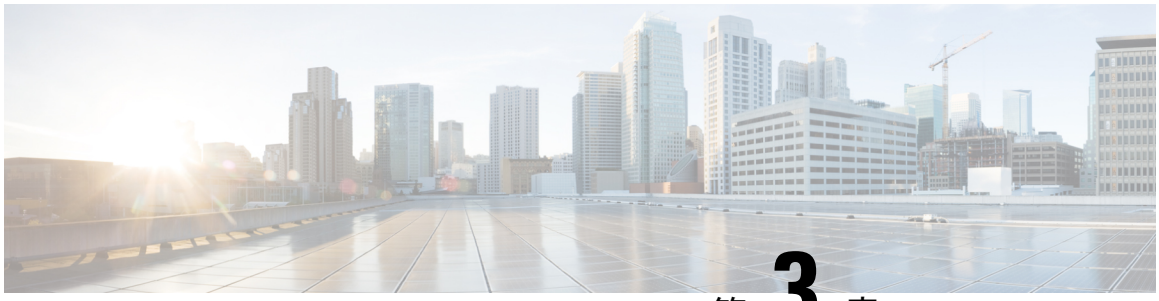
| MIB | MIB のリンク |
|---|---|
| • CISCO-CFS-CAPABILITY-MIB<br>• CISCO-CFS-MIB | MIB を検索およびダウンロードするには、次の URL にアクセスしてください。<br>http://www.cisco.com/en/US/products/ps5989/prod_technical_reference_list.html |

# CFS の機能の履歴

表 2 : CFS の機能の履歴 （27 ページ） に、この機能のリリース履歴を示します。リリース 3.x 以降のリリースで導入または変更された機能のみが表に記載されています。

**表 *2 : CFS* の機能の履歴**

| 機能名 | リリース | 機能情報 |
|---|---|---|
| CFS 向け静的 IP ピア（非 NPV） | 6.2(11) | 非 NPV スイッチで有効な IP 静的ピア |
| CFS 向け静的 IP ピア（NPV） | 4.1(1a) | 新規 NPV CFS Setup Wizard. IP を介した CFS 配信用に IP スタティック ピア設定のステップが追加されました。 |
| CFS 拡張機能 | 3.2(1) | CFS リージョンをサポートします。 |
| IP を介した CFS | 3.0(1) | IP 接続を介した CFS 配信を可能にします。 |
| 許可ドメイン ID リストの CFS サポート | 3.0(1) | CFS インフラストラクチャを使用して許可ドメイン ID リストをファブリック内で配信できます。 |
| RCSN の CFS サポート | 3.0(1) | CFS インフラストラクチャを使用して RSCN タイマー値をファブリック内で配信できます。 |



第 3 章

# 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。



## システム メッセージ ロギングについて

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

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

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

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

表 3 : 内部ロギング ファシリティ （30 ページ） 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:* 内部ロギング ファシリティ

| ファシリティ キーワード | 説明 | 標準であるか、または**Cisco MDS** 固有であるか |
|---|---|---|
| **acl** | ACL マネージャ | Cisco MDS 9000 ファミリ固有 |
| **all** | すべてのファシリティ | Cisco MDS 9000 ファミリ固有 |
| **auth** | 許可システム | 規格 |
| **authpriv** | 認証（プライベート）システム | 規格 |
| **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 | 規格 |
| **daemon** | システム デーモン | 規格 |
| **fcc** | FCC | Cisco MDS 9000 ファミリ固有 |
| **fcdomain** | fcdomain | Cisco MDS 9000 ファミリ固有 |
| **fcns** | ネーム サーバ | Cisco MDS 9000 ファミリ固有 |
| **fcs** | FCS | Cisco MDS 9000 ファミリ固有 |
| **flogi** | FLOGI | Cisco MDS 9000 ファミリ固有 |
| **fspf** | FSPF | Cisco MDS 9000 ファミリ固有 |
| **ftp** | 『File Transfer Protocol』 | 規格 |
| **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 | 規格 |
| **local0 to local7** | ローカルに定義されたメッセージ | 規格 |
| **lpr** | ライン プリンタ システム | 規格 |
| **mail** | メール システム | 規格 |
| **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 | 規格 |
| **ntp** | NTP | Cisco MDS 9000 ファミリ固有 |

| 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 |
|---|---|---|
| **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 | 規格 |
| **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 | 規格 |
| **uucp** | UNIX 間コピー プログラム | 規格 |
| **vhbad** | 仮想ホスト ベース アダプタ デーモン | Cisco MDS 9000 ファミリ固有 |
| **vni** | 仮想ネットワーク インターフェイス | Cisco MDS 9000 ファミリ固有 |
| **vrrp_cfg** | VRRP の設定 | Cisco MDS 9000 ファミリ固有 |
| **vrrp_eng** | VRRP エンジン | Cisco MDS 9000 ファミリ固有 |
| **vsan** | VSAN システム メッセージ | Cisco MDS 9000 ファミリ固有 |
| **vshd** | vshd | Cisco MDS 9000 ファミリ固有 |
| **wwn** | WWN マネージャ | Cisco MDS 9000 ファミリ固有 |
| **xbar** | クロスバー システム メッセージ | Cisco MDS 9000 ファミリ固有 |
| **zone** | ゾーン サーバ | Cisco MDS 9000 ファミリ固有 |

表 4 : エラー メッセージの重大度 （32 ページ） 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 *4:* エラー メッセージの重大度

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

（注） Refer to the *Cisco MDS 9000 Family System Messages Reference* for details on the error log message format.

# 『System Message Logging』

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

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

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

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

# SFP 診断

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

- TX 電力
- RX 電力
- 温度
- Voltage
- Current

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

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

# 出力されるシステム メッセージ ロギング サーバ ファシリティ

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

The single system message logging daemon (syslogd) sends the information based on the configured **facility** option. 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 : 内部ロギング ファシリティ （30 ページ） 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 5 : 送信ロギング ファシリティ （33 ページ）に記載されています。

**表 *5:* 送信ロギング ファシリティ**

| ファシリティ キーワード | 説明 | 標準であるか、または Cisco MDS 固有であるか |
|---|---|---|
| **auth** | 許可システム | 規格 |
| **authpriv** | 認証（プライベート）システム | 規格 |
| **cron** | cron ファシリティまたは at ファシリティ | 規格 |
| **daemon** | システム デーモン | 規格 |
| **ftp** | 『File Transfer Protocol』 | 規格 |
| **kernel** | カーネル | 規格 |

| 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 |
|---|---|---|
| **local0 to 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 | 規格 |
| **mail** | メール システム | 規格 |
| **news** | USENET ニュース | 規格 |
| **syslog** | 内部システム メッセージ | 規格 |
| **user** | ユーザ プロセス | 規格 |
| **uucp** | UNIX 間コピー プログラム | 規格 |

# システム メッセージ ロギング設定の配信

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

スイッチでの配信をイネーブルにした後で最初のコンフィギュレーション コマンドを発行すると、ファブリック全体が自動的にロックされます。システム メッセージ ロギング サーバは、有効/保留データベース モデルを使用して、設定をベースにコマンドを保存またはコミットします。設定の変更を確定すると、有効データベースが保留データベースの設定変更で上書きされ、ファブリック内のすべてのスイッチで設定が同じになります。設定を変更した後、変更を廃棄するには、変更を確定せずに中断します。いずれの場合でも、ロックは解除されます。CFS アプリケーションの詳細については、CFS インフラストラクチャの使用 （5 ページ）を参照してください。

# ファブリックのロックの上書き

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

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

# 注意事項と制約事項

概念の詳細については、CFS 結合のサポート （10 ページ）を参照してください。

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

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

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

# デフォルト設定

表 6 : システム メッセージ ログのデフォルト設定値 （35 ページ） に、システム メッセージ ロギングのデフォルト設定を示します。

**表 *6:* システム メッセージ ログのデフォルト設定値**

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

# システム メッセージ ロギングの設定

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

## システム メッセージ ロギングを設定するためのタスク フロー

システム メッセージ ロギングを設定するには、次の手順を実行します。

**手順**

**ステップ 1** メッセージ ロギングをイネーブルまたはディセーブルにします。
**ステップ 2** コンソール重大度を設定します。
**ステップ 3** モニタ重大度を設定します。
**ステップ 4** モジュール ロギングを設定します。
**ステップ 5** ファシリティ重大度を設定します。
**ステップ 6** ログ ファイルを送信します。
**ステップ 7** システム メッセージ ロギング サーバを設定します。
**ステップ 8** システム メッセージ ロギング配信を設定します。

## メッセージ ロギングの有効化または無効化

コンソールへのロギングを無効にしたり、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有効にできます。

- 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。

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。

**手順**

**ステップ 1** switch# **terminal monitor**

Telnet または SSH セッションのロギングを有効にします。

（注）　コンソール セッションは、デフォルトで有効にされています。

**ステップ 2**　switch# **terminal no monitor**

Telnet または SSH セッションのロギングを無効にします。

（注）　デフォルトで、Telnet または SSH セッションが無効になっています。

# コンソール重大度の設定

コンソールセッションに対するロギングが有効になっている場合（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。

（注）　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。

コンソール セッションの重大度を設定するには、次の手順を実行します。

**手順**

**ステップ 1**　switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2**　switch(config)# **logging console 3**

レベル 3（エラー）でコンソール ロギングを設定します。重大度が 3 以上のロギング メッセージがコンソールに表示されます。

**ステップ 3**　switch(config)# **no logging console**

コンソール ロギングを工場出荷時のデフォルトの重大度 2（重大）に戻します。重大度が 2 以上のロギング メッセージがコンソールに表示されます。

# モニタ重大度の設定

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

モニタ セッションの重大度を設定するには、次の手順を実行します。

**手順**

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **logging monitor 3**

レベル 3 (error) ロギング モニタを設定します。Logging messages with a severity level of 3 or above are displayed on the monitor.

**ステップ 3** switch(config)# **no logging monitor**

モニタ ロギングを工場出荷時のデフォルトの重大度 5（notifications）に戻します。重大度が 5 以上のロギング メッセージがコンソールに表示されます。

# モジュール ロギングの設定

デフォルトでは、すべてのモジュールに対してレベル 7 でロギングが有効になっています。各モジュールの対するロギングを、特定のレベルで有効または無効にできます。

モジュールのロギングを有効また無効にして、重大度レベルを設定するには、次の手順に従います。

**手順**

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **logging module 1**

すべてのモジュールのレベル 1（アラート）でモジュール ロギングを設定します。

**ステップ 3** switch(config)# **logging module**

スイッチのすべてのモジュールのモジュール ロギングをデフォルトのレベル 5（notifications）に設定します。

**ステップ 4** switch(config)# **no logging module**

モジュール ロギングを無効します。

# ファシリティ重大度の設定

ロギング ファシリティの重大度を設定するには（表 3 : 内部ロギング ファシリティ （30 ページ） を参照してください）、次の手順を実行します。

**手順**

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **logging level kernel 4**

レベル 4（警告）で、カーネル ファシリティに関する Telnet または SSH ロギングを設定します。その結果、重大度レベルが 4 以上のロギング メッセージが表示されます。

**ステップ 3** switch(config)# **no logging level kernel 4**

カーネル ファシリティの Telnet または SSH ロギング機能は、カーネルのデフォルトの重大度 6（情報） に戻ります。

（注） Use the **show logging info** command to display the default logging levels for the facilities listed in 表 3 : 内部ロギング ファシリティ （30 ページ）.

# ログ ファイルの送信

デフォルトでは、スイッチにより、正常だが重要なシステム メッセージがログ ファイルに記録され、それらのメッセージがシステム コンソールに送信されます。ログ メッセージは、システム再起動後には消去されています。生成されるログメッセージは、ログファイルに保存される可能性があります。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。

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。

**手順**

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **logging logfile messages 3**

重大度レベル 3 以上のエラーまたは上のイベントの情報のログを設定という名前のメッセージのデフォルトのログファイルにします。

**ステップ 3** switch(config)# **logging logfile ManagerLog 3**

デフォルト サイズ 10,485,760 バイトを使用して、重大度 3 以上の errors または events の情報を ManagerLog という名前のファイルに記録するように設定します。

**ステップ 4** switch(config)# **logging logfile ManagerLog 3 size 3000000**

重大度 3 以上のエラーまたはイベントの情報を ManagerLog という名前のファイルに記録するように設定します。サイズの設定により、ファイル サイズを 3,000,000 バイトに制限しています。

**ステップ 5** switch(config)# **no logging logfile**

ログファイルへのロギング メッセージを無効にします。

You can rename the log file using the **logging logfile** command.

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。 You can use the **show logging logfile** and clear logging logfile commands to view and delete the contents of this file. You can use the **dir log:** command to view logging file statistics. You can use the **delete log:** command to remove the log file.

You can copy the logfile to a different location using the **copy log:** command using additional copy syntax.

# システム メッセージ ロギング サーバの設定

最大 3 台のシステム メッセージ ロギング サーバを設定できます。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。

**手順**

**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） Be sure to add five tab characters between **local1.debug** and **/var/log/*myfile*.log**. 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。The **local1** keyword specifies the UNIX logging facility used. 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。The **debug** keyword specifies the severity level of the condition being logged. スイッチからのすべてのメッセージを受信するように UNIX システムを設定できます。

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

**$ touch /var/log/ myfile .log**

**$ chmod 666 /var/log/ myfile .log**

**ステップ 3** 次のコマンドを実行して、システム メッセージ ロギング デーモンに新しい変更を読み込ませます。

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

## システム メッセージ ロギング サーバ IPv4 アドレスの設定

システム メッセージ ロギング サーバ Ipv4 アドレスを設定するには、これらの手順に従います。

**手順**

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **logging server 172.22.00.00**

指定されたファシリティ タイプおよびセキュリティ レベルに従ってログ メッセージを、ホスト名または Ipv4 アドレス（172,22,00,00）に指定されたリモートの複数サーバに転送するようにスイッチを設定します。

**ステップ 3** switch(config)# **logging server 172.22.00.00 facility local1**

サーバ IPv4アドレス（172.22.00.00）に指定されたファシリティ（（local1）に従って、ログ メッセージを転送するようにスイッチを設定します。デフォルトの発信ファシリティは local7 です。

**ステップ 4** switch(config)# **no logging server 172.11.00.00**

指定されたサーバ（172.11.00.00）を削除し、出荷時のデフォルトに戻します。

## サーバの IPv6 アドレスをシステム メッセージ ロギングの設定

To configure system message logging server IPv6 addresses, follow these steps:

**手順**

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **logging server 2001::0db8:800:200c:417a**

指定されたファシリティ タイプに従って転送ログ メッセージをスイッチと、IPv6 アドレスで指定したリモート サーバへの重大度レベルを設定します。

**ステップ 3** switch(config)# **logging server 2001::0db8:800:200c:417a facility local1**

サーバ IPv6 アドレスの指定されたファシリティ (local1) に従って転送ログ メッセージにスイッチを設定します。デフォルトの発信ファシリティは local7 です。

**ステップ 4** switch(config)# **no logging server 2001::0db8:800:200c:417a**

指定したサーバを削除し、出荷時のデフォルトに戻します。

# システム メッセージ ロギング配信の設定

システム メッセージ ロギング サーバ設定のファブリック配信を有効にするのには、次の次の手順を実行します。

**手順**

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **logging distribute**

ファブリック内のすべてのスイッチに配布するシステム メッセージ ロギング サーバ設定を有効にして、ロックを取得、保留中のデータベースに将来の設定の変更を保存します。

**ステップ 3** switch(config)# **no logging distribute**

Disables (default) system message logging server configuration distribution to all switches in the fabric.

## 変更のコミット

システム メッセージ ロギング サーバ設定の変更を確定するには、次の次の手順を実行します。

**手順**

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **logging commit**

ファブリック内のすべてのスイッチに設定の変更を配信、ロックを解除し、保留中のデータベースに加えた変更を効果的なデータベースを上書きします。

## 変更の破棄

システム メッセージ ロギング サーバ設定の変更を廃棄するには、次の手順を実行します。

**手順**

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **logging abort**

保留中のデータベースのシステム ロギング サーバ設定の変更を廃棄し、ファブリック ロックを解除します。

# ファブリックのロックの上書き

To use administrative privileges and release a locked system message logging session, use the **clear logging session** command.

```
switch# clear logging session
```

# システム メッセージ ロギング情報の表示

システム メッセージ ロギング情報を表示するには、次のタスクのいずれかを実行します。

| コマンド | 目的 |
|---|---|
| **show logging** | 現在のシステム メッセージ ロギングを表示します。. |
| **show logging nvram** | NVRM ログの内容を表示します。 |
| **show logging logfile** | ログ ファイルを表示します。 |
| **show logging level** | ロギング ファシリティを表示します。 |
| **show logging info** | ロギング情報を表示します。 |
| **show logging last 2** | ログ ファイルの最後の数行を表示します。. |
| **show logging module** | スイッチング モジュール ロギング ステータスを表示します。 |
| **show logging monitor** | モニタ ロギング ステータスを表示します。 |
| **show logging server** | サーバ情報を表示します。 |

For detailed information about the fields in the output from these commands, refer to the *Cisco MDS 9000 Family Command Reference* .

Use the **show logging** command to display the current system message logging configuration . 例 現在のシステム メッセージ ロギング （44 ページ） ～ サーバ情報 （49 ページ） を参照してください。

（注） When using the **show logging** command, output is displayed only when the configured logging levels for the switch are different from the default levels.

### 現在のシステム メッセージ ロギング

次の例では、現在のシステム メッセージ ロギングを示します。

```
switch# show logging

Logging console:                 enabled (Severity: critical)
Logging monitor:                 enabled (Severity: debugging)
Logging linecard:                enabled (Severity: debugging)
Logging server:                  enabled
{172.20.102.34}
        server severity:         debugging
        server facility:         local7
{10.77.202.88}
        server severity:         debugging
        server facility:         local7
{10.77.202.149}
        server severity:         debugging
        server facility:         local7
Logging logfile:                 enabled
        Name - messages: Severity - debugging Size - 4194304
Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
kern                    6                       6
user                    3                       3
mail                    3                       3
daemon                  7                       7
auth                    0                       7
syslog                  3                       3
lpr                     3                       3
news                    3                       3
uucp                    3                       3
cron                    3                       3
authpriv                3                       7
ftp                     3                       3
local0                  3                       3
local1                  3                       3
local2                  3                       3
local3                  3                       3
local4                  3                       3
local5                  3                       3
local6                  3                       3
local7                  3                       3
vsan                    2                       2
fspf                    3                       3
fcdomain                2                       2
module                  5                       5
```

```
sysmgr                  3                       3
zone                    2                       2
vni                     2                       2
ipconf                  2                       2
ipfc                    2                       2
xbar                    3                       3
fcns                    2                       2
fcs                     2                       2
acl                     2                       2
tlport                  2                       2
port                    5                       5
flogi                   2                       2
port_channel            5                       5
wwn                     3                       3
fcc                     2                       2
qos                     3                       3
vrrp_cfg                2                       2
ntp                     2                       2
platform                5                       5
vrrp_eng                2                       2
callhome                2                       2
mcast                   2                       2
rdl                     2                       2
rscn                    2                       2
bootvar                 5                       2
securityd               2                       2
vhbad                   2                       2
rib                     2                       2
vshd                    5                       5
0(emergencies)          1(alerts)       2(critical)
3(errors)               4(warnings)     5(notifications)
6(information)          7(debugging)
Feb 14 09:50:57 excal-113 %TTYD-6-TTYD_MISC: TTYD TTYD started
Feb 14 09:50:58 excal-113 %DAEMON-6-SYSTEM_MSG: precision = 8 usec
...
```

Use the **show logging nvram** command to view the log messages saved in NVRAM. 重大度が Critical 以下（レベル 0、1、2）のログ メッセージのみ NVRAM に保存されます。

### NVRM ログの内容

次の例では、NVRM ログの内容を示します。

```
switch# show logging nvram

Jul 16 20:36:46 172.22.91.204 %KERN-2-SYSTEM_MSG: unable to alloc and fill in a
new mtsbuf (pid=2209, ret_val = -105)
Jul 16 20:36:46 172.22.91.204 %KERN-2-SYSTEM_MSG: unable to alloc and fill in a
new mtsbuf (pid=2199, ret_val = -105)
Jul 16 20:36:46 172.22.91.204 %KERN-2-SYSTEM_MSG: unable to alloc and fill in a
new mtsbuf (pid=2213, ret_val = -105)
Jul 16 20:36:46 172.22.91.204 %KERN-2-SYSTEM_MSG: unable to alloc and fill in a
new mtsbuf (pid=2213, ret_val = -105)
...
```

### Log File

次の例では、ログ ファイルを示します。

```
switch# show logging logfile

Jul 16 21:06:50 %DAEMON-3-SYSTEM_MSG: Un-parsable frequency in /mnt/pss/ntp.drift
Jul 16 21:06:56 %DAEMON-3-SYSTEM_MSG: snmpd:snmp_open_debug_cfg: no snmp_saved_dbg_uri
;
Jul 16 21:06:58 172.22.91.204 %PORT-5-IF_UP: Interface mgmt0 is up
Jul 16 21:06:58 172.22.91.204 %MODULE-5-ACTIVE_SUP_OK: Supervisor 5 is active
...
```

### コンソール ロギング ステータス

次の例では、コンソール ロギング ステータスを示します。

```
switch# show logging console

Logging console:                enabled (Severity: notifications)
```

### ロギング ファシリティ

次の例では、 ロギング ファシリティを示します。

```
switch# show logging level

Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
kern                    6                       6
user                    3                       3
mail                    3                       3
daemon                  7                       7
auth                    0                       7
syslog                  3                       3
lpr                     3                       3
news                    3                       3
uucp                    3                       3
cron                    3                       3
authpriv                3                       7
ftp                     3                       3
local0                  3                       3
local1                  3                       3
local2                  3                       3
local3                  3                       3
local4                  3                       3
local5                  3                       3
local6                  3                       3
local7                  3                       3
vsan                    2                       2
fspf                    3                       3
fcdomain                2                       2
module                  5                       5
sysmgr                  3                       3
zone                    2                       2
vni                     2                       2
ipconf                  2                       2
ipfc                    2                       2
xbar                    3                       3
fcns                    2                       2
fcs                     2                       2
```

```
acl                     2                       2
tlport                  2                       2
port                    5                       5
flogi                   2                       2
port_channel            5                       5
wwn                     3                       3
fcc                     2                       2
qos                     3                       3
vrrp_cfg                2                       2
ntp                     2                       2
platform                5                       5
vrrp_eng                2                       2
callhome                2                       2
mcast                   2                       2
rdl                     2                       2
rscn                    2                       2
bootvar                 5                       2
securityd               2                       2
vhbad                   2                       2
rib                     2                       2
vshd                    5                       5
0(emergencies)          1(alerts)       2(critical)
3(errors)               4(warnings)     5(notifications)
6(information)          7(debugging)
```

## ロギング情報

次の例では、ロギング情報を示します。

```
switch# show logging info

Logging console:                enabled (Severity: critical)
Logging monitor:                enabled (Severity: debugging)
Logging linecard:               enabled (Severity: debugging)
Logging server:                 enabled
{172.20.102.34}
        server severity:        debugging
        server facility:        local7
{10.77.202.88}
        server severity:        debugging
        server facility:        local7
{10.77.202.149}
        server severity:        debugging
        server facility:        local7
Logging logfile:                enabled
        Name - messages: Severity - debugging Size - 4194304
Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
kern                    6                       6
user                    3                       3
mail                    3                       3
daemon                  7                       7
auth                    0                       7
syslog                  3                       3
lpr                     3                       3
news                    3                       3
uucp                    3                       3
cron                    3                       3
authpriv                3                       7
ftp                     3                       3
local0                  3                       3
```

```
local1                  3                       3
local2                  3                       3
local3                  3                       3
local4                  3                       3
local5                  3                       3
local6                  3                       3
local7                  3                       3
vsan                    2                       2
fspf                    3                       3
fcdomain                2                       2
module                  5                       5
sysmgr                  3                       3
zone                    2                       2
vni                     2                       2
ipconf                  2                       2
ipfc                    2                       2
xbar                    3                       3
fcns                    2                       2
fcs                     2                       2
acl                     2                       2
tlport                  2                       2
port                    5                       5
flogi                   2                       2
port_channel            5                       5
wwn                     3                       3
fcc                     2                       2
qos                     3                       3
vrrp_cfg                2                       2
ntp                     2                       2
platform                5                       5
vrrp_eng                2                       2
callhome                2                       2
mcast                   2                       2
rdl                     2                       2
rscn                    2                       2
bootvar                 5                       2
securityd               2                       2
vhbad                   2                       2
rib                     2                       2
vshd                    5                       5
0(emergencies)          1(alerts)       2(critical)
3(errors)               4(warnings)     5(notifications)
6(information)          7(debugging)
```

### ログ ファイルの最後の数行

次の例では、ログ ファイルの最後の数行を示します。

```
switch# show logging last2

Nov 8 16:48:04 excal-113 %LOG_VSHD-5-VSHD_SYSLOG_CONFIG_I: Configuring console from pts/1
 (171.71.58.56)
Nov 8 17:44:09 excal-113 %LOG_VSHD-5-VSHD_SYSLOG_CONFIG_I: Configuring console from pts/0
 (171.71.58.72)
```

### スイッチング モジュール ロギング ステータス

次の例では、スイッチング モジュール ロギング ステータスを示します。

```
switch# show logging module

Logging linecard:                enabled (Severity: debugging)
```

### モニタ ロギング ステータス

次の例では、モニタ ロギング ステータスを示します。

```
switch# show logging monitor

Logging monitor:                 enabled (Severity: information)
```

### サーバ情報

次の例では、サーバ情報を示します。

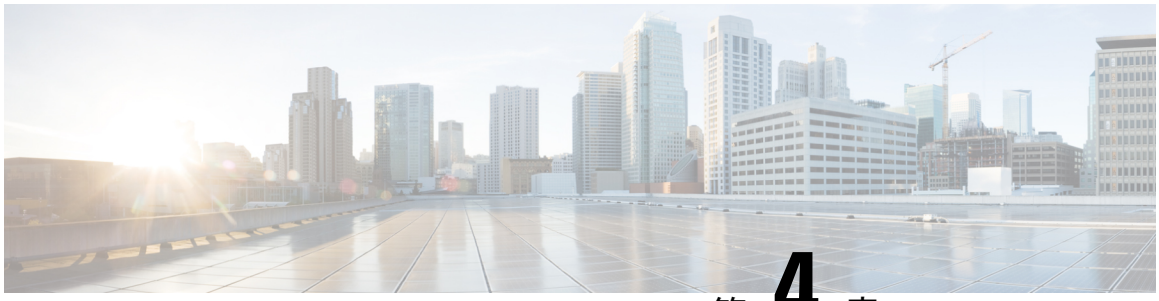
```
switch# show logging server

Logging server:                  enabled
{172.22.95.167}
        server severity:         debugging
        server facility:         local7
{172.22.92.58}
        server severity:         debugging
        server facility:         local7
```

# その他の参考資料

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

### MIB

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



第 4 章

# Call Home の設定

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

（注） Cisco Autonotify は、Smart Call Home と呼ぶ新機能にアップグレードされています。Smart Call Home は、Autonotify に比べて機能が大幅に改良されており、シスコの製品レンジ全体にわたって使用できます。For detailed information on Smart Call Home, see the Smart Call Home page at this location: http://www.cisco.com/go/smartcall/ .

この章は、次の項で構成されています。



## Call Home の概要

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

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

一般的な機能として次のものがあります。

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

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

Call Home 機能には、次の利点があります。

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

# Call Home の機能

Call Home 機能は、Cisco MDS 9000 シリーズ スイッチと Cisco Nexus 5000 シリーズ スイッチから直接利用できます。It provides multiple Call Home profiles (also referred to as *Call Home destination profiles* ), each with separate potential destinations. 事前に定義されたプロファイルに加えて、独自の宛先プロファイルを定義できます。

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

Call Home 機能には、次の利点があります。

- スイッチ上の固定の事前に定義されたアラートおよびトリガー イベント。
- 関連するコマンドの自動的な実行と出力の添付。
- 複数のメッセージ フォーマット オプション
  - ショート テキスト：ポケットベルまたは印刷形式のレポートに最適。
  - プレーン テキスト：人間が読むのに適した形式に完全整形されたメッセージ情報。
  - XML：Extensible Markup Language（XML）と、Messaging Markup Language（MML）と呼ぶ Document Type Definitions（DTD）を使用した、機械で読み取り可能なフォーマット。MML DTD は、Cisco.com の Web サイト http://www.cisco.com/ で公開されています。XML フォーマットでは、シスコの TAC との通信が可能になります。

- 複数のメッセージ宛先への同時配信が可能。各宛先プロファイルには最大50件の電子メール宛先アドレスを設定できます。
- システム、環境、スイッチング モジュール ハードウェア、スーパーバイザ モジュール、ハードウェア、インベントリ、syslog、RMON、テストなど、複数のメッセージ カテゴリ。
- お使いのデバイスから直接、またはHTTPプロキシ サーバやダウンロード可能な転送ゲートウェイ（TG）を介した、セキュアなメッセージ転送。TG集約ポイントは、複数のデバイスをサポートする場合またはセキュリティ要件によって、デバイスをインターネットに直接接続できない場合に使用できます。

（注） Cisco MDS リリース 7.3(0)D1(1) 以降では、すべてのアラートは、タイプ、環境、サブタイプ、マイナーに分類されます。

- SUP_FAILURE、POWER_SUPPY_FAILURE、LINECARD_FAILURE アラートは、タイプ、環境、およびサブタイプ、メジャーに分類されます。

# Smart Call Home の概要

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

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

Smart Call Home には、次の機能があります。

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

.

表 7 : Smart Call Home の Autonotify と比較した利点 （54 ページ） に Smart Call Home の利点の一覧を示します。

表 *7: 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、完全なインベントリ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。 | いいえ。 |
| 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）。 | いいえ。 |
| シスコ デバイスのサポート | デバイスのサポートはシスコの製品レンジ全体に拡張されます。サポートされている製品の表については、www.cisco.com/go/smartcall を参照してください。。 | Smart Call Home への移行を推進するため、2008 年 10 月に廃止されました。 |

## Smart Call Home の取得

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

次の項目を登録する必要があります。

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

- Cisco.com ID

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

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

# Call Home 宛先プロファイル

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

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

# Call Home アラート グループ

An alert group is a predefined subset of Call Home alerts supported in all switches in the Cisco MDS 9000 Series and Cisco Nexus 5000 Series. アラート グループを使用することで、（定義済みまたはユーザ定義の）宛先プロファイルで受信される Call Home アラートのセットを選択できます。Call Home アラートが、宛先プロファイル内の E メールの宛先に送信されるのは、その Call Home アラートが、その宛先プロファイルに関連付けられているいずれかのアラート グループに属する場合だけです。

定義済みの Call Home アラート グループを使用して、スイッチに特定のイベントが発生したときに通知メッセージを生成できます。You can customize predefined alert groups to execute additional **show** commands when specific events occur and to notify you of output other than from the predefined **show** commands.

## カスタマイズされたアラート グループ メッセージ

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

The output from these additional **show** commands is included in the notification message along with the output of the predefined **show** commands.

# Call Home のメッセージ レベル機能

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

# Syslog ベースのアラート

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

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

syslog-group-port アラート グループは、そのポート ファシリティの syslog メッセージを選択します。Call Home アプリケーションは、syslog の重大度を対応する Call Home の重大度にマッピングします（表 8 : イベント トリガー （60 ページ） を参照）。たとえば、Call Home メッセージ レベルに対してレベル 5 を選択すると、レベル 0、1、2 の syslog メッセージが Call Home ログに追加されます。

syslog メッセージが生成されるたびに、Call Home アプリケーションは、宛先プロファイルとアラート グループ マッピングの間のマッピングに従い、生成された syslog メッセージの重大度に基づいて、Call Home メッセージを送信します。Syslog ベースの Call Home アラートを受信するには、宛先プロファイルと Syslog アラート グループを関連付けて（現在は syslog-group-port という 1 つの Syslog アラート グループだけが存在する）、適切なメッセージ レベルを設定する必要があります（表 8 : イベント トリガー （60 ページ） を参照）。

（注） Call Home は、メッセージ テキストで Syslog メッセージ レベルを変更しません。The syslog message texts in the Call Home log appear as they are described in the *Cisco MDS 9000 Series System Messages* Reference.

# RMON ベースのアラート

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

# HTTPS サポートを使用した一般的な電子メール オプション

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

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

# 複数 SMTP サーバ サポート

Cisco MDS NX-OS および Cisco NX-OS 5000 シリーズ スイッチでは、Call Home の複数の SMTP サーバをサポートします。各 SMTP サーバでは、1 ~ 100 の 1 が最高の優先度、最も低い 100 で設定されている優先度があります。If the priority is not specified, a default value of 50 is used.

Call Home に対して最大 5 つの SMTP サーバを設定できます。The servers are contacted based on their priority. The highest priority server is contacted first. If the message fails to be sent, the next server in the list is contacted until the limit is exhausted. If two servers have equal priority, the one that was configured earlier is contacted.

優先度の高い SMTP サーバが失敗すると、他のサーバに接続されます。タイミングの遅延は、メッセージの送信中が発生する可能性があります。遅延は、最初の SMTP サーバ経由でメッセージを送信しようとするが成功した場合は、最小限です。別の SMTP サーバで失敗した試行の数によって、遅延が増えることがあります。

（注） 新しい configuration process(構成プロセス、設定プロセス) は、以前の構成とは無関係です。ただし、新旧の両方の方式を使用して、SMTP サーバが設定されている場合、古い設定は、最高の優先度のです。

複数の SMTP サーバ、MDS 9000 シリーズ スイッチ、Cisco Nexus 5000 シリーズ スイッチでは、およびリリース 5.0(1a) を実行する Cisco Nexus 7000 シリーズ スイッチで構成されているまたはそれ以降を使用できます。

新しい設定は、複数の SMTP サーバのスイッチにのみ分配されます。ファブリックで古いスイッチでは、CFS 経由で受信した新しい設定を無視します。

CFS が有効になっているは、混合ファブリックでは、NX-OS リリース 5.0 を実行するスイッチは新しい機能を設定し、CFS over fabric リリース 5.0 で他のスイッチに新しい設定を配布します。ただし、既存のスイッチ リリース 5.0 に NX-OS リリース 4.x のアップグレードを実行し

ているかどうか、新しい設定はしないに分配されますそのスイッチCFSマージがアップグレードでトリガーされませんよう。アップグレードには次の2つのオプションがあります。

- ファブリック内のすべてのスイッチをサポートする(推奨オプション)場合にのみ、新しい設定を適用します。
- 新しい設定を持つ既存の NX-OS リリース 5.0 スイッチから空のコミットしないでください。

## 定期的なインベントリ通知

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、ハードウェアインベントリ情報とともに、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。インベントリは、スイッチを停止せずに再起動するたびに変更されます。

## 重複するメッセージのスロットリング

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

## Call Home 設定の配信

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

スイッチで配信をイネーブルにしてから初めてコンフィギュレーション コマンド操作を入力するとき、ファブリック全体が自動的にロックされます。Call Home アプリケーションは、設定の変更を保存または確定するために、有効および保留データベース モデルを使用します。設定の変更を確定すると、有効データベースが保留データベースの設定変更で上書きされ、ファブリック内のすべてのスイッチで設定が同じになります。設定を変更した後、変更を廃棄するには、変更を確定せずに中断します。いずれの場合でも、ロックは解除されます。CFS アプリケーションの詳細については、CFS インフラストラクチャの使用 （5 ページ） を参照してください。

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

## ファブリックのロックの上書き

Call Home で作業を行い、変更の確定か廃棄を行ってロックを解除するのを忘れた場合、管理者はファブリック内の任意のスイッチからロックを解除できます。管理者がこの操作を行う

と、ユーザによる保留データベースの変更は廃棄され、ファブリックのロックは解除されます。

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

# Call Home ネーム サーバ データベースのクリア

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

# EMC E-mail Home 遅延トラップ

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

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

# イベント トリガー

ここでは、Call Home のトリガー イベントについて説明します。トリガー イベントは複数のカテゴリにわかれており、各カテゴリには、イベントが発生したときに実行される CLI コマンドが割り当てられています。The command output is included in the transmitted message. 表 8 : イベント トリガー （60 ページ） lists the trigger events.

表 *8*:イベント トリガー

| Event | アラート グループ | Event Name | 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 | |

| Event | アラート グループ | Event Name | 説明 | Call Home メッセージ レベル |
|---|---|---|---|---|
| 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。<br>（注） アクティブ スーパーバイザが削除されると、スイッチ オーバーが発生します。このイベントの call home 通知は送信されません。 | 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 | |
| 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 |

| Event | アラート グループ | Event Name | 説明 | Call Home メッセージ レベル |
|---|---|---|---|---|
| インベントリ | インベントリおよび 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 |
| Test | 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 グループ ポート | SYSLOG_ALERT | ポート ファシリティに対応する syslog メッセージ。 | 2 |
| RMON | RMON | RMON_ALERT | RMON アラート トリガー メッセージ。 | 2 |

# Call Home メッセージ レベル

表 *9:* イベント カテゴリと実行されるコマンド

| Event Category | 説明 | 実行されるコマンド |
|---|---|---|
| システム<br>show module<br>show version<br>show tech-support platform<br>show tech-support sysmgr<br>show hardware<br>show sprom all | 装置の動作に必要なソフトウェア システムの障害によって生成されたイベント。 | **show tech-supportshow system redundancy status** |

| Event Category | 説明 | 実行されるコマンド |
|---|---|---|
| Environmental<br>show module<br>show version<br>show environment<br>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 moduleshow environment** |
| ラインカード ハードウェア<br>show module<br>show version<br>show tech-support platform<br>show tech-support sysmgr<br>show hardware<br>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<br>show module<br>show version<br>show tech-support platform<br>show tech-support sysmgr<br>show hardware<br>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** |
| インベントリ<br>show module<br>show version<br>show hardware<br>show inventory<br>show system uptime<br>show sprom all<br>show license usage | インベントリ 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、重大ではないイベントと見なされ、情報はステータスと資格設定に使用される | **show version** |
| Test<br>show module<br>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 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 （56 ページ）を参照）。

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

重大度の範囲は 0 ～ 9 で、9 の緊急度が最も高くなっています。各 syslog レベルには、表 10 : 重大度と syslog レベルのマッピング （64 ページ） に示すように、キーワードと対応する syslog レベルがあります。

（注） Call Home は、メッセージ テキストで Syslog メッセージ レベルを変更しません。The syslog message texts in the Call Home log appear as they are described in the *Cisco MDS 9000 Series System Messages* Reference.

（注） Call Home severity levels are not the same as system message logging severity levels (see the *Cisco MDS 9000 Series System Messages* Reference).

**表 *10* : 重大度と *syslog* レベルのマッピング**

| **Call Home** レベル | 使用されるキーワード | **Syslog** レベル | 説明 |
|---|---|---|---|
| Catastrophic (9) | **Catastrophic** | 該当なし | ネットワーク全体の破滅的な障害。 |
| Disaster (8) | **Disaster** | 該当なし | ネットワークに重大な影響が及びます。 |
| Fatal (7) | **Fatal** | 緊急（0） | システムが使用不可能な状態。 |
| Critical (6) | **Critical** | アラート（1） | クリティカルな状態、ただちに注意が必要。 |
| Major (5) | **Major** | 重要（2） | 重大な状態。 |
| Minor (4) | **Minor** | エラー（3） | 軽微な状態。 |
| Warning (3) | **Warning** | 警告（4） | 警告状態。 |
| Notify (2) | **Notification** | 通知（5） | 基本的な通知および情報メッセージです。他と関係しない、重要性の低い障害です。 |
| Normal (1) | **Normal** | 情報（6） | 標準状態に戻ることを示す標準イベントです。 |

| Call Home レベル | 使用されるキーワード | Syslog レベル | 説明 |
|---|---|---|---|
| Debug (0) | **Debugging** | デバッグ（7） | デバッグ メッセージ。 |

# メッセージの内容

スイッチ上で次の連絡先情報を設定できます。

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

表 11 : ショート テキスト メッセージ （65 ページ） 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 *11* : ショート テキスト メッセージ**

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

表 12 : 対処的イベント メッセージ フォーマット （66 ページ）、表 13 : インベントリ エラー メッセージのフォーマット （69 ページ）、および表 14 : ユーザーが生成したテスト メッセージのフォーマット （72 ページ） 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 *12 :* 対処的イベント メッセージ フォーマット

| データ項目（プレーンテキストと XML） | 説明（プレーンテキストと XML） | XML タグ（XML のみ） |
|---|---|---|
| Time stamp | ISO 時刻表記によるイベントの日付とタイムスタンプ：*YYYY-MM-DD*T*HH:MM:SS*。<br>（注） UTC からの時間帯または夏時間（DST）オフセットは、すでに適用済みです。T は、ハードコードされた時刻の区切りです。 | /mml/header/time - ch:EventTime |
| メッセージ名 | メッセージの名前。具体的なイベント名のリストはイベント トリガー （59ページ）に示されています。 | /mml/header/name |
| メッセージ タイプ | 「Call Home」指定。 | /mml/header/type - ch:Type |
| メッセージ グループ | 「reactive」指定。 | /mml/header/group |
| 重大度 | メッセージの重大度（表 10 : 重大度と syslog レベルのマッピング （64 ページ） を参照）。 | /mml/header/level - aml-block:Severity |
| 送信元 ID | ルーティングのための製品タイプ | /mml/header/source - ch:Series |
| デバイス ID | メッセージを生成するエンド デバイスの Unique Device Identifier（UDI）。メッセージがファブリック スイッチ専用でない場合、このフィールドは空白になります。Format is *type@Sid@seria* l, where:<br>• *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。<br>• *@* 区切り文字です。<br>• *Sid* is “C,” identifying the serial ID as a chassis serial number.<br>• *serial* は、Sid フィールドによって識別される番号です。<br>例：DS-C9509@C@12345678 | /mml/ header/deviceId |
| Customer ID | 任意のサポート サービスによって、連絡先情報またはその他の ID に使用される、オプションのユーザ設定可能フィールド。 | /mml/header/customerID - ch:CustomerId |
| 契約 ID | 任意のサポート サービスによって、連絡先情報またはその他の ID に使用される、オプションのユーザ設定可能フィールド。 | /mml/header/contractId - ch:ContractId> |

| データ項目（プレーンテキストと XML） | 説明（プレーンテキストと XML） | XML タグ（XML のみ） |
|---|---|---|
| サイト ID | シスコが提供したサイト ID または別のサポート サービスにとって意味のあるその他のデータに使用されるオプションのユーザ設定可能なフィールド | /mml/header/siterId - ch:SiteId |
| Server 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）。<br>Format is *type*@*Sid*@*serial* , where:<br>• *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。<br>• @ 区切り文字です。<br>• *Sid* is “C,” identifying the serial ID as a chassis serial number.<br>• *serial* は、Sid フィールドによって識別される番号です。<br>例：DS-C9509@C@12345678 | /mml/header/serverId - -blank- |
| メッセージの説明 | エラーを説明する短い文章。 | /mml/body/msgDesc - ch:MessageDescription |
| デバイス名 | イベントが発生するノード。これは、デバイスのホスト名です。 | /mml/body/sysName - ch:SystemInfo/Name |
| 担当者名 | イベント発生中のノードに関する問題の問い合わせ先の担当者名。 | /mml/body/sysContact - ch:SystemInfo/Contact |
| 連絡先 E メール | このユニットの連絡先である人物の電子メール アドレス。 | /mml/body/sysContacte-mail - ch:SystemInfo/Contacte-mail |
| 連絡先電話番号 | このユニットの連絡先である人物の電話番号 | /mml/body/sysContactPhoneNumber - ch:SystemInfo/ContactPhoneNumber |
| 住所 | このユニットに関連した RMA 部品の送付先住所を格納しているオプションのフィールド。 | /mml/body/sysStreetAddress - ch:SystemInfo/StreetAddress |
| Model name | スイッチのモデル名。これは、製品シリーズ名の一部である固有モデルです。 | /mml/body/chassis/name - rme:Chassis/Model |
| シリアル番号 | ユニットのシャーシのシリアル番号 | /mml/body/chassis/serialNo - rme:Chassis/SerialNumber |
| シャーシの部品番号 | シャーシの最上アセンブリ番号 | /mml/body/fru/partNo - rme:chassis/Card/PartNumber |

| データ項目（プレーンテキストと XML） | 説明（プレーンテキストと XML） | XML タグ（XML のみ） |
|---|---|---|
| シャーシのハードウェア バージョン | シャーシのハードウェア バージョン。 | /mml/body/chassis/hwVersion - rme:Chassis/HardwareVersion |
| スーパーバイザ モジュール ソフトウェア バージョン | トップ レベル ソフトウェア バージョン。 | /mml/body/fru/swVersion - rme:chassis/Card/SoftwareIdentity |
| 影響のある FRU の名前 | イベント メッセージを生成する、影響のある FRU の名前。 | /mml/body/fru/name - rme:chassis/Card/Model |
| 影響のある FRU のシリアル番号 | 影響のある FRU のシリアル番号。 | /mml/body/fru/serialNo - rme:chassis/Card/SerialNumber |
| 影響のある FRU の製品番号 | 影響のある FRU の製品番号。 | /mml/body/fru/partNo - rme:chassis/Card/PartNumber |
| FRU スロット | イベント メッセージを生成している FRU のスロット番号。 | /mml/body/fru/slot - rme:chassis/Card/LocationWithinContainer |
| FRU ハードウェア バージョン | 影響のある FRU のハードウェア バージョン。 | /mml/body/fru/hwVersion - rme:chassis/Card/SoftwareIdentity |
| FRU ソフトウェア バージョン | 影響のある FRU 上で動作しているソフトウェア バージョン。 | /mml/body/fru/swVersion - rme:chassis/Card/SoftwareIdentity |
| コマンド出力名 | 実行されたコマンドの正確な名前。 | /mml/attachments/attachment/name - aml-block:Attachment/Name |
| 添付タイプ | コマンド出力を指定します。 | /mml/attachments/attachment/type - aml-block:Attachment type |
| MIME タイプ | 通常は、テキスト、プレーン、符号化タイプのいずれか。 | /mml/attachments/attachment/mime - aml-block:Attachment/Data encoding |
| コマンド出力テキスト | 表 9 : イベント カテゴリと実行されるコマンド （62 ページ） を自動的に実行するコマンドの出力 | /mml/attachments/attachment/atdata - aml-block:Attachment/Data |

表 *13:* インベントリ 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） |
|---|---|---|
| Time stamp | ISO 時刻表記によるイベントの日付とタイムスタンプ：*YYYY-MM-DD*T*HH:MM:SS*。<br>（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（59 ページ） を参照してください。 | /mml/header/name |
| メッセージ タイプ | 「Inventory Update」指定。 | /mml/header/type - ch-inv:Type |
| メッセージ グループ | 「proactive」指定。 | /mml/header/group |
| 重大度 | インベントリ イベントの重大度はレベル 2 です（表 10 : 重大度と syslog レベルのマッピング （64 ページ） 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」指定。 | /mml/header/source - ch-inv:Series |
| デバイス ID | メッセージを生成するエンドデバイスの Unique Device Identifier（UDI）。メッセージがファブリック スイッチ専用でない場合、このフィールドは空白になります。Format is *type*@*Sid*@*seria* l, where:<br>• *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。<br>• @ 区切り文字です。<br>• *Sid* is “C,” identifying the serial ID as a chassis serial number.<br>• *serial* は、Sid フィールドによって識別される番号です。<br>例：DS-C9509@C@12345678 | /mml/ header /deviceId |
| Customer ID | 任意のサポート サービスによって、連絡先情報またはその他の ID に使用される、オプションのユーザ設定可能フィールド。 | /mml/header/customerID - ch-inv:CustomerId |

| 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） |
|---|---|---|
| 契約 ID | 任意のサポート サービスによって、連絡先情報またはその他の ID に使用される、オプションのユーザ設定可能フィールド。 | /mml/header/contractId - ch-inv:ContractId> |
| サイト ID | シスコが提供するサイト ID で使用されるオプションのユーザ設定可能フィールドか、他のサポート サービスにとって意味のあるその他のデータ。 | /mml/header/siterId - ch-inv:SiteId |
| Server 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）。<br>Format is *type*@*Sid*@*seria* l, where:<br>• *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。<br>• @ 区切り文字です。<br>• *Sid* is “C,” identifying the serial ID as a chassis serial number.<br>• *serial* は、Sid フィールドによって識別される番号です。<br>例：DS-C9509@C@12345678 | /mml/header/serverId - -blank- |
| メッセージの説明 | エラーを説明する短い文章。 | /mml/body/msgDesc - ch-inv:MessageDescription |
| デバイス名 | イベントが発生するノード。 | /mml/body/sysName - ch-inv:SystemInfo/Name |
| 担当者名 | イベント発生中のノードに関する問題の問い合わせ先の担当者名。 | /mml/body/sysContact - ch-inv:SystemInfo/Contact |
| 連絡先 E メール | このユニットの連絡先である人物の電子メール アドレス。 | /mml/body/sysContacte-mail - ch-inv:SystemInfo/Contacte-mail |
| 連絡先電話番号 | このユニットの連絡先である人物の電話番号 | /mml/body/sysContactPhoneNumber - ch-inv:SystemInfo/ContactPhoneNumber |
| 住所 | このユニットに関連した RMA 部品の送付先住所を格納しているオプションのフィールド。 | /mml/body/sysStreetAddress - ch-inv:SystemInfo/StreetAddress |
| Model name | ユニットのモデル名。これは、製品シリーズ名の一部である固有モデルです。 | /mml/body/chassis/name - rme:Chassis/Model |

| 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） |
|---|---|---|
| シリアル番号 | ユニットのシャーシのシリアル番号 | /mml/body/chassis/serialNo - rme:Chassis/SerialNumber |
| シャーシの部品番号 | シャーシの最上アセンブリ番号 | /mml/body/fru/partNo - rme:chassis/Card/PartNumber |
| シャーシのハードウェア バージョン | シャーシのハードウェア バージョン。 | /mml/body/fru/hwVersion - rme:chassis/Card/SoftwareIdentity |
| スーパーバイザ モジュール ソフトウェア バージョン | トップ レベル ソフトウェア バージョン。 | /mml/body/fru/swVersion - rme:chassis/Card/SoftwareIdentity |
| FRU name | イベント メッセージを生成する、影響のある FRU の名前。 | /mml/body/fru/name - rme:chassis/Card/Model |
| FRU s/n | FRU のシリアル番号。 | /mml/body/fru/serialNo - rme:chassis/Card/SerialNumber |
| FRU 製品番号 | FRU の製品番号。 | /mml/body/fru/partNo - rme:chassis/Card/PartNumber |
| FRU スロット | FRU のスロット番号。 | /mml/body/fru/slot - rme:chassis/Card/LocationWithinContainer |
| FRU ハードウェア バージョン | FRU のハードウェア バージョン。 | /mml/body/fru/hwVersion - rme:chassis/Card/SoftwareIdentity |
| FRU ソフトウェア バージョン | FRU 上で動作しているソフトウェア バージョン。 | /mml/body/fru/swVersion - rme:chassis/Card/SoftwareIdentity |
| コマンド出力名 | 実行されたコマンドの正確な名前。 | /mml/attachments/attachment/name - aml-block:Attachment/Name |
| 添付タイプ | コマンド出力を指定します。 | /mml/attachments/attachment/type - aml-block:Attachment type |
| 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 （59 ページ）を参照）。 | /mml/attachments/attachment/atdata - aml-block:Attachment/Data |

表 *14* : ユーザーが生成したテスト 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） |
|---|---|---|
| Time stamp | ISO 時刻表記によるイベントの日付とタイムスタンプ：*YYYY-MM-DD*T*HH:MM:SS*。<br>（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 （59 ページ）を参照してください。 | /mml/header/name |
| メッセージ タイプ | 「Test Call Home」指定。 | /mml/header/type - ch:Type |
| メッセージ グループ | 受信側の Call Home 処理アプリケーションではこのフィールドを無視する必要がありますが、「proactive」または「reactive」を入力できます。 | /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 10 : 重大度と syslog レベルのマッピング （64 ページ） を参照）。 | /mml/header/level - aml-block:Severity |
| 送信元 ID | ルーティングのための製品タイプ | /mml/header/source - ch:Series |
| デバイス ID | メッセージを生成するエンド デバイスの Unique Device Identifier（UDI）。メッセージがファブリック スイッチに固有のものでない場合、このフィールドは空です。Format is *type@Sid@seria* l, where:<br>• *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。<br>• @ は区切り文字です。<br>• *Sid* is “C” identifying the serial ID as a chassis serial number.<br>• *serial* は、Sid フィールドによって識別される番号です。<br>例：DS-C9509@C@12345678 | /mml/ header /deviceId |
| Customer ID | 任意のサポート サービスによって、連絡先情報またはその他の ID に使用される、オプションのユーザ設定可能フィールド。 | /mml/header/customerID - ch:CustomerId |
| 契約 ID | 任意のサポート サービスによって、連絡先情報またはその他の ID に使用される、オプションのユーザ設定可能フィールド。 | /mml/header/contractId - ch:ContractId |

| 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） |
|---|---|---|
| サイト ID | シスコが提供したサイト ID または別のサポート サービスにとって意味のあるその他のデータに使用されるオプションのユーザ設定可能なフィールド | /mml/header/siterId - ch:SiteId |
| Server 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）。<br>Format is *type@Sid@seria* l, where:<br>• *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。<br>• @ は区切り文字です。<br>• *Sid* is “C” identifying the serial ID as a chassis serial number.<br>• *serial* は、[Sid] フィールドによって特定される数字。<br>例：「DS-C9509@C@12345678 | /mml/header/serverId - -blank- |
| メッセージの説明 | エラーを説明する短い文章。 | /mml/body/msgDesc - ch:MessageDescription |
| デバイス名 | イベントが発生したスイッチ。 | /mml/body/sysName - ch:SystemInfo/Name |
| 担当者名 | イベント発生中のノードに関する問題の問い合わせ先の担当者名。 | /mml/body/sysContact - ch:SystemInfo/Contact |
| 連絡先 E メール | このユニットの連絡先である人物の電子メールアドレス。 | /mml/body/sysContacte-mail - ch:SystemInfo/Contacte-mail |
| 連絡先電話番号 | このユニットの連絡先である人物の電話番号 | /mml/body/sysContactPhoneNumber - ch:SystemInfo/ContactPhoneNumber |
| 住所 | このユニットに関連した RMA 部品の送付先住所を格納しているオプションのフィールド。 | /mml/body/sysStreetAddress - ch:SystemInfo/StreetAddress |
| Model name | スイッチのモデル名。これは、製品シリーズ名の一部である固有モデルです。 | /mml/body/chassis/name - rme:Chassis/Model |
| シリアル番号 | ユニットのシャーシのシリアル番号 | /mml/body/chassis/serialNo - rme:Chassis/SerialNumber |
| シャーシの部品番号 | シャーシの最上アセンブリ番号例：800-xxx-xxxx | /mml/body/fru/partNo - rme:chassis/Card/PartNumber |
| コマンド出力テキスト | イベント カテゴリに従って自動的に実行されるコマンドの出力（表 9 : イベント カテゴリと実行されるコマンド （62 ページ） を参照）。 | /mml/attachments/attachment/atdata - aml-block:Attachment/Data |

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

# 注意事項と制約事項

## Call Home データベースのマージに関する注意事項

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

- マージされたデータベースには次の情報が格納されることに注意してください。
  - マージプロトコルに参加する、上位スイッチと下位スイッチのすべての宛先プロファイルのスーパーセット。
  - 宛先プロファイルの E メール アドレスとアラート グループ。
  - マージ前に上位スイッチ内に存在した、スイッチからのその他の設定情報（メッセージ スロットリング、定期的インベントリなど）。

概念の詳細については、CFS 結合のサポート （10 ページ）を参照してください。

## Call Home の設定に関する注意事項

Call Home を設定する場合は、次の注意事項に従ってください。

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

- Cisco MDS 9000 シリーズ スイッチと Cisco Nexus 5000 シリーズ スイッチは、電子メール サーバへの IP 接続が確立されている必要があります。
- Cisco Smart Call Home を使用する場合、設定しようとしているデバイスが、アクティブ サービス契約の対象になっている必要があります。

# デフォルト設定

表 15 : Call Home のデフォルト設定 （75 ページ） に Call Home のデフォルト設定の一覧を示します。

**表 *15 : Call Home* のデフォルト設定**

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

# Call Home の設定

## Call Home を設定するためのタスク フロー

次の手順を実行して、Call Home を設定します。

### 手順

**ステップ 1** 連絡先情報を設定します。

**ステップ 2** Call Home をイネーブルまたはディセーブルにします。

**ステップ 3** 宛先プロファイルを設定します。

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

**ステップ 5** E メール オプションを設定します。

**ステップ 6** Call Home メッセージをテストします。

## 連絡先情報の設定

スイッチプライオリティは、ファブリック内の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。

連絡先情報を割り当てるには、次の手順を実行します。

### 始める前に

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。

### 手順

**ステップ 1** コンフィギュレーション モードに入ります。

switch# **configure terminal**

**ステップ 2** SNMP 連絡先名を設定します。

switch(config)# **snmp-server contact personname@companyname.com**

**ステップ 3** Call Home 設定サブモードに入ります。

```
switch(config)# callhome
switch(config-callhome)#
```

**ステップ 4** 顧客のメール アドレスを割り当てます。最大 128 文字の英数字を E メール アドレス形式で指定できます:

```
switch(config-callhome)# e-mail-contact username@company.com
```

（注） 任意の有効な E メール アドレスを使用できます。スペースは使用できません。

**ステップ 5** 顧客の電話番号を割り当てます。最大 20 文字の英数字を国際形式で指定できます:

```
switch(config-callhome)# phone-contact +1-800-123-4567
```

（注） スペースは使用できません。数字の前に、必ず + プレフィックスを使用してください。

**ステップ 6** 機器がある顧客の住所を割り当てます。最大 256 文字の英数字を自由形式で指定できます:

```
switch(config-callhome)# streetaddress 1234 Picaboo Street, Any city, Any state, 12345
```

**ステップ 7** 0（最高優先度）～ 7（最低優先度）でスイッチのプライオリティを割り当てます。

```
switch(config-callhome)# switch-priority 0
```

ヒント 階層型の管理構造を作成するには、このフィールドを使用します。

**ステップ 8** （任意） 顧客 ID を識別します。

```
switch(config-callhome)# customer-id Customer1234
```

最大 256 文字の英数字を自由形式で指定できます。

**ステップ 9** （任意） 顧客サイト ID を識別します。

```
switch(config-callhome)# site-id Site1ManhattanNY
```

最大 256 文字の英数字を自由形式で指定できます。

**ステップ 10** スイッチの顧客 ID を割り当てます。

```
switch(config-callhome)# contract-id Company1234
```

最大 64 文字の英数字を自由形式で指定できます。

# DCNM SAN を使用した連絡先情報の設定

DCNM SAN 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。

手順

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

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

ステップ 2 In Device Manager, click **Admin** > **Events** > **Call Home**.

ステップ 3 Click the **General** tab, then assign contact information and enable the Call Home feature. 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 Click the **Destination(s)** tab to configure the destination e-mail addresses for Call Home notifications. 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。

1. [Create] タブをクリックして、新しい宛先を作成します。[create destination] ウィンドウが表示されます。
2. 宛先のプロファイル名、ID、およびタイプを入力します。[Type] フィールドでは、[email] または [http] を選択できます。

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

   [http] を選択した場合、[HttpUrl] フィールドに HTTP URL を入力します。[EmailAddress] フィールドはディセーブルになります。
3. [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 Click the **e-mail Setup** tab to identify the SMTP server. 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 In DCNM-SAN, click the **Apply Changes** icon. Device Manager で、[Apply] をクリックします。

# Call Home 機能のイネーブル化

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

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。

手順

ステップ 1 コンフィギュレーション モードに入ります。

switch# **configure terminal**

**ステップ 2** Call Home 設定サブモードに入ります:

switch(config)# **callhome**

**ステップ 3** Call Home 機能を有効にします。

switch(config-callhome)# **enable**

Call Home が正常に有効になりました。

**ステップ 4** （任意） Call Home 機能を無効にします。

switch(config-callhome)# **disable**

（注） Call Home が無効になっている場合でも、各 Call Home のイベントの基本情報は送信されます。

Call Home の機能を無効にすると、すべての入力イベントが無視されます。

# DCNM SAN を使用して Call Home の機能を有効化

To enable the Call Home function using DCNM-SAN, follow these steps:

**手順**

**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** **Events** を展開して、物理属性ペインの **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。

**ステップ 4** [information] ペインでスイッチを選択します。

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

**ステップ 6** [Apply Changes] アイコンをクリックします。

# 宛先プロファイルの設定

宛先プロファイルには、アラート通知に必要な配信情報が入っています。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。次の属性を宛先プロファイルに設定できます。

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

- 宛先アドレス：アラートの送信先となる実際のアドレス（トランスポート メカニズムに関係します）。
- メッセージ フォーマット：アラート送信に使用されるメッセージ フォーマット（フル テキスト、ショート テキスト、または XML）。

（注） Cisco Smart Call Home サービスを使用する場合、XML 宛先プロファイルが必要です。

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。

（注） この手順の手順 3、4、および 5 をスキップするか、任意の順序で設定できます。

### 始める前に

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

### 手順

**ステップ 1** コンフィギュレーション モードに入ります。

switch# **configure terminal**

**ステップ 2** Call Home 設定サブモードに入ります。

switch(config)# **callhome**

switch(config-callhome)#

**ステップ 3** 電子メール アドレスや、事前に定義された全 txt 宛先プロファイルの宛先メッセージの最大サイズを設定します。

switch(config-callhome)# **destination-profile full-txt-destination** {**e-mail-addr** *email-address* | **message-size** *msg-size-in-bytes*}

宛先プロファイルのメール アドレスによりフルテキスト フォーマットでメッセージを受信します。フルテキスト形式では、障害の完全かつ詳細な説明を提供します。

**ヒント** テキスト サイズの制限がない標準電子メール アドレスを使用します。

指定できる範囲は 0 ～ 1,000,000 バイトです。デフォルト値は 500,000 です。値 0 は、任意のサイズのメッセージを送信できることを意味します。

（注） メッセージ内の個々の各添付ファイルの最大サイズは、250,000バイトです。添付ファイルがこの最大サイズを超える場合、添付ファイルのキャプチャ出力が省略されます。

**ステップ 4** 電子メールアドレスや、事前に定義されたショート txt 宛先プロファイルの宛先メッセージの最大サイズを設定します。

switch(config-callhome)# **destination-profile short-txt-destination** {**e-mail-addr** *email-address* | **message-size** *msg-size-in-bytes*}

この宛先プロファイルのメール アドレスにより、ショート テキスト形式でメッセージを受信します。この形式は、Call Home メッセージ内の障害に関する基本的な説明を提供します。

**ヒント** このオプションのページャに関連する電子メールアドレスを使用します。

指定できる範囲は 0 ～ 1,000,000 バイトです。デフォルト値は 4000 です。値 0 は、任意のサイズのメッセージを送信できることを意味します。

（注） メッセージ内の個々の各添付ファイルの最大サイズは、250,000バイトです。添付ファイルがこの最大サイズを超える場合、添付ファイルのキャプチャ出力が省略されます。

**ステップ 5** 事前に定義された XML 接続先プロファイルに、電子メールアドレスまたは最大接続先のメッセージのサイズを設定します。

switch(config-callhome)# **destination-profile XML-destination** {**e-mail-addr** *email-address* | **message-size** *msg-size-in-bytes*}

この宛先プロファイルの電子メール アドレスは、メッセージを XML フォーマットで受け取ります。この形式は、Cisco Systems TAC サポートとの互換性がある情報を提供します。

**ヒント** メッセージサイズが大きいため、この接続先のプロファイルにページャに関連する電子メール アドレスを追加しないでください。

指定できる範囲は 0 ～ 1,000,000 バイトです。デフォルト値は 500,000 です。値 0 は、任意のサイズのメッセージを送信できることを意味します。

（注） メッセージ内の個々の各添付ファイルの最大サイズは、250,000バイトです。添付ファイルがこの最大サイズを超える場合、添付ファイルのキャプチャ出力が省略されます。

## DCNM SAN を使用して事前に定義された接続先プロファイルの設定

DCNM-SAN を使用して事前定義された宛先プロファイル 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。

手順

**ステップ 1** Expand **Events** and select **Call Home** in the Physical Attributes pane.

The **Destination** tab is disabled until you click the **Profiles** tab. [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** Click the **Profiles** tab in the Information pane.

複数のスイッチに対する Call Home プロファイルが表示されます。

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

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

**ステップ 5** Click **Apply Changes** icon to create this profile on the selected switches.

## 新しい宛先プロファイルの設定

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。

（注） この手順の手順 4、5、6 は任意の順序でスキップまたは設定できます。

手順

**ステップ 1** コンフィギュレーション モードに入ります。

switch# **configure terminal**

**ステップ 2** Call Home 設定サブモードに入ります。

switch(config)# **callhome**

**ステップ 3** テストと呼ばれる新しい接続先のプロファイルを設定します。

switch(config-callhome)# **destination-profile test**

**ステップ 4** デフォルトのXML形式で送信されるユーザー定義の接続先プロファイル（テスト）の電子メールアドレスを設定します。

switch(config-callhome)# **destination-profile test e-mail-addr** *email-address*

**ステップ 5** デフォルトの XML 形式で送信されるユーザー定義の接続先のプロファイル（テスト）の宛先メール アドレスの最大メッセージ サイズを設定します。

switch(config-callhome)# **destination-profile test message-size** *msg-size*

指定できる範囲は 0 ～ 1,000,000 バイトです。デフォルト値は 500,000 です。値 0 は、任意のサイズのメッセージを送信できることを意味します。

**ステップ 6** ユーザー定義の宛先プロファイル（テストの）メッセージ形式を、フルテキストまたはショート テキスト形式に設定します。

switch(config-callhome)# **destination-profile test format** {**full-txt** | **short-txt**}

## DCNM SAN を使用して、新しい接続先プロファイルの設定

To configure a new destination-profile (and related parameters) using DCNM-SAN, follow these steps:

**手順**

**ステップ 1** Expand **Events** and select **Call Home** in the Physical Attributes pane.

（注） The **Destination** tab is disabled until you click the **Profiles** tab. [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** Click the **Profiles** tab in the Information pane.

複数のスイッチに対する Call Home プロファイルが表示されます。

**ステップ 3** Click the **Create Row** icon to add a new profile.

**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。You can select **email**, **http** or **emailandhttp**.

**ステップ 7** Click **Create** to create this profile on the selected switches.

# アラート グループの関連付け

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

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

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。

### 始める前に

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

### 手順

**ステップ 1** コンフィギュレーション モードに入ります。

switch# **configure terminal**

**ステップ 2** Call Home 設定サブモードに入ります。

switch(config)# **callhome**

switch(config-callhome)#

**ステップ 3** （任意）ユーザー定義の宛先プロファイル（test1）または事前定義のショートテキスト宛先プロファイルを設定して、すべてのユーザー生成 Call Home テストの通知を受信します。

switch(config-callhome)# **destination-profile** {*test1* | **short-txt-destination**} **alert-group** *test*

**ステップ 4** （任意） ユーザー定義の宛先プロファイル（test1）を設定してすべてのイベントの Call Home 通知を受信するか、事前定義のショートテキスト宛先プロファイルを設定してデフォルトイベントの Call Home の通知を受信します。

switch(config-callhome)# **destination-profile** {*test1* | **short-txt-destination**} **alert-group all**

**ステップ 5** （任意）ユーザー定義の宛先プロファイル（test1）または事前定義のショートテキスト宛先プロファイルを設定して、Cisco TAC または自動通知のみイベントの Call Home 通知を受信します。

switch(config-callhome)# **destination-profile** {*test1* | **xml-destination**} **alert-group Cisco-TAC**

**ステップ 6** （任意）ユーザー定義の宛先プロファイル（test1）または事前定義のショートテキスト宛先プロファイルを設定して、電源、ファン、温度関連のイベントの Call Home 通知を受信します。

switch(config-callhome)# **destination-profile** {*test1* | **short-txt-destination**} **alert-group environmental**

**ステップ 7** （任意）ユーザー定義の宛先プロファイル（test1）または事前定義のショートテキスト宛先プロファイルを設定して、インベントリ ステータス イベントの Call Home 通知を受信します。

switch(config-callhome)# **destination-profile** {*test1* | **short-txt-destination**} **alert-group inventory**

**ステップ 8** （任意）ユーザー定義の宛先プロファイル（test1）または事前定義のショートテキスト宛先プロファイルを設定して、モジュール関連イベントの Call Home 通知を受信します。

switch(config-callhome)# **destination-profile** {*test1* | **short-txt-destination**} **alert-group linecard-hardware**

**ステップ 9** （任意）ユーザー定義の宛先プロファイル（test1）または事前定義のショートテキスト宛先プロファイルを設定して、スーパーバイザ関連の Call Home 通知を受信します。

switch(config-callhome)# **destination-profile** {*test1* | **short-txt-destination**} **alert-group supervisor-hardware**

**ステップ 10** （任意）ユーザー定義の宛先プロファイル（test1）または事前定義のショートテキスト宛先プロファイルを設定して、ソフトウェア関連イベントの Call Home 通知を受信します。

switch(config-callhome)# **destination-profile** {*test1* | **short-txt-destination**} **alert-group system**

# DCNM SAN を使用したアラート グループの関連付け

DCNM-SAN 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。

**手順**

**ステップ 1** Expand **Events** and select **Call Home** in the Physical Attributes pane.

**ステップ 2** Click the **Profiles** tab in the Information pane.

複数のスイッチに対する Call Home プロファイルが表示されます。

**ステップ 3** Click the **Alert Groups** column in the row for the profile you want to associate.

[alert groups] ドロップダウン メニューが表示されます。

**ステップ 4** 関連付けるアラート グループをクリックして選択します。

**ステップ 5** そのアラート グループの横にチェックが表示されます。

選択を解除してチェックを外すには、再度クリックします。

**ステップ 6** **Apply Changes**アイコンをクリックします。

# アラート グループ メッセージのカスタマイズ

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。

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。

始める前に

- 1 つのアラート グループにユーザ定義の show コマンドを 5 つまで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。
- 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。

手順

**ステップ 1** コンフィギュレーション モードに入ります。

switch# **configure terminal**

**ステップ 2** Call Home 設定サブモードに入ります。

switch(config)# **callhome**

switch(config-callhome)#

**ステップ 3** Configure a user-defined **show** command for an alert group license:

switch(config-callhome)# **alert-group license user-def-cmd show license usage**

（注） Only valid **show** commands are accepted.

**ステップ 4** （任意） Remove the user-defined **show** command from the alert group:

switch(config-callhome)# **no alert-group license user-def-cmd show license usage**

# Customizing Alert Group Messages Using DCNM-SAN

To customize Call Home alert group messages using DCNM-SAN, follow these steps:

手順

**ステップ 1** Expand **Events** and select **Call Home** in the Physical Attributes pane.

**ステップ 2** Click the **User Defined Command** tab in the Information pane.

ユーザ定義コマンドの情報が表示されます。

**ステップ 3** **Create Row**アイコンをクリックします。

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

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

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

**ステップ 7** Enter the CLI **show** command in the **CLI Command** field.

**ステップ 8** **Create** をクリックします。

**ステップ 9** Repeat Step 3 through Step 7 for each command you want to associate with the profile.

**ステップ 10** Click **Close** to close the dialog box.

## Call Home メッセージ レベルの設定

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。

### 始める前に

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

### 手順

**ステップ 1** コンフィギュレーション モードに入ります。

switch# **configure terminal**

**ステップ 2** Call Home 設定サブモードに入ります。

switch(config)# **callhome**

**ステップ 3** （任意） 上記のユーザー定義プロファイル（test1）のメッセージ レベルの緊急性を 5（レベル）以上に設定します。

switch(config-callhome)# **destination-profile** *test* **message-level** *level*

**ステップ 4** 以前に設定されている緊急性レベルを削除し、デフォルトの 0 に戻します（すべてのメッセージが送信されます）。

switch(config-callhome)# **no destination-profile** *oldtest* **message-level** *level*

## Syslog ベースのアラートの設定

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。

### 手順

**ステップ 1** コンフィギュレーション モードに入ります。

switch# **configure terminal**

**ステップ 2** Call Home 設定サブモードに入ります。

```
switch(config)# callhome
switch(config-callhome)#
```

**ステップ 3** Call Home の通知に対応するポート ファシリティの syslog メッセージを受信する事前に定義された接続先のプロファイル (short txt 宛先) の設定します。

```
switch(config-callhome)# destination-profile short-txt-destination alert-group syslog-group-port
```

**ステップ 4** （任意） Call Home の重大度レベル 5 以上の重大度レベルにマップの syslog メッセージの Call Home のメッセージの送信に事前に定義された宛先-プロファイル (short txt 宛先) の設定します。

```
switch(config-callhome)# destination-profile short-txt-destination message-level level
```

デフォルトでは、メッセージ レベル 0 (すべての syslog メッセージ) です。

## DCNM SAN を使用して Syslog ベース アラートの設定

DCNM-SAN 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。

### 手順

**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** Expand **Events** and select **Call Home** in the Physical Attributes pane.

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

**ステップ 3** **Profiles** タブをクリックします。

Call Home プロファイルが表示されます。

**ステップ 4** **Create Row**アイコンをクリックします。

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

**ステップ 5** アラートを送信するスイッチを選択します。

**ステップ 6** プロファイル名を [Name] フィールドに入力します。

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

**ステップ 8** Check the **syslogGroupPort** check box in the AlertGroups section.

**ステップ 9** Click **Create** to create the profile for the syslog-based alerts.

**ステップ 10** ダイアログボックスを閉じます。

## RMON アラートの設定

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。

手順

**ステップ 1** コンフィギュレーション モードに入ります。

switch# **config t**

**ステップ 2** Call Home 設定サブモードに入ります:

switch(config)# **callhome**

**ステップ 3** （任意） 設定済みの RMON メッセージの Call Home 通知を送信するため、宛先メッセージ プロファイル (rmon_group) を設定します。

switch(config-callhome)# **destination-profile**

## DCNM SAN を使用した RMON アラートの設定

DCNM-SAN 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。

手順

**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** Expand **Events** and select **Call Home** in the Physical Attributes pane.

[情報] ペインに Call Home 情報が表示されます。

**ステップ 3** **Profiles** タブをクリックします。

Call Home プロファイルが表示されます。

**ステップ 4** **Create Row** アイコンをクリックします。

[Call Home プロファイル] 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** Check the **RMON** check box in the AlertGroups section.

**ステップ 9** Click **Create** to create the profile for the RMON-based alerts.

**ステップ 10** ダイアログボックスを閉じます。

# イベント トラップ通知の設定

Call Homeイベント通知トラップを設定するには（Call Homeの定期的なメッセージを除く）、次の手順に従います。

手順

**ステップ 1** コンフィギュレーション モードに入ります。

switch# **configure terminal**

**ステップ 2** Call Home 設定サブモードに入ります:

switch(config)# **callhome**

**ステップ 3** Call Home の SNMP 通知トラップを有効にします。

switch(config-callhome)# **snmp-server enable**

# 一般的な電子メール オプションの設定

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

一般的な電子メール オプションを設定するには、次の手順を実行します。

手順

**ステップ 1** コンフィギュレーション モードに入ります。

switch# **configure terminal**

**ステップ 2** Call Home 設定サブモードに入ります:

switch(config)# **callhome**

**ステップ 3** E メール アドレスを設定します:

switch(config-callhome)# **transport**

**ステップ 4** すべての応答が送信される返信用メール アドレスを設定します。

switch(config-callhome)# **transport**

# DCNM-SAN を使用した一般的な E メール オプションの設定

DCNM-SAN 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。

手順

**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** Expand **Events** and select **Call Home** in the Physical Attributes pane.

[情報] ペインに Call Home 情報が表示されます。

**ステップ 3** **e-mail Setup** タブをクリックします。

**ステップ 4** [Information] ペインでスイッチを選択します。

**ステップ 5** 一般的な E メール情報を入力します。

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

**ステップ 7** Click the **Apply Changes** icon to update the e-mail options.

# HTTPS サポートの設定

HTTPS の URL アドレスを持つ、事前に定義されたまたはユーザ定義の接続先プロファイルを設定できます。

任意の接続先プロファイルの HTTPS の URL アドレスを設定するには、次の手順に従います。

手順

**ステップ 1** コンフィギュレーション モードに入ります。

switch# **configure terminal**

**ステップ 2** Call Home 設定サブモードに入ります:

switch(config)# **callhome**

**ステップ 3** （任意） HTTPS の URL アドレスを持つ定義済みの全 txt 宛先プロファイルを設定します。

switch(config-callhome)# **destination-profile full-txt-destination http**

全 txt 形式の Call Home のメッセージは、設定されている HTTPS の URL アドレスにアップロードされます。

**ステップ 4** （任意） HTTPS の URL アドレスを持つ、事前に定義された ciscotac-1 プロファイルを設定します。

switch(config-callhome)# **destination-profile CiscoTAC-1 http**

XML 形式での Call Home のメッセージは、設定されている HTTPS の URL アドレスにアップロードされます。

**ステップ 5** （任意） HTTPS の URL アドレスを持つユーザ定義の接続先プロファイルを設定します。

switch(config-callhome)# **destination-profile test1 http**

設定されている形式の Call Home のメッセージは、設定されている HTTPS の URL アドレスにアップロードされます。

# 転送方法を有効化または無効化

特定の転送方式を有効または無効するように、定義済みまたはユーザ定義の宛先プロファイルを設定できます。転送方式は HTTP および E メールです。

宛先プロファイルの転送方式をイネーブルまたはディセーブルにする手順は、次のとおりです。

**手順**

**ステップ 1** コンフィギュレーション モードに入ります。

switch# **configure terminal**

**ステップ 2** Call Home 設定サブモードに入ります:

switch(config)# **callhome**

**ステップ 3** （任意） 定義済みの宛先プロファイル CiscoTAC-1 を HTTP 転送方式に対して有効にします:

switch(config-callhome)# **destination-profile CiscoTAC-1 transport-method http**

（注） ユーザ定義宛先プロファイルでは、E メールがデフォルトです。片方または両方の転送メカニズムをイネーブルにできます。両方の方法をディセーブルにすると、E メールがイネーブルになります。

**ステップ 4** （任意） 定義済みの宛先プロファイル CiscoTAC-1 を E メール転送方式に対して無効にします:

switch(config-callhome)# **no destination-profile CiscoTAC-1 transport-method email**

**ステップ 5** （任意） 定義済みのフルテキスト宛先プロファイルを HTTP 転送方式に対して有効にします:

switch(config-callhome)# **destination-profile full-txt transport-method http**

# HTTP プロキシ サーバの設定

Cisco NX-OS Release 5.2 以降では、HTTP プロキシ サーバを介して HTTP メッセージを送信するように Smart Call Home を設定できます。HTTP プロキシ サーバを設定しない場合、Smart Call Home は、Cisco Transport Gateway（TG）に HTTP メッセージを直接送信します。

HTTP プロキシ サーバを設定するには、次の手順を実行します。

手順

**ステップ 1** コンフィギュレーション モードに入ります。

switch# **configure terminal**

**ステップ 2** Call Home 設定サブモードに入ります:

switch(config)# **callhome**

**ステップ 3** HTTP プロキシ サーバのドメイン ネーム サーバ（DNS）の名前、IPv4 アドレス、または IPv6 アドレスを設定します。

switch(config-callhome)# **transport http proxy server 192.0.2.1**

任意でポート番号を設定します。ポート範囲は 1 ～ 65535 です。デフォルト ポート番号は、8080 です。

**ステップ 4** Smart Call Home で、HTTP プロキシ サーバ経由ですべての HTTP メッセージを送信できるようにします。

switch(config-callhome)# **transport http proxy enable**

（注） プロキシ サーバ アドレスが設定された後にだけ、このコマンドを実行できます。

**ステップ 5** （任意） Smart Call Home に対する転送関係の設定を表示します:

switch(config-callhome)# **show callhome transport**

（注） フル テキストの宛先と XML のデフォルト値は 1 MB です。

# DCNM-SAN を使用して HTTP プロキシ サーバを設定する

DCNM-SAN を使用して Call Home HTTP プロキシ サーバを設定するには、次の手順を実行します。

手順

**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** Expand **Events**, select **Call Home**, and **HTTP Proxy Server** in the Physical Attributes pane.
[情報] ペインに Call Home HTTP プロキシ サーバの情報が表示されます。

**ステップ 3** **Address Type** タブをクリックします。
アドレス タイプのオプションが表示されます。

**ステップ 4** Click the **Address** tab and enter the address of the HTTP proxy server.

**ステップ 5** Click the **Port** tab and enter a integer number to specify the port of the HTTP proxy server.

**ステップ 6** Check the **Enable** check box to enable the HTTP proxy configured for Call Home.

**ステップ 7** （任意） Set an empty value in the **Address** tab to delete the HTTP proxy server from the MDS switch.

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

（注） アドレスが空の場合、プロキシ サーバは設定されません。

**ステップ 9** Click **Apply** to update HTTP Proxy Server options.

# Call Home ウィザードの設定

## Call Home ウィザードを設定するためのタスク フロー

次の手順を実行して、Call Home ウィザードを設定します。

### 手順

**ステップ 1** 連絡先情報を設定します。

**ステップ 2** SMTP 情報を設定します。

**ステップ 3** 電子メールの送信元と宛先の情報を設定します。

**ステップ 4** CFS を使用して、設定データを読み込みます。

**ステップ 5** ステータスを表示します。

## Call Home ウィザードの起動

Call Home ウィザードを設定するには、次の手順を実行します。

### 始める前に

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

### 手順

**ステップ 1** 論理ドメイン ツリー内のファブリックを選択します。

**ステップ 2** 、 **ToolsEvents**および**Call Home**を選択します。

[master switch] ペインが表示されます。

**ステップ 3** （任意） You can also launch the Call Home wizard by clicking the **CallHome Wizard** icon in the Call Home **Control** tab.

**ステップ 4** Select a **Master Switch** and click **Next**.
[contact information] ペインが表示されます。

**ステップ 5** Enter the **Contact**, **Phone Number**, **Email Address** and the **Street Address** information.

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

**ステップ 6** **Next** をクリックします。
[Email Setup] ペインが表示されます。

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

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

ウィザードは、SMTP サーバ テーブルに新しい行を作成します。

**ステップ 8** In the **Destination** tab, click **Add** to enter the Call Home destinations.

Call Home 宛先は 3 つまで入力できます。

**ステップ 9** （任意） Click **Remove** to delete a Call Home destination entry.

**ステップ 10** ドロップダウンリストから、[and **ProtocolProfile**] を選択します。
[Profile] ドロップダウンには、[xml]、[short_txt]、および [full_txt] の 3 つのデフォルト プロファイルがリスト表示されます。

**ステップ 11** Click **Finish** to configure the wizard.

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

[**Status Dialog**] ウィンドウが表示されます。

**ステップ 12** Click **Run Test** to perform the Call Home test.

**ステップ 13** Click **Yes** to test the command on all switches in the selected fabric or click **No** to close the window.

# SMTP サーバおよびポートの設定

SMTP サーバおよびポートを設定するには、次の手順を実行します。

**手順**

**ステップ 1** コンフィギュレーション モードに入ります。

switch# **configure terminal**

**ステップ 2** Call Home 設定サブモードに入ります:

switch(config)# **callhome**

**ステップ 3** DNS、IPv4アドレスを設定または、サーバに到達する SMTP サーバの IPv6 アドレス。

switch(config-callhome)# **transport email smtp-server 192.168.1.1**

switch(config-callhome)# **transport email smtp-server 192.168.1.1 port 30**

ポート使用率は、ポートが指定されていない場合に、25 をデフォルト設定されます。

（注） ポート番号がオプションで、必要な場合は、サーバの場所に応じて変更可能性があります。

# 複数の SMTP サーバ サポートの設定

複数の SMTP サーバ サポートを設定するには、次の手順を実行します。

**手順**

**ステップ 1** コンフィギュレーション モードに入ります。

switch# **configure terminal**

**ステップ 2** Call Home 設定サブモードに入ります:

switch(config)# **callhome**

**ステップ 3** 次のいずれかのコマンドを使用します。

- NX-OS リリース 5.0 以前のソフトウェア リリースを実行しているデバイスに SMTP サーバ設定を配布します。

  switch(config-callhome)# **transport email smtp-server**

- 複数の SMTP サーバ機能を配布します。

  switch(config-callhome)# [**no**] **transport email mail-server** {**ipv4** | **IPV6** | **hostname**} [**port** *number*] [**priority** *number*]

上記の設定に基づいて、SMTP サーバはこの順序で試行されます。

10.1.1.174（プライオリティ 0）

192.0.2.10（プライオリティ 4）

172.21.34.193（プライオリティ 50 - デフォルト）

64.72.101.213（プライオリティ 60）

The **transport email mail-server** command is distributed only to devices running Cisco NX-OS Release 5.0(1a) or later. The **transport email smtp-server** command is distributed only to devices running earlier software releases.

# 定期的なインベントリ通知のイネーブル化

間隔の値を設定せずにこの機能をイネーブルにすると、Call Home メッセージは 7 日間おきに送信されます。この値の範囲は、1 ～ 30 日間です。By default, this feature is disabled in all switches in the Cisco MDS 9000 Series and Cisco Nexus 5000 Series switches.

To enable periodic inventory notification in a Cisco MDS 9000 Series switch or a Cisco Nexus 5000 Series switch, follow these steps:

**手順**

**ステップ 1** コンフィギュレーション モードに入ります。

switch# **configure terminal**

**ステップ 2** Call Home 設定サブモードに入ります。

switch(config)# **callhome**

**ステップ 3** Enable the periodic inventory notification feature:

switch(config-callhome)# **periodic-inventory notification**

Disable the periodic inventory notification feature (default):

switch(config-callhome)# **no periodic-inventory notification**

デフォルトでは、Call Home メッセージは 7 日ごとに送信されます。

**ステップ 4** 15 日おきに送信される定期的なインベントリ通知メッセージを設定します。

switch(config-callhome)# **periodic-inventory notification interval 15**

7 日おき Call Home のメッセージの送信の factory default(工場出荷時、ファクトリー デフォルト) を使用するデフォルト:

switch(config-callhome)# **no periodic-inventory notification interval 15**

この値の範囲は、1 ～ 30 日間です。

# DCNM-SAN を使用した定期的なインベントリ通知の有効化

DCNM-SAN を使用した Cisco MDS 9000 シリーズまたは Cisco Nexus 5000 シリーズ スイッチで定期的なインベントリ通知を有効にするには、次の手順を実行します。

手順

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 Expand **Events** and select **Call Home** in the Physical Attributes pane.
[情報] ペインに Call Home 情報が表示されます。

ステップ 3 **Periodic Inventory** タブをクリックします。
Call Home 定期的なインベントリ情報が表示されます。

ステップ 4 [Information] ペインでスイッチを選択します。

ステップ 5 **Enable** チェックボックスをオンにします。

ステップ 6 インベントリをチェックする間隔を日単位で入力します。

ステップ 7 **Apply Changes**アイコンをクリックします。

# 重複するメッセージのスロットリングの設定

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

**[Restrictions（機能制限）]**

- デフォルトでは、Cisco MDS 9000 シリーズと Cisco Nexus 5000 シリーズのすべてのスイッチにおいてこの機能は有効になっています。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。

Cisco MDS 9000 シリーズ スイッチまたは Cisco Nexus 5000 シリーズ スイッチでメッセージ スロットリングを有効にするには、次の手順を実行します。

手順

ステップ 1 コンフィギュレーション モードに入ります。

switch# **configure terminal**

ステップ 2 Call Home 設定サブモードに入ります。

switch(config)# **callhome**

ステップ 3 重複メッセージのスロットリング機能を無効にします。

switch(config-callhome)# **no duplicate-message throttle**

**ステップ 4** 重複メッセージのスロットリング機能を有効にします（デフォルト）。

switch(config-callhome)# **duplicate-message throttle**

# DCNM SAN を使用した重複メッセージ スロットルの設定

DCNM-SAN を使用して Cisco MDS 9000 シリーズ スイッチまたは Cisco Nexus 5000 シリーズ スイッチのメッセージ スロットルを有効にするには、次の手順を実行します。

**手順**

**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** **Events** を展開して、物理属性ペインの **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。

**ステップ 4** [Information] ペインでスイッチを選択します。

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

**ステップ 6** [Apply Changes] アイコンをクリックします。

# Call Home ファブリック配信の有効化

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。

**手順**

**ステップ 1** コンフィギュレーション モードに入ります。

switch# **configure terminal**

**ステップ 2** Call Home 設定サブモードに入ります。

switch(config)# **callhome**

**ステップ 3** Call Home 設定の配信をファブリック内のすべてのスイッチで有効化します。

switch(config-callhome)# **distribute**

ファブリックのロックを取得して、その後の設定変更をすべて保留データベースに格納します。

**ステップ 4** Call Home 設定の配信をファブリック内のすべてのスイッチでディセーブル（デフォルト）にします。

switch(config-callhome)# **no distribute**

## Committing the Call Home Configuration Changes

To commit the Call Home configuration changes, follow these steps:

**手順**

**ステップ 1** コンフィギュレーション モードに入ります。

switch# **configure terminal**

**ステップ 2** Call Home 設定サブモードに入ります。

switch(config)# **callhome**

**ステップ 3** Distribute the configuration changes to all switches in the fabric and release the lock:

switch(config-callhome)# **commit**

保留データベースに対する変更を有効データベースに上書きします。

## Call Home 設定の変更を破棄する

Call Home 設定の変更を廃棄するには、次の手順を実行します。

**手順**

**ステップ 1** コンフィギュレーション モードに入ります。

switch# **configure terminal**

**ステップ 2** Call Home 設定サブモードに入ります。

switch(config)# **callhome**

**ステップ 3** 保留中のデータベースの設定変更を破棄し、ファブリック ロックを解除します:

switch(config-callhome)# **abort**

# DCNM-SAN を使用した Call Home ファブリック配信の有効化

DCNM-SAN を使用して Call Home ファブリック配信を有効にするには、次の手順を実行します。

**手順**

**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** **Events** を展開して、物理属性ペインの **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。

Call Home の CFS 情報が表示されます。

**ステップ 4** [Information] ペインでスイッチを選択します。

**ステップ 5** Select **Enable** from the drop-down list in the Admin column in the row for that switch.

**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

管理権限を使用してロックされた Call Home セッションをリリースするには、次の手順を実行します。

**手順**

管理者権限を使用し、ロックされた Call Home のセッションをリリースします。

switch# **clear callhome session**

# 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 インベントリ 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。

Use the **test** command to simulate a message generation.

Call Home 機能を有効にするには、次の手順を実行します。

手順

ステップ 1 設定された宛先にテスト メッセージを送信します。

switch# **callhome test**

ステップ 2 設定された宛先にテスト インベントリ メッセージを送信します。

switch(config)# **callhome test inventory**

# Call Home Communications テスト DCNM SAN の使用

To test the Call Home function and simulate a message generation using DCNM-SAN, follow these steps:

手順

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 **Events** を展開して、物理属性ペインの **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 Click the **Test** tab.

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 From the **TestAction** drop-down list in the row for that switch, select **test** or **testWithInventory**

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

表 16 : EMC Call Home のトラップ （102 ページ） に、EMC Call Home 用のトラップをすべて示します。

表 *16 : EMC Call Home* のトラップ

| SNMP トラップ（SNMP Trap） | EMC Call Home の送信条件 |
|---|---|
| connUnitStatusChange | operStatus == failed(5) |
| cefcModuleStatusChange | operStatus != {ok(2), boot(5), selfTest(6), poweredUp(16), syncInProgress(21)} |
| cefcPowerStatusChange | operStatus = {offDenied(4), offEnvPower(5),offEnvTemp(6),offEnvFan(7),failed(8)} |
| cefcFRURemoved | all |
| cefcFanTrayStatusChange | all |

| | |
|---|---|
| cieDelayedLinkUpDown | operStatusReason != {linkFailure, adminDown, portGracefulShutdown} |
| cefcFRUInserted | all |
| entSensorThresholdNotification | 値 >= しきい値 |

# 遅延トラップの設定

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

## Enabling the Delayed Trap Feature

To enable the delayed trap feature, perform this task:

### 始める前に

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

### 手順

**ステップ 1** コンフィギュレーション モードに入ります。

switch# **configure terminal**

**ステップ 2** システム遅延トラップ機能を有効にします。

switch(config)# **system delayed-traps enable mode** *FX*

**ステップ 3** システム遅延トラップタイムアウト値を設定します。

switch(config)# **system delayed-traps timer** *<1-60>*

If no value is entered, a default value of 4 minutes is used. 1～60 分の範囲内の値を選択できます。

## DCNM SAN を使用した遅延トラップ機能の有効化

NX-OS リリース 4.1(3) 以降が動作するスイッチ上で、DCNM-SAN を使用して遅延トラップを有効にするには、次の手順を実行します。

手順

ステップ 1 Expand **Events** and select **SNMP Traps** in the Physical Attributes pane.

In the table above the map layout in DCNM-SAN, click the **Delayed Traps** tab.

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内容を保存します。

（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。

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

デバイスマネージャを使用して遅延したトラップ機能を有効にするには、次の手順を実行します。

手順

ステップ 1 In Device Manager, choose **Admin** > **Events** > **Filters** > **Delayed Traps**.

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

ステップ 2 [Delayed Traps] タブをクリックします。

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

遅延時間は、この機能をイネーブルにしないと設定できません。

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

# イベント フィルタ通知の表示

デバイス マネージャで、Admin を選択します > イベント > フィルタを記述通知を参照してください。

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

[Event Filters] 画面に、通知に関する説明が表示されます。

# Call Home の設定の確認

Call Home 設定情報を表示するには、次のいずれかの作業を行います。

## Call Home 情報の表示

Use the **show callhome** command to display the configured Call Home information.

### 設定済みの Call Home 情報の表示

```
switch# show callhome

callhome enabled
Callhome Information:
contact person name:who@where
contact person's e-mail:person@place.com
contact person's phone number:310-408-4000
street addr:1234 Picaboo Street, Any city, Any state, 12345
site id:Site1ManhattanNewYork
customer id:Customer1234
contract id:Cisco1234
switch priority:0
```

### すべての宛先プロファイルの情報（定義済みおよびユーザ定義）の表示

```
switch# show callhome destination-profile

XML destination profile information
maximum message size:500000
message format:XML
message-level:0
e-mail addresses configured:
alert groups configured:
cisco_tac
test destination profile information
maximum message size:100000
message format:full-txt
message-level:5
e-mail addresses configured:
admin@yourcompany.com
alert groups configured:
test
full-txt destination profile information
maximum message size:500000
message format:full-txt
message-level:0
e-mail addresses configured:
alert groups configured:
all
short-txt destination profile information
maximum message size:4000
message format:short-txt
message-level:0
e-mail addresses configured:
alert groups configured:
all
```

### ユーザ定義の宛先プロファイルの情報の表示

```
switch# show callhome destination-profile
 test
test destination profile information
maximum message size:100000
message format:full-txt
message-level:5
e-mail addresses configured:
user
@
company
.com
alert groups configured:
test
```

### フルテキスト プロファイルの表示

```
switch# show callhome destination-profile profile full-txt-destination

full-txt destination profile information
maximum message size:250000
e-mail addresses configured:
person2@company2.com
```

### ショートテキスト プロファイルの表示

```
switch# show callhome destination-profile profile short-txt-destination
Short-txt destination profile information
maximum message size:4000
e-mail addresses configured:
person2@company2.com
```

### XML の接続先のプロファイルを表示します。

```
switch# show callhome destination-profile profile XML-destination
XML destination profile information
maximum message size:250000
e-mail addresses configured:
findout@.cisco.com
```

### 表示電子メールおよび SMTP 情報

```
switch# show callhome transport-e-mail
from e-mail addr:user@company1.com
reply to e-mail addr:pointer@company.com
return receipt e-mail addr:user@company1.com
smtp server:server.company.com
smtp server port:25
```

### Callhome の実行設定情報の表示

```
switch# show running-config callhome
!Command: show running-config callhome
!Time: Tue Sep  9 12:16:45 2014
```

```
version 6.2(9)
logging level callhome 5
callhome
  contract-id contact1
  customer-id cust1
  site-id Site1
  email-contact sakpuri@cisco.com
  phone-contact +1-800-000-0000
  streetaddress 12345 Cisco Way, San Jose, CA
  destination-profile Inventory
  destination-profile Inventory format full-txt
  destination-profile Inventory message-size 1000000
  destination-profile Service
  destination-profile Service format full-txt
  destination-profile Service message-size 1000000
  destination-profile dest1
  destination-profile dest1 format XML
  destination-profile dest1 message-size 500000
  destination-profile full_txt message-size 1000000
  destination-profile httpProf
  destination-profile httpProf format XML
  destination-profile httpProf message-size 0
  destination-profile short_txt message-size 4000
  destination-profile xml message-size 1000000
  destination-profile xml message-size 1000000
  destination-profile Inventory email-addr sakpuri@cisco.com
  destination-profile Service email-addr sakpuri@cisco.com
  destination-profile full_txt email-addr sakpuri@cisco.com
  destination-profile short_txt email-addr sakpuri@cisco.com
  destination-profile xml email-addr sakpuri@cisco.com
  destination-profile Service alert-group environmental
  destination-profile xml alert-group environmental
  destination-profile Inventory alert-group inventory
  destination-profile xml alert-group inventory
  destination-profile Service alert-group linecard-hardware
```

### デフォルトで Callhome の実行設定情報の表示

```
switch# show running-config callhome all
EG-9506-1-176# show running-config callhome all
!Command: show running-config callhome all
!Time: Tue Sep  9 12:18:22 2014
version 6.2(9)
logging level callhome 5
callhome
  contract-id contact1
  customer-id cust1
  switch-priority 7
  site-id Site1
  email-contact sakpuri@cisco.com
  phone-contact +1-800-000-0000
  streetaddress 12345 Cisco Way, San Jose, CA
  destination-profile Inventory
  destination-profile Inventory format full-txt
  destination-profile Inventory transport-method email
  no destination-profile Inventory transport-method http
  destination-profile Inventory message-size 1000000
  destination-profile Inventory message-level 0
  destination-profile Service
  destination-profile Service format full-txt
  destination-profile Service transport-method email
  no destination-profile Service transport-method http
  destination-profile Service message-size 1000000
```

```
  destination-profile Service message-level 0
  destination-profile dest1
  destination-profile dest1 format XML
  destination-profile dest1 transport-method email
  no destination-profile dest1 transport-method http
  destination-profile dest1 message-size 500000
  destination-profile dest1 message-level 0
  destination-profile full_txt
  destination-profile full_txt format full-txt
  destination-profile full_txt transport-method email
  no destination-profile full_txt transport-method http
  destination-profile full_txt message-size 1000000
  destination-profile full_txt message-level 0
  destination-profile httpProf
```

### Callhome のスタートアップ設定の表示

```
switch# show startup-config callhome
!Command: show startup-config callhome
!Time: Tue Sep  9 12:19:27 2014
!Startup config saved at: Fri Sep  5 12:13:53 2014
version 6.2(9)
logging level callhome 5
callhome
  contract-id contact1
  customer-id cust1
  site-id Site1
  email-contact sakpuri@cisco.com
  phone-contact +1-800-000-0000
  streetaddress 12345 Cisco Way, San Jose, CA
  destination-profile Inventory
  destination-profile Inventory format full-txt
  destination-profile Inventory message-size 1000000
  destination-profile Service
  destination-profile Service format full-txt
  destination-profile Service message-size 1000000
  destination-profile dest1
  destination-profile dest1 format XML
  destination-profile dest1 message-size 500000
  destination-profile full_txt message-size 1000000
  destination-profile httpProf
  destination-profile httpProf format XML
  destination-profile httpProf message-size 0
  destination-profile short_txt message-size 4000
  destination-profile xml message-size 1000000
  destination-profile xml message-size 1000000
  destination-profile Inventory email-addr sakpuri@cisco.com
  destination-profile Service email-addr sakpuri@cisco.com
  destination-profile full_txt email-addr sakpuri@cisco.com
  destination-profile short_txt email-addr sakpuri@cisco.com
  destination-profile xml email-addr sakpuri@cisco.com
  destination-profile Service alert-group environmental
  destination-profile xml alert-group environmental
  destination-profile Inventory alert-group inventory
  destination-profile xml alert-group inventory
```

## Displaying Delayed Trap Information

Use the **show running-config | in delay** command to display the system-delayed trap state. タイマーの値が指定されていない場合、またはタイマーの値は4分に設定されている場合は、次のように表示されます。

**No タイマー値を持つ遅延トラップ情報が表示されます (デフォルトに設定 4 分)**

```
switch# show running-config | in delay
system delayed-traps enable mode FX
```

次の例は、タイマーの値は、他の値 4 分以外に設定されている場合に、出力を示します。

**4 分以外のタイマー値での遅延のトラップ情報を表示します。**

```
switch# show running-config | in delay
system delayed-traps enable mode FX
system delayed-traps timer 5
```

# アラート グループのカスタマイズの確認

To verify the alert group customization, use the **show callhome user-def-cmds** command.

```
switch# show callhome user-def-cmds
User configured commands for alert groups :
alert-group test user-def-cmd "show version"
```

# イベント通知トラップの確認

SNMP イベント通知トラップを確認するには、show snmp トラップを使用して |inc callhome コマンド。

```
switch# show snmp trap | inc callhome
callhome : event-notify Yes
callhome : smtp-send-fail No
```

# Call Home トランスポートの確認

Show callhome トランスポート コマンドは、Call Home のトランスポート関連の設定をすべて表示します。

```
switch# show callhome transport
http vrf:management
from email addr:xyz-1@cisco.com
reply to email addr:xyz-1@cisco.com
smtp server:72.163.62.211
smtp server port:25
smtp server vrf:management
smtp server priority:0
http proxy server:10.64.65.52
http proxy server port:8080
http proxy status:Enabled
```

次の例では、SMTP サーバ ポートの設定方法を示します。

```
switch# callhome
switch(config-callhome)# transport email mail-server 192.168.10.23 port 4
switch# config t
```

次の例では、SMTP サーバ優先順位の設定方法の例を示します。

```
switch(config-callhome)# transport email mail-server 192.168.10.23 priority 60
switch# config t
```

# Call Home のモニタリング

この項では、次のトピックについて取り上げます。

## フルテキスト形式の Syslog アラート通知の例

```
source:MDS9000
Switch Priority:7
Device Id:DS-C9506@C@FG@07120011
Customer Id:basu
Contract Id:123
Site Id:San Jose
Server Id:DS-C9506@C@FG@07120011
Time of Event:2004-10-08T11:10:44
Message Name:SYSLOG_ALERT
Message Type:Syslog
Severity Level:2
System Name:10.76.100.177
Contact Name:Basavaraj B
Contact e-mail:admin@yourcompany.com
Contact Phone:+91-80-310-1718
Street Address:#71 , Miller's Road
Event Description:2004 Oct  8 11:10:44 10.76.100.177 %PORT-5-IF_TRUNK_UP: %$VSAN 1%$
Interface fc2/5, vsan 1 is up
syslog_facility:PORT
start chassis information:
Affected Chassis:DS-C9506
Affected Chassis Serial Number:FG@07120011
Affected Chassis Hardware Version:0.104
Affected Chassis Software Version:3.1(1)
Affected Chassis Part No:73-8607-01
end chassis information:
```

## XML 形式での 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: <<%LICMGR-3-LOG_LICAPP_NO_LIC>> 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'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' - kernel
2003 Feb 21 04:12:08  %KERN-3-SYSTEM_MSG: klm_ips_portcfg: Unknown parameter `start' -
kernel
2003 Feb 21 04:12:08  %KERN-3-SYSTEM_MSG: klm_flamingo: Unknown parameter `start' -
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't caught signal 9 (no core).
2003 Feb 21 04:16:18 switch %LICMGR-3-LOG_LIC_FILE_MISSING: License file(s) missing for
 feature ENTERPRISE_PKG.
2003 Feb 21 04:16:18 switch %LICMGR-3-LOG_LIC_FILE_MISSING: License file(s) missing for
 feature SAN_EXTN_OVER_IP.
2003 Feb 21 04:16:18 switch %LICMGR-3-LOG_LIC_FILE_MISSING: License file(s) missing for
 feature ENTERPRISE_PKG.
2003 Feb 21 04:16:18 switch %LICMGR-3-LOG_LIC_FILE_MISSING: License file(s) missing for
 feature SAN_EXTN_OVER_IP.
2003 Feb 21 04:16:18 switch %CALLHOME-2-EVENT: LICENSE_VIOLATION
2003 Feb 21 04:16:18 switch %CALLHOME-2-EVENT: LICENSE_VIOLATION
2003 Feb 21 04:16:18 switch %CALLHOME-2-EVENT: LICENSE_VIOLATION
2003 Feb 21 04:16:18 switch %CALLHOME-2-EVENT: LICENSE_VIOLATION ]]> </aml-block:Data>
</aml-block:Attachment> <aml-block:Attachment type="inline"> <aml-block:Name>show license
 usage</aml-block:Name> <aml-block:Data encoding="plain">
<![CDATA[Feature                        Ins  Lic   Status Expiry Date Comments
                                      Count
--------------------------------------------------------------------------------
DMM_184_PKG                    No    0   Unused             Grace expired
FM_SERVER_PKG                  No    -   Unused             Grace expired
MAINFRAME_PKG                  No    -   Unused             Grace expired
ENTERPRISE_PKG                 Yes   -   Unused never       license missing
DMM_FOR_SSM_PKG                No    0   Unused             Grace expired
SAN_EXTN_OVER_IP               Yes   8   Unused never       8 license(s) missing
PORT_ACTIVATION_PKG            No    0   Unused             -
SME_FOR_IPS_184_PKG            No    0   Unused             Grace expired
STORAGE_SERVICES_184           No    0   Unused             Grace expired
SAN_EXTN_OVER_IP_18_4          No    0   Unused             Grace expired
SAN_EXTN_OVER_IP_IPS2          No    0   Unused             Grace expired
SAN_EXTN_OVER_IP_IPS4          No    0   Unused             Grace expired
STORAGE_SERVICES_SSN16         No    0   Unused             Grace expired
10G_PORT_ACTIVATION_PKG        No    0   Unused             -
STORAGE_SERVICES_ENABLER_PKG   No    0   Unused             Grace expired
--------------------------------------------------------------------------------
**** WARNING: License file(s) missing. **** ]]> </aml-block:Data> </aml-block:Attachment>
 </aml-block:Attachments> </aml-block:Block> </soap-env:Body> </soap-env:Envelope>
```

# XML 形式の RMON 通知の例

```
<?xml version="1.0" encoding="UTF-8" ?>
<soap-env:Envelope xmlns:soap-env="http://www.w3.org/2003/05/soap-envelope">
<soap-env:Header>
<aml-session:Session xmlns:aml-session="http://www.cisco.com/2004/01/aml-session"
soap-env:mustUnderstand="true"
soap-env:role="http://www.w3.org/2003/05/soap-envelope/role/next">
<aml-session:To>http://tools.cisco.com/neddce/services/DDCEService</aml-session:To>
<aml-session:Path>
```

```
<aml-session:Via>http://www.cisco.com/appliance/uri</aml-session:Via>
</aml-session:Path>
<aml-session:From>http://www.cisco.com/appliance/uri</aml-session:From>
<aml-session:MessageId>1086:FHH0927006V:48BA26BD</aml-session:MessageId>
</aml-session:Session>
</soap-env:Header>
<soap-env:Body>
<aml-block:Block xmlns:aml-block="http://www.cisco.com/2004/01/aml-block">
<aml-block:Header>
<aml-block:Type>http://www.cisco.com/2005/05/callhome/diagnostic</aml-block:Type>
<aml-block:CreationDate>2008-08-31 05:06:05 GMT+00:00</aml-block:CreationDate>
<aml-block:Builder>
<aml-block:Name>MDS</aml-block:Name>
<aml-block:Version>4.1</aml-block:Version>
</aml-block:Builder>
<aml-block:BlockGroup>
<aml-block:GroupId>1087:FHH0927006V:48BA26BD</aml-block:GroupId>
<aml-block:Number>0</aml-block:Number>
<aml-block:IsLast>true</aml-block:IsLast>
<aml-block:IsPrimary>true</aml-block:IsPrimary>
<aml-block:WaitForPrimary>false</aml-block:WaitForPrimary>
</aml-block:BlockGroup>
<aml-block:Severity>2</aml-block:Severity>
</aml-block:Header>
<aml-block:Content>
<ch:CallHome xmlns:ch="http://www.cisco.com/2005/05/callhome" version="1.0">
<ch:EventTime>2008-08-31 05:06:05 GMT+00:00</ch:EventTime>
<ch:MessageDescription>RMON_ALERT WARNING(4) Falling:iso.3.6.1.4.1.9.9.305.1.1.1.0=1 <=
 89:1, 4</ch:MessageDescription>
<ch:Event>
<ch:Type>environment</ch:Type>
<ch:SubType>minor</ch:SubType>
<ch:Brand>Cisco</ch:Brand>
<ch:Series>MDS9000</ch:Series>
</ch:Event>
<ch:CustomerData>
<ch:UserData>
<ch:e-mail>mchinn@cisco.com</ch:e-mail>
</ch:UserData>
<ch:ContractData>
<ch:CustomerId>12ss</ch:CustomerId>
<ch:SiteId>2233</ch:SiteId>
<ch:ContractId>rrr55</ch:ContractId>
<ch:DeviceId>DS-C9513@C@FHH0927006V</ch:DeviceId>
</ch:ContractData>
<ch:SystemInfo>
<ch:Name>sw172-22-46-174</ch:Name>
<ch:Contact>Mani</ch:Contact>
<ch:Contacte-mail>mchinn@cisco.com</ch:Contacte-mail>
<ch:ContactPhoneNumber>+1-800-304-1234</ch:ContactPhoneNumber>
<ch:StreetAddress>1234 wwee</ch:StreetAddress>
</ch:SystemInfo>
</ch:CustomerData>
<ch:Device>
<rme:Chassis xmlns:rme="http://www.cisco.com/rme/4.0">
<rme:Model>DS-C9513</rme:Model>
<rme:HardwareVersion>0.205</rme:HardwareVersion>
<rme:SerialNumber>FHH0927006V</rme:SerialNumber>
</rme:Chassis>
</ch:Device>
</ch:CallHome>
</aml-block:Content>
</aml-block:Block>
```

```
</soap-env:Body>
</soap-env:Envelope>
```

# Call Home のフィールドの説明

This section displays the field descriptions for this feature:

## Call Home 一般

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

**Related Topics**

Call Home の概要 （51 ページ）

## Call Home 宛先

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

**Related Topics**

Call Home 宛先プロファイル （55 ページ）

# Call Home SMTP サーバ

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

# Call Home 電子メール セットアップ

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

**Related Topics**

HTTPS サポートを使用した一般的な電子メール オプション （57 ページ）

# Call Home アラート

| フィールド | 説明 |
|---|---|
| アクション | [Test]：Call Home メッセージを送信します。<br>[TestWithInventory]：インベントリの詳細付きメッセージを送信します。 |
| Status（ステータス） | 最後の Call Home アクション呼び出しのステータス。 |

| フィールド | 説明 |
|---|---|
| FailureCause | 最後の Call Home テスト呼び出しの失敗原因。 |
| LastTimeSent | 最後の Call Home アラートが送信された時刻。 |
| NumberSent | Call Home アラートの送信数。 |
| Interval | 定期的なソフトウェア インベントリ Call Home メッセージを送信するためのタイム フレーム。 |
| Throttling Enable | オンの場合、システムに実装されているメッセージ スロットリング メカニズムがイネーブルになり、一定のタイム フレーム内での特定のアラート タイプの Call Home メッセージの数が制限されます。最大は 2 時間のタイム フレーム内で 30 件であり、それ以上のそのアラート タイプのメッセージは廃棄されます。 |
| Enable | オンの場合、システム上での定期的なソフトウェア インベントリ Call Home メッセージの送信がイネーブルになります。 |

**Related Topics**

Call Home アラート グループ （55 ページ）

Call Home のメッセージ レベル機能 （56 ページ）

# Call Home ユーザ定義コマンド

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

# 遅延トラップ

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

# Call Home プロファイル

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

# イベント宛先アドレス

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

# イベント宛先セキュリティ（詳細）

| フィールド | 説明 |
|---|---|
| MPModel | このエントリを使用して SNMP メッセージを生成する際に使用されるメッセージ処理モデル。 |
| SecurityModel | このエントリを使用して SNMP メッセージを生成する際に使用されるセキュリティ モデル。 |

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

# イベント フィルター般

| フィールド | 説明 |
|---|---|
| FSPF - Nbr State Changes | ローカル スイッチが VSAN 上のインターフェイスでネイバーの状態（FSPF ネイバー有限状態マシンの状態）の変化を検出したときに通知を発行するかどうかを指定します。 |
| Domain Mgr - ReConfig Fabrics | ローカル スイッチが VSAN 上での ReConfigureFabric（RCF）の送受信時に通知を発行するかどうかを指定します。 |
| Zone Server - Request Rejects | ゾーン サーバが拒否時に通知を発行するかどうかを指定します。 |
| Zone Server - Merge Failures | ゾーン サーバがマージ失敗時に通知を発行するかどうかを指定します。 |
| Zone Server - Merge Successes | ゾーン サーバがマージ成功時に通知を発行するかどうかを指定します。 |
| Zone Server - Default Zone Behavior Change | 伝播ポリシーが変化した場合にゾーン サーバが通知を発行するかどうかを指定します。 |
| Zone Server - Unsupp Mode | ゾーン サーバが unsupp モードの変化時に通知を発行するかどうかを指定します。 |
| FabricConfigServer - Request Rejects | ファブリック コンフィギュレーション サーバが拒否時に通知を発行するかどうかを指定します。 |
| RSCN - ILS Request Rejects | SW_RSCN 要求が拒否されるときに RSCN モジュールが通知を生成するかどうかを指定します。 |
| RSCN - ILS RxRequest Rejects | SW_RSCN 要求が拒否されるときに RSCN モジュールが通知を生成するかどうかを指定します。 |
| RSCN - ELS Request Rejects | SCR または RSCN 要求が拒否されるときに RSCN モジュールが通知を生成するかどうかを指定します。 |
| FRU Changes | false 値の場合、このシステムによって現場交換可能ユニット（FRU）通知は生成されません。 |

| フィールド | 説明 |
|---|---|
| SNMP - Community Auth Failure | SNMP エンティティが authenticationFailure トラップの生成を許可されているかどうかを示します。 |
| VRRP | VRRP 対応ルータがこの MIB に定義されているイベントに対して SNMP トラップを生成するかどうかを示します。 |
| FDMI | 登録要求が拒否されるときに FDMI が通知を生成するかどうかを指定します。 |
| License Manager | システムが通知を生成するかどうかを示します。 |
| Port/Fabric Security | ポート/ファブリック セキュリティの問題が発生したときにシステムが通知を生成するかどうかを指定します。 |
| FCC | エージェントが通知を生成するかどうかを指定します。 |
| Name Server | オンの場合、要求が拒否されるときにネーム サーバが通知を生成します。オフの場合、通知は生成されません。 |

# イベント フィルタ インターフェイス

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

# イベント フィルタ制御

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

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

# その他の参考資料

Call Home の実装に関連した情報については、次を参照してください。

### MIB

| MIB | MIB のリンク |
|---|---|
| • CISCO-CALLHOME-CAPABILITY-MIB<br>• CISCO-CALLHOME-MIB | MIB を検索およびダウンロードするには、次の URL にアクセください。<br>http://www.cisco.com/en/US/products/ps5989/prod_technical_referenc |

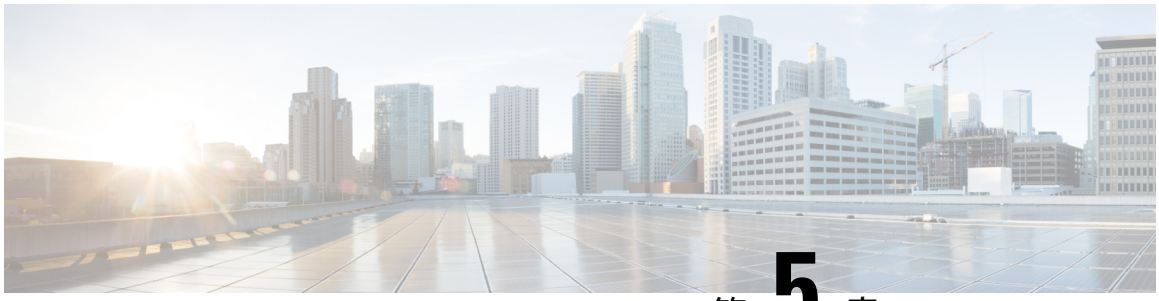
# Call Home の機能履歴

Call Home の機能履歴 （121 ページ） に、この機能のリリース履歴を示します。リリース 3.x 以降のリリースで導入または変更された機能のみが表に記載されています。

表 *17 : Call Home* の機能履歴

| 機能名 | リリース | 機能情報 |
|---|---|---|
| Call Home HTTP プロキシ サーバ | 5.2 | Call Home HTTP プロキシ サーバ サポートの詳細が追加されました。 |
| Call Home ウィザード | 5.2 | Call Home ウィザード設定の詳細が追加されました。 |
| Call Home HTTP プロキシ サーバ | 5.2 | Call Home HTTP プロキシ サーバ サポートの詳細が追加されました。<br>Callhome 転送を確認するコマンドが追加されました。 |
| 複数 SMTP サーバ サポート | 5.0(1a) | 複数 SMTP サーバ サポートの詳細が追加されました。<br>Callhome 転送を確認するコマンドが追加されました。 |
| 通知の拡張 | 5.0(1a) | Device Manager を使用したイベント フィルタの通知の拡張が追加されました。 |
| Call Home | 4.1(1b) | Call Home の HTTPS サポートが追加されました。 |
| DCNM-SAN における [Call Home - Delayed Traps for EMC Call Home] 設定ウィンドウ | 4.1(1a) | EMC Call Home の遅延トラップの拡張が追加されました。 |
| [Call Home Destination] タブ | 4.2(1) | [Destination] タブの拡張を追加。 |
| Call Home HTTP のサポート | 4.2(1) | Call Home HTTP 拡張を追加。 |

| 機能名 | リリース | 機能情報 |
|---|---|---|
| EMC Email Home | 3.3(3) | この章に EMC Email Home 設定情報が追加されました。 |
| EMC Call Home | 3.0(1) | EMC 仕様に従い、電子メールを使用してトラップを XML データとして転送できるようになります。 |
| Call Home の拡張 | 3.0(1) | アラートグループメッセージをカスタマイズできるようになります。 |



第 5 章

# メンテナンス ジョブのスケジューリング

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



## コマンド スケジューラについて

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

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

### スケジューラの用語

この章では次の用語を使用します。

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

# コマンド スケジューラのライセンス要件

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。

# 注意事項と制約事項

Before scheduling jobs on a Cisco MDS switch, note the following guidelines:

- 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。
- While defining a job, verify that no interactive or disruptive commands (for example, **copy bootflash:** *file* **ftp:** *URI*, **write erase**, and other similar commands) are specified as part of a job because the job is executed noninteractively at the scheduled time.

# デフォルト設定

表 18 : コマンド スケジューラのパラメータのデフォルト （125 ページ） 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 *18 :* コマンド スケジューラのパラメータのデフォルト**

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

# コマンド スケジューラの設定

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。

## コマンド スケジューラを設定するためのタスク フロー

次の手順を実行して、コマンド スケジューラを設定します。

**手順**

**ステップ 1** スケジューラをイネーブルにします。
**ステップ 2** リモート ユーザ アクセスを許可します（オプション）。
**ステップ 3** ジョブを定義します。
**ステップ 4** スケジュールを定義して、スケジュールにジョブを割り当てます。
**ステップ 5** スケジュールの時刻を指定します。
**ステップ 6** スケジューリングされた設定を確認します。

## コマンド スケジューラのイネーブル化

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

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。

### 手順

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 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。

**ステップ 3** 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）。

## 例

To display the command schedule status, use the **show scheduler config** command.

```
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。

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。

### 始める前に

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。

### 手順

**ステップ 1** switch# **configuration terminal**

コンフィギュレーション モードに入ります。

**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

# 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。This action places you in the job definition (config-job ) submode. 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。

- 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。

### 手順

**ステップ 1** switch# **configuration terminal**

コンフィギュレーション モードを開始します。

**ステップ 2** switch(config)# **scheduler job name addMemVsan99**

switch(config-job)#

Defines a job name and enters the job definition submode.

**ステップ 3** switch(config-job)# *command1* ;[*command2* ;*command3* ;...]

switch(config-job-submode) # **end**

**例**：

```
switch(config-job)# configure 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**：

```
switch(config)# scheduler job name offpeakQOS
switch(config-job)# configuration terminal; 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#
```

一連のコンフィギュレーション 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 コンフィギュレーション 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
```

（任意）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
```

（任意）この設定の変更を保存します。

## 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。

**手順**

**ステップ 1** switch# **configuration terminal**

コンフィギュレーション モードを開始します。

**ステップ 2** switch(config)# **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。

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

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。

**手順**

**ステップ 1** switch# **configuration terminal**

コンフィギュレーション モードを開始します。

**ステップ 2** switch(config)# **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)# **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 4** 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 5** 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。

# 例

次に示す設定は参考例です。

| コマンド | 目的 |
|---|---|
| switch(config-schedule)# **time daily 23:00** | Executes the specified jobs at 11 p.m. every day. |
| 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** | 開始から 2 分 48 時間ごとに実行するジョブを指定　今すぐ　: 今日は 2004 年 9 月 24 日、時間が 2時 00分 pm で、コマンドので実行が開始 2 2004 年 9 月 24 日、午後 2: 過去の時間 (分) し、引き続き実行ごとその後 48 時間。 |
| switch(config-schedule)# **time start 14:00 repeat 14:00:00** | 今日が 2004 年 9 月 24 日の場合 (金曜日)、このコマンドでは、すべて代替金曜日午後 2 (14 日おき) で実行するジョブ指定します。 |

The most significant fields in the **time** parameter are optional. 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。

- The **time start 23:00 repeat 4:00:00** command implies a start time of September 24, 2004, 23:00 hours.
- The **time daily 55** command implies every day at 22:55 hours.
- The **time weekly 23:00** command implies every Friday at 23:00 hours.
- The **time monthly 23:00** command implies the 24th of every month at 23:00 hours.

（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。

**手順**

**ステップ 1** switch# **configuration terminal**

コンフィギュレーション モードを開始します。

**ステップ 2** switch(config)# **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。

**ステップ 5** 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。

手順

ステップ 1 switch# **configuration terminal**

コンフィギュレーション モードを開始します。

ステップ 2 switch(config)# **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。

手順

ステップ 1 switch# **configuration terminal**

コンフィギュレーション モードを開始します。

ステップ 2 switch(config)# **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。

手順

ステップ 1 switch# **configuration terminal**

コンフィギュレーション モードを開始します。

ステップ 2 switch(config)# **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。

# 実行ログの設定

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 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。

**手順**

**ステップ 1** switch# **configuration terminal**

コンフィギュレーション モードを開始します。

**ステップ 2** switch(config)# **scheduler logfile size 1024**

ログファイルを最大 1024 KB に設定します。

**ステップ 3** 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
```

# スケジューラ設定の確認

To display the command scheduler configuration information, perform one of the following tasks:

| コマンド | 目的 |
|---|---|
| **show scheduler config** | Displays the scheduler configuration |
| **show scheduler schedule** | Verifies the command scheduler execution status |
| **show scheduler job** | Verifies the job definition |
| **show scheduler logfile** | システムで実行されるすべてのジョブの実行のログを表示します。 |
| **clear scheduler logfile** | スケジューラ実行ログファイルの内容をクリアします。 |

For detailed information about the fields in the output from these commands, refer to the *Cisco MDS 9000 Family Command Reference* .

## コマンド スケジューラの設定確認

To display the scheduler configuration, use the **show scheduler config** command.

```
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
```

## コマンド スケジューラの実行ステータスの確認

To verify the command scheduler execution status, use the **show scheduler schedule** command.

```
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
```

# ジョブ定義の確認

To verify the job definition, use the **show scheduler job** command.

```
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
```

# 実行ログ ファイルの内容の表示

To display the execution log for all jobs executed in the system, use the **show scheduler logfile** command.

```
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`
```

To display the scheduler password configuration for remote users, use the **show running-config** command.

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

（注） The scheduler remote user passwords are always displayed in encrypted form in the **show running-config** command output. The encrypted option (**7**) in the command exists to support applying the ASCII configuration to the switch.

To display the execution log file configuration, use the **show scheduler config** command.

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

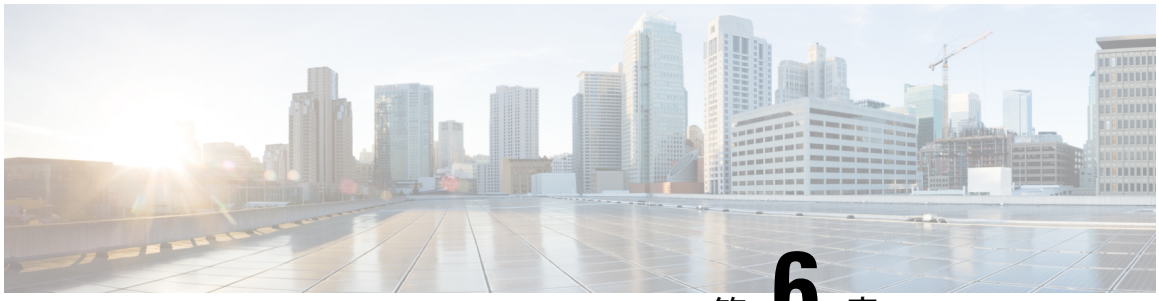
# 実行ログ ファイルの内容のクリア

To clear the contents of the scheduler execution log file, issue the **clear scheduler logfile** command in EXEC mode.

```
switch# clear scheduler logfile
-----------------------------------------------
addMemVsan99                          Success (0)
```

# スケジューラのコンフィギュレーション例

```
configure terminal

scheduler job name start
 configure
 no cli var name time
 exit
 echo $(TIMESTAMP) | sed 's/^/cli var name time /' | vsh
 show switchname > debug-$(time)-1
 show switchname > debug-$(time)-2
 exit

scheduler job name part1
 show clock >> debug-$(time)-1
 show interface mgmt 0 >> debug-$(time)-1
 sleep 60
 show clock >> debug-$(time)-1
 show interface mgmt 0 >> debug-$(time)-1
 sleep 200
 gzip debug-$(time)-1
 exit

scheduler job name part2
 show clock >> debug-$(time)-2
 show processes cpu history >> debug-$(time)-2
 sleep 60
 show clock >> debug-$(time)-2
 show processes cpu history >> debug-$(time)-2
 show clock >> debug-$(time)-2
 gzip debug-$(time)-2
 exit

scheduler schedule name cpu-stats
  job name start
  job name part1
  job name part2
  time start 2001:12:31:01:00
  exit

end
```



第 6 章

# システム プロセスとログのモニタリング

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。



# システム プロセスおよびログについて

## コアの保存

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

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

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

## ブートフラッシュへの最後のコアの保存

この最後のコア ダンプは、スイッチオーバーまたはリブートが起こる前に、/mnt/pss/ パーティションにあるブートフラッシュに自動的に保存されます。スーパーバイザ モジュールがリブー

トしてから 3 分間後に、保存された最後のコアがフラッシュ パーティション（/mnt/pss）から元のメモリ上に復元されます。この復元はバックグラウンドプロセスであり、ユーザからは見えません。

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

To view the last core information, enter the **show cores** command in EXEC mode.

To view the time of the actual last core dump, enter the **show process log** command in EXEC mode.

# 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。

To display the core files saved in the system, use the **show cores** command.

# オンラインでのシステム ヘルス管理

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

OHMS は、システム ハードウェアを次のようにモニタリングします。

- アクティブ スーパーバイザ稼働する 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働する他のすべての 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 モジュール上で稼働するシステム ヘルス アプリケーションは、そのモジュールが HA スタンバイ モードで使用できる場合でも、スタンバイ スーパーバイザ モジュールだけを監視します。

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

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

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

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

# ループバック テストの設定頻度

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

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

# ループバック テストのフレーム長の設定

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

ループバック テストは、0 ～ 128 バイトの範囲のフレーム サイズで実行できます。ループバック フレーム長の値を設定しなければ、スイッチ内のすべてのモジュールに対してランダムなフ

レーム長がスイッチによって生成されます（自動モード）。ループバック テストのフレーム長は、モジュールごとに変更できます。

# ハードウェア障害時の処理

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

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

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

# テストの実行要件

テストをイネーブルにしても、テストの実行が保障されるわけではありません。

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

- スイッチ全体
- 必要なモジュール
- 必要なインターフェイス

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

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

# 特定モジュールのテスト

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

- ファブリックに対してスーパーバイザのインバンド接続をアクティブ化。
- スーパーバイザの arbiter のスタンバイ状態。
- すべてのモジュール上でのブートフラッシュの接続性とアクセシビリティ。
- すべてのモジュール上での EOBC の接続性とアクセシビリティ。
- すべてのモジュール上の各インターフェイスのデータ パスの完全性。

- 管理ポートの接続性。
- 外部接続性検証のためのユーザによるテスト。テスト中はポートがシャットダウンされます（ファイバ チャネル ポートのみ）。
- 内部接続性検証のためのユーザによるテスト（ファイバ チャネル ポートと iSCSI ポート）。

（注） Cisco MDS 9700 シリーズ スイッチでは、iSCSI ポートは適用されません。

# 前回のエラー レポートのクリア

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

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

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

# 現在のステータスの説明

各モジュールまたはテストのステータスは、その特定のモジュールでの OHMS テストの現在の設定状態によって異なります（表 19: テストおよびモジュールに関する OHMS の設定ステータス （141 ページ） を参照）。

**表 *19:* テストおよびモジュールに関する *OHMS* の設定ステータス**

| Status（ステータス） | 説明 |
|---|---|
| イネーブル | このモジュールのテストはイネーブルに設定されていますが、現在は実行されていません。 |
| 無効 | 現在このモジュールのテストはディセーブルに設定されています。 |
| Running | このモジュールのテストはイネーブルに設定され、現在実行中です。 |
| Failing | このステートは、このモジュールで実行中のテストで障害が発生しそうな場合に表示されます。このステートは、テストで回復できる可能性があります。 |

| Status（ステータス） | 説明 |
|---|---|
| 不合格 | このモジュールのテストで障害が発生しました。ステートは回復できません。 |
| Stopped | テストは、Cisco NX-OS ソフトウェアによってこのモジュールのテストが内部的に停止されました。 |
| Internal failure | このモジュールのテストで、内部障害が発生しました。たとえば、システム ヘルス アプリケーションがテスト手順の一部でソケットをオープンできません。 |
| Diags failed | このモジュールまたはインターフェイスの起動時の診断で障害が発生しました。 |
| On demand | 現在、このモジュールで、システム ヘルス外部ループバックまたはシステム ヘルス内部ループバック テストが実行中です。オンデマンドで発行できるのは、これらの 2 つのコマンドだけです。 |
| Suspended | 1 つのオーバーサブスクライブ ポートが E または TE ポート モードに移行することにより、MDS 9100 シリーズでのみ発生します。1 つのオーバーサブスクライブ ポートがこのモードに移行すると、グループ内の他の 3 つのオーバーサブスクライブ ポートは中断されます。 |

The status of each test in each module is visible when you display any of the **show system health** commands.システム ヘルスの表示 （163 ページ）を参照してください。

# オンボード障害ロギング

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

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

OBFL 機能によって保存されるデータは、次のとおりです。

- 最初の電源投入時刻
- カードのシャーシ スロット番号
- カードの初期温度
- ファームウェア、BIOS、FPGA、および ASIC のバージョン
- カードのシリアル番号
- クラッシュのスタック トレース
- CPU hog 情報

- メモリ リーク情報
- ソフトウェア エラー メッセージ
- ハードウェア例外ログ
- 環境履歴
- OBFL 固有の履歴情報
- ASIC 割り込みおよびエラー統計の履歴
- ASIC レジスタ ダンプ

# デフォルト設定

表 20 : システム ヘルスおよびログのデフォルト設定値 （143 ページ） 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 *20 :* システム ヘルスおよびログのデフォルト設定値**

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

# コア ファイルおよびログ ファイル

## コアの保存

コア ファイルおよびログ ファイルを必要に応じてコピーするには、この手順を実行します。

### 始める前に

このタスクを実行する前に、必要なディレクトリを作成していることを確認します。この操作で指定されたディレクトリが存在しない場合、スイッチ ソフトウェアはコピー コアが試行されるたびにシステム メッセージを記録します。

### 手順

**ステップ 1** switch# **show cores**

すべてのコア ファイルを表示します。

**ステップ 2** switch# **copy core:7407 slot0:coreSample**

スロット 0 に coreSample としてプロセス ID 7407 でコア ファイルをコピーします。

**ステップ 3** switch# **copy core://5/1524 tftp://1.1.1.1/abcd**

スロット 5[1]またはスロット 7[2] で生成された PID 1524 で、プロセスのコア（存在する場合）を IPv4 アドレス 1.1.1.1.の TFTP サーバにコピーします。

（注） TFTP サーバを特定するのに IPv6 アドレスを使用することもできます。

## 定期的にファイルのコピー

コア ファイルおよびログ ファイルを定期的にコピーするには、次の手順を実行します。

### 手順

**ステップ 1** switch# **show system cores**

すべてのコア ファイルを表示します。

**ステップ 2** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 3** switch(config)# **system cores slot0:coreSample**

コア ファイル（coreSample）をスロット 0 にコピーします。

**ステップ 4** switch(config)# **system cores tftp://1.1.1.1/abcd**

指定されたディレクトリ内のコア ファイル（abcd）を IPv4 アドレス 1.1.1.1 の TFTP サーバにコピーします。

（注） TFTP サーバを特定するのに IPv6 アドレスを使用することもできます。

**ステップ 5** switch(config)# **no system cores**

コア ファイルのコピー機能をディセーブルにします。

## 例

指定されたプロセス ID (PID) のコア ファイルが使用できない場合は、次の応答が表示されます。

```
switch# copy core://7/123 slot0:abcd
```

[1] Cisco MDS 9506 または Cisco MDS 9509 スイッチ
[2] Cisco MDS 9513 Director

```
No matching core file found

switch# copy core:133 slot0:foo
Enter module number:7
No matching core file found

switch# copy core://7/133 slot0:foo
No matching core file found
```

次のように、別のインスタンス番号を持つ同じ PID をコピーするには:

```
switch# copy core:?
  core:  Enter URL "core://<module-number>/<process-id>[/instance-num]"
```

## コア ディレクトリのクリア

Use the **clear cores** command to clean out the core directory. ソフトウェアは、すべてのコア ファイルをクリアし、他のコアがアクティブ スーパーバイザ モジュールに存在します。

```
switch# clear cores
```

# システム ヘルスの設定

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

## システム ヘルスを設定するためのタスク フロー

システム ヘルスを設定するには、次の手順を実行します。

### 手順

**ステップ 1** システム ヘルス開始を有効にします。
**ステップ 2** ループバック テストの設定頻度を設定します。
**ステップ 3** ループバック テストのフレーム長を設定します。
**ステップ 4** ハードウェア障害処理を設定します。
**ステップ 5** テストの実行要件を実行します。
**ステップ 6** 古いエラー通知をクリアします。
**ステップ 7** 内部ループバック テストを実行します。
**ステップ 8** 外部ループバック テストを実行します。
**ステップ 9** Serdes ループバックを実行します。

# システム正常化の開始を有効にする

デフォルトでは、システム ヘルス機能は Cisco MDS 9000 ファミリの各スイッチでイネーブルです。

Cisco MDS 9000 ファミリの任意のスイッチでこの機能をディセーブルまたはイネーブルにするには、次の手順を実行します。

**手順**

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **no system health**

システムの正常性が無効です。

このスイッチでテストを実行できないようにシステム ヘルスを設定します。

**ステップ 3** switch(config)# **system health**

システムの正常性が有効です。

このスイッチでテストを実行できるようにシステム ヘルスを設定します（デフォルト）。

**ステップ 4** switch(config)# **no system health interface fc8/1**

インターフェイス fc8/13 のシステム ヘルスは無効です。

指定されたインターフェイスのテストを実行できないようにシステム ヘルスを設定します。

**ステップ 5** switch(config)# **system health interface fc8/1**

インターフェイス fc8/13 のシステム ヘルスが有効になっているとします。

システム ヘルスをイネーブル（デフォルト）にして、指定されたインターフェイスをテストします。

# ループバック テストの設定頻度の設定

スイッチのすべてのモジュールにループバック テストの頻度を設定するには、次の手順を実行します。

**手順**

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **system health loopback frequency 50**

```
The new frequency is set at 50 Seconds.
```

ループバック頻度を 50 秒に設定します。デフォルトのループバック頻度は 5 秒です。有効な範囲は 5 ～ 255 秒です。

# ループバック テスト設定のフレーム長の設定

スイッチのすべてのモジュールにループバック テストのフレーム長を設定するには、次の手順を実行します。

**手順**

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **system health loopback frame-length 128**

ループバック フレーム長を 128 バイトに設定します。有効範囲は 0 ～ 128 バイトです。

**ステップ 3** switch(config)# **system health loopback frame-length auto**

ループバック フレーム長を自動的にランダム長（デフォルト）を生成するように設定します。

# ハードウェアの障害処理の設定

スイッチの障害処理を設定するには、次の手順を実行します。

**手順**

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **system health failure-action**

```
System health global failure action is now enabled.
```

障害処理を実行できるようにスイッチを設定します（デフォルト）。

**ステップ 3** switch(config)# **no system health failure-action**

```
System health global failure action now disabled.
```

障害処理が実行されないようにスイッチの設定を取り消します。

**ステップ 4** switch(config)# **system health module 1 failure-action**

```
System health failure action for module 1 is now enabled.
```

モジュール 1 の障害処理を実行できるようにスイッチを設定します。

**ステップ 5** switch(config)# **no system health module 1 loopback failure-action**

```
System health failure action for module 1 loopback test is now disabled.
```

モジュール 1 のループバック テストによって発見された障害に対する障害処理を実行しないようにスイッチを設定します。

# テストの実行要件

特定のモジュールで必要なテストを実行するには、次の手順を実行します。

**手順**

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

（注） 次のステップは、任意の順序で実行できます。

（注） それぞれのテストの各種オプションについては、次のステップで説明します。各コマンドは任意の順序で設定できます。説明のため、各種オプションを同じステップに記述しています。

**ステップ 2** switch(config)# **system health module 8 bootflash**

スロット 8 のモジュールでブートフラッシュ テストをイネーブルにします。

**ステップ 3** switch(config)# **system health module 8 bootflash frequency 200**

モジュール 8 のブートフラッシュ テストの新しい頻度を 200 秒に設定します。

**ステップ 4** switch(config)# **system health module 8 eobc**

スロット 8 のモジュールで EOBC テストをイネーブルにします。

**ステップ 5** switch(config)# **system health module 8 loopback**

スロット 8 のモジュールでループバック テストをイネーブルにします。

**ステップ 6** switch(config)# **system health module 5 management**

スロット 5 のモジュールで管理テストをイネーブルにします。

# 前回のエラー レポートのクリア

Use the EXEC-level **system health clear-errors** command at the interface or module level to erase any previous error conditions logged by the system health application. The **bootflash**, the **eobc**, the **inband**, the **loopback**, and the **mgmt** test options can be individually specified for a given module.

次の例では、指定されたファイバチャネルインターフェイスのエラー履歴がクリアされます。

```
switch# system health clear-errors interface fc 3/1
```

次の例では、指定されたモジュールのエラー履歴がクリアされます。

```
switch# system health clear-errors module 3
```

次の例では、指定されたモジュールの管理テストのエラー履歴がクリアされます。

```
switch# system health clear-errors module 1 mgmt
```

# 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。

Use the EXEC-level **system health internal-loopback** command to explicitly run this test on demand (when requested by the user) within ports for the entire module.

```
switch# system health internal-loopback interface iscsi 8/1
Internal loopback test on interface iscsi8/1 was  successful.
Sent 1 received 1 frames
Round trip time taken is 79 useconds
```

Use the EXEC-level **system health internal-loopback** command to explicitly run this test on demand (when requested by the user) within ports for the entire module and override the frame count configured on the switch.

```
switch# system health internal-loopback interface iscsi 8/1 frame-count 20
Internal loopback test on interface iscsi8/1 was  successful.
Sent 1 received 1 frames
```

```
Round trip time taken is 79 useconds
```

Use the EXEC-level **system health internal-loopback** command to explicitly run this test on demand (when requested by the user) within ports for the entire module and override the frame length configured on the switch.

```
switch# system health internal-loopback interface iscsi 8/1 frame-count 32
Internal loopback test on interface iscsi8/1 was  successful.
Sent 1 received 1 frames
Round trip time taken is 79 useconds
```

（注） テストを正常に完了できない場合、ソフトウェアが障害を分析し、次のエラーを出力します。「インターフェイス fc 7/2 の外部ループバック テストに失敗しました。Failure reason: Failed to loopback, analysis complete Failed device ID 3 on module 1

# 外部ループバック テストの実行

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

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

Use the EXEC-level **system health external-loopback interface** *interface* command to run this test on demand for external devices connected to a switch that is part of a long-haul network.

```
switch# system health external-loopback interface fc 3/1
This will shut the requested interfaces Do you want to continue (y/n)?  [n] y
External loopback test on interface fc3/1 was  successful.
Sent 1 received 1 frames
```

Use the EXEC-level **system health external-loopback source** *interface* **destination interface** *interface* command to run this test on demand between two ports on the switch.

```
switch# system health external-loopback source interface fc 3/1 destination interface
fc 3/2
This will shut the requested interfaces Do you want to continue (y/n)?  [n] y
External loopback test on interface fc3/1 and interface fc3/2 was  successful.
Sent 1 received 1 frames
```

Use the EXEC-level **system health external-loopback** *interface* **frame-count** command to run this test on demand for external devices connected to a switch that is part of a long-haul network and override the frame count configured on the switch.

```
switch# system health external-loopback interface fc 3/1 frame-count 10
This will shut the requested interfaces Do you want to continue (y/n)?  [n] y
External loopback test on interface fc3/1 was  successful.
Sent 1 received 1 frames
```

Use the EXEC-level **system health external-loopback** *interface* **frame-length** command to run this test on demand for external devices connected to a switch that is part of a long-haul network and override the frame length configured on the switch.

```
switch# system health external-loopback interface fc 3/1 frame-length 64
This will shut the requested interfaces Do you want to continue (y/n)?  [n] y
External loopback test on interface fc3/1 was  successful.
Sent 1 received 1 frames
```

Use the **system health external-loopback** *interface* **force** command to shut down the required interface directly without a back out confirmation.

```
switch# system health external-loopback interface fc 3/1 force
External loopback test on interface fc3/1 was  successful.
Sent 1 received 1 frames
```

（注） テストを正常に完了できない場合、ソフトウェアが障害を分析し、次のエラーを出力します。「インターフェイス fc 7/2 の外部ループバック テストに失敗しました。Failure reason: Failed to loopback, analysis complete Failed device ID 3 on module 1

# Serdes ループバックの実行

シリアライザ/デシリアライザ（serdes）ループバックでは、ポートのハードウェアがテストされます。このテストは、ファイバ チャネル インターフェイスで使用できます。

Use the EXEC-level **system health serdes-loopback** command to explicitly run this test on demand (when requested by the user) within ports for the entire module.

```
switch# system health serdes-loopback interface fc 3/1
This will shut the requested interfaces Do you want to continue (y/n)?  [n] y
Serdes loopback test passed for module 3 port 1
```

Use the EXEC-level **system health serdes-loopback** command to explicitly run this test on demand (when requested by the user) within ports for the entire module and override the frame count configured on the switch.

```
switch# system health serdes-loopback interface fc 3/1 frame-count 10
This will shut the requested interfaces Do you want to continue (y/n)?  [n] y
Serdes loopback test passed for module 3 port 1
```

Use the EXEC-level **system health serdes-loopback** command to explicitly run this test on demand (when requested by the user) within ports for the entire module and override the frame length configured on the switch.

```
switch# system health serdes-loopback interface fc 3/1 frame-length 32
This will shut the requested interfaces Do you want to continue (y/n)?  [n] y
Serdes loopback test passed for module 3 port 1
```

（注） 正常に完了するテストが失敗すると、本ソフトウェアの障害を分析およびは次のエラーを出力: インターフェイス fc 3/1 の外部ループバック テストに失敗しました。Failure reason: Failed to loopback, analysis complete Failed device ID 3 on module 3.

# オンボード障害ロギングの設定

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

## スイッチの OBFL の設定

スイッチのすべてのモジュールに OBFL を設定するには、次の手順を実行します。:

**手順**

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **hw-module logging onboard**

すべての OBFL 機能をイネーブルにします。

（注） この CLI は、no hw-module logging onboard コマンドによって無効になっている OBFL 機能のみ有効にできます。個別に無効になっている OBFL 機能については、hw-module logging onboard obfl-feature コマンドを使用して有効にしてください。

**ステップ 3** switch(config)# **hw-module logging onboard cpu-hog**

OBFL CPU hog イベントをイネーブルにします。

**ステップ 4** switch(config)# **hw-module logging onboard environmental-history**

OBFL 環境履歴をイネーブルにします。

**ステップ 5** switch(config)# **hw-module logging onboard error-stats**

OBFL エラー統計をイネーブルにします。

**ステップ 6** switch(config)# **hw-module logging onboard interrupt-stats**

OBFL 割り込み統計をイネーブルにします。

**ステップ 7** switch(config)# **hw-module logging onboard mem-leak**

OBFL メモリ リーク イベントをイネーブルにします。

**ステップ 8** switch(config)# **hw-module logging onboard miscellaneous-error**

OBFL のその他の情報をイネーブルにします。

**ステップ 9** switch(config)# **hw-module logging onboard obfl-log**

ブート動作時間、デバイス バージョン、および OBFL 履歴をイネーブルにします。

**ステップ 10** switch(config)# **no hw-module logging onboard**

すべての OBFL 機能をディセーブルにします。

# モジュールに対する OBFL の設定

スイッチの特定のモジュールに OBFL を設定するには、次の手順を実行します。:

**手順**

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **hw-module logging onboard module 1**

モジュールのすべての OBFL 機能をイネーブルにします。

**ステップ 3** switch(config)# **hw-module logging onboard module 1 cpu-hog**

モジュールの OBFL CPU hog イベントをイネーブルにします。

**ステップ 4** switch(config)# **hw-module logging onboard module 1 environmental-history**

モジュールの OBFL 環境履歴をイネーブルにします。

**ステップ 5** switch(config)# **hw-module logging onboard module 1 error-stats**

モジュールの OBFL エラー統計情報をイネーブルにします。

**ステップ 6** switch(config)# **hw-module logging onboard module 1 interrupt-stats**

モジュールの OBFL 割り込み統計情報をイネーブルにします。

**ステップ 7** switch(config)# **hw-module logging onboard module 1 mem-leak**

モジュールの OBFL メモリ リーク イベントをイネーブルにします。

**ステップ 8** switch(config)# **hw-module logging onboard module 1 miscellaneous-error**

モジュールの OBFL のその他の情報をイネーブルにします。

**ステップ 9** switch(config)# **hw-module logging onboard module 1 obfl-log**

モジュールのブート動作時間、デバイス バージョン、および OBFL 履歴をイネーブルにします。

**ステップ 10** switch(config)# **no hw-module logging onboard module 1**

モジュールのすべての OBFL 機能をディセーブルにします。

# モジュール カウンタの消去

（注） モジュール カウンタは、デバイス マネージャまたは DCNM SAN を使用してクリアすることはできません。

モジュール カウンタをリセットするには、次の手順に従います。

**手順**

**ステップ 1** switch# **attach module 1**

ModuleX#

モジュール 1 をシャーシに接続します。

**ステップ 2** ModuleX# **clear asic-cnt all**

モジュールのすべてのデバイスのカウンタをクリアします。

**ステップ 3** ModuleX# **clear asic-cnt list-all-devices**

modulex # **clear asic-cnt device-id** デバイス *id*

指定されたデバイス ID のみのカウンタをクリアします。デバイス ID は 1 ～ 255 の範囲で変わります。

## すべてのモジュールのカウンタをリセットする

すべてのモジュール からカウンタをリセットするには、次の手順を実行します。

### 手順

switch# **debug system internal clear-counters all**

スイッチ内のすべてのモジュールのカウンタを消去します。

# システム プロセスおよびログの設定の確認

システム プロセスおよびログ設定情報を表示するには、次のいずれかの作業を行います。

| コマンド | 目的 |
|---|---|
| **show processes** | システム プロセスを表示します |
| **show system** | システムに関連するステータス情報を表示します |
| **show system cores** | コアをコピーするため、現在設定されている方式を表示します |
| **show system health** | システムに関連するステータス情報を表示します |
| **show system health loopback frame-length** | ループバック頻度設定を確認します |
| **show logging onboard status** | OBFL の設定ステータスを表示します |

これらのコマンドの出力に表示されるフィールドの詳細については、「http://www.cisco.com/c/en/us/support/storage-networking/mds-9000-nx-os-san-os-software/products-command-reference-list.htmlCisco MDS 9000 Family Command Reference」を参照してください。

# システム プロセスの表示

Use the **show processes** command to obtain general information about all processes (see CPU 使用率情報 （156 ページ） to プロセスに関するメモリ情報 （158 ページ）).

### システム プロセスの表示

次の例では、システム プロセスを示します。

```
switch# show processes
```

```
PID    State  PC        Start_cnt    TTY   Process
-----  -----  --------  -----------  ----  -------------
  868      S  2ae4f33e            1     -  snmpd
  869      S  2acee33e            1     -  rscn
  870      S  2ac36c24            1     -  qos
  871      S  2ac44c24            1     -  port-channel
  872      S  2ac7a33e            1     -  ntp
    -     ER         -            1     -  mdog
    -     NR         -            0     -  vbuilder
```

それぞれの説明は次のとおりです。

- ProcessId = プロセス ID
- State = プロセスの状態
  - D = 中断なしで休止（通常 I/O）
  - R = 実行可能（実行キュー上）
  - S = 休止中
  - T = トレースまたは停止
  - Z = defunct (「ゾンビ」) プロセス.
- NR = 実行されていない。
- ER = 実行されているべきだが、現在は実行されていない
- PC = 現在のプログラム カウンタ（16 進形式）
- Start_cnt = プロセスがこれまでに開始（または再開）された回数
- TTY = プロセスを制御している端末通常、「-」（ハイフン）は、特定の TTY 上で実行されていないデーモンを表します。
- process name = プロセスの名前。

### CPU 使用率情報

次の例では、CPU 使用率情報を表示する方法を示します。

```
switch# show processes cpu
PID    Runtime(ms)  Invoked   uSecs  1Sec   Process
-----  -----------  --------  -----  -----  -----------
  842         3807    137001     27    0.0  sysmgr
 1112         1220     67974     17    0.0  syslogd
 1269          220     13568     16    0.0  fcfwd
 1276         2901     15419    188    0.0  zone
 1277          738     21010     35    0.0  xbar_client
 1278         1159      6789    170    0.0  wwn
 1279          515     67617      7    0.0  vsan
```

それぞれの説明は次のとおりです。

- 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。
- Runtime CPU Time (ms) = プロセスが使用した CPU 時間（ミリ秒）
- Invoked = プロセスがこれまでに開始された回数
- uSecs = プロセスの呼び出しごとの平均 CPU 時間（ミリ秒単位）

- 1Sec = 最近の 1 秒間における CPU 使用率（パーセント単位）

### プロセス ログ情報

次の例では、プロセス ログ情報を示します。

```
switch# show processes log
Process           PID     Normal-exit  Stack-trace  Core     Log-create-time
---------------  ------  -----------  -----------  -------  ---------------
fspf              1339              N            Y        N  Jan  5 04:25
lcm               1559              N            Y        N  Jan  2 04:49
rib               1741              N            Y        N  Jan  1 06:05
```

それぞれの説明は次のとおりです。

- Normal-exit = プロセスが正常に終了したかどうか。
- Stack-trace = スタック トレースがログに存在したかどうか。
- Core = コア ファイルが存在するかどうか。
- Log-create-time = ログ ファイルが生成される時間。

### プロセスに関する詳細ログ情報

次の例では、プロセスについての詳細ログ情報を示します。

```
switch# show processes log pid 1339

Service: fspf
Description: FSPF Routing Protocol Application
Started at Sat Jan  5 03:23:44 1980 (545631 us)
Stopped at Sat Jan  5 04:25:57 1980 (819598 us)
Uptime: 1 hours 2 minutes 2 seconds
Start type: SRV_OPTION_RESTART_STATELESS (23)
Death reason: SYSMGR_DEATH_REASON_FAILURE_SIGNAL (2)
Exit code: signal 9 (no core)
CWD: /var/sysmgr/work
Virtual Memory:
    CODE      08048000 - 0809A100
    DATA      0809B100 - 0809B65C
    BRK       0809D988 - 080CD000
    STACK     7FFFFD20
    TOTAL     23764 KB
Register Set:
    EBX 00000005         ECX 7FFFF8CC         EDX 00000000
    ESI 00000000         EDI 7FFFF6CC         EBP 7FFFF95C
    EAX FFFFFDFE         XDS 8010002B         XES 0000002B
    EAX 0000008E (orig)  EIP 2ACE133E         XCS 00000023
    EFL 00000207         ESP 7FFFF654         XSS 0000002B
Stack: 1740 bytes. ESP 7FFFF654, TOP 7FFFFD20
0x7FFFF654: 00000000 00000008 00000003 08051E95 .................
0x7FFFF664: 00000005 7FFFF8CC 00000000 00000000 .................
0x7FFFF674: 7FFFF6CC 00000001 7FFFF95C 080522CD ........\....".."
0x7FFFF684: 7FFFF9A4 00000008 7FFFFC34 2AC1F18C ........4......*
```

### すべてのプロセス ログの詳細

次の例では、すべてのプロセス ログ詳細を示します。

```
switch# show processes log details
============================================================
Service: snmpd
Description: SNMP Agent
Started at Wed Jan  9 00:14:55 1980 (597263 us)
Stopped at Fri Jan 11 10:08:36 1980 (649860 us)
Uptime: 2 days 9 hours 53 minutes 53 seconds
Start type: SRV_OPTION_RESTART_STATEFUL (24)
Death reason: SYSMGR_DEATH_REASON_FAILURE_SIGNAL (2)
Exit code: signal 6 (core dumped)
CWD: /var/sysmgr/work
Virtual Memory:
    CODE      08048000 - 0804C4A0
    DATA      0804D4A0 - 0804D770
    BRK       0804DFC4 - 0818F000
    STACK     7FFFFCE0
    TOTAL     26656 KB
...
```

### プロセスに関するメモリ情報

次の例では、プロセスについてメモリ情報を示します。

```
switch# show processes memory
PID    MemAlloc  MemLimit    MemUsed     StackBase/Ptr      Process
-----  --------  ----------  ----------  -----------------  ----------------
    1    147456  0      1667072     7ffffe50/7ffff950      init
    2         0  0            0                  0/0         ksoftirqd/0
    3         0  0            0                  0/0         desched/0
    4         0  0            0                  0/0         events/0
    5         0  0            0                  0/0         khelper
```

それぞれの説明は次のとおりです。

- MemAlloc = プロセスで割り当てられたメモリの総容量。
- StackBase/Ptr = プロセス スタック ベースと現在のスタック ポインタ（16 進形式）。.

# システム ステータスの表示

Use the **show system** command to display system-related status information (see デフォルトのスイッチ ポートの状態 （158 ページ） to システム関連 CPU およびメモリ情報 （160 ページ）).

### デフォルトのスイッチ ポートの状態

次の例では、デフォルトのスイッチ ポート状態を示します。

```
switch# show system default switchport
```

```
System default port state is down
System default trunk mode is on
```

### 指定された ID のエラー情報

次の例では、指定した ID のエラー情報を示します。

```
switch# show system error-id 0x401D0019
Error Facility: module
Error Description: Failed to stop Linecard Async Notification.
```

### システム リセット情報

次の例では、システム リセット情報を示します。

```
switch# Show system reset-reason module 5
----- reset reason for module 5 -----
1) At 224801 usecs after Fri Nov 21 16:36:40 2003
    Reason: Reset Requested by CLI command reload
    Service:
    Version: 1.3(1)
2) At 922828 usecs after Fri Nov 21 16:02:48 2003
    Reason: Reset Requested by CLI command reload
    Service:
    Version: 1.3(1)
3) At 318034 usecs after Fri Nov 21 14:03:36 2003
    Reason: Reset Requested by CLI command reload
    Service:
    Version: 1.3(1)
4) At 255842 usecs after Wed Nov 19 00:07:49 2003
    Reason: Reset Requested by CLI command reload
    Service:
    Version: 1.3(1)
```

The **show system reset-reason** command displays the following information:

- Cisco MDS 9513 ディレクタでは、スロット 7 およびスロット 8 にあるスーパーバイザ モジュールの最後の 4 つのリセット理由コードが表示されます。いずれかのスーパーバイザ モジュールが不在の場合、そのスーパーバイザ モジュールのリセット理由コードは表示されません。
- Cisco MDS 9506 または Cisco MDS 9509 スイッチでは、スロット 5 およびスロット 6 にあるスーパーバイザ モジュールの最後の 4 つのリセット理由コードが表示されます。いずれかのスーパーバイザ モジュールが不在の場合、そのスーパーバイザ モジュールのリセット理由コードは表示されません。
- Cisco MDS 9200 シリーズ スイッチでは、スロット 1 にあるスーパーバイザ モジュールの最後の 4 つのリセット理由コードが表示されます。
- The **show system reset-reason module** *number* command displays the last four reset-reason codes for a specific module in a given slot. モジュールが不在の場合、そのモジュールのリセット理由コードは表示されません。

Use the **clear system reset-reason** command to clear the reset-reason information stored in NVRAM and volatile persistent storage.

- Cisco MDS 9500 シリーズ スイッチでは、このコマンドで、アクティブおよびスタンバイ スーパーバイザ モジュールの NVRAM に保存されているリセット理由情報をクリアします。
- Cisco MDS 9200 シリーズ スイッチでは、このコマンドで、アクティブ スーパーバイザ モジュールの NVRAM に保存されているリセット理由情報をクリアします。

### System Uptime

次の例は、システム稼働時間を示しています。

```
switch# show system uptime
Start Time: Sun Oct 13 18:09:23 2030
Up Time:    0 days, 9 hours, 46 minutes, 26 seconds
```

Use the **show system resources** command to display system-related CPU and memory statistics (see システム関連 CPU およびメモリ情報 （160 ページ）).

### システム関連 CPU およびメモリ情報

次の例では、システム関連 CPU およびメモリ情報を示します。

```
switch# show system resources
Load average:   1 minute: 0.43   5 minutes: 0.17   15 minutes: 0.11
Processes   :   100 total, 2 running
CPU states  :   0.0% user,   0.0% kernel,   100.0% idle
Memory usage:   1027628K total,    313424K used,    714204K free
                   3620K buffers,   22278K cache
```

それぞれの説明は次のとおりです。

- Load average：実行中のプロセス数が表示されます。Load average には、過去 1 分間、5 分間、および 15 分間のシステム負荷が表示されます。
- Processes：システム内のプロセス数、およびコマンド発行時に実際に実行されていたプロセス数が表示されます。
- CPU states：直前の 1 秒間における CPU のユーザ モードとカーネル モードでの使用率およびアイドル時間がパーセントで表示されます。
- Memory usage：合計メモリ、使用中メモリ、空きメモリ、バッファに使用されているメモリ、およびキャッシュに使用されているメモリが KB 単位で表示されます。また、バッファおよびキャッシュには、使用中メモリの統計情報も含まれます。

# コア ステータスの表示

Use the **show system cores** command to display the currently configured scheme for copying cores. 例 コアが TFTP に転送されるときのメッセージ （161 ページ） ～ Logs on the Local System （161 ページ） を参照してください。

### コアが TFTP に転送されるときのメッセージ

次の例では、コアが TFTP に転送されると、メッセージが表示されます。

```
switch# show system cores
Cores are transferred to tftp://171.69.21.28/ernguyen/CORE/
```

### コアが外部 CF に転送されるときのメッセージ

次の例では、コアが外部 CF に転送されると、メッセージが表示されます。

```
switch(config)# show system cores
Cores are transferred to slot0:abcd
```

### All Cores Available for Upload from the Active Supervisor Module

The following example displays all cores available for upload from the active supervisor module:

```
switch# show cores
Module-num  Process-name    PID     Core-create-time
----------  ------------    ---     ----------------
5           fspf            1524    Nov 9 03:11
6           fcc             919     Nov 9 03:09
8           acltcam         285     Nov 9 03:09
8           fib             283     Nov 9 03:08
```

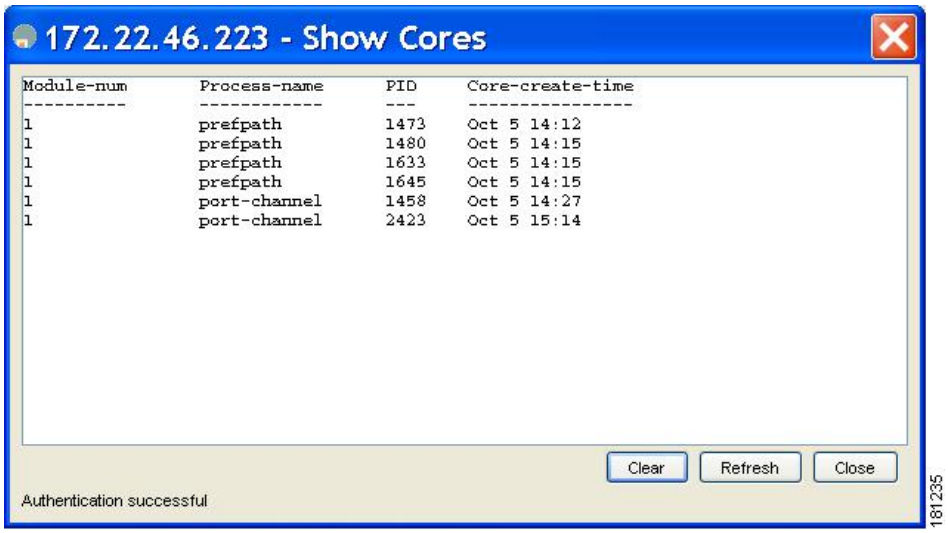
### Logs on the Local System

次の例では、ローカル システムのログを表示します。

```
switch# show processes log
Process           PID     Normal-exit  Stack  Core   Log-create-time
----------------  ------  -----------  -----  -----  ---------------
ExceptionLog      2862              N      Y      N  Wed Aug  6 15:08:34 2003
acl               2299              N      Y      N  Tue Oct 28 02:50:01 2003
bios_daemon       2227              N      Y      N  Mon Sep 29 15:30:51 2003
capability        2373              N      Y      N  Tue Aug 19 13:30:02 2003
core-client       2262              N      Y      N  Mon Sep 29 15:30:51 2003
fcanalyzer        5623              N      Y      N  Fri Sep 26 20:45:09 2003
fcd               12996             N      Y      N  Fri Oct 17 20:35:01 2003
fcdomain          2410              N      Y      N  Thu Jun 12 09:30:58 2003
ficon             2708              N      Y      N  Wed Nov 12 18:34:02 2003
ficonstat         9640              N      Y      N  Tue Sep 30 22:55:03 2003
flogi             1300              N      Y      N  Fri Jun 20 08:52:33 2003
idehsd            2176              N      Y      N  Tue Jun 24 05:10:56 2003
lmgrd             2220              N      N      N  Mon Sep 29 15:30:51 2003
platform          2840              N      Y      N  Sat Oct 11 18:29:42 2003
port-security     3098              N      Y      N  Sun Sep 14 22:10:28 2003
port              11818             N      Y      N  Mon Nov 17 23:13:37 2003
rlir              3195              N      Y      N  Fri Jun 27 18:01:05 2003
rscn              2319              N      Y      N  Mon Sep 29 21:19:14 2003
securityd         2239              N      N      N  Thu Oct 16 18:51:39 2003
snmpd             2364              N      Y      N  Mon Nov 17 23:19:39 2003
```

```
span                2220            N       Y       N  Mon Sep 29 21:19:13 2003
syslogd             2076            N       Y       N  Sat Oct 11 18:29:40 2003
tcap                2864            N       Y       N  Wed Aug  6 15:09:04 2003
tftpd               2021            N       Y       N  Mon Sep 29 15:30:51 2003
vpm                 2930            N       N       N  Mon Nov 17 19:14:33 2003
```

図 *4 : [Show Cores]* ダイアログボックス




# 最初と最後のコア ステータスの確認

You can view specific information about the saved core files. 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 （162 ページ） provides further details on saved core files.

### 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
```

# システム ヘルスの表示

Use the **show system health** command to display system-related status information (see スイッチ内のすべてのモジュールの現在のヘルス情報 （163ページ） to指定されたモジュールのループバック テスト時間ログ （165 ページ）).

### スイッチ内のすべてのモジュールの現在のヘルス情報

次の例では、スイッチ内のすべてのモジュールの現在のヘルス情報を示します。

```
switch# show system health

Current health information for module 2.
Test                        Frequency    Status          Action
------------------------------------------------------------------
Bootflash                  5 Sec         Running         Enabled
EOBC                       5 Sec         Running         Enabled
Loopback                   5 Sec         Running         Enabled
------------------------------------------------------------------
Current health information for module 6.
Test                        Frequency    Status          Action
------------------------------------------------------------------
InBand                     5 Sec         Running         Enabled
Bootflash                  5 Sec         Running         Enabled
EOBC                       5 Sec         Running         Enabled
Management Port            5 Sec         Running         Enabled
------------------------------------------------------------------
```

### 指定されたモジュールの現在のヘルス情報

次の例では、指定されたモジュールの現在のヘルス情報を示します。

```
switch# show system health module 8
Current health information for module 8.
Test                        Frequency    Status          Action
------------------------------------------------------------------
Bootflash                  5 Sec         Running         Enabled
EOBC                       5 Sec         Running         Enabled
Loopback                   5 Sec         Running         Enabled
------------------------------------------------------------------
```

### すべてのモジュールのヘルス統計情報

次の例では、すべてのモジュールのヘルス統計情報を示します。

```
switch# show system health statistics
Test statistics for module # 1
-------------------------------------------------------------------------------
Test Name           State            Frequency Run    Pass    Fail CFail Errs
-------------------------------------------------------------------------------
Bootflash           Running             5s    12900   12900       0     0    0
EOBC                Running             5s    12900   12900       0     0    0
Loopback            Running             5s    12900   12900       0     0    0
-------------------------------------------------------------------------------
```

```
Test statistics for module # 3
----------------------------------------------------------------------------
Test Name           State            Frequency Run    Pass    Fail CFail Errs
----------------------------------------------------------------------------
Bootflash           Running             5s    12890   12890       0     0    0
EOBC                Running             5s    12890   12890       0     0    0
Loopback            Running             5s    12892   12892       0     0    0
----------------------------------------------------------------------------
Test statistics for module # 5
----------------------------------------------------------------------------
Test Name           State            Frequency Run    Pass    Fail CFail Errs
----------------------------------------------------------------------------
InBand              Running             5s    12911   12911       0     0    0
Bootflash           Running             5s    12911   12911       0     0    0
EOBC                Running             5s    12911   12911       0     0    0
Management Port     Running             5s    12911   12911       0     0    0
----------------------------------------------------------------------------
Test statistics for module # 6
----------------------------------------------------------------------------
Test Name           State            Frequency Run    Pass    Fail CFail Errs
----------------------------------------------------------------------------
InBand              Running             5s    12907   12907       0     0    0
Bootflash           Running             5s    12907   12907       0     0    0
EOBC                Running             5s    12907   12907       0     0    0
----------------------------------------------------------------------------
Test statistics for module # 8
----------------------------------------------------------------------------
Test Name           State            Frequency Run    Pass    Fail CFail Errs
----------------------------------------------------------------------------
Bootflash           Running             5s    12895   12895       0     0    0
EOBC                Running             5s    12895   12895       0     0    0
Loopback            Running             5s    12896   12896       0     0    0
----------------------------------------------------------------------------
```

### 指定されたモジュールの統計情報の表示

次の例では、指定されたモジュール の統計情報を示します。

```
switch# show system health statistics module 3
Test statistics for module # 3
----------------------------------------------------------------------------
Test Name           State            Frequency Run    Pass    Fail CFail Errs
----------------------------------------------------------------------------
Bootflash           Running             5s    12932   12932       0     0    0
EOBC                Running             5s    12932   12932       0     0    0
Loopback            Running             5s    12934   12934       0     0    0
----------------------------------------------------------------------------
```

### スイッチ全体のループバック テストの統計情報

次の例では、スイッチ全体のループバック テストの統計情報を示します。

```
switch# show system health statistics loopback
-----------------------------------------------------------------
Mod Port Status                Run     Pass     Fail   CFail Errs
  1   16 Running             12953    12953        0       0    0
  3   32 Running             12945    12945        0       0    0
```

```
  8    8 Running             12949    12949        0       0    0
----------------------------------------------------------------------
```

### 指定されたインターフェイスのループバック テスト統計情報

次の例では、指定されたインターフェイスのループバック テスト統計情報を示します。

```
switch# show system health statistics loopback interface fc 3/1
----------------------------------------------------------------------
Mod Port Status                Run     Pass     Fail   CFail Errs
  3    1 Running                 0        0        0       0    0
----------------------------------------------------------------------
```

（注） モジュール固有のループバック テストでエラーまたは障害が報告されない限り、インターフェイス固有のカウンタはゼロのままです。

### すべてのモジュールのループバック テスト時間ログ

次の例では、すべてのモジュールのループバック テスト時間ログを示します。

```
switch# show system health statistics loopback timelog
----------------------------------------------------------------------
Mod        Samples     Min(usecs)     Max(usecs)     Ave(usecs)
  1           1872            149            364            222
  3           1862            415            743            549
  8           1865            134            455            349
----------------------------------------------------------------------
```

### 指定されたモジュールのループバック テスト時間ログ

次の例では、指定されたモジュールのループバック テスト時間ログを示します。

```
switch# show system health statistics loopback module 8 timelog
----------------------------------------------------------------------
Mod        Samples     Min(usecs)     Max(usecs)     Ave(usecs)
  8           1867            134            455            349
----------------------------------------------------------------------
```

# ループバック テストのフレーム長の設定の確認

To verify the loopback frequency configuration, use the **show system health loopback frame-length** command.

```
switch# show system health loopback frame-length
Loopback frame length is set to auto-size between 0-128 bytes
```

# スイッチの OBFL の表示

Use the **show logging onboard status** command to display the configuration status of OBFL.

```
switch# show logging onboard status
    Switch OBFL Log:                                        Enabled
    Module:  6 OBFL Log:                                    Enabled
    error-stats                                             Enabled
    exception-log                                           Enabled
    miscellaneous-error                                     Enabled
    obfl-log (boot-uptime/device-version/obfl-history)  Enabled
    system-health                                           Enabled
    stack-trace                                             Enabled
```

# モジュールの OBFL の表示

Use the **show logging onboard status** command to display the configuration status of OBFL.

```
switch# show logging onboard status
    Switch OBFL Log:                                        Enabled
Module:  6 OBFL Log:                                    Enabled
    error-stats                                             Enabled
    exception-log                                           Enabled
    miscellaneous-error                                     Enabled
    obfl-log (boot-uptime/device-version/obfl-history)  Enabled
    system-health                                           Enabled
    stack-trace                                             Enabled
```

# OBFL ログの表示

モジュールの CompactFlash に保存されている OBFL 情報を表示するには、次のコマンドを使用します。

| コマンド | 目的 |
|---|---|
| **show logging onboard boot-uptime** | ブートおよび動作時間の情報を表示します。 |
| **show logging onboard cpu-hog** | CPU hog イベントの情報を表示します。 |
| **show logging onboard device-version** | デバイス バージョン情報を表示します。 |
| **show logging onboard endtime** | 終了時刻までの OBFL ログを表示します。 |
| **show logging onboard environmental-history** | 環境履歴を表示します。 |
| **show logging onboard error-stats** | エラー統計情報を表示します。 |
| **show logging onboard exception-log** | 例外ログ情報を表示します。 |
| **show logging onboard interrupt-stats** | 割り込み統計情報を表示します。 |
| **show logging onboard mem-leak** | メモリ リーク情報を表示します。 |

| コマンド | 目的 |
|---|---|
| **show logging onboard miscellaneous-error** | 各種エラー情報を表示します。 |
| **show logging onboard module** *slot* | 指定したモジュールのOBFL情報を表示します。 |
| **show logging onboard obfl-history** | 履歴情報を表示します。 |
| **show logging onboard register-log** | 登録ログ情報を表示します。 |
| **show logging onboard stack-trace** | カーネル スタック トレース情報を表示します。 |
| **show logging onboard starttime** | 指定した開始時刻からの OBFL ログを表示します。 |
| **show logging onboard system-health** | システム ヘルス情報を表示します。 |

## モジュール カウンタ情報の表示

この例では、モジュールのすべてのデバイスのデバイス ID を示します。

```
switch# attach  module 4
Attaching to module 4 ...
To exit type 'exit', to abort type '$.'
Linux lc04 2.6.10_mvl401-pc_target #1 Tue Dec 16 22:58:32 PST 2008 ppc GNU/Linux

module-4# clear asic-cnt list-all-devices
           Asic Name  |        Device ID
         Stratosphere  |               63
          transceiver  |               46
         Skyline-asic  |               57
           Skyline-ni  |               60
         Skyline-xbar  |               59
          Skyline-fwd  |               58
         Tuscany-asic  |               52
         Tuscany-xbar  |               54
          Tuscany-que  |               55
          Tuscany-fwd  |               53
       Fwd-spi-group  |               73
          Fwd-parser  |               74
                eobc  |               10
            X-Bus IO  |                1
   Power Mngmnt Epld  |               25
```

# 警告、通知の設定とカウンタのモニタリング

ここでは、アラート、通知、およびモニタカウンタを設定する方法について説明します。

## CPU 使用率のモニタリング

To display the system CPU utilization, use the **show processes cpu** command.

この例では、現在の VDC のプロセスと CPU 使用率を表示する方法を示します。

```
switch# show processes cpu
PID    Runtime(ms)  Invoked   uSecs  1Sec    Process
-----  -----------  --------  -----  ------  -----------
    4       386829  67421866      5    0.9%  ksoftirqd/0
3667       270567    396229    682    9.8%  syslogd
3942          262       161   1632    7.8%  netstack
4006    106999945  354495641    301   28.2%  snmpd
4026      4454796    461564   9651    0.9%  sac_usd
4424        84187    726180    115    0.9%  vpc
4426       146378    919073    159    0.9%  tunnel
CPU util  :   25.0% user,   30.5% kernel,   44.5% idle
```

# RAM の使用状況情報の入手

この SNMP 変数を使用して、プロセッサ RAM 使用率を取得することができます：ceExtProcessorRam。

```
ceExtProcessorRam OBJECT-TYPE
    SYNTAX  Unsigned32
    UNITS   "bytes"
        MAX-ACCESS  read-only
        STATUS  current
        DESCRIPTION
        "Total number of bytes of RAM available on the
         Processor."
        ::= { ceExtPhysicalProcessorEntry 1 }
```

# Rx および Tx トラフィック カウンタのモニタリング

Rx および Tx トラフィックのカウンタをモニタリングする場合は、Rx カウンタ OID を含める必要があります。

```
ifHCInOctets
```

# インターフェイスのステータス モニタリング

インターフェイスのステータスをモニタするには、ifAlias（このトラップはインターフェイスの説明を設定できます）と ifDescr を持つ IETF extended-linkDown を使用して、ポート名を以下に示すように ascii 形式で表示します。

```
switch (config)# snmp-server enable traps link
  cieLinkDown                 Cisco extended link state down notification
  cieLinkUp                   Cisco extended link state up notification
  cisco-xcvr-mon-status-chg   Cisco interface transceiver monitor status change
                             notification
  delayed-link-state-change  Delayed link state change
  extended-linkDown           IETF extended link state down notification
  extended-linkUp             IETF extended link state up notification
  linkDown                   IETF Link state down notification
  linkUp                      IETF Link state up notification
```

```
switch (config)#
```

トラップの例を次に示します。

```
[+]          10           16:41:39.79         IF-MIB:linkDown trap:SNMPv2c  from
[172.25.234.200  Port: 162 Community: public]
SNMPv2-MIB:sysUpTime.0 :  (35519336)      Syntax: TimeTicks
SNMPv2-MIB:snmpTrapOID.0 :  (IF-MIB:linkDown)      Syntax: ObjectID
IF-MIB:ifIndex.440414208 :   (440414208)  Syntax: INTEGER,  Instance IDs: (440414208)
IF-MIB:ifAdminStatus.440414208 :   (down)  Syntax: INTEGER,  Instance IDs: (440414208)
IF-MIB:ifOperStatus.440414208 :   (down)  Syntax: INTEGER,  Instance IDs: (440414208)
IF-MIB:ifDescr.440414208 :   (Ethernet9/4)  Syntax: RFC1213-MIB:DisplayString,  Instance
 IDs: (440414208)
IF-MIB:ifAlias.440414208 :   (eth9/4)  Syntax: SNMPv2-TC:DisplayString,  Instance IDs:
(440414208)
SNMPv2-MIB:snmpTrapEnterprise.0 :  (IF-MIB:linkDown)      Syntax: ObjectID
```

# トランシーバのしきい値をモニタリング

以下に示すように、しきい値のデジタル診断統計情報をモニタするトラップの cisco-警告: mon-ステータスの変更方法を使用します。

```
switch (config)# snmp-server enable traps link cisco-xcvr-mon-status-chg
switch (config)#
```

トラップ MIB は、次に示すようです。

```
cIfXcvrMonStatusChangeNotif NOTIFICATION-TYPE
    OBJECTS         {
                        ifName,
                        cIfXcvrMonDigitalDiagTempAlarm,
                        cIfXcvrMonDigitalDiagTempWarning,
                        cIfXcvrMonDigitalDiagVoltAlarm,
                        cIfXcvrMonDigitalDiagVoltWarning,
                        cIfXcvrMonDigitalDiagCurrAlarm,
                        cIfXcvrMonDigitalDiagCurrWarning,
                        cIfXcvrMonDigitalDiagRxPwrAlarm,
                        cIfXcvrMonDigitalDiagRxPwrWarning,
                        cIfXcvrMonDigitalDiagTxPwrAlarm,
                        cIfXcvrMonDigitalDiagTxPwrWarning,
                        cIfXcvrMonDigitalDiagTxFaultAlarm
                    }
    STATUS          current
```

この例は、トランシーバの詳細を表示する方法を示します。

```
switch(config)# show interface ethernet 1/17 transceiver details
Ethernet1/17
    transceiver is present
    type is 10Gbase-SR
    name is CISCO-AVAGO
    part number is SFBR-7702SDZ
    revision is G2.3
    serial number is AGA1427618P
    nominal bitrate is 10300 MBit/sec
    Link length supported for 50/125um OM2 fiber is 82 m
```

```
  Link length supported for 62.5/125um fiber is 26 m
  Link length supported for 50/125um OM3 fiber is 300 m
  cisco id is --
  cisco extended id number is 4
        SFP Detail Diagnostics Information (internal calibration)
  ----------------------------------------------------------------------------
              Current             Alarms                  Warnings
              Measurement     High        Low         High          Low
  ----------------------------------------------------------------------------
  Temperature   27.65 C        75.00 C     -5.00 C     70.00 C        0.00 C
  Voltage        3.29 V         3.63 V      2.97 V      3.46 V        3.13 V
  Current        5.42 mA       10.50 mA     2.50 mA    10.50 mA       2.50 mA
  Tx Power      -2.51 dBm       1.69 dBm  -11.30 dBm   -1.30 dBm     -7.30 dBm
  Rx Power      -2.64 dBm       1.99 dBm  -13.97 dBm   -1.00 dBm     -9.91 dBm
  Transmit Fault Count = 0
  ----------------------------------------------------------------------------
  Note: ++  high-alarm; +  high-warning; --  low-alarm; -  low-warning
switch(config)#
```

# スーパバイザ スイッチ オーバー通知の設定

CiscoRFSwactNotif トラップをリッスンすることで、スーパバイザ スイッチ オーバー通知をモニタできます。

```
ciscoRFSwactNotif NOTIFICATION-TYPE
OBJECTS {
cRFStatusUnitId,
sysUpTime,
cRFStatusLastSwactReasonCode
}
```

# CRC および FCS エラーを含むカウンタの設定

次の例に示すように、dot3StatsFCSErrors カウンタをポーリングすることで、インターフェイスの CRC と FCS エラーを含めることができます。

dot3StatsFCSErrors Counter32

```
      Dot3StatsEntry ::= SEQUENCE {
 dot3StatsIndex                    InterfaceIndex,
 dot3StatsAlignmentErrors          Counter32,
 dot3StatsFCSErrors                Counter32,
 dot3StatsSingleCollisionFrames    Counter32,
 dot3StatsMultipleCollisionFrames  Counter32,
 dot3StatsSQETestErrors            Counter32,
 dot3StatsDeferredTransmissions    Counter32,
 dot3StatsLateCollisions           Counter32,
 dot3StatsExcessiveCollisions      Counter32,
 dot3StatsInternalMacTransmitErrors Counter32,
 dot3StatsCarrierSenseErrors       Counter32,
 dot3StatsFrameTooLongs            Counter32,
 dot3StatsInternalMacReceiveErrors Counter32,
 dot3StatsEtherChipSet             OBJECT IDENTIFIER,
 dot3StatsSymbolErrors             Counter32,
 dot3StatsDuplexStatus             INTEGER,
 dot3StatsRateControlAbility       TruthValue,
 dot3StatsRateControlStatus        INTEGER
}
```

# アラートの CallHome の設定

CallHome の機能により、システムで例外が発生したときに CallHome 電子メールを受信します。CLI または SNMP を使用して、CallHome 設定をセットアップし、すべてのアラートグループを下記のように有効にします。

```
switch (config)# callhome
switch-FC-VDC(config-callhome)# destination-profile full-txt-destination alert-group
All                     This alert group consists of all of the callhome
                        messages
  Cisco-TAC             Events which are meant for Cisco TAC only
  Configuration         Events related to Configuration
  Diagnostic            Events related to Diagnostic
  EEM                   EEM events
  Environmental         Power,fan,temperature related events
  Inventory             Inventory status events
  License               Events related to licensing
  Linecard-Hardware     Linecard related events
  Supervisor-Hardware   Supervisor related events
  Syslog-group-port     Events related to syslog messages filed by port manager
  System                Software related events
  Test                  User generated test events
switch-FC-VDC(config-callhome)#
```

# ユーザー認証の障害のモニタリング

authenticationFailure トラップをリスニングすることで、ユーザー認証の障害をモニタできます。

```
SNMPv2-MIB: authenticationFailure trap
```

# その他の参考資料

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

### MIB

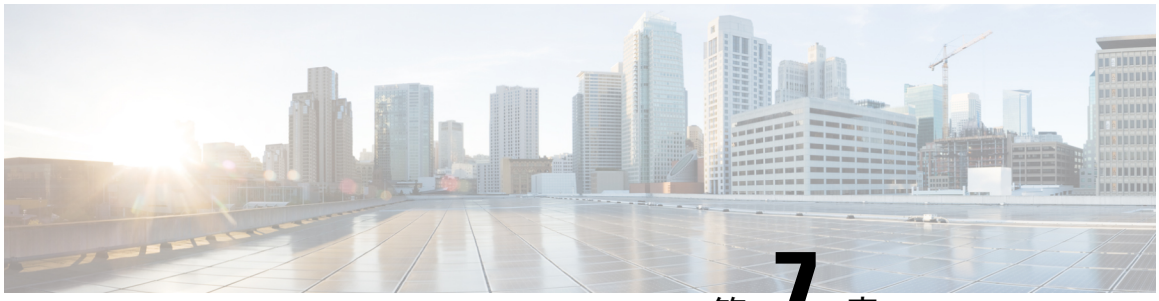
| MIB | MIB のリンク |
|---|---|
| • CISCO-SYSTEM-EXT-MIB<br>• CISCO-SYSTEM-MIB | MIB を検索およびダウンロードするには、次の URL にアクセスしてください。<br>http://www.cisco.com/en/US/products/ps5989/prod_technical_reference_list.html |

# システム プロセスおよびログの機能の履歴

表 21 : システム プロセスおよびログの機能の履歴 （172 ページ） に、この機能のリリース履歴を示します。リリース 3.x 以降のリリースで導入または変更された機能のみが表に記載されています。

表 *21* : システム プロセスおよびログの機能の履歴

| 機能名 | リリース | 機能情報 |
|---|---|---|
| 共通情報モデル（CIM） | 3.3(1a) | 一般的な情報モデルを表示する追加コマンドです。 |
| オンラインのシステム ヘルス メンテナンス (OHMS) の機能拡張 | 3.0(1) | には、次の OHMS 拡張機能が含まれています。<br>• スイッチ上のすべてのモジュールのループバック テストのグローバル フレーム長を設定します。<br>• 特定のモジュールでループバック テスト用のフレーム カウントおよびフレーム長を指定します。<br>• 外部ループバック テストの送信元と宛先ポートを設定します。<br>• ハードウェアをチェックする serdes ループバック テストに提供します。 |
| On-board failure logging (OBFL) | 3.0(1) | OBFL、第 2 世代モジュールを設定する方法、およびログ情報を表示する方法について説明します。 |



第 7 章

# Embedded Event Manager の設定

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



## EEM について

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

### EEM の概要

EEM は次の 3 種類の主要コンポーネントからなります。

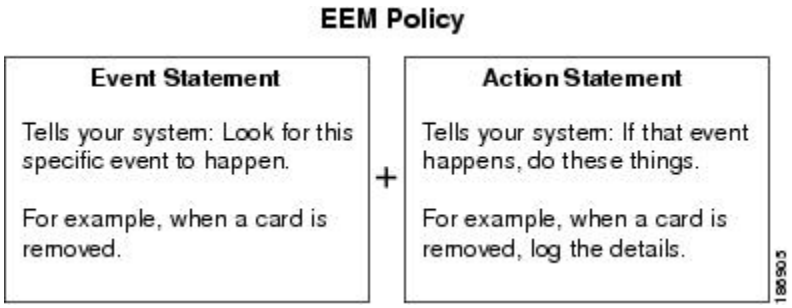
- イベント文：別の Cisco NX-OS コンポーネントからモニタし、アクション、回避策、または通知が必要になる可能性のあるイベント。
- アクション文：電子メールの送信、インターフェイスの無効化など、イベントから回復するために EEM が実行できるアクション。
- ポリシー：イベント文とアクション文の組み合わせ。指定されたイベントの発生時に、設定されているアクションが実行されます。

# ポリシー

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

図 5 : EEM ポリシー文 （174 ページ） に、EEM ポリシーの基本的な 2 種類の文を示します。

**図 *5 : EEM* ポリシー文**




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

（注） EEM ポリシー照合は、MDS スイッチ上ではサポートされません。

EEM はスーパーバイザ上でイベント ログを維持します。

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

以下は、Cisco MDS 9000 シリーズ スイッチで利用可能な事前設定システム ポリシーの一部です。

- ゾーン
  - __zone_dbsize_max_per_vsan：ゾーン データベースのサイズが vsan の 4000000 バイトの最大制限を超えた場合の Syslog 警告。
  - __zone_members_max_per_sw：ゾーン メンバの数が スイッチの 32000 の最大制限を超えた場合の Syslog 警告。
  - __zone_zones_max_per_sw：ゾーンの数がスイッチの 16000 の最大制限を超えた場合の Syslog 警告。
  - __zone_zonesets_max_per_sw：ゾーンセット数がスイッチの 1000 の最大制限を超えた場合の Syslog 警告。
- ファブリック ログイン（FLOGI）

- __flogi_fcids_max_per_switch：スイッチの flogis 数が 2000 の最大制限を超えた場合の Syslog 警告。
- __flogi_fcids_max_per_module：モジュールの flogis 数が 400 の最大制限を超えた場合の Syslog 警告。
- __Flogi_fcids_max_per_intf:：インターフェイスの flogis 数が 256 の最大制限を超えた場合の Syslog 警告。

（注） 上記 3 つの FLOGI ポリシーすべてが上書きされます。

- ファイバ チャネル名サーバ（FCNS）
  - __fcns_entries_max_per_switch：スイッチごとにすべての Vsan 間で検証される名前サーバ エントリの最大制限を設定します。

アクション：syslog を表示します。

（注） ユーザ ^ は、異なるコンポーネントのポリシーのイベントを設定する必要があります。

使用するネットワークに合わせてユーザ ポリシーを作成できます。ユーザー ポリシーで定義されたアクションは、システム ポリシーで定義されたアクションとともに実行されます。ユーザ ポリシーを設定する場合には、CLI によるユーザ ポリシーの定義（180 ページ）を参照してください。

一部のシステム ポリシーは上書きすることもできます。オーバーライド ポリシーは、システム ポリシーに置き換わります。イベントまたはアクションの上書きが可能です。

Use the **show event manager system-policy** command to view the preconfigured system policies and determine which policies that you can override.

上書きポリシーを設定する場合は、ポリシーの上書き （189 ページ）を参照してください。

（注） You should use the **show running-config eem** command to check the configuration of each policy. イベント文が指定されていて、アクション文が指定されていない上書きポリシーを設定した場合、アクションは開始されません。また、障害も通知されません。

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

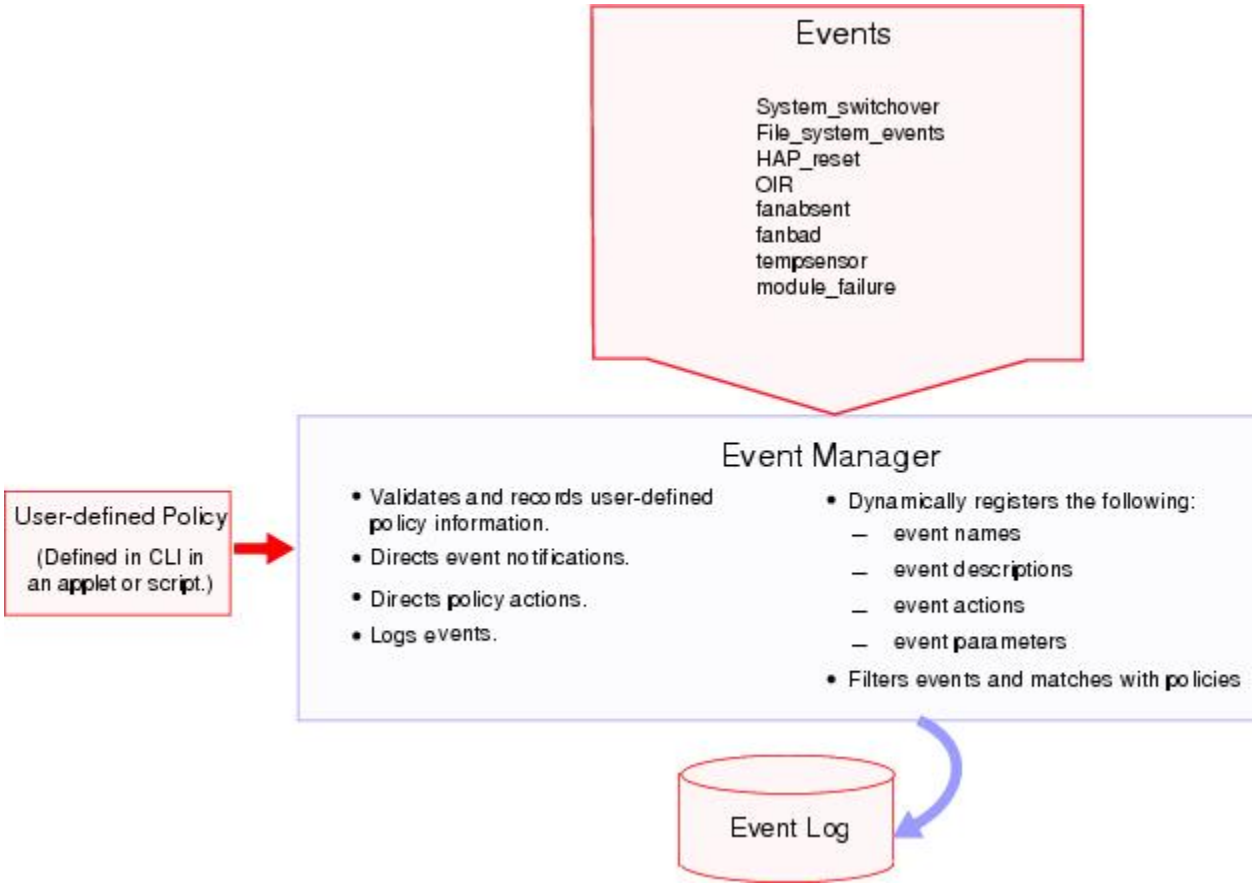
# イベント文

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

図 6 : EEM の概要 （176 ページ） EEM ではイベント フィルタを定義して、クリティカル イベントまたは指定された時間内で繰り返し発生したイベントだけが関連付けられたアクションのトリガーになるようにします。

に、EEM が処理するイベントを示します。

**図 *6 : EEM* の概要**




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

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

# アクション ステートメント

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

EEM がアクション文でサポートするアクションは、次のとおりです。

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

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

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

# VSH スクリプト ポリシー

テキスト エディタを使用し、VSH スクリプトでポリシーを作成することもできます。このようなポリシーにも、他のポリシーと同様、イベント文およびアクション文（複数可）を使用します。また、これらのポリシーでシステム ポリシーを補うことも上書きすることもできます。スクリプト ポリシーの作成後、そのポリシーをデバイスにコピーしてアクティブにします。スクリプト ポリシーを設定する場合は、VSH スクリプトによるポリシーの定義（188 ページ）を参照してください。

# 環境変数

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

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

### アクション文

この例では、「EEM action」というリセット理由を指定し、モジュール 1 を強制的にシャットダウンするアクション文の例を示します。

```
switch (config-eem-policy)# action 1.0 forceshut module 1 reset-reason "EEM action"
```

### 環境変数を使用するアクション文

シャットダウンの理由に default-reason という環境変数を定義すると、次の例のように、リセット理由を環境変数に置き換えることができます。

```
switch (config-eem-policy)# action 1.0 forceshut module 1 reset-reason $default-reason
```

この環境変数は、任意のポリシーで再利用できます。環境変数の詳細については、環境変数の定義 （190 ページ）を参照してください

# EEM イベント相関

Cisco NX-OS Release 5.2 以降では、イベントの組み合わせに基づいて EEM ポリシーをトリガーできます。First, you use the **tag** keyword to create and differentiate multiple events in the EEM policy. Then using a set of boolean operators (**and**, **or**, and **not**), along with the count and time, you can define a combination of these events to trigger a custom action.

# ハイ アベイラビリティ

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

# EEM のライセンス要件

次の表に、この機能のライセンス要件を示します。

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

# EEM の前提条件

EEM の前提条件は、次のとおりです。

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

# 注意事項と制約事項

EEM に関する設定時の注意事項および制約事項は、次のとおりです。

- ユーザ ポリシーまたは上書きポリシー内のアクション文が、相互に否定したり、関連付けられたシステム ポリシーに悪影響を与えたりするようなことがないようにする必要があります。
- トリガーされたイベントでデフォルト アクションも処理されるようにする場合は、EEM アクションをポリシーのタイプに応じて event-default または policy-default で明示的に設定する必要があります。たとえば、match 文で CLI コマンドを照合する場合、EEM ポリシーに event-default アクション文を追加する必要があります。この文がないと、EEM では CLI コマンドを実行できません。
- イベント文が指定されていて、アクション文が指定されていない上書きポリシーを設定した場合、アクションは開始されません。また、障害も通知されません。
- 上書きポリシーにイベント文が含まれていないと、システム ポリシーで可能性のあるイベントがすべて上書きされます。
- 複数のイベント文が EEM ポリシーに存在する場合は、各イベント文に **tag** キーワードと一意な tag 引数が必要です。

# デフォルト設定

表 22 : デフォルトの EEM パラメータ （179 ページ） に、EEM パラメータのデフォルト設定を示します。

**表 *22 :* デフォルトの *EEM* パラメータ**

| パラメータ | デフォルト |
|---|---|
| システム ポリシー | active |

# EEM の設定

## CLI によるユーザ ポリシーの定義

CLI を使用したユーザ ポリシーを定義できます。

CLI を使用してユーザー ポリシーを定義するには、次の手順を実行します。

### 手順

**ステップ 1** **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** **event manager applet** *applet-name*

EEM にアプレットを登録し、アプレット コンフィギュレーション モードを開始します。*applet-name* は大文字と小文字を区別し、最大 29 の英数字を使用できます。

**ステップ 3** **description** *policy-description*

（任意）ポリシーの説明になるストリングを設定します。string には最大 80 文字の英数字を使用できます。ストリングは引用符で囲みます。

**ステップ 4** **event** *event-statement*

ポリシーのイベント文を設定します。イベント文の設定 （181 ページ）を参照してください。

**ステップ 5** 次のいずれかを実行します。

- **tag***tagname1* {**and** |**andnot**} *tagname2* [{**and** |**andnot**} tagname3[{**and** |**andnot**} *tagname4*]] **happens** が発生し **in**た秒数

（任意）ポリシー内の複数のイベントを相関付けます。

発生数の範囲は 1 ～ 4294967295 です。秒の範囲は 0 ～ 4294967295 秒です。

**ステップ 6** **action** *action-statement*

ポリシーのアクション文を設定します。アクション文の設定 （186 ページ）を参照してください。

アクション文が複数の場合は、ステップ 5 を繰り返します。

**ステップ 7** **show event manager policy internal** *name*

（任意）設定したポリシーに関する情報を表示します。

**ステップ 8** **copy running-config startup-config**

（任意）この設定の変更を保存します。

# イベント文の設定

イベント ステートメントを設定するには、EEM 設定モードで次のコマンドを使用します。

| コマンド | 目的 |
|---|---|
| **event cli** [**tag** *tag_name* **match** *expression* ] [**count** *repeats* \|**time** *seconds* ] | 正規表現と一致する CLI コマンドが入力された場合に、イベントを発生させます。<br>The **tag** *tag_name* keyword-argument pair identifies this specific event when multiple events are included in the policy.<br>*repeats* の範囲は 1 ～ 65000 です。time の範囲は 0 ～ 4294967295 秒です。0 は無制限を示します。 |
| **event counter name** *counter* **entry-val** *entry* **entry-op** {**eq**\|**ge**\|**gt**\|**le**\|**lt**\|**ne** }[**exit-val** *exit* **exit-op** *exit* {**eq**\|**ge**\|**gt**\|**le**\|**lt**\|**ne** }] | カウンタがエントリのしきい値を超えた場合、イベントを発生させます。（エントリ操作に基づく。値が大きい、小さいなど）。イベントはただちにリセットされます。任意で、カウンタが終了のしきい値を超えたあとでリセットされるように、イベントを設定できます。*counter* name は大文字と小文字を区別し、最大 28 の英数字を使用できます。*entry* および *exit* の値の範囲は 0 ～ 2147483647 です。 |
| **event fanabsent** [**fan** *number* ] **time** *seconds* | 秒数で設定された時間を超えて、ファンがデバイスから取り外されている場合に、イベントを発生させます。ファンの番号範囲はスイッチによって異なります（例：9513 スイッチの範囲は、1 ～ 2、9506/9509 スイッチでは 1 です）。第二の範囲は 10 ～ 64000 です。 |
| **event fanbad** [**fan** *number* ] **time** *seconds* | 秒数で設定された時間を超えて、ファンが故障状態の場合に、イベントを発生させます。ファンの番号範囲はスイッチによって異なります（例：9513 スイッチの範囲は、1 ～ 2、9506/9509 スイッチでは 1 です）。第二の範囲は 10 ～ 64000 です。 |

| コマンド | 目的 |
|---|---|
| **event memory** {**critical** \| **minor** \|**severe**} | メモリのしきい値を超えた場合にイベントを発生させます。 |
| **event module-failure type** *failure-type* **module** { *slot* \| **all** { *slot* \| **count** *repeats* [**time** *seconds*] | モジュールが設定された障害タイプになった場合に、イベントを発生させます。<br>スロットの範囲は異なるスイッチに依存しています（例：9513 スイッチの範囲は 1 ～ 13 で、9509 スイッチでは 1 ～ 9 です)。*repeats* の範囲は 0 ～ 4294967295 です。*seconds* の範囲は 0 ～ 4294967295 です。 |
| **event oir** {**fan** \| **module** \| **powersupply**} {**anyoir** \| **insert** \| **remove** [*number*]} | 設定されたデバイス構成要素（ファン、モジュール、または電源モジュール）がデバイスに取り付けられた場合、またはデバイスから取り外された場合に、イベントを発生させます。任意で、ファン、モジュール、または電源モジュールの具体的な番号を設定できます。*number* の範囲は次のとおりです。<br>• ファンの番号は異なるスイッチに依存します。<br>• モジュール番号は異なるスイッチに依存します。<br>• 電源モジュール番号の範囲は 1 ～ 2 です。 |
| **event policy-default count** *repeats* [**time** *seconds* ] | システム ポリシーで設定されているイベントを使用します。このオプションは、ポリシーを上書きする場合に使用します。<br>*repeats* の範囲は 1 ～ 65000 です。*seconds* の範囲は 0 ～ 4294967295 です。 |
| **event poweroverbudget** | 電力バジェットが設定された電源モジュールの容量を超えた場合に、イベントを発生させます。 |

| コマンド | 目的 |
| --- | --- |
| **event snmp oid** *oid* **get-type**{**exact** \| **next**} **entry-op** {**eq** \| **ge** \| **gt** \| **le** \| **lt** \|**ne**} **entry-val** *entry* [**exit-comb** {**and** \| **or**}] **exit-op** {**eq** \| **ge** \| **gt** \| **le** \| **lt** \|**ne**} **exit-val** *exit***exit-time** *time***polling-interval** *interval* | SNMP OID のエントリしきい値を超えた場合、イベントを発生させますトリガー(エントリ操作に基づく。値が大きい、小さいなど）。イベントはただちにリセットされます。または任意で、カウンタが終了のしきい値を超えたあとでリセットされるように、イベントを設定できます。OID はドット付き 10 進表記です。*entry* および *exit* の値の範囲は 0 ～ 18446744073709551615 です。時間範囲は 0 ～ 2147483647 です。間隔範囲は 1 ～ 2147483647 です。 |

| コマンド | 目的 |
| --- | --- |
| **event syslog**{**occurs occurs number** \| **pattern syslog** パターン\| **period** 時間間隔\| **priority syslog** *priority* \| **tag***tag_name* } | |

| コマンド | 目的 |
| --- | --- |
| | Syslog logfile にログインしているメッセージに基づくイベントをトリガします。<br><br>occurs occurs number：発生番号を指定します。指定できる範囲は 1 ～ 65000 です。<br><br>pattern syslog pattern：syslog パターンを指定します。通常の正規表現パターン マッチングが使用されます。最長で英数字256文字です。<br><br>period time intervals：メッセージの間の最大時間間隔を指定します。値の範囲は 0 ～ 4294967295 秒です。<br><br>priority syslog priority：syslog の優先順位を指定します。<br>• alerts：アラート ログ メッセージを指定します<br>• critical：重要なログ メッセージを指定します<br>• debugging：デバッグ メッセージを指定します<br>• emergencies：緊急ログ メッセージを指定します<br>• errors：エラー ログ メッセージを指定します<br>• informational：情報ログ メッセージを指定します<br>• notification：通知ログ メッセージを指定します<br>• pattern：一致するパターンを指定します<br>• warnings：警告メッセージを指定します<br><br>tag tag：タグ名を指定します。最長で英数字 29 文字です。<br><br>tag tag_name キーワードと引数のペアは、複数のイベントがポリシーに含まれてい |

| コマンド | 目的 |
|---|---|
| | る場合、この特定のイベントを識別します。 |
| **event temperature** [**module** *slot* ] [**sensor** *sensor number* ]**threshold** {**any** \| **major** \| **minor**} | 温度センサーが設定されたしきい値を超えた場合に、イベントを発生させます。スロット 値の範囲は異なるスイッチに依存します。センサ範囲はMDSモジュールの 1 ～ 8 ですが、現在 MDS モジュールは 1 から 3 のみの範囲を使用しており、一部のモジュールでは 1 ～ 2 の範囲を使用します。 |

# アクション文の設定

To configure action statements, use the following commands in EEM configuration mode:

| コマンド | 目的 |
|---|---|
| **action** 番号 [ **.** *number2* ] command1 [ *command2...* [ **cli** ] [ **local** ] | 設定された CLI コマンドを実行します。You can optionally execute the commands on the module where the event occurred. アクション ラベルのフォーマットは number1.number2 です。<br>*number* は 16 桁までの任意の数値にできます。*number2* の範囲は 0 ～ 9 です。 |
| **action** *number* [ **.** *number* ] **counter name** *counter* **value** *val* **op** { **dec** \| **inc** \| **nop** \| **set** } | 設定された値および操作でカウンタを変更します。アクション ラベルのフォーマットは number1.number2 です。<br>*number* は 16 桁までの任意の数値にできます。*number2* の範囲は 0 ～ 9 です。<br>counter name は大文字と小文字を区別し、最大 28 の英数字を使用できます。*val* には 0 ～ 2147483647 の整数または置換パラメータを指定できます。 |
| **action** *number* [ **.** *number* ] **event-default** | 関連付けられたイベントのデフォルト アクションを実行します。アクション ラベルのフォーマットは number1.number2 です。<br>*number* は 16 桁までの任意の数値にできます。*number2* の範囲は 0 ～ 9 です。 |

| コマンド | 目的 |
|---|---|
| **errcode devid errtype phylayer** number [**. module** number2] **exceptionlog** module **syserr** error id type code layer **action ports** list **harderror** *error* [**desc** *string* ] | EEM アプレットがトリガーされると、特定の条件が発生した場合は、例外を記録します。 |
| **action** 番号 [ **.** 数値 *number2* ] **forceshut** [**module** *slot* \|xbar番号*]* **xbar reset-reason** 秒 | モジュール、クロスバー、またはシステム全体を強制的にシャットダウンします。アクション ラベルのフォーマットは number1.number2 です。<br>*number* は 16 桁までの任意の数値にできます。*number2* の範囲は 0 ～ 9 です。<br>スロット 値の範囲は異なるスイッチに依存します。*Xbar* 番号 範囲は 1 ~ 2 と、MDS 9513 モジュールでのみ使用します。<br>リセット理由は、引用符で囲んだ最大 80 文字の英数字ストリングです。 |
| **action** *number* [ **.** *number* ] **overbudgetshut** [ **module** *slot* [ **-** *slot* ]] | 電力バジェット超過の問題により、1つまたは複数のモジュールまたはシステム全体を強制的にシャットダウンします。<br>*number* は 16 桁までの任意の数値にできます。*number2* の範囲は 0 ～ 9 です。<br>スロット 値の範囲は異なるスイッチに依存します。 |
| **action** *number* [ **.** *number* ] **policy-default** | 上書きしているポリシーのデフォルト アクションを実行します。アクション ラベルのフォーマットは number1.number2 です。<br>*number* は 16 桁までの任意の数値にできます。*number2* の範囲は 0 ～ 9 です。 |
| **action** *number* [ **.** *number* ] **reload** [ **module** *slot* [ **-** *slot* ]] | 1 つまたは複数のモジュールまたはシステム全体を強制的にリロードします。<br>*number* は 16 桁までの任意の数値にできます。*number2* の範囲は 0 ～ 9 です。<br>スロット 値の範囲は異なるスイッチに依存します。 |
| **action** 番号 [ **.** *number2* ]{[ **strdata string**データ [**intdata2** データ[]]} **intdata1 snmp-trap** | 設定されたデータを使用して SNMP トラップを送信します。*number*には、16桁までの任意の数値を指定できます。*number2* の範囲は 0 ～ 9 です。<br>*data* 引数には、最大 80 桁の任意の数を指定できます。*string* には最大 80 文字の英数字を使用できます。 |

| コマンド | 目的 |
|---|---|
| **action** *number* [ **.** *number2* ] **syslog** [ **priority** *prio-val* ] **msg** *error message* | 設定されている優先度にカスタマイズされた Syslog メッセージを送信します。番号 16 桁までの任意の数値にできます。*number2* の範囲は 0 ～ 9 です。<br>*error-message* には最大 80 文字の英数字を引用符で囲んで使用できます。 |

（注） トリガーされたイベントでデフォルト アクションも処理されるようにする場合は、EEM アクションをポリシーのタイプに応じて event-default または policy-default で明示的に設定する必要があります。たとえば、match 文で CLI コマンドを照合する場合、EEM ポリシーに event-default アクション文を追加する必要があります。この文がないと、EEM では CLI コマンドを実行できません。端末のイベント manager バイパス コマンドを使用してすべての CLI ベースの EEM ポリシーをバイパスできます。使用して端末を元に戻す event manager のコマンドはバイパスありません。

# VSH スクリプトによるポリシーの定義

VSH スクリプトを使用してポリシーを定義するには、次の手順を実行します。

**手順**

**ステップ 1** テキスト エディタで、ポリシーを定義する CLI コマンド リストを指定します。

**ステップ 2** テキスト ファイルに名前をつけて保存します。

**ステップ 3** ファイルを次のシステム ディレクトリにコピーします。

bootflash://eem/user_script_policies

# VSH スクリプト ポリシーの登録およびアクティブ化

VSH スクリプトで定義されているポリシーを登録し有効にするには、次の手順に従います。

**手順**

**ステップ 1** **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** **event manager policy** *policy-script*

EEM スクリプト ポリシーを登録してアクティブにします。*policy-script* は大文字と小文字を区別し、最大 29 の英数字を使用できます。

**ステップ 3** **show event manager internal policy** *name*

（任意）設定したポリシーに関する情報を表示します。

**ステップ 4** **copy running-config startup-config**

（任意）この設定の変更を保存します。

# ポリシーの上書き

システム ポリシーを上書きするには、これらの手順に従います。

**手順**

**ステップ 1** **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** **show event manager policy-state** *system-policy*

（任意）上書きするシステム ポリシーの情報をしきい値を含めて表示します。Use the **show event manager system-policy** command to find the system policy names.

**ステップ 3** [**no**] **event manager applet** *applet-name* **override** *system-policy*

システム ポリシーを上書きし、アプレット コンフィギュレーション モードを開始します。*applet-name* は大文字と小文字を区別し、最大 29 の英数字を使用できます。The *system-policy* must be one of the existing system policies.

**ステップ 4** **description** *policy-description*

（任意）ポリシーの説明になるストリングを設定します。string には最大 80 文字の英数字を使用できます。ストリングは引用符で囲みます。

**ステップ 5** [**no**] **event** *event-statement*

ポリシーのイベント文を設定します。イベント文の設定（181 ページ）を参照してください。Using the **no** keyword deletes the overridden event, if any.

- オーバーライドされたポリシーを削除しても、デフォルトのシステム ポリシーは削除されません。
- オーバーライドされたポリシーを変更するには、それぞれのゾーン、FCNS、またはFLOGI制限値を変更します。

**ステップ 6** **action** *action-statement*

ポリシーのアクション文を設定します。アクション文の設定（186ページ）を参照してください。

アクション文が複数の場合は、ステップ 6 を繰り返します。

- ゾーン、FLOGI、およびFCNSではアクションとしてSyslogメッセージの生成のみサポートします。
- アクションが設定されていない場合、デフォルトのシステムポリシーに関連付けられているデフォルトアクションが実行されます。アクションが設定されている場合、設定済みおよびデフォルトのアクション両方が実行されます。この機能は、ゾーン、FLOGI、およびFCNS システム ポリシーにのみ適用されます。

**ステップ 7** **show event manager policy-state** *name*

（任意）設定したポリシーに関する情報を表示します。

**ステップ 8** **copy running-config startup-config**

（任意）この設定の変更を保存します。

（注） ゾーン、FLOGI、FCNS EEMポリシーに対する複数のオーバライドは許可されていません。

# 環境変数の定義

EEM ポリシーのパラメータとして機能する変数を定義するには、次の手順を実行します。

**手順**

**ステップ 1** **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** **event manager environment** *variable-name variable-value*

EEM 用の環境変数を作成します。*variable-name* は大文字と小文字を区別し、最大 29 の英数字を使用できます。*variable-value* には最大 39 文字の英数字を引用符で囲んで使用できます。

**ステップ 3** **show event manager environment**

（任意）設定した環境変数に関する情報を表示します。

**ステップ 4** **copy running-config startup-config**

（任意）この設定の変更を保存します。

# EEM 設定の確認

EEM のコンフィギュレーション情報を表示するには、次の作業のいずれかを行います。

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

# EEM のコンフィギュレーション例

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

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

次の例では、FCNS データベース エントリ数を 1500 に変更することで、オーバーライドのポリシーを変更します。これにより、デフォルト システム ポリシーの設定済みおよびデフォルト syslog メッセージも生成されます。

```
event manager applet fcns_policy override __fcns_entries_max_per_switch
event fcns entries max-per-switch 1500
     action 1.0 syslog priority warnings msg  FCNS DB entries have reached the EEM limit
```

次の例では、オーバーライドされたポリシーのイベントを削除します。

```
no event manager applet zone_policy
```

CLI コマンドの実行を許可し、ユーザがデバイスでコンフィギュレーション モードを開始すると SNMP 通知を送る EEM ポリシーを作成する例を次に示します。

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

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

# その他の参考資料

EEM の実装に関連する詳細情報については、次の項を参照してください。

### MIB

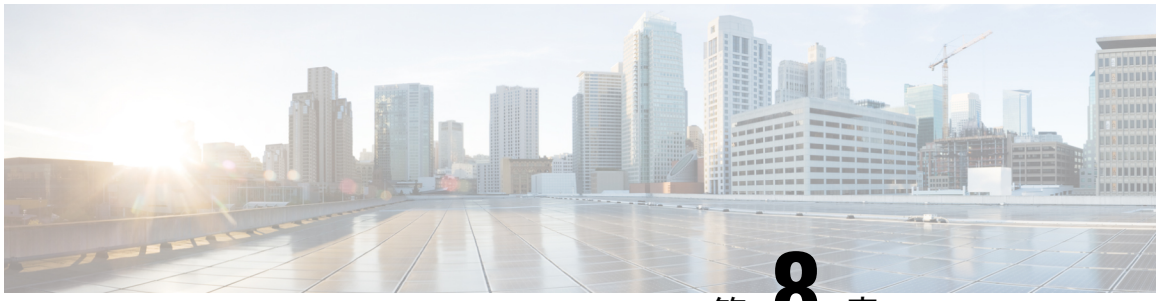
| MIB | MIB のリンク |
|---|---|
| • CISCO-EMBEDDED-EVENT-MGR-MIB | MIB を検索およびダウンロードするには、次の URL にアクセスしてください。<br>http://www.cisco.com/en/US/products/ps5989/prod_technical_reference_list.html |

# EEM の機能の履歴

表 23 : EEM の機能の履歴 （193 ページ） に、この機能のリリース履歴を示します。リリース 3.x 以降のリリースで導入または変更された機能のみが表に記載されています。

表 *23 : EEM* の機能の履歴

| 機能名 | リリース | 機能情報 |
|---|---|---|
| Embedded Event Manager（EEM） | 4.1(3) | Embedded Event Manager（EEM）の設定方法に関する新しい章が追加されました。 |
| EEM: ゾーン、FCNS、およびFLOGI | 6.2(11) | この機能では、デフォルトのゾーン、FCNS、および FLOGI システムポリシーのカスタムの制限を設定することができます。 |



第 8 章

# RMON の設定

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



## RMON について

スイッチでは RMON はデフォルトでディセーブルに設定されており、イベントまたはアラームは設定されていません。

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

- アラーム：指定された期間、特定の管理情報ベース（MIB）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応報にちては、「*Cisco MDS 9000 Family MIB Quick Reference.*」を参照してください

SNMP 互換性ネットワーク管理ステーションに関する詳細は、「System Management Configuration Guide, Cisco DCNM for SAN」を参照してください。

SNMP セキュリティに関連する CLI の設定については、 を参照してください。

# RMON 設定情報

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

ヒント　RMON のネットワーク管理機能を活用するために、ネットワーク管理ステーション（NMS）で追加の汎用 RMON コンソール アプリケーションを使用することを推奨します。「System Management Configuration Guide, Cisco DCNM for SAN」を参照してください。

# しきい値マネージャを使用した RMON 設定

スイッチでは RMON はデフォルトでディセーブルに設定されており、イベントまたはアラームは設定されていません。RMON のアラームおよびイベントを設定するには、CLI を使用するか、Device Manager の Threshold Manager を使用します。

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

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

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

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

# RMON アラーム設定情報

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

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

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

- Use the **delta** option to test the change between samples of a MIB variable.
- Use the **absolute** option to test each MIB variable directly.
- Use the **delta** option to test any MIB objects that are counters.

The range for the **rising threshold** and **falling threshold** values is -2147483647 to 2147483647.

注意 は、 **rising**より**threshold**小さい必要があります。 **falling threshold**

次のパラメータを任意で指定することもできます。

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

# デフォルト設定

表 24 : RMON のデフォルト設定値 （197 ページ） 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 *24 : 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 | 無効 |
| RMON イベント | ディセーブル |

# RMON の設定

スイッチでは RMON はデフォルトでディセーブルに設定されており、イベントまたはアラームは設定されていません。

## SNMP の RMON トラップの設定

SNMP 構成の RMON トラップを有効にするには、次の手順を実行します。

### 始める前に

正常に機能させるため、RMON 構成の SNMP 構成では、RMON トラップを有効にする必要があります。

### 手順

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **snmp-server enable traps rmon**

RMON トラップのタイプを有効にします。

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

## RMON アラームの設定

RMON アラームを有効にするには、次の手順を実行します。

### 手順

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **rmon alarm 20 1.3.6.1.2.1.2.2.1.14.16777216 2900 delta rising-threshold 15 1 falling-threshold 0 owner test**

Configures RMON alarm number 20 to monitor the 1.3.6.1.2.1.2.2.1.14.16777216 once every 900 seconds until the alarm is disabled and checks the change in the variables rise or fall. 値が 15 以上の MIB カウンタの増加を示した場合、アラームが発生します。そのアラームによってさらにイベント番号

1 が発生します。イベント番号 1 は、RMON イベント コマンドで設定されています。使用できるイベントは、ログ エントリまたは SNMP トラップです。MIB 値の変化が 0 の場合、アラームはリセットされ、再び発生が可能になります。

（注） 次の RMON イベントを設定することもできます。

- イベント 1：致命的
- イベント 3：エラー
- イベント 4：警告
- イベント 5：情報

**ステップ 3** switch(config)# **no rmon alarm 2**

アラーム テーブルから指定されたエントリを削除します。

# RMON イベントの設定

RMON イベントを有効にするには、次の手順を実行します。

**手順**

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **rmon event 2 log trap eventtrap description CriticalErrors owner Test2**

CriticalErrors を定義する RMON イベント番号 2 を作成し、アラームによるイベント発生時にログ エントリを生成します。ユーザ Test2 が、このコマンドによってイベント テーブルに作成される行を所有します。次の例の場合も、イベント発生時に SNMP トラップが生成されます。

（注） 次の RMON イベントを設定することもできます。

- イベント 1：致命的
- イベント 3：エラー
- イベント 4：警告
- イベント 5：情報

**ステップ 3** switch(config)# **no rmon event 5**

RMON イベント テーブルからエントリを削除します。

# RMON 設定の確認

RMON の設定情報を表示するには、次のいずれかの作業を行います。

| コマンド | 目的 |
|---|---|
| **show rmon alarms** | 設定済みの RMON アラームの表示 |
| **show rmon hcalarms** | 設定済みの RMON 高容量アラームの表示 |
| **show rmon events** | 設定済みの RMON イベントの表示 |

これらのコマンドの出力に表示されるフィールドの詳細については、「Cisco MDS 9000 NX-OS Command Reference」を参照してください。

Use the **show rmon** and **show snmp** commands to display configured RMON and SNMP information (see 設定済みの RMON アラーム （200 ページ） and 設定済みの RMON イベント （201 ページ）).

### 設定済みの RMON アラーム

次の例では、設定済みの RMON アラームを表示します。

```
switch# show rmon alarms
Alarm 1 is active, owned by admin
 Monitors 1.3.6.1.2.1.2.2.1.16.16777216 every 1 second(s)
 Taking delta samples, last value was 0
 Rising threshold is 1, assigned to event 0
 Falling threshold is 0, assigned to event 0
 On startup enable rising or falling alarm
```

### 確認済みの RMON 大容量アラーム

次の例では、確認済みの RMON 大容量アラームが表示されます。

```
switch# show rmon hcalarms
High Capacity Alarm 10 is active, owned by Testuser
 Monitors 1.3.6.1.2.1.31.1.1.1.6.16785408 every 300 second(s)
 Taking absolute samples, last value was 0 (valuePositive)
 Rising threshold low is 4294967295 & high is 15 (valuePositive)
 Rising threshold assigned to event 1
 Falling threshold low is 0 & high is 0 (valueNotAvailable)
 Falling threshold assigned to event 0
 On startup enable rising alarm
 Number of Failed Attempts is 0
```

（注） 高容量 RMON アラームは、CISCO-HC-ALARM-MIB を使用して設定できます。詳細については、「*Cisco MDS 9000* シリーズ *MIB Quick Reference*」を参照してください。

### 設定済みの RMON イベント

次の例では、設定済みの RMON イベントを表示します。

```
switch# show rmon events
Event 2 is active, owned by Test2
 Description is CriticalErrors
 Event firing causes log and trap to community eventtrap, last fired 0
Event 500 is active, owned by admin
 Description is
 Event firing causes log, last fired 138807208
```

# その他の参考資料

RMON の実装に関する詳細情報については、次の項を参照してください。

### MIB

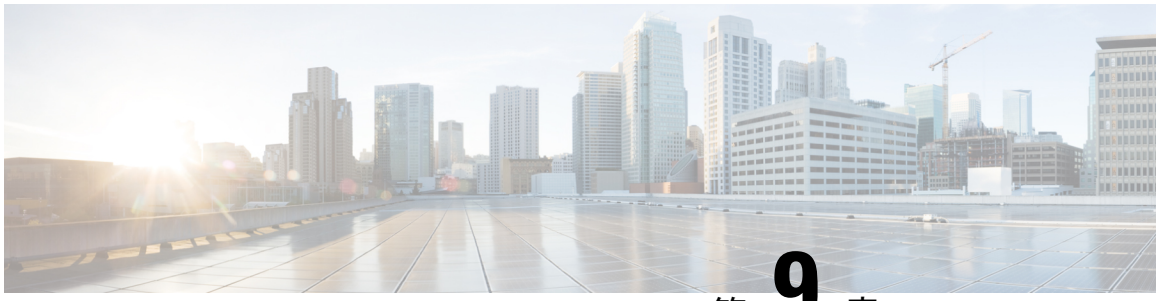
| MIB | MIB のリンク |
|---|---|
| • CISCO-RMON-CAPABILITY.my<br>• CISCO-RMON-CONFIG-CAPABILITY.my<br>• CISCO-RMON-CONFIG-MIB | MIB を検索およびダウンロードするには、次の URL にアクセスしてください。<br>http://www.cisco.com/en/US/products/ps5989/prod_technical_reference_list.html |

# RMON の機能の履歴

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

表 *25 : RMON* の機能の履歴

| 機能名 | リリース | 機能情報 |
|---|---|---|
| RMON 大容量アラーム | 3.0(1) | RMON 高容量アラーム値を表示する、show rmon high capacity alarms コマンドを提供します。 |



第 9 章

# オンライン診断の設定

Cisco MDS NX-OS リリース 6.2 以降で、Cisco MDS 9700 ファミリは GOLD（Generic Online Diagnostics）機能をサポートします。GOLD は Cisco Nexus 7000 および 7700 シリーズ スイッチでもサポートされている診断サービスです。この章では、Cisco MDS 9700 ファミリ スイッチの GOLD 機能を設定する方法を説明しています。



## オンライン診断について

オンライン診断では、ハードウェアおよびデータ パスを確認し、障害のあるデバイスを特定します。

### オンライン診断機能の概要

ゴールド (Generic Online Diagnostics) フレームワークでは、テストし、ライブ システムで、ハードウェア デバイスとデータ パスを確認します。

ゴールド テストは、次の 3 つのモードで実行できます。

- ブートアップ
- ヘルス モニタリング (ランタイムとも呼ばれる)
- On-demand

次は、診断テスト スイート属性について説明します。

- B/C/* - Bypass bootup level test / Complete bootup level test / NA

- P/* - 1 回のポートのテスト/NA
- M/S/* - Only applicable to active / standby unit / NA
- D/N/* - Disruptive test / Non-disruptive test / NA
- H/O/* - モニタリングのテストは常に有効/条件付きでテストを有効/NA
- F/* - Fixed monitoring interval test / NA
- X/* - Not a health monitoring test / NA
- E/*-ライン カードのテストを Sup/NA
- L/* 排他的]: このテストの実行/NA
- T/*-オンデマンド テストではない/NA
- A/I/* - Monitoring is active / Monitoring is / NA

# ブートアップ診断

Bootup diagnostics run during bootup and detect faulty hardware before a Cisco MDS 9700 Family switch brings a module online. たとえば、デバイスに障害のあるモジュールがある場合は、適切なブートアップ診断テストに失敗おり、障害を示しています。

（注） ブートアップの診断テストは、ブートアップ時にトリガーされます。

表 26 : ブートアップ診断 （204 ページ） describes the bootup diagnostic tests for a linecard and a supervisor.

**表 *26 :* ブートアップ診断**

| 診断 | Attributes | 説明 |
|---|---|---|
| ラインカード | | |
| EOBCPortLoopback | C * * D X * * * * T * | EOBC (イーサネット アウトオブ バンド接続) インターフェイスの状態を確認します。 |
| OBFL | C * * N X * * * * T * | Verifies the integrity of the OBFL (Onboard Failure Logging) flash. |
| BootupPortLoopback | CP * N * * XE * T * | PortLoopback test that runs only during module bootup.<br>（注） Cisco MDS NX-OS リリース 6.2(11) から以降では、FC(モジュールのポート、Cisco MDS 48 ポート 16 Gbps ファイバ チャネル) の BootupPortLoopback 障害、失敗したポートを diagfailure モードになります。 |
| スーパーバイザ | | |

| 診断 | Attributes | 説明 |
|---|---|---|
| USB | C * * N X * * * * T * | Verifies the USB controller initialization on a module. |
| ManagementPortLoopback | C * * D X * * * * T * | モジュールの管理インターフェイスの状態を確認します。 |
| EOBCPortLoopback | C * * D X * * * * T * | EOBC (イーサネット アウトオブ バンド接続) インターフェイスの状態を確認します。 |
| OBFL | C * * N X * * * * T * | Verifies the integrity of the OBFL (Onboard Failure Logging) flash. |

When the **show module** command is executed, the result of bootup diagnostics is displayed as Online Diag Status. The result of individual test is displayed when the **show diagnostic result** command is executed for appropriate module and test ID or test name.

Cisco MDS 9700 ファミリ スイッチは、ブートアップ診断をバイパスするか、ブートアップ診断の完全なセットを実行するように設定できます。起動診断レベルの設定 （213 ページ）を参照してください。

# ヘルスモニタリング診断

ヘルスモニタリング（HM）診断は、定期的な間隔でライブ システムの状態を確認するためデフォルトで有効になっています。モニタリングの間隔（許可された範囲内）は、ユーザーにより設定可能で、各テストによって異なります。詳細については、診断テストのヘルスモニタリングのアクティブ化 （214ページ）を参照してください。診断テストは、ハードウェアのエラーとデータ パスの問題を検出します。

ヘルスモニタリング診断は非破壊的です（データまたは制御トラフィックは中断されません）。ヘルス モニタリング テストは、ユーザーによって無効にすることができます。詳細については、診断テストのヘルスモニタリングを非アクティブ化 （215 ページ）を参照してください。

次の表では、スーパーバイザのヘルス モニタリング診断を説明しています。

| 診断 | デフォルトのテスト間隔 | Attributes | 説明 |
|---|---|---|---|
| スーパーバイザ | | | |
| ASICRegisterCheck | 20 seconds | ***N******A | スーパーバイザ上の ASIC のレジスタをスクラッチするための読み取りと書き込みアクセス権を確認します。 |
| NVRAM | 5 分 | ***N******A | スーパーバイザの NVRAM ブロックの健全性を確認します。 |

| 診断 | デフォルトのテスト間隔 | Attributes | 説明 |
|---|---|---|---|
| RealTimeClock | 5 分 | ***N******A | スーパーバイザ上のリアルタイム クロックが時を刻んでいるかどうかを確認します。 |
| PrimaryBootROM | 30 分 | ***N******A | スーパーバイザ上のプライマリ ブート デバイスの完全性を確認します。 |
| SecondaryBootROM | 30 分 | ***N******A | スーパーバイザ上のセカンダリ ブート デバイスの完全性を確認します。 |
| CompactFlash | 30 分 | ***N******A | コンパクト フラッシュ デバイスにアクセスできるかどうかを確認します。 |
| ExternalCompactFlash | 30 分 | ***N******A | 外部コンパクト フラッシュ デバイスにアクセスできるかどうかを確認します。 |
| PwrMgmtBus | 30 秒 | **MN******A | スタンバイの電源管理制御バスを確認します。 |
| SystemMgmtBus | 30 秒 | **MN******A | スタンバイ システム管理バスの使用可能性を確認します。 |
| StatusBus | 30 秒 | **MN******A | スーパーバイザ、モジュール、およびファブリック カードに対するステータス バイパスによって送信されるステータスを確認します。 |
| StandbyFabricLoopback | 30 秒 | **SN******A | ファブリック モジュールへのスタンバイ スーパバイザの接続を確認します。 |

表 27 : ヘルスモニタリング診断 （206 ページ） describes the health monitoring diagnostics for the *Cisco MDS 48-Port 16-Gbps Fibre Channel module.*

**表 *27* : ヘルスモニタリング診断**

| 診断 | デフォルトのテスト間隔 | Attributes | 説明 |
|---|---|---|---|
| ラインカード | | | |
| ASICRegisterCheck | 1 分 | ***N******A | モジュール上の ASIC のレジスタをスクラッチするための読み取りと書き込みアクセス権を確認します。 |

| 診断 | デフォルトのテスト間隔 | Attributes | 説明 |
|---|---|---|---|
| PrimaryBootROM | 30 分 | ***N******A | モジュール上のプライマリ ブート デバイスの完全性を確認します。 |
| SecondaryBootROM | 30 分 | ***N******A | モジュール上のセカンダリ ブート デバイスの完全性を確認します。 |
| SnakeLoopback | 20 分 | *P*N***E** | Sup からラインカードのすべてのポートへの接続を確認します。プログレッシブな方法で、最大 MAC コンポーネントまでデータ パスの整合性を確認します。（テストを 1 つ実行するだけですべてのポートをカバーします）。これは、状態に関係なくすべてのポートで実行されます。<br>これは、中断のないテストです。 |
| IntPortLoopback | 5 分 | *P*N***E*** | Sup からラインカードのすべてのポートへの接続を確認します（1 回に 1 ポート）。最大 MAC コンポーネントまでデータ パスの整合性を確認します。このテストは「オンデマンドモード」でトリガされると同様に、ヘルス モニタリング（HM）モードで実行されます。<br>このテストは、中断のないテストです。<br>（注） Cisco MDS NX-OS リリース 6.2(7) 以降 IntPortLoopback テストがサポートされています。 |
| RewriteEngine ループバック | 1 分 | *P*N***E**A | Sup からラインカードまでのファブリック モジュールの各リンクの整合性を確認します。 |

表 28 : ヘルスモニタリング診断 （207 ページ） describes the health monitoring diagnostics for the *Cisco MDS 48-Port 10-Gbps Fibre Channel over Ethernet Module.*

**表 *28 :* ヘルスモニタリング診断**

| 診断 | デフォルトのテスト間隔 | Attributes | 説明 |
|---|---|---|---|
| ラインカード | | | |
| ASICRegisterCheck | 1 分 | ***N******A | モジュール上の ASIC のレジスタをスクラッチするための読み取りと書き込みアクセス権を確認します。 |

| 診断 | デフォルトのテスト間隔 | Attributes | 説明 |
|---|---|---|---|
| PrimaryBootROM | 30 分 | ***N******A | モジュール上のプライマリ ブート デバイスの完全性を確認します。 |
| SecondaryBootROM | 30 分 | ***N******A | モジュール上のセカンダリ ブート デバイスの完全性を確認します。 |
| PortLoopback | 15 分 | *P*D***E**A | Sup からラインカードのすべてのポートへの接続を確認します。最大 PHY までのデータ パスの整合性を確認します。このテストは「オンデマンドモード」でトリガされると同様に、ヘルスモニタリング（HM）モードで実行されます。これはがダウンしているポートでのみ実行されます（管理上）。<br>これは、中断があるテストです。<br>（注） PortLoopback テストは、管理上ダウンしているポートでのみ実行されます。 |
| RewriteEngine ループバック | 1 分 | *P*N***E**A | ラインカード間の各リンク、またはファブリック モジュールを経由する sup およびラインカードの整合性を確認します。 |
| SnakeLoopback | 20 分 | *P*N***E** | Sup からラインカードのすべてのポートへの接続を確認します。プログレッシブ方法で、最大 MAC コンポーネントまでデータ パスの整合性を確認します。これは、状態に関係なくすべてのポートで実行されます。<br>これは、中断のないテストです。 |

# オンデマンド診断

すべてのヘルス モニタリングのテストは、オンデマンドもカラーボタンことができます。オンデマンド診断は、ユーザが呼び出される場合にのみ実行されます。

Cisco MDS 48 ポート 16 Gbps ファイバ チャネル モジュール: オンデマンド モードでのみ呼び出すことができますを参照してくださいする 2 のテストはのみ 表 29 : オンデマンド診断 （209 ページ） 。

Cisco MDS 48 ポート 10 Gbps Fibre Channel over Ethernet モジュール: オンデマンド モードでのみ呼び出すことができるテストはありません。

（注） その他のヘルス モニタリングのテストでは検証されないするデータ パス (PHY と SFP) は、PortLoopback によって確認でき、ExtPortLoopback をテストします。

必要なときにオンデマンド診断を実行できます。詳細については、オンデマンド診断テストの開始または中止 （216 ページ）を参照してください。

Cisco MDS 48 ポート 16 Gbps ファイバ チャネルのモジュールで PortLoopback と ExtPortLoopback の両方のテストは、破壊的ためオンデマンド モードで使用可能な。

表 29 : オンデマンド診断 （209 ページ） describes the on-demand diagnostics (for linecard only) on the *Cisco MDS 48-Port 16-Gbps Fibre Channel module.*

**表 *29* : オンデマンド診断**

| 診断 | Attributes | 説明 |
|---|---|---|
| ラインカード | | |
| PortLoopback | * P D * * * XE。 | Sup から、ラインカードのすべてのポートへの接続を確認します。PHY 最大データ パスの完全性を確認します。このテストは、「オンデマンドモード」でのみ使用できます。ポートの状態に関係なく、すべてのポートでのテストが実行されます。<br>（注） Portloopback テストは OHMS の Serdes ループバック テストに相当します。 |
| ExtPortLoopback | * P D * * * XE。 | SFP を含む PHY を最大には、[全体のデータ パスでのハードウェアのエラーを特定します。<br>（注） テストを実行する前に、ポートの Rx へのポートの Tx のループをループバック プラグを接続します。ループバック プラグが接続されていない場合は、このテストが失敗します。<br>（注） Cisco MDS NX-OS リリース 6.2(11c) から開始 ExtPortLoopback テストがサポートされています。 |

**注意** PortLoopback および ExtPortLoopback テストは、診断操作目的のポートを落としますに中断されます。

# 指定のヘルス モニタリング診断の回復アクション

ヘルス モニタリング診断テストが最大 10 回のしきい値超えて連続して失敗した場合、EEM を通してアラートの生成（callhome、syslog）やロギング（ログを除く OBFL）を含むデフォルト アクションが実行され、失敗したインスタンスで診断テストが無効になります（ポート、ファブリック、デバイス）。

これらのアクションは有益ですが、ネットワーク中断、トラフィック ブラック ホールなどの結果が生じるデバイス障害をライブ システムから除くものではありません。

（注） テストの結果をクリアし非アクティブにして、失敗したインスタンスでヘルス モニタリングを再起動してから、同じモジュールでテストをアクティブにします。詳細については、診断結果の消去（219 ページ）、診断テストのヘルス モニタリングを非アクティブ化（215 ページ）および診断テストのヘルス モニタリングのアクティブ化（214 ページ）を参照してください。

Cisco MDS NX-OS リリース 6.2(11) 以降では、次のヘルス モニタリングのテストのいずれかの連続失敗数がしきい値に到達した後、システムがデフォルト アクションに加えて修正 (回復) アクションを実行するように設定できます。

- PortLoopback テスト（Cisco MDS 48 ポート 10 Gbps の FCoE モジュールでのみサポートされます）
- RewriteEngineLoopback テスト
- StandbyFabricLoopback テスト
- 内部 PortLoopback テスト

（注） 修正（回復）アクションはデフォルトでは無効です。

## スーパーバイザへの修正（回復）アクション

スーパーバイザへの修正アクションは次のとおりです。

StandbyFabricLoopback test：システムがスタンバイ スーパバイザをリロードし、3 回試行した後、システムがスタンバイ スーパバイザの電源をオフにします。

（注） リロード後、スタンバイ スーパバイザがオンラインになったときに、デフォルトでヘルス モニタリング診断が起動します。

（注） 1 回の再試行は、StandbyFabricLoopback テストの連続エラーしきい値に続いて、スタンバイ スーパバイザのリロードの完全なサイクルを意味します。

## Cisco MDS 48 ポート 16 Gbps ファイバ チャネル モジュールの対処（回復）

各テストの修正アクションは次のとおりです。

- 内部 PortLoopback テスト：システムでは失敗したポートがダウンし、障害が発生している状態に変更されます。
- RewriteEngineLoopback テスト：システムは、障害のあるコンポーネント（スーパーバイザまたはファブリック）によって異なる修正措置を行います。
  - スタンバイ スーパバイザを持つシャーシ（ha-standby 状態）では、システムがアクティブ スーパーバイザで障害を検出した場合、システムがスイッチ オーバーをトリガし、スタンバイ スーパバイザに経由で切り替えます。シャーシにスタンバイ スーパーバイザがない場合、システムはアクションを実行しません。

（注） PortLoopback テストが Cisco MDS 48 ポート 16 Gbps ファイバ チャネルのモジュールでオンデマンド モードでのみ使用可能なため、修正措置をサポートしていません。

（注） Cisco MDS NX-OS リリース 6.2(13) から RewriteEngineLookpback テストおよび RewriteEngineLoopback テストの修正措置は、Cisco MDS 48 ポート 16 Gbps ファイバ チャネルのモジュールでサポートされます。

## Cisco MDS 48 ポート 10 Gbps の FCoE モジュールの対処 (回復)

- PortLoopback テスト]: システムが失敗したポートがダウンし、エラーディセーブル状態にします。
- RewriteEngineLoopback テスト]: システムは、障害のあるコンポーネント (スーパーバイザまたはファブリック) によって異なる corrective action(是正措置、修正措置):
  - (これは ha-standby 状態で) スタンバイ スーパバイザ、シャーシのアクティブ スーパーバイザで障害が検出されると、システム、「スイッチ オーバー」をトリガーとスタンバイ スーパバイザに経由でスイッチします。シャーシにスタンバイ スーパーバイザがない場合、システムはアクションを実行しません。

（注） シャーシ内のスタンバイ スーパバイザの電源がオフになって (StandbyFabricLoopback テストに関連付けられている) corrective action(是正措置、修正措置) への応答で、システムは、アクションをされません。

- • 障害のあるコンポーネントがファブリック モジュールと判断した場合、RewriteEngineLoopback が連続して失敗すると 10 はテスト後に、、その特定のファブリック モジュールをリロードします。連続 3 回の 10 の連続したエラーおよびリロードのこのサイクルが発生し、ファブリック モジュールの電源がオフになってし。

- PortLoopback が連続して失敗すると 10 をテストする場合は、ポートとして、障害のあるコンポーネントが決定される、後に、システムは Faultyポートを error-disabled ステートに移動します。

## ハイ アベイラビリティ

ハイ アベイラビリティの重要な機能は、ライブ システムでハードウェア障害を検出して、対処することです。GOLD はハードウェア障害を検出し、スイッチオーバーを決定するソフトウェアのコンポーネントへのフィードバックを提供することによって、システムのハイ アベイラビリティを提供します。

Cisco MDS 9700 ファミリ スイッチは、再起動後に実行中の設定を適用することによってGOLD ステートレス再起動をサポートします。スーパーバイザ スイッチオーバーの後に、GOLD は新しいアクティブ スーパーバイザから診断を再開します。

# オンライン診断機能のライセンス要件

| 製品 | ライセンス要件 |
|---|---|
| Cisco NX-OS | オンライン診断機能にライセンスは不要です。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。For a complete explanation of the Cisco NX-OS licensing scheme, see the Cisco MDS 9000 Family NX-OS Licensing Guide. |

# デフォルト設定

表 30 : デフォルトのオンライン診断パラメータ （212 ページ） に、オンライン診断パラメータのデフォルト設定を示します。

**表 *30* : デフォルトのオンライン診断パラメータ**

| パラメータ | デフォルト |
|---|---|
| 起動時診断レベル | complete |
| Health Monitoring tests | active |
| 修正(回復)アクション | disabled |

# オンライン診断の設定

## 起動診断レベルの設定

一連のすべてのテストを実行するように起動診断機能を設定する、またはモジュールが短時間で起動するように、すべての起動診断テストをバイパスするように設定するには、次のタスクを実行します。

（注） It is recommended to set the bootup online diagnostics level to **complete**.

手順

**ステップ 1** **configure terminal**

例：

```
switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)#
```

グローバル設定モードを開始します。

**ステップ 2** **diagnostic bootup level** {**complete** | **bypass** }

例：

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

デバイスの起動時に、診断テストが開始されるように起動診断レベルを設定します。

- **complete**：すべての起動時診断を実行します。complete がデフォルトです。
- **bypass**：起動時診断を実行しません。

**ステップ 3** **show diagnostic bootup level**

例：

```
switch(config)# show diagnostic bootup level
```

（任意）デバイスに現在設定されている起動診断レベル（bypass または complete）を表示します。

**ステップ 4** **copy running-config startup-config**

例：

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

（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

# 使用可能なテストのリストを表示します。

手順

**show diagnostic content module** *slot*

例：

```
switch# show diagnostic content module 1
```

(オプション)特定のモジュールでについては、診断とその属性のリストを表示します。

スロット: テストがアクティブになるモジュールの数。

# 診断テストのヘルス モニタリングのアクティブ化

手順

ステップ 1 **configure terminal**

例：

```
switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)#
```

グローバル コンフィギュレーション モードを開始します。

ステップ 2 **diagnostic monitor interval module** *slot* **test** [*test-id* | *name* | **all**] **hour** *hour* **min** *minutes* **second** *sec*

例：

```
switch(config)# diagnostic monitor interval module 6 test 3 hour 1 min 0 sec 0
```

（任意）指定されたテストを実行するインターバルを設定します。インターバルを設定しなかった場合は、過去に設定されたインターバルまたはデフォルトのインターバルでテストが実行されます。

引数は次のとおりです。

- スロット: テストがアクティブになるモジュールの数。
- test-id：テストの固有の識別番号。
- name：テストの定義済みの名前。
- hour：範囲は 0 ～ 23 時間
- 分：範囲は 0 ～ 59 分です。
- 秒：範囲は 0 ～ 59 秒です。

**ステップ 3** **diagnostic monitor module** *slot* **test** [*test-id* | *name* | **all** ]

**例**：

```
switch(config)# diagnostic monitor module 6 test 3
switch(config)# diagnostic monitor module 6 test SecondaryBootROM
```

指定されたテストをアクティブにします。

引数は次のとおりです。

- スロット: テストがアクティブになるモジュールの数。
- test-id：テストの固有の識別番号。
- 名前: テストの定義済みの名前。

**ステップ 4** **show diagnostic content module** {*slot* | **all**}

**例**：

```
switch(config)# show diagnostic content module 6
```

（任意）診断テストおよび対応する属性の情報を表示します。

引数は以下のようになります。

- slot：テストがアクティブになるモジュールの数。

# 診断テストのヘルス モニタリングを非アクティブ化

（注） 非アクティブにしたテストでは、現在の設定が維持されますが、スケジュール上のインターバルではテストは実行されません。

テストを非アクティブ化するには、次の作業を行います。

| コマンド | 目的 |
| --- | --- |
| **no diagnostic monitor module** *slot* **test** [*test-id* \| *name* \| **all**]<br>**Examples:**<br>`switch(config)# no diagnostic monitor interval module 8 test 3`<br>`switch(config)# no diagnostic monitor interval module 8 test SecondaryBootROM` | 指定されたテストを非アクティブ化します。<br>引数は次のとおりです。<br>• スロット: テストがアクティブになるモジュールの数。<br>• test-id：テストの固有の識別番号。<br>• 名前: テストの定義済みの名前。 |

# オンデマンド診断テストの開始または中止

オンデマンド診察テストを開始または停止すると、アクション（オプション）にテストを繰り返す反復回数を変更し、テスト失敗時に実行するアクションを決定できます。

（注） スケジュールされたネットワーク メンテナンス時に、中断診断テストを手動で開始することを推奨します。

オンデマンド診断テストを開始または停止するには、次のタスクを実行します。

**手順**

**ステップ 1** **diagnostic ondemand iteration** *number*

**例**：

```
switch# diagnostic ondemand iteration 5
```

（任意）オンデマンドテストの実行回数を設定します。範囲は 1 ～ 999 です。デフォルトは 1 です。

**ステップ 2** **diagnostic ondemand action-on-failure** {**continue failure-count** *num-fails* | **stop**}

**例**：

```
switch# diagnostic ondemand action-on-failure stop
```

（任意）オンデマンドテストが失敗した場合のアクションを設定します。

**ステップ 3** **show diagnostic ondemand setting**

**例**：

```
switch# show diagnostic ondemand setting
Test iterations = 1
```

```
Action on test failure = continue until test failure limit reaches 1
```

（オプション）オンデマンド診断に関する情報を表示します。

**ステップ 4** **diagnostics**slot [テスト id | **start module test** 名前|**all** |] [ポート番号|**port non-disruptive all**]

**例**：

```
switch# diagnostic start module 6 test all
```

モジュール上で 1 つまたは複数の診断テストを開始します。

引数は次のとおりです。

- すべて：すべてのテストがトリガされます。

（注） 複数のテスト ID または名前はカンマで区切って指定することができます。

- 非中断：すべての非中断テストがトリガされます。
- ポート：単一ポート、ポートの範囲、すべてのポートでテストを呼び出すことができます。

**ステップ 5** **diagnosticmodule** slot **run** { **test** |**PortLoopbackRewriteEngineLoopback** |**SnakeLoopback** |**IntPortLoopback** |**ExtPortLoopback** }{**port** ポート *id* }

**例**：

```
switch# diagnostic run module 3 test PortLoopback port 1
```

モジュールで選択されたテストを開始し、テストの完了時に結果を表示します。

（注） このコマンドは、Cisco MDS NX-OS リリース 6.2(11c) から導入されています。

詳細については、オンデマンド モードにオンデマンド診断テストを開始します。 （218 ページ）を参照してください。

**ステップ 6** **diagnostic stop module** *slot* **test** [*test-id* | *name* | **all** ]

**例**：

```
switch# diagnostic stop module 6 test all
```

（オプション）モジュール上で 1 つまたは複数の診断テストを停止します。

**ステップ 7** **show diagnostic status module** *slot*

**例**：

```
switch# show diagnostic status module 6
```

（オプション）モジュールのテストモードについての応報とともに実行およびキューされたすべてのテストを表示します。

特定のモジュールでテストが実行またはキューされない場合、統計情報がNAとして表示されます。

**ステップ 8** **show diagnostic result module** *slot* **test** [*test-id* | *name*]

**例**：

```
switch# show diagnostic result module 1 test 3 SecondaryBootROM
```

（オプション）指定されたテストの結果を表示します。

## オンデマンド モードにオンデマンド診断テストを開始します。

OHMS(オンライン状態管理システム)には、テストの実行後に即座に結果を表示する「オンデマンド モード」で起動テストがサポートされています。

Cisco MDS NX-OS リリース 6.2(11c) からゴールドには、「オンデマンド モード」でテストのセットから特定テストを起動し、、テストの実行後即座にテスト結果を表示するがサポートされています。

GOLD tests can be invoked in an 'on-demand' mode using the **diagnostic start module** command. The **diagnostic run module** command also supports the same action but there are a few key differences between the two. 次に、2つのコマンドの違いを示します。

- In contrast to the **diagnostic start module** command, the **diagnostic run module** command blocks the current CLI session till the completion of test. テスト、CLI セッションの完了後には、ブロックされたであり、結果は同じコンソールに表示されます。

（注） または、最大15秒のテストの完了、CLIセッションがブロックされます。15秒の時間内内で、テストが完了していない場合、ゴールドはCLIセッションのブロックを解除し、により、テストを完了、バック グラウンドで実行します。

（注） Only one test can be invoked on a particular module using the **diagnostic run module** command. ユーザが同じモジュール上の別のテストを呼び出してしようとするとエラーが表示されます、テストが呼び出されます。

- The **diagnostic start module** command requires the user to execute the **show diagnostic result** command in order to display the test result. As the test runs in the background (the current CLI session is not blocked), the user needs to issue **show diagnostic result** command to view the result, whereas the test result is implicitly displayed on the same console when the **diagnostic run module** command is executed.
- Show 診断結果コマンドからよりも多く直感的なは、結果をコマンドを実行して診断で表示されます。

（注） The maximum number of ports recommended for the **diagnostic run module** command is 5.

# 診断結果の消去

To clear the diagnostic test results, use the following command:

| コマンド | 目的 |
|---|---|
| **diagnostic clear result module** [*slot* \|**all**] **test** {*test-id* \| **all** }<br>**Example:**<br>`switch# diagnostic clear result module 2 test all`<br>`switch# diagnostic clear result module 2 test 3` | 指定されたテストのテスト結果を消去します。 |

# 診断結果のシミュレーション

ゴールドの診察テスト障害が発生した場合の動作をテストするには、ゴールドは、ポート、sup、またはファブリックでテストの失敗をシミュレートするためのメカニズムを提供します。

（注） 修正処理を有効にした後、障害をシミュレートすると、障害がシミュレートされるコンポーネントのアクション (是正措置を参照してください) がトリガーされます。

診察テスト結果をシミュレートするには、次のコマンドを使用します。

| コマンド | 目的 |
|---|---|
| **diagnostictest test fail**スロットテスト*id* {\| **simulation modulerandom-fail** \|} **success** [番号 \|**port all**]<br>**Example:**<br>`switch# diagnostic test simulation module 2 test 2 fail` | テスト結果のシミュレーションを行います。 |

シミュレートされたテスト結果を消去するには、次のコマンドを使用します。

| コマンド | 目的 |
|---|---|
| **diagnostic test simulation module** *slot* **test** *test-id* **clear**<br>**Example:**<br>`switch# diagnostic test simulation module 2 test 2 clear` | シミュレーションしたテスト結果を消去します。 |

# 修正 (回復) アクションの有効化

修正 (回復) アクションを有効にするには、次のコマンドを使用します。

**手順**

**ステップ 1** **configure terminal**

グローバル コンフィギュレーション モードを開始します。

**ステップ 2** **diagnostic eem action conservative**

**例**：

```
switch(config)# diagnostic eem action conservative
```

是正またはリカバリのアクションを有効にします。

（注） このコマンドは、システム全体に適用されます、具体的には、特定の設定されているモジュールまたはできませんをテストします。

**ステップ 3** **no diagnostic eem action conservative**

修正 (回復) のアクションを無効になります。

# オンライン診断の検証

ゴールドテストを表示するには、結果、ステータス、および設定情報を使用して、次のコマンドのいずれか。

| コマンド | 目的 |
|---|---|
| **show diagnostic bootup level** | 起動診断に関する情報を表示します。 |
| **show diagnostic content module** {*slot* \| **all**} | モジュールの診断テスト内容に関する情報を表示します。 |
| **show diagnostic description module** *slot* **test** [*test-name* \| **all**] | 診断テストの説明を表示します。 |
| **show diagnostic events** [**error** \| **info**] | 診断イベントをエラーおよび情報イベント タイプ別に表示します。 |
| **show diagnostic ondemand setting** | オンデマンド診断に関する情報を表示します。 |
| **test** slot [**show diagnostic result module** *[ test-name* \| **all**]] [**detail**] | 診断結果に関する情報を表示します。 |

| コマンド | 目的 |
|---|---|
| **show diagnostic simulation module** *slot* | シミュレーションした診断テストに関する情報を表示します。 |
| **show diagnostic status module** *slot* | モジュールのすべてのテストについて、テスト状況を表示します。 |
| **show module** | オンライン診断テストの状況を含むモジュール情報を表示します。 |
| **show diagnostic eem action** | 修正（回復）措置の状況を表示します。 |

# オンライン診断のコンフィギュレーション例

This example shows how to start all on-demand tests on a module:

**diagnostic start module 6 test all**

この例では、テストを有効化し、モジュール上で、テストのテスト間隔を設定する方法を示します。

**configure terminal**

**diagnostic monitor module 6 test 2**

**diagnostic monitor interval module 6 test 2 hour 3 min 30 sec 0**

# その他の参考資料

オンライン診断の実装に関する詳細情報については、次の項を参照してください。

### 関連資料

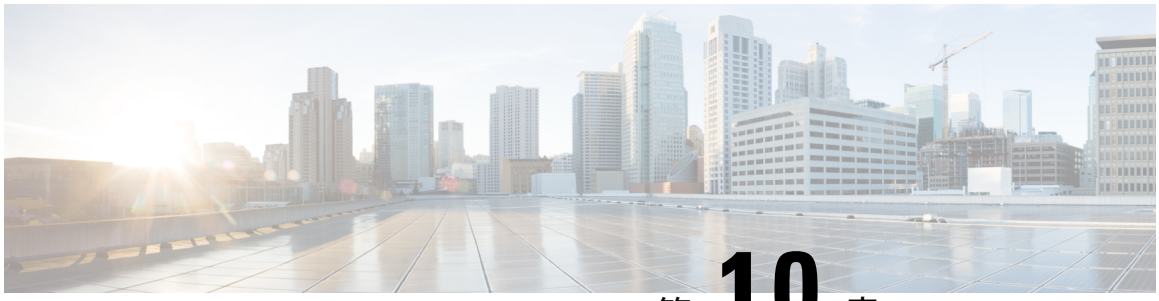
| 関連項目 | マニュアル タイトル |
|---|---|
| オンライン診断 CLI コマンド | 『Cisco MDS 9000 Family Command Reference』 |

### オンライン診断機能の履歴

表 31 : オンライン診断機能の履歴 （222 ページ） に、この機能のリリース履歴を示します。

表 *31* : オンライン診断機能の履歴

| 機能名 | リリース | 機能情報 |
|---|---|---|
| Cisco MDS 48 ポート 16 Gbps ファイバ チャネル モジュールの RewriteEngine ループバックのサポート | 6.2(13) | この機能が導入されました。 |
| Cisco MDS 48 ポート 16 Gbps ファイバ チャネル モジュールの ExtPortLoopback テストのサポート | 6.2(11c) | この機能が導入されました。 |
| Cisco MDS 48 ポート 16 Gbps ファイバ チャネル モジュールの修正（回復）アクションのサポート | 6.2(11) | この機能が導入されました。 |
| FC ポートのシーケンスを起動する PortLoopback テスト | 6.2(11) | この機能が導入されました。 |
| イーサネット モジュールを経由する Cisco MDS 48 ポート 10 ギガビット ファイバ チャネルの修正アクションのサポート | 6.2(11) | この機能が導入されました。 |
| RNG 10Gbps FCoE モジュールの GOLD サポート | 6.2(7) | この機能が導入されました。 |
| Cisco MDS 48 ポート 16-Gbps ファイバ チャネル モジュールの IntPortLoopback | 6.2(7) | この機能が導入されました。 |
| Generic Online Diagnostics（GOLD） | 6.2 | この機能が導入されました。 |



第 10 章

# スイッチ間のリンク診断の設定

Cisco MDS NX-OS リリース 7.3(0)D1(1) より、した Cisco MDS 9700 および 9500 シリーズ スイッチは、新たな Interswitch Link（ISL）診断機能をサポートします。この章では、Cisco MDS 9500 および 9700 ファミリ スイッチで ISL 診断を設定する方法を説明します。



## ISL 診断についての情報

ISL 診断機能は、ネットワーク内の Cisco MDS スイッチ間でスイッチ間のリンクの健全性を検証するのに役立ちます。

### ISL 診断機能の概要

ISL 診断は、Cisco MDS スイッチの次の FC モジュールでサポートされます。

- Cisco MDS 9500 シリーズ スイッチのアドバンスト 8 Gbps モジュール
  - DS-X9232-256K9
  - DS-X9248-256K9
- Cisco MDS 9700 シリーズ スイッチの 16 Gbps モジュール
  - DS-X9448-768K9
  - DS-X9334-K9
- Cisco MDS 9700 シリーズ スイッチの 32 Gbps モジュール
  - DS-X9648-1536 K 9

（注） モジュール上のISL診断サポートは、ジェネレータおよびリフレクタ ポートにのみ限定されます。

- 両側でサポートされている異なるスイッチ ファミリの2つのモジュール間で診断テストを実行できます。

次のテストは、ISL 診断を使用して実行できます。

- 遅延テスト/ケーブル長テスト
- シングルホップ トラフィックのテスト
- マルチホップ エンドツー エンドのトラフィックのテスト

ISL 診断は、Cisco MDS スイッチの次の FC モジュールではサポートされません。

- DS-X9224-96K9
- DS-X9248-96K9
- DS-X9248-48K9
- DS-X9304-18K9

（注）

- ISL 診断は、Nexus 2000 および Nexus 5000 などその他の非 MDS スイッチではサポートされません。
- ISL 診断は、Cisco MDS 9148S 16G マルチレイヤ ファブリック スイッチと Cisco MDS 9250i マルチサービス ファブリック スイッチではサポートされません。
- ISL 診断は、Cisco MDS スイッチの FCoE および IPS モジュールのいずれかではサポートされません。
- ISL診断機能は、Cisco MDS 9700および9500スイッチ間で相互運用することができます。(たとえば、特定の ISL 診断テストでは、ジェネレータ スイッチは Cisco MDS 9700 スイッチになり、リフレクタ スイッチは Cisco MDS 9500 スイッチまたはその逆になります。)

# 遅延テストまたはケーブル長のテスト

遅延のテストは、2 つの Cisco MDS スイッチ間の ISL の遅延と長さを測定します。

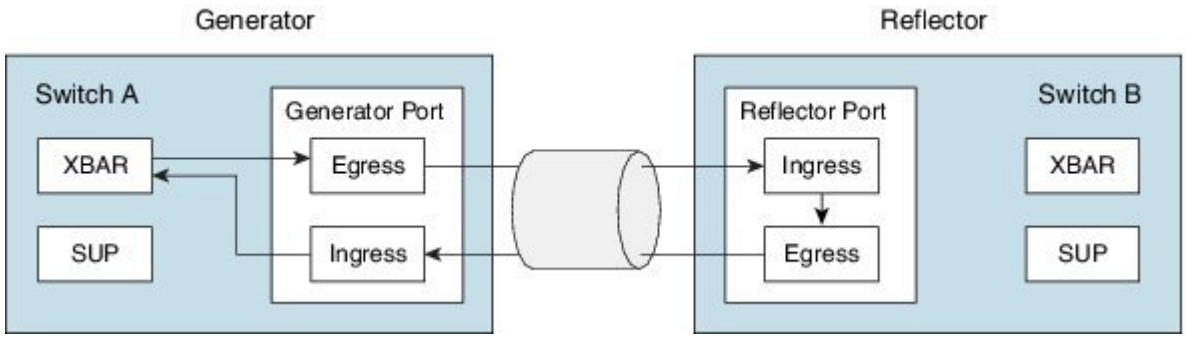
フレームは、リフレクタ スイッチ ポートによりタイムスタンプがキャプチャされているジェネレータ スイッチ ポートにループバックされます。

タイムスタンプは、リフレクタ ポートの遅延と同様に両方向でリンクの遅延を測定できます。ケーブル長は、リンク遅延のみを使用して計算されます。

（注） 遅延のテストを実行すると、同じリンク上で実行しているその他のトラフィックが存在しない可能性があります。

図 7 : 遅延テスト （225 ページ） 遅延テストの詳細を表示します。

**図 7 : 遅延テスト**




# 1 つのホップ トラフィックのテスト

シングル ホップ トラフィックのテストは、さまざまなフレーム レートでトラフィックを処理する ISL の効率性を確認することによって、ISL の健全性を検証します。

MAC ハードウェアで使用可能な内部トラフィック ジェネレータ機能を使用して、ジェネレータ スイッチでは、ファイバ チャネル (FC) フレームが生成されます。これらのフレームは、テスト対象 ISL over ジェネレータ スイッチポートから送信されます。リフレクタ スイッチは、フレームを受信し、通常のファブリック パスのスイッチング経由でスイッチに、ISL テストの下に受信したポート経由で戻るフレームを送信します。

ISL トラフィックの効率がジェネレータ スイッチポートに戻り受信したパケットの数に基づいて計算されます。

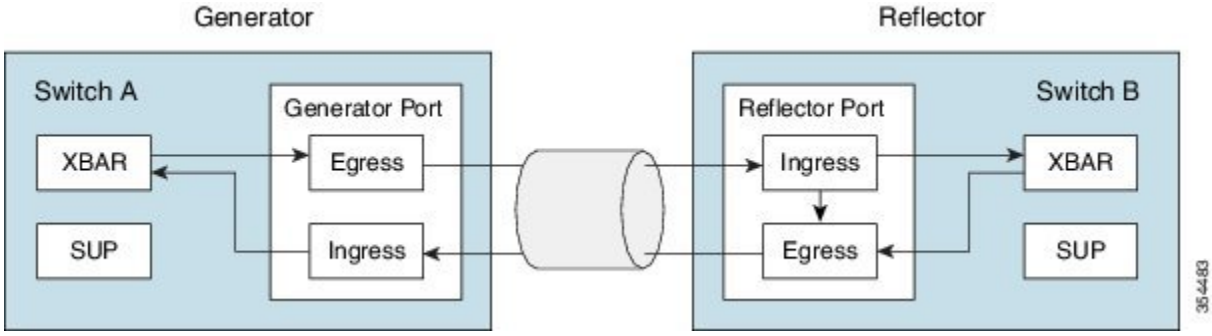
（注） シングル ホップ テストを実行すると、ときにありません同じリンク上で実行しているその他のすべてのトラフィック。

次のシナリオでエラーが返さトラフィック テスト。

- 場合は、ISL は稼働ではありません。
- 場合は、ジェネレータ ポートには、内部トラフィック ジェネレータ機能はありません。
- 場合に、リフレクタは、ループバック モードでは配置されません。

図 8 : 1 つのホップ トラフィックのテスト （226 ページ） シングル ホップ トラフィックのテストの詳細を示します。

図 *8 : 1* つのホップ トラフィックのテスト




# マルチホップ エンドツー エンドのトラフィックのテスト

マルチホップ テストは、ホスト スイッチとファブリック間の ISL の健全性と、ファブリックのターゲット スイッチを評価します。

ホストをファブリックのターゲットにホストを接続する前に、マルチホップ テストを使用して、ホスト ポートとターゲット ポート間のファブリック パスをテストします。

ホスト スイッチとターゲット スイッチ間で複数のホップが存在する可能性があります。特定の設定は中間スイッチで必要です。

（注） ファブリック内の中間のスイッチには、ジェネレータとリフレクタ ポート間にルートが存在する限り、例えばFC、FCoE、IPS、などのインターフェイスまたはリンクを有する可能性があります。

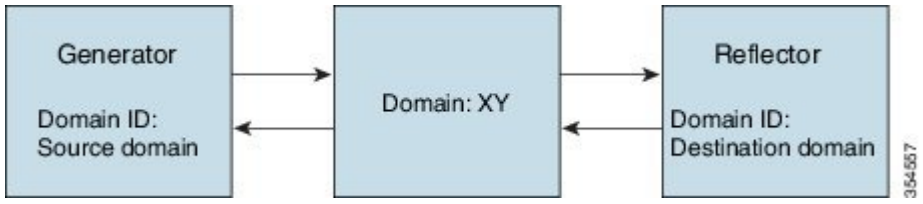
ファイバ チャネル（FC）フレームがジェネレータ スイッチポートで生成され、最初のホップ リンクに送信します。これらのフレームは、リフレクタ スイッチに到達するまで中間のスイッチを通過します。その後リフレクタ スイッチはフレームを切り替え、ジェネレータ スイッチにそれらを返します。ジェネレータ スイッチで受信したパケット数に基づいて、ISL の効率性が表示されます。

マルチホップ トラフィック テストは、ジェネレータおよびリフレクタ スイッチのドメイン ID に基づいています。

（注） マルチホップ トラフィック テストを実行する場合、ジェネレータおよびリフレクタ ポートの両方で実行されているその他のトラフィックではない可能性がありますが、マルチホップ トラフィック テストにより使用される ISL 上で実行されているトラフィックになる可能性があります。

図 9 : マルチホップ エンドツー エンドのトラフィックのテスト （227 ページ） マルチホップ エンドツー エンド トラフィックのテストの詳細を示します。

図 *9:* マルチホップ エンドツー エンドのトラフィックのテスト




# ISL診断の設定

## Cisco MDS 9700 シリーズ スイッチの遅延テストまたはケーブル長のテストの設定

ジェネレータとリフレクタ スイッチ間の遅延テストを設定するには、次のタスクを実行します。

### 手順

**ステップ 1** 次のコマンドを使用してループバック モードに設定することで、テスト用リフレクタ スイッチでテスト インターフェイスを有効にします。

スイッチ B # **diagnostic isl reflector latency_test loop-back interface** インターフェイス *id* **enable**

**ステップ 2** ジェネレータ スイッチを設定して、テストを実行し結果を表示します。

スイッチ A # **diagnostic isl latency-test interface** インターフェイス *id*

**ステップ 3** 遅延テストのリフレクタ ポートを無効にするには、リフレクタ スイッチの次のコマンドを設定します。

switch B# **diagnostic isl reflector latency_test loop-back interface** *interface id* **disable**

### 遅延テストまたはケーブル長テスト

この例では、遅延テスト用のリフレクタ スイッチのポートを有効にする方法を示します。

```
switch B# diagnostic isl reflector latency_test loop-back interface fc1/13 enable
Reflector Configuration Successful.
```

この例では、遅延テストを実行し、遅延およびケーブル長の両方の結果を表示する方法を示します。

```
switch A# diagnostic isl latency-test interface fc4/1
Waiting for sync to be achieved on the link ....
Sync is achieved, Link has been initialized.
Starting the test ....
-----------------------------------------------------------
Latency test Result for port:                    fc4/1
Latency in the switch (in ns):                   399
Latency in the cable (in ns):                    39
Length of the cable (accuracy +/- 2m):           4 m
-----------------------------------------------------------
```

この例では、遅延テスト用のリフレクタ スイッチのポートを無効にする方法を示します。

```
switch B# diagnostic isl reflector latency_test loop-back interface fc1/13 disable
Reflector Configuration Successful.
```

# Cisco MDS 9500 シリーズ スイッチの遅延テストまたはケーブル長テストの設定

ジェネレータおよびリフレクタ スイッチ間の遅延テストを設定するには、次のタスクを実行します。

### 手順

**ステップ 1** 次のコマンドを使用してループバック モードに設定することで、テスト用リフレクタ スイッチでテスト インターフェイスを有効にします。

switch B# **system health isl reflector latency_test loop-back interface** *interface id* **enable**

**ステップ 2** ジェネレータ スイッチを設定して、テストを実行し結果を表示します。

switch A# **system health isl latency-test interface** *interface id*

**ステップ 3** 遅延テストのリフレクタ ポートを無効にするには、リフレクタ スイッチの次のコマンドを設定します。

switch B# **system health isl reflector latency_test loop-back interface** *interface id* **disable**

### 遅延テストまたはケーブル長テスト

この例では、遅延テスト用のリフレクタ スイッチのポートを有効にする方法を示します。

```
switch B# system health isl reflector latency_test loop-back interface fc4/25 enable
Reflector Configuration Successful.
```

この例では、遅延テストを実行し、遅延およびケーブル長の両方の結果を表示する方法を示します。

```
switch A# system health isl latency-test interface fc12/16
Waiting for sync to be achieved on the link ....
Sync is achieved, Link has been initialized.
Starting the test ....
------------------------------------------------------------
Latency test Result for port:                    fc12/16
Latency in the switch (in ns):                   1404
Latency in the cable (in ns):                    162
Length of the cable (accuracy +/- 2m):           8 m
------------------------------------------------------------
```

この例では、遅延テスト用のリフレクタ スイッチのポートを無効にする方法を示します。

```
switch B# system health isl reflector latency_test loop-back interface fc4/25 disable
Reflector Configuration Successful.
```

# Cisco MDS 9700 シリーズ スイッチのシングル ホップ トラフィック テストの設定

ジェネレータ スイッチとリフレクタ スイッチ間のシングルホップ トラフィック テストを設定するには、次のタスクを実行します。

### 手順

**ステップ 1** 次のコマンドを使用してループバック モードに設定することで、シングル ホップ トラフィック テストのリフレクタ スイッチ上のテスト インターフェイスを有効にします。

switch B# **diagnostic isl reflector traffic_test loop-back interface** *interface id* **enable**

**ステップ 2** 次のいずれかのオプションを使用してインターフェイスを設定します。

- 指定されたフレーム数、フレーム サイズ、およびレート（リンク速度）パラメータのトラフィックのテストを実行するジェネレータ スイッチ上のインターフェイスを設定します。

  switch A # **diagnostic isl generator interface** *interface id* **start frame-count** *number* **rate** *value* **frame_size min** *minimum size* **max** maximum **step** size *num*

- 指定の期間、フレーム サイズ、およびレート（リンク速度）パラメータのトラフィック テストを実行するジェネレータ スイッチ上のインターフェイスを設定します。

  switch A # **diagnostic isl generator interface** *interface id* **start duration** *seconds* **rate** *value* **frame_size min** *minimum size* **max** maximum **step** size *num*

**ステップ 3** ジェネレータ スイッチでシングルホップ トラフィック テストを停止するか、テスト結果を表示するには、次のコマンドを使用します。

switch A# **diagnostic isl generator interface** *interface id* **stop**

**ステップ 4** シングル ホップ テストのリフレクタ ポートを無効にするには、リフレクタ スイッチで次のコマンドを設定します。

switch B# **diagnostic isl reflector traffic_test loop-back interface** *interface id* **disable**

### 単一のホップ トラフィックのテスト

この例では、ループバック モードに設定することで、シングル ホップ トラフィック テストのリフレクタ上でテスト インターフェイスを有効にする方法を示します。

```
switch B# diagnostic isl reflector traffic_test loop-back interface fc9/37 enable
Reflector Configuration Successful.
```

この例では、特定の期間、速度、フレーム サイズ パラメータでジェネレータ スイッチのトラフィック テストを実行する方法を示します。

```
switch A# diagnostic isl generator interface fc4/5 start duration 100 rate 16G frame_size
 min 16 max 517 step 1
```

この例では、トラフィック テストの実行および停止方法、期間パラメータの結果の表示方法を示します。

```
switch A# diagnostic isl generator interface fc4/3 start duration 10
Waiting for sync to be achieved on the link ....
Link initialized successfully. Starting the test.

switch A# diagnostic isl generator interface fc4/3 stop
-------------------------------------------------------
Traffic test Result for port:                   fc4/3
Packets Transmitted:                            6245142
Packets Recieved:                               6245142
ISL traffic Efficiency (percent):               100.0000
-------------------------------------------------------

switch B# diagnostic isl reflector traffic_test loop-back interface fc9/37 disable
Reflector Configuration Successful.
```

# Cisco MDS 9500 シリーズ スイッチの単一つのホップ トラフィック テストの設定

ジェネレータ スイッチとリフレクタ スイッチ間のシングルホップ トラフィック テストを設定するには、次のタスクを実行します。

### 手順

**ステップ 1** 次のコマンドを使用してループバック モードに設定することによって、シングル ホップ トラフィック テストにリフレクタ スイッチ上のテスト インターフェイスを有効にします。

switch B# **system health isl reflector traffic_test loop-back interface** *interface id* **enable**

**ステップ 2** 次のいずれかのオプションを使用してインターフェイスを設定します。

- 指定されたフレーム数、フレーム サイズ、およびレート（リンク速度）パラメータのトラフィックのテストを実行するジェネレータ スイッチ上のインターフェイスを設定します。

  switch A# **system health isl generator interface** *interface id* **start frame-count** *number* **rate** *value* **frame_size min** *minimum size* **max** *maximum size* **step** *num*

- 指定の期間、フレーム サイズ、およびレート（リンク速度）パラメータのトラフィック テストを実行するジェネレータ スイッチ上のインターフェイスを設定します。

  switch A# **system health isl generator interface** *interface id* **start duration** *seconds* **rate** *value* **frame_size min** *minimum size* **max** *maximum size* **step** *num*

**ステップ 3** シングルホップ トラフィック テストを停止するか、ジェネレータ スイッチでテストの結果を表示するには、次のコマンドを使用します。

switch A# **system health isl generator interface** *interface id* **stop**

**ステップ 4** シングル ホップ テストのリフレクタ ポートを無効にするには、リフレクタ スイッチで次のコマンドを設定します。

switch B# **system health isl reflector traffic_test loop-back interface** *interface id* **disable**

### 単一ののホップ トラフィックのテスト

この例では、ループバック モードを設定して、シングル ホップ トラフィック テストにリフレクタ スイッチ上のテスト インターフェイスを有効にする方法を示します。

```
switch B# system health isl reflector traffic_test loop-back interface fc9/37 enable
Reflector Configuration Successful.
```

この例では、トラフィックを実行および停止して、ジェネレータ スイッチの期間パラメータの結果を表示する方法を示します。

```
switch A# system health isl generator interface fc12/16 start duration 100
Waiting for sync to be achieved on the link .....
Link initialized successfully. Starting the test.

switch A# system health isl generator interface fc12/16 stop
-------------------------------------------------------
Traffic test Result for port:                  fc12/16
Packets Transmitted:                           5293153
```

```
Packets Recieved:                                5293153
ISL traffic Efficiency (percent):                100.0000
-------------------------------------------------------------

switch B# system health isl reflector traffic_test loop-back interface fc9/37 disable
Reflector Configuration Successful.
```

# Cisco MDS 9700 シリーズ スイッチのマルチホップ トラフィック テストの設定

ジェネレータ スイッチとリフレクタ スイッチ間のマルチホップ トラフィック テストを設定するには、次のタスクを実行します。

### 手順

**ステップ 1** 設定することによってループバック モードにジェネレータ スイッチの特定 VSAN およびドメイン ID のマルチホップ トラフィックのテストのリフレクタ スイッチ上のテスト インターフェイスを有効にします。

スイッチ B # **diagnostic isl multi_hop reflector loop-back interface** インターフェイス *id* **vsan** *vsan id* **source-domain** ソース *id* **enable**

取得するには、ソース ドメインはリフレクタ スイッチで、次のコマンドを使用します。

スイッチ B # **show fcdomain vsan** *vsan id*

**ステップ 2** 特定 VSAN、宛先ドメイン (リフレクタ スイッチのドメイン ID)、フレームの数、リンク速度とフレーム サイズ パラメータのマルチホップ トラフィック テストを実行するようにジェネレータ スイッチで、インターフェイスを設定します。

switch A # **diagnostic isl multi_hop generator interface** *interface id* **vsan** *vsan id* **dest-domain** *dest id* **start frame-count** *number* **rate** *value* **frame_size min** *minimum size* **max** *maximum size* **step***num*

特定 VSAN、宛先ドメイン (リフレクタ スイッチのドメイン ID))]、期間、レート (リンク速度) およびフレーム サイズ パラメータのマルチホップ トラフィック テストを実行するようにジェネレータ スイッチで、インターフェイスを設定します。

switch A # **diagnostic isl multi_hop generator interface** *interface id* **vsan** *vsan id* **dest-domain** *dest id* **start duration** *seconds* **rate** *value* **frame_size min** *minimum size* **max** *maximum size* **step***num*

取得するには、宛先ドメインはジェネレータ スイッチで、次のコマンドを使用します。

スイッチ A # **show fcdomain vsan** *vsan id*

**ステップ 3** マルチホップ トラフィックのテストを停止するか、テストを表示するジェネレータ スイッチでの結果は、次のコマンドを使用します。

switch A # **diagnostic isl multi_hop generator interface** *interface id* **vsan** *vsan id* **dest-domain** *dest id* **stop**

**ステップ 4** リフレクタ ポートを無効にするのには、Mutlihop トラフィックのテストには、リフレクタ スイッチで、次のコマンドを設定します。

switch B# **diagnostic isl multi_hop reflector loop-back interface** *interface id* **vsan** *vsan id* **source-domain** *source id* **disable**

### マルチホップ トラフィックのテスト

この例では、ジェネレータとリフレクタの両方のスイッチで、ドメインのリストを表示する方法を示します。

```
switch# show fcdomain domain-list vsan 1
Number of domains: 3
Domain ID              WWN
---------    -----------------------
0x85(133)    20:01:00:0d:ec:b7:20:01 [Principal]
0xef(239)    20:01:40:55:39:0c:70:81 [Local]
0x02(2)      20:01:00:0d:ec:b7:28:c1
```

この例では、設定することによってループバック モードにジェネレータ スイッチの特定 VSAN およびドメイン ID のマルチホップ トラフィックのテストのリフレクタ スイッチ上のテスト インターフェイスを有効にする方法を示します。

```
switch B# diagnostic isl multi_hop reflector loop-back interface fc9/36 vsan 1
source_domain 239 enable
```

この例では、実行、停止、およびフレーム数のパラメータのジェネレータ スイッチでのトラフィックのテストの結果を表示する方法を示します。

```
switch A# diagnostic isl multi_hop generator interface fc4/10 vsan 1 dest_domain 133
start duration 100
switch A# diagnostic isl multi_hop generator interface fc4/10 vsan 1 dest_domain 133
stop
Generator is stopped.  Clean-up in progress.
Please wait....
-----------------------------------------------------------
Traffic test Result for port:                    fc4/10
Packets Transmitted:                             6291024
Packets Recieved:                                6291024
ISL traffic Efficiency (percent):                100.0000
-----------------------------------------------------------
switch B# diagnostic isl multi_hop reflector loop-back interface fc9/36 vsan 1
source_domain 239 disable
```

この例では、テストを実行するトラフィック ジェネレータ スイッチでの特定の期間、速度とフレーム サイズ パラメータ方法を示します。

```
switch A# diagnostic isl multi_hop generator interface fc4/10 vsan 1 dest_domain 133
start duration 100 rate 16G frame_size min 16 max 517 step 1
```

スイッチ A # **診断 isl multi_hop ジェネレータ インターフェイス fc4/10 vsan 1 dest_domain 133 stop** ジェネレータを停止します。Clean-up in progress. Please wait.... --ポートのトラフィック テスト結果: パケットの送信 fc4/10: 6291024 パケットを受信しました: 6291024 ISL トラフィック (%) の効率性: 100.0000--。-------

# Cisco MDS 9500 シリーズ スイッチのマルチホップ トラフィック テストの設定

ジェネレータ スイッチとリフレクタ スイッチ間のマルチホップ トラフィック テストを設定するには、次のタスクを実行します。

**手順**

**ステップ 1** 設定することによってループバック モードにジェネレータ スイッチの特定 VSAN およびドメイン ID のマルチホップ トラフィックのテストのリフレクタ スイッチ上のテストインターフェイスを有効にします。

switch B# **system health isl multi_hop generator interface** *interface id* **vsan** *vsan id* **source-domain** *source id* **enable**

取得するには、ソース ドメインはリフレクタ スイッチで、次のコマンドを使用します。

switch B# **show fcdomain vsan** *vsan id*

**ステップ 2** 特定 VSAN、宛先ドメイン (リフレクタ スイッチのドメイン ID)、フレームの数、リンク速度とフレーム サイズ パラメータのマルチホップ トラフィック テストを実行するようにジェネレータ スイッチで、インターフェイスを設定します。

switch A# **system health isl multi_hop generator interface** *interface id* **vsan** *vsan id* **dest-domain** *dest id* **start frame-count** *number* **rate** *value* **frame_size min** *minimum size* **max** *maximum size* **step** *num*

特定 VSAN、宛先ドメイン (リフレクタ スイッチのドメイン ID))]、期間、レート (リンク速度) およびフレーム サイズ パラメータのマルチホップ トラフィック テストを実行するようにジェネレータ スイッチで、インターフェイスを設定します。

switch A# **system health isl multi_hop generator interface** *interface id* **vsan** *vsan id* **dest-domain** *dest id* **start duration** *seconds* **rate** *value* **frame_size min** *minimum size* **max** *maximum size* **step** *num*

取得するには、宛先ドメインはジェネレータ スイッチで、次のコマンドを使用します。

switch A# **show fcdomain vsan** *vsan id*

**ステップ 3** マルチホップ トラフィックのテストを停止するか、テストを表示するジェネレータ スイッチでの結果は、次のコマンドを使用します。

switch A# **system health isl multi_hop generator interface** *interface id* **vsan** *vsan id* **dest-domain** *dest id* **stop**

**ステップ 4** リフレクタ ポートを無効にするのには、Mutlihop トラフィックのテストには、リフレクション スイッチで、次のコマンドを設定します。

switch B# **system health isl multi_hop reflector loop-back interface** *interface id* **vsan** *vsan id* **source-domain** *source id* **disable**

### マルチホップ トラフィックのテスト

この例では、ジェネレータとリフレクタの両方のスイッチで、ドメインのリストを表示する方法を示します。

```
switch# show fcdomain domain-list vsan 1
Number of domains: 3
Domain ID              WWN
---------    -----------------------
0x85(133)    20:01:00:0d:ec:b7:20:01 [Principal]
0xef(239)    20:01:40:55:39:0c:70:81 [Local]
0x02(2)      20:01:00:0d:ec:b7:28:c1
```

この例では、マルチホップ トラフィック テストのジェネレータ スイッチインターフェイスの VSAN 内に存在するリフレクタ スイッチからのループバックをイネーブルに方法を示します。

```
switch B# system health isl multi_hop reflector loop-back interface fc9/36 vsan 1
source_domain 239 enable
```

この例では、開始、停止、およびフレーム数のパラメータのジェネレータ スイッチでのトラフィックのテストの結果を表示する方法を示します。

```
switch A# system health isl multi_hop generator interface fc3/18 vsan 1 dest_domain 2
start frame-count 1000000
switch A# system health isl multi_hop generator interface fc3/18 vsan 1 dest_domain 2
stop
Generator is stopped.  Clean-up in progress.
Please wait....
------------------------------------------------------------
Traffic test Result for port:                   fc3/18
Packets Transmitted:                            1000000
Packets Recieved:                               1000000
ISL traffic Efficiency (percent):               100.0000
------------------------------------------------------------
```

```
switch B# system health isl multi_hop reflector loop-back interface fc9/36 vsan 1
source_domain 239 disable
```

この例では、テストを実行するトラフィック ジェネレータ スイッチでの特定の期間、速度とフレーム サイズ パラメータ方法を示します。

```
switch A# system health isl multi_hop generator interface fc4/5 vsan 1 dest_domain 133
start duration 100 rate 16G frame_size min 16 max 517 step 1
```

# ISL 診断のデバッグ

表 32 : Cisco MDS 9700 および 9500 スイッチのデバッグ コマンド （236 ページ） では Cisco MDS 9700 および 9500 スイッチのデバッグ コマンドの一覧が表示されます。ISL 診断テストのステータスを表示するには、次のコマンドのいずれかを使用します。

**表 *32 : Cisco MDS 9700* および *9500* スイッチのデバッグ コマンド**

| コマンド | 参照先 |
|---|---|
| Cisco MDS 9700 スイッチ | |
| **show diagnostic isl status index start** *index* **num** *number* | ポートごとに設定されている ISL 診断テストのステータスを表示します。 |
| Cisco MDS 9500 スイッチ | |
| **system health isl show status**<br>例：<br>`switch# system health isl show status index start 0 num 10`<br>`show status of isl_daig:`<br>`----------`<br>`Index: 0 if_index:0x110f000 :is_running: 0 is_reflector:1 is_latency:1 is_multihop:0`<br>`Index: 1 if_index:0x0 :is_running: 0 is_reflector:0 is_latency:0 is_multihop:0`<br>`Index: 2 if_index:0x0 :is_running: 0 is_reflector:0 is_latency:0 is_multihop:0`<br>`Index: 3 if_index:0x0 :is_running: 0 is_reflector:0 is_latency:0 is_multihop:0`<br>`Index: 4 if_index:0x0 :is_running: 0 is_reflector:0 is_latency:0 is_multihop:0`<br>`Index: 5 if_index:0x0 :is_running: 0 is_reflector:0 is_latency:0 is_multihop:0`<br>`Index: 6 if_index:0x0 :is_running: 0 is_reflector:0 is_latency:0 is_multihop:0`<br>`Index: 7 if_index:0x0 :is_running: 0 is_reflector:0 is_latency:0 is_multihop:0`<br>`Index: 8 if_index:0x0 :is_running: 0 is_reflector:0 is_latency:0 is_multihop:0`<br>`Index: 9 if_index:0x0 :is_running: 0 is_reflector:0 is_latency:0 is_multihop:0` | ポートごとに設定されている ISL 診断テストのステータスを表示します。 |

# その他の参考資料

オンライン診断の実装に関する詳細情報については、次の項を参照してください。

### 関連資料

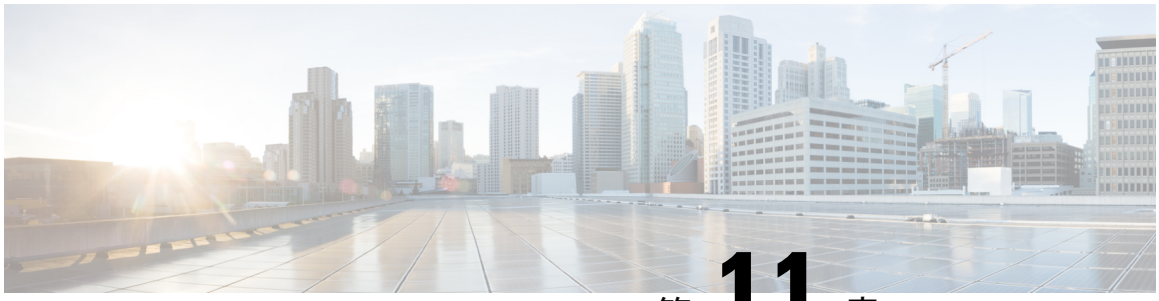
| 関連項目 | マニュアル タイトル |
|---|---|
| スイッチ間のリンク診断CLIコマンド | 『Cisco MDS 9000 Family Command Reference』 |

### オンライン診断機能の履歴

表 33 : オンライン診断機能の履歴 （237 ページ） に、この機能のリリース履歴を示します。

**表 *33* : オンライン診断機能の履歴**

| 機能名 | リリース | 機能情報 |
|---|---|---|
| ISL 診断 | 7.3(0)D1(1) | この機能が導入されました。 |



第 11 章

# HBA リンク診断の設定



## 概要

HBA リンク診断機能は、ホスト バス アダプタ (Hba) と、ネットワーク内の Cisco MDS スイッチ間のリンクの状態を検証する際に役立ちます。

サーバは、Hba と呼ばれるハードウェア デバイス経由でストレージ エリア ネットワーク (San) に接続します。この接続は、その有効期間中に障害を開発する可能性が多くの光および電気のコンポーネントで構成されます。この機能は、廃棄されたフレームを排除することと、サーバの信頼性の高い I/O 操作を保証するようにすることの障害のあるケーブル、トランシーバ、Asic、ドライバ、ファームウェアの問題、またはソフトウェアの問題については、id を使用します。

## サポートされるプラットフォーム

HBA リンク診断は次のプラットフォームでサポートされています。

- Cisco MDS 48 ポート 16 Gbps ファイバ チャネル スイッチング モジュール:DS：DS-X9448-768K9
- Cisco MDS 48 ポート 32 Gbps ファイバ チャネル スイッチング モジュール:DS：DS-X9648-1536K9
- Cisco MDS 24/10 SAN 拡張モジュール（FC ポートのみ）：DS-X9334-K9
- Cisco MDS 9396S マルチレイヤ ファブリック スイッチ

# 注意事項と制約事項

- N ポート仮想化（NPV）モードの Cisco MDS 9396S マルチレイヤ ファブリック スイッチでは、HBA リンク診断機能はサポートされていません。
- リンク診断テストを実行しているときに、ジェネレータおよびホストバスアダプタ（HBA）ポートは、通常のファイバ チャネル（FC）や、Inter Switch Link（ISL）診断などのその他のテストに使用できません。
- トラフィック ジェネレータ ポートとして使用可能なスイッチでは、少なくとも 1 つの空きまたは未使用のポートが存在する必要があります。このポートは、HBA リンクの診断テスト中に管理シャット ダウン状態である必要があります。
- シャーシのリロード、スイッチ オーバー、またはジェネレータや診断ポートをホストするモジュールのモジュール リロード時に、診断テストが中止されます。
- 1 個以上のループバック テストが失敗すると、最も低いレベルの障害のみが報告されます。最初に報告のエラーを修正し、再度テストを実行することをお勧めします。
- 診断ポートのポート LEDは、トラフィック テストが実行中であっても緑色に点灯しています。
- テスト可能な診断ポートの最大のライン レートは、ジェネレータ ポートの機能とユーザー指定のライン レートに依存します。たとえば、診断ポートが 32 Gbps スイッチング モジュールで実行されており、ジェネレータ ポートが 16 Gbps スイッチング モジュールで実行されている場合、トラフィック生成のレートは 50% に設定されており、診断ポートでサポートされている最大ライン レートは 8Gbps です。

# HBA リンク診断テスト

HBA リンク診断は、パフォーマンスを検証し、障害のあるリモート ピアと HBA コンポーネントを特定するのに役立ちます。さまざまなタイプのテストへのパスでのさまざまなコンポーネントの動作とターゲット デバイスのスタックを確認します。

リンク診断テストが設定されているし、MDS スイッチから制御します。ターゲット HBA および SFP がテストの目的のタイプをサポートする必要があります。リンクは、SAN ファブリックから削除する診断モードに設定されます。テスト トラフィックは、ファブリック トラフィックに干渉せず、特定のリンク上でのみ実行できます。テストが完了したら、リンクを診断モードから取得および SAN ファブリックでのサービスに返されることができます。

テストを実行するには、2つのポート、診断ポートおよびジェネレータ ポートが必要です。診断ポートは、テストが実行されているポートです。ジェネレータ ポートは、テストの実行に必要なトラフィックを生成します。ジェネレータ ポートは、ユーザが診断テストの開始中に明示的に指定されていないため場合、は、admin シャット ダウン状態に任意のポートがジェネレータ ポートとして選択されます。

以下は、Cisco MDS スイッチで使用可能なリンク診断テストのさまざまなタイプです。

- 遅延テスト
- ループバック トラフィックのテスト

サポートされている別のレベルでは、両方のリンク診断テストを実行できます。詳細についてを参照してください、 HBA リンク診断テストのレベル セクション。

# 遅延テスト

テストの遅延は、HBA と Cisco MDS スイッチ間のリンクのラウンドトリップ遅延を測定します。

テスト フレームが HBA ポートへのタイムスタンプはキャプチャされたジェネレータ スイッチポートしてコールバック ループバックされます。タイムスタンプは、両方の方向で測定するリンクの遅延低 HBA ポートの遅延を許可します。

ケーブル長を決定する際に光ループバック役立ちますと、遅延をテストします。ケーブル長の計算では、他の遅延のテストには適用されません。報告のケーブル長の精度は、5 m +/-内です。

# ループバック トラフィックのテスト

ループバック テストでは単一ポートからデータを送受信し、ポートが動作しているか確認します。ループバック トラフィックのテストは、さまざまなレベルで実行できます。詳細については、「HBA リンク診断テストのレベル」セクションを参照してください。

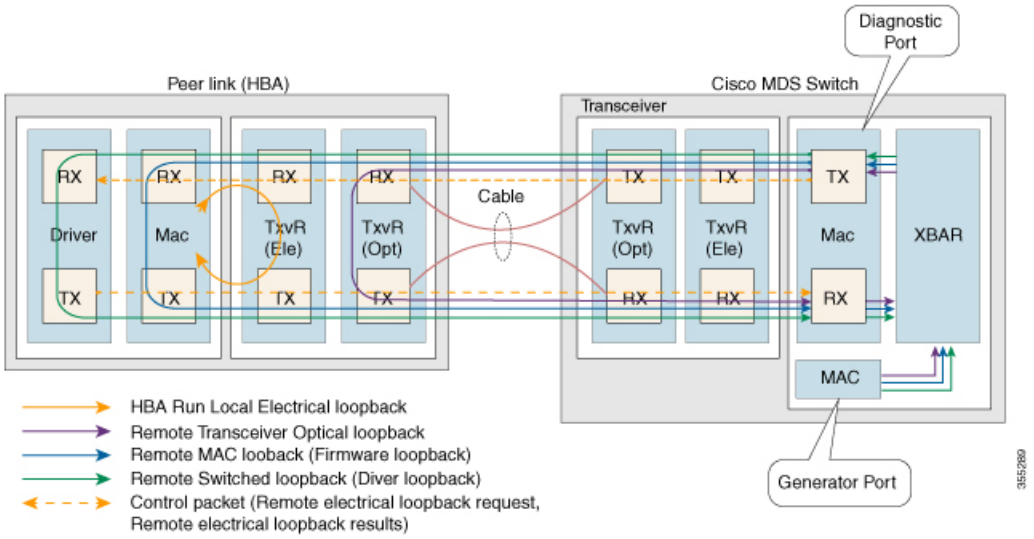
# HBA リンク診断テストのレベル

HBA リンク診断機能には、リンク診断テストを実行可能な次のレベルがサポートされています。

- リモート スイッチド
- MAC
- 電気
- Optical

次の図は、HBA リンク診断テストのさまざまなレベルを示しています。

図 *10 : HBA* リンク診断テストのレベル




## スイッチの切り替え

フレームはスタックの診断によりサポートされている最高レイヤーのピア デバイスでループバックされます（FC 2 または上記）。この機能は、ピア サーバ CPU の FC ドライバに実装されます。

## MAC

フレームはピア HBA の MAC（FC-1）レイヤでピア デバイスによりループ バックされます。この機能は、HBA のファームウェア コードに実装されます。

## 電気

フレームは、ピア デバイスしてコールバック ピア HBA のトランシーバ (FC-0) の電気段階でループです。この機能は、電気ループバックのローカルのトランシーバをプログラミング ピア HBA のファームウェアによって実装されます。

（注） 電気ループバック レベルは、遅延のテストをサポートしていません。

## Optical

フレーム ループバックは、HBA 側のトランシーバ(FC-0)の光部分で実行されます。光ループバックは、HBA のファームウェア層からトランシーバをプログラミングすることで達成されます。

HBA リンク診断の設定

# HBA リンク診断の設定

HBA リンク診断テストを実行するには、最初に HBA に接続されているポートを診断モードに設定し、このポートからテストを実行します。

リンクのテストが完了したら、HBA に接続されているポートをサービスに戻します。

## ポート上のリンク診断モードの設定

ポートでリンク診断モードを設定するには、次のタスクを実行します。

### 始める前に

- サポートされている SFP が HBA で使用されていることを確認します。
- HBA のドライバまたはファームウェアのサポートされているバージョンをインストールし、診断のパラメータを設定します。

### 手順

**ステップ 1** グローバル コンフィギュレーション モードを開始します。

switch# **configure terminal**

**ステップ 2** インターフェイスを指定してインターフェイス設定モードを開始します。

switch(config)# **interface fc** *slot/port*

**ステップ 3** インターフェイスをグレースフルにシャット ダウンし、トラフィック フローを管理で無効にします。

switch(config-if)# **shutdown**

（注） ASCII ファイルで行われた設定は、インターフェイスが管理シャット状態ではない場合リンク診断モードが開始されません。

**ステップ 4** 指定されたポートでリンク診断モードを設定します。

switch(config-if)# **switchport link-diag**

**ステップ 5** （任意） 指定されたポートでリンク診断モードを設定解除します。

switch(config-if)# **no switchport link-diag**

**ステップ 6** インターフェイスをイネーブルにします。

switch(config-if)# **no shutdown**

**ステップ 7** インターフェイスを閉じます。

switch(config-if)# **end**

**例**

（注）
- 「ポートのリンク診断モードを設定する」セクションで一覧になっている設定を使用して設定されている場合、診断ポートが初期化状態になります。
- ドライバのロード、ロード解除、HBA ポートのリセットなど HBA に変更があった場合、スイッチのリンク診断モードを設定解除し、再設定します。

次の実行設定では、インターフェイスでリンク診断モードを有効にする方法を示します。プレースホルダを、セットアップに関連する値に置き換えます。

```
configure terminal
 interface fc <1/1>
  shutdown
  switchport link-diag
  no shutdown
  end
```

次の実行設定では、インターフェイスでリンク診断モードの設定を解除する方法を示します。プレースホルダを、セットアップに関連する値に置き換えます。

```
configure terminal
 interface fc <1/1>
  shutdown
  no switchport link-diag
  no shutdown
  end
```

# ポートでリンク診断テストの実行

ポートでリンクの診断テストを実行するには、次のタスクを実行します。

.

**手順**

指定されたポートでリンクの診断テストを実行します。

switch # **diagnostic start interface fc** *slot/port* **test link-diag** [ **duration** *seconds* |**frame-count** *count* ] [ **frame-size min** *min_bytes* **max** *max_bytes* **level remote remote-all gen-interface fc** step_size] [slot/port] [{levels |}] **step**[ **payload** { **random | fixed** *fixed_payload* }][ **rate** *line_rate*]

（注）
- By default, tests are run at all supported levels if it is not explicitly selected using the **level remote** *levels* option.
- The generator port is autoselected if it is not explicitly configured using the **gen-interface fc** *slot/port* option. このコマンドの詳細については、「Cisco IOS 9000シリーズ コマンド参照資料」を参照してください。
- User specified **frame-count** *count* may not match the actual number of transmitted frames due to in-switch drops.
- カウンタまたはリンク診断テストを実行しているインターフェイスの統計情報のクリアを回避します。
- リンク診断テストを実行しているインターフェイスに試行される新しい設定は成功するリンクの診断テストの完了後にのみ。

### ポートの例: 実行中のリンクの診断テスト

この例では、診断ポートでリンクの診断テストを実行する方法を示します。

```
switch# diagnostic start interface fc 1/1 test link-diag
```

次のコマンドの出力には、診断ポートで実行されているテストの結果が表示されます。

```
switch# diagnostic result interface fc7/28 test link-diag
PWWN of peer port: 21:00:00:24:ff:17:09:ac
Status: Supported (Reflector)
Reflector loopback capabilities:  Xcvr-optical Electrical
Time of Test: Thu Sep 14 00:20:11 2017
Total time taken: 30 seconds
================|============|============|====================|============|============

                |            |            |     Discards               |
 Latency (ns)   |
Loopback Level      |    Tx Frames    |    Rx Frames    |  IN    |  OUT   |BAD
WORDS|In-Switch|External|    Status
================|============|============|======|======|=======|=======|======|============
Remote-Switched(R) |              0|              0|       0|       0|       0|
     0|       0|       -NA-
Mac(R)             |              0|              0|       0|       0|       0|
     0|       0|       -NA-
Xcvr-optical(R)    |        1000000|        1000000|       0|       0|       0|
  2136|     632|    Success
Electrical(R)      |          20000|          20000|            -NA-           |
  -NA-|    -NA-|    Success
=============================================================================================


Overall Status                          : Success
Cable Length (approx. +/- 5 metres)     : 38.2 metres
```

（注） 注釈 (R) は、リモート ピアまたは HBA ポートを示します。

次のコマンドの出力には、ピア デバイスのリンク診断機能が表示されます。

```
switch# diagnostic result interface fc1/1 test link-diag peer-capability
pWWN of Peer Port: 10:23:34:90:fa:cd:16:6c
Status: Supported (Reflector)
Reflector Loopback Capabilities:   Remote-switched MAC Xcvr-optical
```

# ポートのリンク診断テストの中止

ポートでリンク診断テストを中止するには、次のタスクを実行します。

### 手順

---

指定されたポートでリンク診断テストを中止するには。

switch # **diagnostic stop interface fc** *slot/port* **test link-diag**

---

### 例：ポートでリンク診断テストを中止します

次の例では、ポートでリンク診断テストを中止する方法を示します。

```
switch# diagnostic stop interface fc 1/1 test link-diag
```

次のコマンド出力では、診断ポートで中止されたテストの結果を表示します。

```
switch# diagnostic result interface fc1/23 test link-diag
PWWN of peer port: 10:00:00:90:fa:c7:e1:e9
Status: Supported (Reflector)
Reflector loopback capabilities:  Remote-switched MAC Xcvr-optical
Time of Test: Wed Sep 20 12:54:59 2017
Total time taken: 10 seconds
═══════════════|═══════════|═══════════|═══════════════════|═══════════|═══════════

                    |                |                  |     Discards              |
 Latency (ns)   |
Loopback Level      |    Tx Frames   |    Rx Frames     |  IN    |  OUT   |BAD
WORDS|In-Switch|External|    Status
═══════════════|═══════════|═══════════|═══════|═══════|═══════|═══════|═══════|═══════════
Remote-Switched(R) |                0|                0|       0|       0|       0|
     0|       0|       -NA-
Mac(R)             |                0|                0|       0|       0|       0|
     0|       0|       -NA-
Xcvr-optical(R)    |              439|              439|            -NA-           |
     0|       0|    Stopped
Electrical(R)      |                0|                0|       0|       0|       0|
     0|       0|       -NA-
═══════════════════════════════════════════════════════════════════════════════════

Overall Status                          : User Stop/Module Reload/PortDown/ELS error
                                          [DIAG TEST STOPPED]
Cable Length (approx. +/- 5 metres)     : -NA-
```

（注） 注釈（R）は、リモート ピアまたは HBA ポートを示します。

# HBA リンク診断のトラブルシューティング

次のコマンドは、共通の HBA リンク診断の問題をトラブルシューティングするために使用できます。

- To check if link diagnostics is enabled on an interface, use the **show interface fc** *slot/port* command.

```
switch#show interface fc 1/37
Hardware is Fibre Channel, SFP is short wave laser w/o OFC (SN)
    Port WWN is 20:25:40:55:39:0c:70:80
    Admin port mode is auto, trunk mode is on
    snmp link state traps are enabled
    Port vsan is 1
    Receive data field Size is 2112
    Beacon is turned off
    Logical type is edge
    Link Diagnostics enabled
    5 minutes input rate 0 bits/sec,0 bytes/sec, 0 frames/sec
    5 minutes output rate 0 bits/sec,0 bytes/sec, 0 frames/sec
      26654656 frames input,53267399028 bytes
        0 discards,0 errors
        0 invalid CRC/FCS,0 unknown class
        0 too long,0 too short
      26654687 frames output,53267399756 bytes
        0 discards,0 errors
      31 input OLS,31  LRR,33 NOS,0 loop inits
      61 output OLS,0 LRR, 27 NOS, 0 loop inits
    Last clearing of "show interface" counters :  never
```

- To check if an interface is being used as the generator port, use the **show interface fc** *slot/port* command.

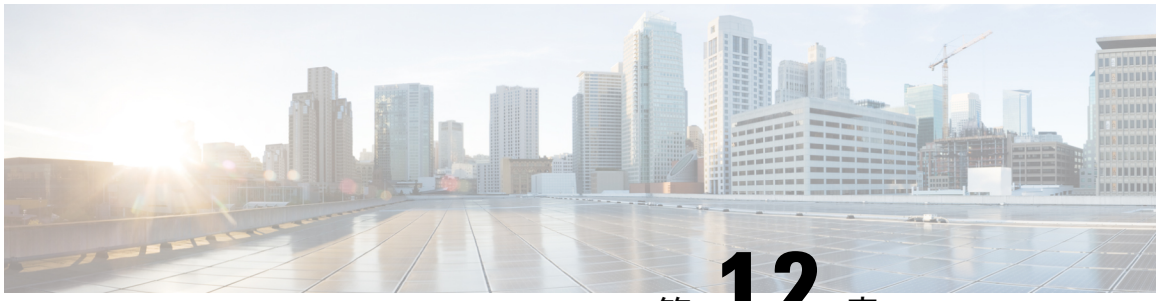
- switch# **show interface fc 1/2**

```
fc1/2 is down (Administratively down)
    Hardware is Fibre Channel, SFP is short wave laser w/o OFC (SN)
    Port WWN is 20:02:8c:60:4f:0d:20:80
    Admin port mode is auto, trunk mode is on
    snmp link state traps are enabled
    Port vsan is 1
    Receive data field Size is 2112
    Beacon is turned off
    Logical type is Unknown(0)
    Link Diagnostics generator port
    5 minutes input rate 0 bits/sec,0 bytes/sec, 0 frames/sec
    5 minutes output rate 0 bits/sec,0 bytes/sec, 0 frames/sec
      0 frames input,0 bytes
        0 discards,0 errors
        0 invalid CRC/FCS,0 unknown class
        0 too long,0 too short
      0 frames output,0 bytes
        0 discards,0 errors
      0 input OLS,0  LRR,0 NOS,0 loop inits
      0 output OLS,0 LRR, 0 NOS, 0 loop inits
    Last clearing of "show interface" counters :  never
```

- To check the link diagnostics tests that are running on the switch, use the **show diagnostic test link-diag status** command.

```
switch# show diagnostic test link-diag status
──────────────────────────────────────────────────────────────────────────────
Index  Diag-Interface    Gen-Interface    Link-diag Status
──────────────────────────────────────────────────────────────────────────────

                                          Remote-Switched(R)      MAC(R)
Electrical(R)    Xcvr-optical(R)
──────────────────────────────────────────────────────────────────────────────
1       fc2/9             fc2/1             NA                   Running
      NA                NA
```

- To collect information for Cisco technical support for this feature, use the **show tech-support link-diag** command.



第 12 章

# 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。

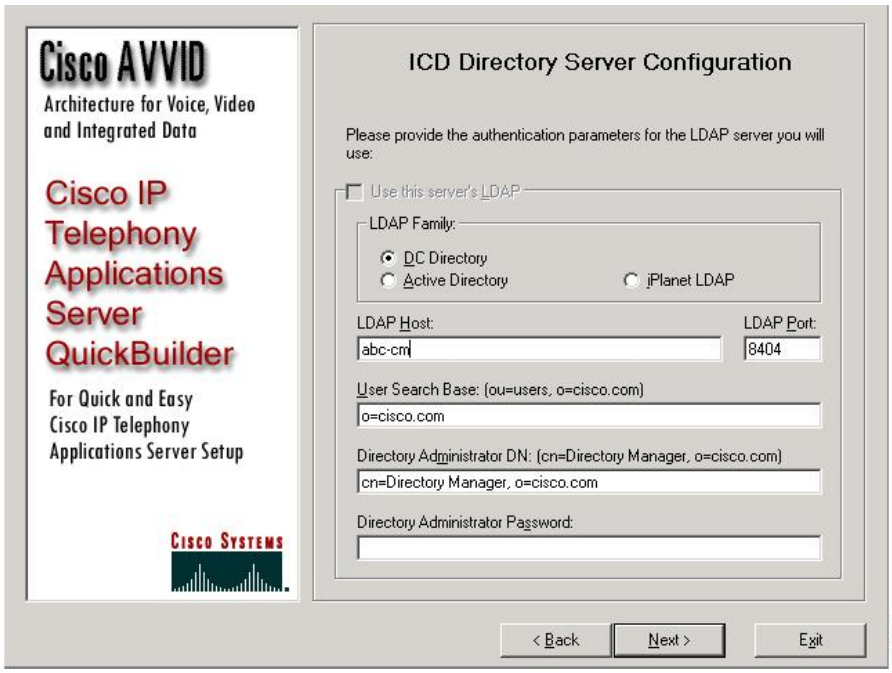
CLI ユーザと SNMP ユーザのユーザ、パスワード、ロールは、すべて同じです。CLI を通して設定されたユーザーは、SNMP を使用してスイッチまたはその逆にアクセスできます（例：Cisco DCNM-SAN またはデバイス マネージャ）。



# SNMP セキュリティについて

SNMPは、ネットワーク デバイス間での管理情報の交換を容易にするアプリケーション層プロトコルです。In all Cisco MDS 9000 Family switches, three SNMP versions are available: SNMPv1, SNMPv2c, and SNMPv3 (see 図 11 : SNMP セキュリティ （250 ページ）).

図 *11 : SNMP* セキュリティ




# SNMP バージョン 1 およびバージョン 2c

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

# SNMP バージョン 3

SNMP バージョン 3（SNMPv3）は、ネットワーク管理のための相互運用可能な標準ベースのプロトコルです。SNMPv3 は、ネットワーク経由のフレームの認証と暗号化を組み合わせることによって、デバイスへのセキュア アクセスを実現します。SNMPv3 で提供されるセキュリティ機能は、次のとおりです。

- メッセージの完全性：パケットが伝送中に改ざんされていないことを保証します。
- 認証：メッセージのソースが有効かどうかを判別します。
- 暗号化：許可されていないソースにより判読されないように、パケットの内容のスクランブルを行います。

SNMPv3 では、セキュリティ モデルとセキュリティ レベルの両方が提供されています。セキュリティ モデルは、ユーザおよびユーザが属するロールを設定する認証方式です。セキュリティ レベルとは、セキュリティ モデル内で許可されるセキュリティのレベルです。セキュリティ

モデルとセキュリティ レベルの組み合わせにより、SNMP パケット処理中に採用されるセキュリティ メカニズムが決まります。

# SNMPv3 CLI のユーザ管理および AAA の統合

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

SNMPv3 のユーザ管理を AAA サーバ レベルで一元化できます。ユーザ管理を一元化すると、Cisco MDS スイッチ上で稼働する SNMP エージェントが AAA サーバのユーザ認証サービスを利用できます。ユーザ認証が検証されると、SNMP PDU の処理が進行します。また、AAA サーバにはユーザ グループ名も格納されます。SNMP はグループ名を使用して、スイッチでローカルに使用できるアクセス ポリシーまたはロール ポリシーを適用します。

# CLI および SNMP ユーザの同期

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。

To create an SNMP or CLI user, use either the **username** or **snmp-server user** commands.

- The auth passphrase specified in the **snmp-server user** command is synchronized as the password for the CLI user.
- The password specified in the **username** command is synchronized as the auth and priv passphrases for the SNMP user.

ユーザの同期化は、次のように処理されます。

- いずれかのコマンドを使用してユーザを削除すると、SNMP と CLI の両方の該当ユーザが削除されます。
- ユーザとロールの対応関係の変更は、SNMP と CLI で同期化されます。

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

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

# スイッチ アクセスの制限

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

# グループベースの SNMP アクセス

（注） グループが業界全体で使用される標準的なSNMP用語のため、このSNMPセクションではロールをグループと称します。

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

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

# ユーザの作成および変更

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

- SNMP：スイッチ上のusmUserTableに存在するユーザのクローンとして、新規のユーザを作成します。ユーザを作成した後、クローンの秘密キーを変更してから、そのユーザをアクティブにします。RFC 2574 を参照してください。
- DCNM-SAN。
- CLI—Create a user or modify an existing user using the **snmp-server user** command.

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

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

# AES 暗号ベースのプライバシー

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

**priv** オプションで、SNMP セキュリティ暗号化方式として、DES または 128 ビット AES 暗号化を選択できます。The **priv** option along with the **aes-128** token indicates that this privacy password is for generating a 128-bit AES key. AES のプライバシー パスワードは最小で 8 文字です。パスフレーズをクリア テキストで指定する場合、最大 64 文字を指定できます。ローカライズド キーを使用する場合は、最大 130 文字を指定できます。

（注） 外部の AAA サーバを使用して SNMPv3 を使う場合、外部 AAA サーバのユーザ設定でプライバシー プロトコルに AES を指定して、SNMP PDU を暗号化する必要があります。

# トラップ、通知、伝達

トラップは、SNMPv1 で SNMP マネージャに SNMP エージェントから送信された未確認メッセージです。SNMPv2 および SNMPv3 の通知とも呼びます。伝達は、SNMP マネージャに SNMP エージェントから送信された確認済みメッセージです。エージェントが応答を受信しない場合、もう一度伝達要求を送信します。

伝達はエージェントおよびネットワークのリソースをより多く消費します。送信と同時にエージェントにより廃棄されるトラップまたは通知と異なり、伝達要求は応答を受信するまで、または要求がタイムアウトになるまで、メモリ内に保持する必要があります。トラップおよび通知は 1 回だけ送信でき、伝達は複数回送信できます。伝達を再送信することでトラフィックが増加し、ネットワーク上のオーバヘッドの向上に貢献します。同じトラップ、通知、および伝達は、複数のホスト レシーバに送信できます。

# EngineID

SNMP エンジン ID は、送信元アドレスの独立したエンティティを識別するために使用されます。エンティティは、SNMP エンジンと SNMP アプリケーションで構成されています。プロトコル データ単位（PDU）がプロキシまたはネットワーク アドレス トランスレータ（NAT）をトラバースする必要があるか、送信元エンティティ自体が動的に割り当てられた転送アドレスまたは複数の送信元アドレスを所持している場合に、エンジン ID が重要です。

SNMPv3 エンジン ID は、セキュリティ保護された PDU をエンコーディングまたはデコーディングするためにも使用されます。これは、SNMPv3 ユーザベース セキュリティ モデル（USM）の要件です。

エンジン ID、ローカル、リモートには二種類あります。Cisco MDS 9000 シリーズ スイッチでは、リモート エンジン ID のみ設定できます。ローカル エンジン ID は、MAC アドレスに基づいてスイッチにより自動的に生成され、変更されません。

# スイッチの LinkUp/LinkDown 通知

スイッチに対して、イネーブルにする LinkUp/LinkDown 通知を設定できます。次のタイプの LinkUp/LinkDown 通知をイネーブルにできます。

- Cisco：インターフェイスに対して ifLinkUpDownTrapEnable（IF-MIB で定義）がイネーブルになっている場合、そのインターフェイスについて CISCO-IF-EXTENSION-MIB.my で定義された通知（cieLinkUp、cieLinkDown）のみが送信されます。
- IETF：インターフェイスに対して ifLinkUpDownTrapEnable（IF-MIB で定義）がイネーブルになっている場合、そのインターフェイスについて IF-MIB で定義された通知（LinkUp、LinkDown）のみが送信されます。通知定義で定義された変数バインドのみが、それらの通知とともに送信されます。
- IEFT extended：インターフェイスに対して ifLinkUpDownTrapEnable（IF-MIB で定義）がイネーブルになっている場合、そのインターフェイスについて IF-MIB で定義された通知（LinkUp、LinkDown）のみが送信されます。通知定義で定義された変数バインドに加え、シスコの実装に固有の IF-MIB で定義された変数バインドも送信されます。これがデフォルト設定です。
- IEFT Cisco：インターフェイスに対して ifLinkUpDownTrapEnable（IF-MIB で定義）がイネーブルになっている場合、そのインターフェイスについて IF-MIB で定義された通知（LinkUp、LinkDown）および CISCO-IF-EXTENSION-MIB.my で定義された通知（cieLinkUp、cieLinkDown）のみが送信されます。通知定義で定義された変数バインドのみが、linkUp 通知や linkDown 通知とともに送信されます。
- IEFT extended Cisco：インターフェイスに対して ifLinkUpDownTrapEnable（IF-MIB で定義）がイネーブルになっている場合、そのインターフェイスについて IF-MIB で定義された通知（LinkUp、LinkDown）および CISCO-IF-EXTENSION-MIB.my で定義された通知（cieLinkUp、cieLinkDown）のみが送信されます。linkUp と linkDown の通知定義で定義された変数バインドに加え、シスコの実装に固有の IF-MIB で定義された変数バインドも LinkUp 通知や LinkDown 通知とともに送信されます。

（注） For more information on the varbinds defined in the IF-MIB specific to the Cisco Systems implementation, refer to the *Cisco MDS 9000 Family MIB Quick Reference*.

## LinkUp および LinkDown トラップ設定の範囲

インターフェイスに対する LinkUp および LinkDown トラップ設定は、次の範囲に基づいてトラップを生成します。

| スイッチレベルのトラップ設定 | インターフェイスレベルのトラップ設定 | インターフェイス リンクについて生成されるトラップか? |
|---|---|---|
| 有効（デフォルト） | 有効（デフォルト） | Yes |
| イネーブル | 無効 | × |

| スイッチレベルのトラップ設定 | インターフェイスレベルのトラップ設定 | インターフェイス リンクについて生成されるトラップか? |
|---|---|---|
| 無効 | イネーブル | × |
| 無効 | ディセーブル | いいえ |

# デフォルト設定

表 34 : SNMP のデフォルト設定 （255 ページ） 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 *34 : SNMP* のデフォルト設定**

| パラメータ | デフォルト |
|---|---|
| ユーザアカウント | 有効期限なし（設定されていない場合） |
| パスワード | なし |

# SNMP の設定

SNMPは、ネットワーク デバイス間での管理情報の交換を容易にするアプリケーション層プロトコルです。

## SNMP スイッチの連絡先および場所の情報の割り当て

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

連絡先および場所の情報を設定するには、次の手順を実行します。

### 手順

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **snmp-server contact NewUser**

スイッチの連絡先名を割り当てます。

**ステップ 3** switch(config)# **no snmp-server contact NewUser**

スイッチの連絡先名を削除します。

**ステップ 4** switch(config)# **snmp-server location SanJose**

スイッチ ロケーションを割り当てます。

**ステップ 5** switch(config)# **no snmp-server location SanJose**

スイッチ ロケーションを削除します。

# CLI から SNMP ユーザーの設定

The passphrase specified in the **snmp-server user** command and the **username** command are synchronized.

（注） パスフレーズまたはパスワードが暗号化形式で**localizedkey**指定されている場合、パスワードは同期されません。If a configuration file is copied to the device, the passwords will not be set correctly if the configuration file was generated at a different device. 明示的に設定をデバイスにコピーした後、適切なパスワードを設定します。

作成または CLI からの SNMP ユーザの変更は、次の手順に従います。

**手順**

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **snmp-server user joe network-admin auth sha abcd1234**

作成または HMAC-SHA-96 認証パスワード (abcd1234) を使用してネットワーク管理者ロールで、ユーザ (joe) の設定を変更します。

**ステップ 3** switch(config)# **snmp-server user sam network-admin auth md5 abcdefgh**

作成または HMAC-MD5-96 認証パスワード (abcdefgh) を使用してネットワーク管理者ロールで、ユーザ (サム) の設定を変更します。

**ステップ 4** switch(config)# **snmp-server user Bill network-admin auth sha abcd1234 priv abcdefgh**

作成または HMAC-SHA-96 認証レベルとプライバシーの暗号化のパラメータを使用してネットワーク管理者ロールでユーザ (請求) の設定を変更します。

**ステップ 5** switch(config)# **no snmp-server user usernameA**

ユーザ (usernameA) と関連付けられているすべてのパラメータを削除します。

**ステップ 6** switch(config)# **no snmp-server usam role vsan-admin**

vsan-admin ロールから指定のユーザ（usam）を削除します。

**ステップ 7** switch(config)# **snmp-server user user1 network-admin auth md5 0xab0211gh priv 0x45abf342 localizedkey**

ローカライズ キー形式 (RFC 2574) にパスワードを指定します。ローカライズされたキーは 16 進形式 (たとえば、0xacbdef) で提供されます。

**ステップ 8** switch(config)# **snmp-server user user2 auth md5 asdgfsadf priv aes-128 asgfsgkhkj**

MD5 認証プロトコルと AES-128 プライバシー プロトコルを使用して user2 を設定します。

**ステップ 9** switch(config)# **snmp-server user joe sangroup**

指定したユーザ（joe）を sangroup ロールに追加します。

**ステップ 10** switch(config)# **snmp-server user joe techdocs**

指定したユーザ（joe）を techdocs ロールに追加します。

## パスワードの作成または変更

作成または CLI からの SNMP ユーザのパスワードの変更は、次の手順に従います。

### 手順

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **snmp-server user user1 role1 auth md5 0xab0211gh priv 0x45abf342 localizedkey**

セキュリティ暗号化 DES] オプションを使用してローカライズのキーの形式にパスワードを指定します。

**ステップ 3** switch(config)# **snmp-server user user1 role2 auth sha 0xab0211gh priv aes-128 0x45abf342 localizedkey**

128 ビット AES オプションを使用してセキュリティ暗号化キーの形式をローカライズにパスワードを指定します。

（注） The **snmp-server user** command takes the engineID as an additional parameter. EngineID 通知対象ユーザを作成する (を参照してください、 通知対象ユーザの設定 （266 ページ） )。EngineID が指定されていない場合、ローカル ユーザが作成されます。

# 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。

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。

### 手順

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **snmp-server user testUser enforcePriv**

このユーザを使用して、SNMPv3 メッセージのメッセージの暗号化が実現します。

（注） auth および priv の両方のキーが設定された既存のユーザに対してだけ、このコマンドを使用できます。NoAuthNoPriv または authNoPriv のいずれかの securityLevel パラメータを使用して SNMPv3 PDU 要求に対し、プライバシーを適用するユーザが設定されている場合は、authorizationError で SNMP エージェントが応答します。

**ステップ 3** switch(config)# **no snmp-server user testUser enforcePriv**

SNMPv3 メッセージ暗号化の強制を無効になります。

## SMNPv3 メッセージの暗号化をグローバルに適用

または、次のコマンドを使用して、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こともできます。

### 手順

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **snmp-server globalEnforcePriv**

スイッチ上のすべてのユーザの SNMPv3 メッセージ暗号化が実行されます。

**ステップ 3** switch(config)# **no snmp-server globalEnforcePriv**

グローバル SNMPv3 メッセージ暗号化の強制を無効になります。

# SNMPv3 ユーザに対する複数のロールの割り当て

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、network-admin ロールに属するユーザだけです。

CLI から SNMPv3 ユーザの複数のロールを設定するには、次の手順に従います。

**手順**

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **snmp-server user NewUser role1**

作成または、SNMPv3 ユーザ (移動) の: role1 ロールの設定を変更します。

**ステップ 3** switch(config)# **snmp-server user NewUser role2**

作成または、SNMPv3 ユーザ (移動) の role2 ロールの設定を変更します。

**ステップ 4** switch(config)# **no snmp-server user User5 role2**

指定されたユーザ (User5) の role2 を削除します。

# 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/書き込みアクセス権を設定できます。RFC 2576 を参照してください。

SNMPv1 または SNMPv2c のコミュニティを作成するには、次の手順を実行します。

**手順**

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **snmp-server community snmp_Community ro**

指定された SNMP コミュニティの読み取り専用アクセスを追加します。

**ステップ 3** switch(config)# **snmp-server community snmp_Community rw**

指定された SNMP コミュニティに読み込み/書き込みアクセス権を追加します。

**ステップ 4** switch(config)# **no snmp-server community snmp_Community**

指定された SNMP コミュニティ（デフォルト）のアクセス権を削除します。

# SNMP トラップとインフォーム通知の設定

特定のイベントが発生したときにSNMPマネージャに通知を送信するようにCisco MDS スイッチを設定できます。

（注） 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。SNMP の 11 番目のターゲット ホストを設定するときに、次のメッセージが表示されます。

```
switch(config)# snmp-server host 10.4.200.173 traps version 2c noauth
reached maximum allowed targets limit
```

- SNMP 設定で RMON トラップをイネーブルにする必要があります。詳細については、RMON の設定 （195 ページ）を参照してください。
- 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。

ヒント The SNMPv1 option is not available with the **snmp-server host** *p-address* **informs** command.

# SNMPv2c 通知の設定

## IPv4 を使用した SNMPv2c 通知の設定

IPv4 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。

**手順**

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **snmp-server host 171.71.187.101 traps version 2c private udp-port 1163**

SNMPv2c コミュニティ文字列（プライベート）を使用して、SNMPv2c トラップを受信するために指定されたホストを設定します。

**ステップ 3** switch(config)# **no snmp-server host 171.71.187.101 traps version 2c private udp-port 2162**

SNMPv2c コミュニティ文字列（プライベート）を使用して、指定されたホストが設定されている UDP ポートで SNMPv2c トラップを受信することを防止します。

**ステップ 4** switch(config)# **snmp-server host 171.71.187.101 informs version 2c private udp-port 1163**

SNMPv2c コミュニティ文字列（プライベート）を使用して、指定されたホストが SNMPv2c 通知を受信するように設定します。

**ステップ 5** switch(config)# **no snmp-server host 171.71.187.101 informs version 2c private udp-port 2162**

SNMPv2c コミュニティ文字列（プライベート）を使用して、指定されたホストが設定されている UDP ポートで SNMPv2c 通知を受信するように設定します。

## IPv6 を使用した SNMPv2c 通知の設定

IPv6 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。

### 手順

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **snmp-server host 2001:0DB8:800:200C::417A traps version 2c private udp-port 1163**

SNMPv2c コミュニティ文字列（プライベート）を使用して、SNMPv2c トラップを受信するために指定されたホストを設定します。

**ステップ 3** switch(config)# **no snmp-server host 2001:0DB8:800:200C::417A traps version 2c private udp-port 2162**

SNMPv2c コミュニティ文字列（プライベート）を使用して、指定されたホストが設定されている UDP ポートで SNMPv2c トラップを受信することを防止します。

**ステップ 4** switch(config)# **snmp-server host 2001:0DB8:800:200C::417A informs version 2c private udp-port 1163**

SNMPv2c コミュニティ文字列（プライベート）を使用して、指定されたホストが SNMPv2c 通知を受信するように設定します。

**ステップ 5** switch(config)# **no snmp-server host 2001:0DB8:800:200C::417A informs version 2c private udp-port 2162**

SNMPv2c コミュニティ文字列（プライベート）を使用して、指定されたホストが設定されている UDP ポートで SNMPv2c 通知を受信するように設定します。

## DNS 名を使用した SNMPv2c 通知の設定

SNMP 通知ホスト myhost.cisco.com の DNS 名を使用して SNMPv2c 通知を設定するには、次の手順に従います。

### 手順

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **snmp-server host myhost.cisco.com traps version 2c private udp-port 1163**

SNMPv2c コミュニティ文字列（プライベート）を使用して、SNMPv2c トラップを受信するために指定されたホストを設定します。

**ステップ 3** switch(config)# **no snmp-server host myhost.cisco.com traps version 2c private udp-port 2162**

SNMPv2c コミュニティ文字列（プライベート）を使用して、指定されたホストが設定されている UDP ポートで SNMPv2c トラップを受信することを防止します。

**ステップ 4** switch(config)# **snmp-server host myhost.cisco.com informs version 2c private udp-port 1163**

SNMPv2c コミュニティ文字列（プライベート）を使用して、指定されたホストが SNMPv2c 通知を受信するように設定します。

**ステップ 5** switch(config)# **no snmp-server host myhost.cisco.com informs version 2c private udp-port 2162**

SNMPv2c コミュニティ文字列（プライベート）を使用して、指定されたホストが設定されている UDP ポートで SNMPv2c 通知を受信するように設定します。

（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

## IPv4 を使用して、SNMPv3 通知の設定

To configure SNMPv3 notifications using IPv4, follow these steps:

手順

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **snmp-server host 16.20.11.14 traps version 3 noauth testuser udp-port 1163**

SNMPv3 ユーザ (testuser) および noAuthNoPriv の securityLevel を使用して SNMPv3 トラップを受信するために指定されたホストを設定します。

**ステップ 3** switch(config)# **snmp-server host 16.20.11.14 informs version 3 auth testuser udp-port 1163**

設定の指定された SNMPv3 ユーザ (testuser) および AuthNoPriv の securityLevel を使用して SNMPv3 を受信するホストに通知します。

**ステップ 4** switch(config)# **snmp-server host 16.20.11.14 informs version 3 priv testuser udp-port 1163**

設定の指定された SNMPv3 ユーザ (testuser) および AuthPriv の securityLevel を使用して SNMPv3 を受信するホストに通知します。

**ステップ 5** switch(config)# **no snmp-server host 172.18.2.247 informs version 3 testuser noauth udp-port 2162**

SNMPv3 に通知を受信から指定されたホストを防止します。

## IPv6 を使用した SNMPv3 通知の設定

IPv6 を使用して SNMPv3 通知を設定するには、次の手順を実行します。

手順

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **snmp-server host 2001:0DB8:800:200C::417A traps version 3 noauth testuser udp-port 1163**

SNMPv3 ユーザ (testuser) および noAuthNoPriv の securityLevel を使用して SNMPv3 トラップを受信するために指定されたホストを設定します。

**ステップ 3** switch(config)# **snmp-server host 2001:0DB8:800:200C::417A informs version 3 auth testuser udp-port 1163**

設定の指定された SNMPv3 ユーザ (testuser) および AuthNoPriv の securityLevel を使用して SNMPv3 を受信するホストに通知します。

**ステップ 4** switch(config)# **snmp-server host 2001:0DB8:800:200C::417A informs version 3 priv testuser udp-port 1163**

設定の指定された SNMPv3 ユーザ (testuser) および AuthPriv の securityLevel を使用して SNMPv3 を受信するホストに通知します。

**ステップ 5** switch(config)# **no snmp-server host 2001:0DB8:800:200C::417A informs version 3 testuser noauth udp-port 2162**

SNMPv3 に通知を受信から指定されたホストを防止します。

## DNS 名を使用した SNMPv3 通知の設定

SNMP 通知ホスト myhost.cisco.com の DNS 名を使用して SNMPv3 通知を設定するには、次の手順に従います。

### 手順

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **snmp-server host myhost.cisco.com traps version 3 noauth testuser udp-port 1163**

SNMPv3 ユーザ (testuser) および noAuthNoPriv の securityLevel を使用して SNMPv3 トラップを受信するために指定されたホストを設定します。

**ステップ 3** switch(config)# **snmp-server host myhost.cisco.com informs version 3 auth testuser udp-port 1163**

設定の指定された SNMPv3 ユーザ (testuser) および AuthNoPriv の securityLevel を使用して SNMPv3 を受信するホストに通知します。

**ステップ 4** switch(config)# **snmp-server host myhost.cisco.com informs version 3 priv testuser udp-port 1163**

設定の指定された SNMPv3 ユーザ (testuser) および AuthPriv の securityLevel を使用して SNMPv3 を受信するホストに通知します。

**ステップ 5** switch(config)# **no snmp-server host myhost.cisco.com informs version 3 testuser noauth udp-port 2162**

SNMPv3 に通知を受信から指定されたホストを防止します。

# SNMP 通知のイネーブル化

表 35 : SNMP 通知のイネーブル化 （265 ページ） lists the CLI commands that enable the notifications for Cisco NX-OS MIBs.

表 *35 : SNMP* 通知のイネーブル化

| MIB | DCNM-SAN チェックボックス |
|---|---|
| CISCO-ENTITY-FRU-CONTROL-MIB | **Click the Other tab and check FRU Changes.** |
| CISCO-FCC-MIB | **Click the Other tab and check FCC.** |
| CISCO-DM-MIB | **Click the FC tab and check Domain Mgr RCF.** |
| CISCO-NS-MIB | **Click the FC tab and check Name Server.** |
| CISCO-FCS-MIB | **Click the Other tab and check FCS Rejects.** |
| CISCO-FDMI-MIB | **Click the Other tab and check FDMI.** |
| CISCO-FSPF-MIB | **Click the FC tab and check FSPF Neighbor Change.** |
| CISCO-LICENSE-MGR-MIB | **Click the Other tab and check License Manager.** |
| CISCO-IPSEC-SIGNALLING-MIB | **Click the Other tab and check IPSEC.** |
| CISCO-PSM-MIB | **Click the Other tab and check Port Security.** |
| CISCO-RSCN-MIB | **Click the FC tab and check RSCN ILS, and RCSN ELS.** |
| SNMPv2-MIB | **Click the Other tab and check SNMP AuthFailure.** |
| VRRP-MIB, CISCO-IETF-VRRP-MIB | **Click the Other tab and check VRRP.** |
| CISCO-ZS-MIB | **Click the FC tab and check Zone Rejects, Zone Merge Failures, Zone Merge Successes, Zone Default Policy Change, and Zone Unsuppd Mode.** |

次の通知はデフォルトでイネーブルになっています。

- entity fru
- license
- link ietf-extended

他の通知はすべて、デフォルトではディセーブルです。

有効化または次のレベルでサポートされるトラップを無効にすることができます。

- スイッチのレベル: スイッチのレベルでサポートされている Mib 内のすべてのトラップを有効にする snmp サーバ有効にするトラップのコマンドを使用することができます。
- レベルの機能:機能レベルでトラップを有効にする機能名でsnmpサーバ有効にするトラップのコマンドを使用できます。

```
switch =>snmp-server enable traps callhome ?
event-notify    Callhome External Event Notification
smtp-send-fail  SMTP Message Send Fail notification
```

- 個々 のトラップ、snmp サーバ enable トラップ コマンドは個々 のレベルでトラップを有効にするのに機能名で使用できます。

```
switch =>snmp-server enable traps callhome event-notify ?
```

（注） The snmp-server enable traps CLI command enables both traps and informs, depending on how you configured SNMP. Snmp サーバ ホストの CLI コマンドで表示される通知を参照してください。

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。

**手順**

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **snmp-server enable traps fcdomain**

指定された SNMP (fcdomain) 通知を有効にします。

**ステップ 3** switch(config)# **no snmp-server enable traps**

指定した SNMP 通知をディセーブルにします。通知名を指定しないと、すべての通知がディセーブルになります。

# 通知対象ユーザの設定

SNMPv3 インフォーム通知を SNMP マネージャに送信するには、スイッチ上で通知対象ユーザを設定する必要があります。

SNMP マネージャは、受信した INFORM PDU を認証および復号化するために、同じユーザ資格情報をユーザのローカル設定データ ストアに持っている必要があります。

通知相手ユーザーを設定するには、次のコマンドを使用します。

**手順**

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **snmp-server user testusr auth md5 xyub20gh priv xyub20gh engineID 00:00:00:63:00:01:00:a1:ac:15:10:03**

指定のエンジン ID で、SNMP マネージャに対して指定のクレデンシャルを持つ通知相手ユーザーを設定します。

**ステップ 3** switch(config)# **no snmp-server user testusr auth md5 xyub20gh priv xyub20gh engineID 00:00:00:63:00:01:00:a1:ac:15:10:03**

通知相手ユーザーを削除します。

The credentials of the notification target user are used for encrypting the SNMPv3 inform notification messages to the configured SNMPmanager (as in the **snmp-server host** command).

# スイッチの LinkUp/LinkDown 通知の設定

NX-OS リリース 4.1(x) 以前のバージョンを使用してスイッチの LinkUp/LinkDown 通知を設定するには、次の手順に従います。

**手順**

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **snmp-server enable traps link**

IETF 拡張 LinkUp/LinkDown 通知のみを有効にします（デフォルト）。

**ステップ 3** switch(config)# **snmp-server enable traps link cisco**

Cisco Systems 定義の通知を有効にします。

**ステップ 4** switch(config)# **snmp-server enable traps link ietf**

IETF LinkUp/LinkDown 通知のみ有効にします。

**ステップ 5** switch(config)# **snmp-server enable traps link ietf-extended**

追加の変数バインドを持つ IETF 拡張 LinkUp/LinkDown 通知のみを有効にします（デフォルト）。

**ステップ 6** switch(config)# **snmp-server enable traps link ietf cisco**

IETF（リンクアップ/リンクダウン）および Cisco Systems 定義（cieLinkUp/cieLinkDown）の通知を有効にします。

**ステップ 7** switch(config)# **snmp-server enable traps link ietf-extended cisco**

追加の変数と Cisco Systems 定義（cieLinkUp/cieLinkDown）の通知とともに、IEFT（LinkUp/LinkDown）の通知を有効にします。

**ステップ 8** switch(config)# **no snmp-server enable traps link**

デフォルト設定に戻します（IETF 拡張）。

（注） IETF および IETF 拡張の両方が有効になっている場合、show snmp traps コマンドにより有効な状態で両方とも表示します。ただし、トラップとして IETF 拡張ペイロードで 1 個のトラップのみ受信します。

# スイッチの LinkUp/LinkDown 通知の設定

NX-OS Release 4.2(1) 以降を使用してスイッチの LinkUp/LinkDown 通知を設定するには、次の手順に従います。

**手順**

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **snmp-server enable traps link extended-link**

IETF 拡張 linkUp 通知を有効にします。

**ステップ 3** switch(config)# **snmp-server enable traps link extended-linkDown**

IETF 拡張 linkDown 通知を有効にします。

**ステップ 4** switch(config)# **snmp-server enable traps link cieLinkDown**

Cisco 拡張リンク状態ダウン通知を有効にします。

**ステップ 5** switch(config)# **snmp-server enable traps link cieLinkUp**

Cisco 拡張リンク状態アップ通知を有効にします。

**ステップ 6** switch(config)# **snmp-server enable traps link connUnitPortStatusChange**

FCMGMT 接続性ユニット通知の全体ステータスを有効にします。

**ステップ 7** switch(config)# **snmp-server enable traps link delayed-link-state-change**

遅延リンク状態の変更を有効にします。

遅延リンク状態トラップを無効にしてデバイスがポートダウンSNMPアラートをすぐに生成できるようにします。

- NX OS **no system delayed-traps enable mode FX** バージョン 6.2 (5) またはそれ以降では、コマンドを使用します。
- NX OS **no snmp-server enable traps link delayed-link-state-change**バージョン 6.2 (7) 以降では、コマンドを使用します。

（注） 特定の NX-OS リリース バージョン間のアップグレードについて、遅延リンク状態トラップが無効になっていることを確認します。When migrating from an earlier release like 5.(x) or 6.1(x) or 6.2(x) to a release 6.2(7) and above, ensure that you explicitly disable the delayed link state traps using **no snmp-server enable traps link delayed-link-state-change** command.

**ステップ 8** switch(config)# **snmp-server enable traps link extended-linkDown**

IETF 拡張リンク ステート ダウン通知を有効にします。

**ステップ 9** switch(config)# **snmp-server enable traps link extended-linkUp**

IETF 拡張リンク ステート ダウン通知を有効にします。

**ステップ 10** switch(config)# **snmp-server enable traps link fcTrunkIfDownNotify**

FCFE リンク状態のダウン通知を有効にします。

**ステップ 11** switch(config)# **snmp-server enable traps link fcTrunkIfUpNotify**

FCFE リンク状態のアップ通知を有効にします。

**ステップ 12** switch(config)# **snmp-server enable traps link fcot-inserted**

FCOT 情報トラップを有効にします。

**ステップ 13** switch(config)# **snmp-server enable traps link fcot-removed**

FCOT 情報トラップを有効にします。

**ステップ 14** switch(config)# **snmp-server enable traps link linkDown**

IETF リンク状態ダウン通知を有効にします。

**ステップ 15** switch(config)# **snmp-server enable traps link linkUp**

IETF リンク状態アップ通知を有効にします。

**ステップ 16** switch(config)# **no snmp-server enable traps link**

デフォルト設定に戻します（IETF 拡張）。

# インターフェイスの Up/Down SNMP リンクステート トラップの設定

デフォルトでは、SNMP リンクステート トラップがすべてのインターフェイスに対してイネーブルになっています。リンクの状態が Up と Down の間で切り替わるたびに、SNMP トラップが生成されます。

何百ものインターフェイスを装備したスイッチが多数存在し、それらの多くでリンクの状態をモニタする必要がない場合があります。そのような場合には、リンクステート トラップをディセーブルにすることも選択できます。

特定のインターフェイスの SNMP リンク状態トラップを無効にするには、次の手順に従います。

**手順**

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **interface bay 6**

SNMP リンク状態トラップを無効にするインターフェイスを指定します。

**ステップ 3** switch(config-if)# **no link-state-trap**

インターフェイスの SNMP リンクステート トラップをディセーブルにします。

**ステップ 4** switch(config-if)# **link-state-trap**

インターフェイスの SNMP リンク状態トラップを有効にします。

# エンティティ トラップ（FRU）の設定

個々 の SNMP トラップ制御を有効にするには、次の手順を実行します。

**手順**

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** **switch(config)# snmp-server enable traps entity**

個々の SNMP トラップ制御を有効にします。

**ステップ 3** **switch(config)# snmp-server enable entity_fan_status_change**

エンティティ ファン ステータスの変更を有効にします。

**ステップ 4** **switch(config)# snmp-server enable entity_mib_change**

エンティティ MIB の変更を有効にします。

**ステップ 5** **switch(config)# snmp-server enable entity_module_inserted**

挿入するエンティティ モジュールを有効にします。

**ステップ 6** **switch(config)# snmp-server enable entity_module_removed**

削除するエンティティ モジュールを有効にします。

**ステップ 7** **switch(config)# snmp-server enable entity_module_status_change**

エンティティ モジュール ステータスの変更を有効にします。

**ステップ 8** **switch(config)# snmp-server enable entity_power_out_change**

エンティティの電源変更を有効にします。

**ステップ 9** **switch(config)# snmp-server enable entity_power_status_change**

エンティティ電源の状態変更を有効にします。

**ステップ 10** **switch(config)# snmp-server enable entity_unrecognised_module**

エンティティの認識されていないモジュールを有効にします。

（注） これらすべてのトラップは、レガシー FRU トラップを行う必要があります。

# SNMP の設定の確認

SNMP のコンフィギュレーション情報を表示するには、次の作業のいずれかを行います。

| コマンド | 目的 |
|---|---|
| **show running-config** | Displays the running configuration |
| **show interface** | 特定のインターフェイスの SNMP リンクステート トラップ設定を表示します。 |
| **show snmp trap** | すべての通知とそのステータスを表示します。 |
| **show snmp** | 表示には、SNMP 情報、SNMP 連絡先、ロケーション、およびパケットの設定についてのカウンタが設定されています。 |

For detailed information about the fields in the output from these commands, refer to the *Cisco MDS 9000 Family Command Reference* .

# インターフェイスの Up/Down SNMP リンク状態トラップの設定

インターフェイスの SNMP リンク状態トラップを無効にするたびに、コマンドもシステムの実行設定に追加されます。

To view the running configuration, use the **show running-config** command for the interface.

```
switch# show running-config
version 3.1(2)
....
interface bay5
interface bay6
  no link-state-trap <-----command is added to the running configuration for the interface
```

```
interface bay7...
```

To view the SNMP link-state trap configuration for a particular interface, enter the **show interface** command.

```
switch# show interface bay 6
bay6 is down (Administratively down)
    Hardware is Fibre Channel
    Port WWN is 20:0b:00:05:30:01:70:2c
    Admin port mode is auto, trunk mode is on
    snmp link-state traps are disabled
Port vsan is 1
    Receive data field Size is 2112
    Beacon is turned off
    5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
      0 frames input, 0 bytes
        0 discards, 0 errors
        0 CRC,  0 unknown class
        0 too long, 0 too short
      0 frames output, 0 bytes
        0 discards, 0 errors
      0 input OLS, 0 LRR, 0 NOS, 0 loop inits
      0 output OLS, 0 LRR, 0 NOS, 0 loop inits
```

# SNMP トラップの表示

You can use the **show snmp trap** command to display all the notifications and their status.

```
switch# show snmp trap
--------------------------------------------------------------------------------
Trap type                                                              Enabled
--------------------------------------------------------------------------------
entity               : entity_mib_change                               Yes
entity               : entity_module_status_change                     Yes
entity               : entity_power_status_change                      Yes
entity               : entity_module_inserted                          Yes
entity               : entity_module_removed                           Yes
entity               : entity_unrecognised_module                      Yes
entity               : entity_fan_status_change                        Yes
entity               : entity_power_out_change                         Yes
link                 : linkDown                                        Yes
link                 : linkUp                                          Yes
link                 : extended-linkDown                               Yes
link                 : extended-linkUp                                 Yes
link                 : cieLinkDown                                     Yes
link                 : cieLinkUp                                       Yes
link                 : connUnitPortStatusChange                        Yes
link                 : fcTrunkIfUpNotify                               Yes
link                 : fcTrunkIfDownNotify                             Yes
link                 : delayed-link-state-change                       Yes
link                 : fcot-inserted                                   Yes
link                 : fcot-removed                                    Yes
callhome             : event-notify                                    No
callhome             : smtp-send-fail                                  No
cfs                  : state-change-notif                              No
cfs                  : merge-failure                                   No
fcdomain             : dmNewPrincipalSwitchNotify                      No
fcdomain             : dmDomainIdNotAssignedNotify                     No
fcdomain             : dmFabricChangeNotify                            No
```

```
rf                   : redundancy_framework                        Yes
aaa                  : server-state-change                         No
license              : notify-license-expiry                       Yes
license              : notify-no-license-for-feature               Yes
license              : notify-licensefile-missing                  Yes
license              : notify-license-expiry-warning               Yes
scsi                 : scsi-disc-complete                          No
fcns                 : reject-reg-req                              No
fcns                 : local-entry-change                          No
fcns                 : db-full                                     No
fcns                 : remote-entry-change                         No
rscn                 : rscnElsRejectReqNotify                      No
rscn                 : rscnIlsRejectReqNotify                      No
rscn                 : rscnElsRxRejectReqNotify                    No
rscn                 : rscnIlsRxRejectReqNotify                    No
fcs                  : request-reject                              No
fcs                  : discovery-complete                          No
fctrace              : route                                       No
zone                 : request-reject1                             No
zone                 : merge-success                               No
zone                 : merge-failure                               No
zone                 : default-zone-behavior-change                No
zone                 : unsupp-mem                                  No
port-security        : fport-violation                             No
port-security        : eport-violation                             No
port-security        : fabric-binding-violation                    No
vni                  : virtual-interface-created                   No
vni                  : virtual-interface-removed                   No
vsan                 : vsanStatusChange                            No
vsan                 : vsanPortMembershipChange                    No
fspf                 : fspfNbrStateChangeNotify                    No
upgrade              : UpgradeOpNotifyOnCompletion                 No
upgrade              : UpgradeJobStatusNotify                      No
feature-control      : FeatureOpStatusChange                       No
vrrp                 : cVrrpNotificationNewMaster                  No
fdmi                 : cfdmiRejectRegNotify                        No
snmp                 : authentication                              No
```

# SNMP セキュリティ情報の表示

Use the **show snmp** commands to display configured SNMP information (see the following examples):

### SNMP ユーザー詳細

次の例の SNMPユーザー詳細：

```
switch# show snmp user
_____________________________________________________________________
                   SNMP USERS
_____________________________________________________________________
User                            Auth  Priv(enforce) Groups
____                            ____  _____________ ______
admin                           md5   des(no)       network-admin
testusr                         md5   aes-128(no)   role111
                                                    role222
_____________________________________________________________________
 NOTIFICATION TARGET USERS (configured  for sending V3 Inform)
_____________________________________________________________________
User                            Auth  Priv
____                            ____  ____
```

```
testtargetusr                 md5   des
(EngineID 0:0:0:63:0:1:0:0:0:15:10:3)
```

### SNMP コミュニティ情報

次の例では、SNMP コミュニティ情報を示します。

```
switch# show snmp community

Community             Group / Access      context
_________             ______________      _______
dcnm_user             network-admin
admin                 network-admin
```

### SNMP ホスト情報

次の例では、SNMP ホスト情報を示します。

```
switch# show snmp host
Host                            Port Version  Level  Type   SecName
____                            ____ _______  ______ ____  _______
171.16.126.34                   2162 v2c      noauth trap   public
171.16.75.106                   2162 v2c      noauth trap   public
...
171.31.58.97                    2162 v2c      auth   trap   public
...
```

The **show snmp** command displays counter information for SNMP contact, location, and packet settings. このコマンドは、Cisco MDS 9000 ファミリ DCNM-SAN 全体で使用されている情報を提供します（システム管理設定ガイド、SAN の Cisco DCNM を参照）。次の例を参照してください。

### SNMP 情報

次の例では、SNMP 情報を示します。

```
switch# show snmp
sys contact:
sys location:
1631 SNMP packets input
        0 Bad SNMP versions
        0 Unknown community name
        0 Illegal operation for community name supplied
        0 Encoding errors
        64294 Number of requested variables
        1 Number of altered variables
        1628 Get-request PDUs
        0 Get-next PDUs
        1 Set-request PDUs
152725 SNMP packets output
        0 Too big errors
        1 No such name errors
        0 Bad values errors
        0 General errors
```

```
Community                      Group / Access
---------                      ------
public                          rw

_____________________________________________________________________
                  SNMP USERS
_____________________________________________________________________
User                           Auth  Priv(enforce) Groups
____                           ____  _____________ ______
admin                          md5   des(no)       network-admin
testusr                        md5   aes-128(no)   role111
                                                   role222

_____________________________________________________________________
 NOTIFICATION TARGET USERS (configured  for sending V3 Inform)
_____________________________________________________________________
User                           Auth  Priv
____                           ____  ____
testtargetusr                  md5   des
(EngineID 0:0:0:63:0:1:0:0:0:15:10:3)
```

### SNMP エンジン ID の表示

次の例では、SNMP エンジン ID を示します。

```
switch# show snmp engineID
Local SNMP engineID: [Hex] 8000000903000DEC2CF180
                     [Dec] 128:000:000:009:003:000:013:236:044:241:128
```

### SNMP セキュリティ グループの情報

次の例では、SNMP セキュリティ グループの情報を示します。

```
switch# show snmp group
groupname: network-admin
security model: any
security level: noAuthNoPriv
readview: network-admin-rd
writeview: network-admin-wr
notifyview: network-admin-rd
storage-type: permanent
row status: active
groupname: network-admin
security model: any
security level: authNoPriv
readview: network-admin-rd
writeview: network-admin-wr
notifyview: network-admin-rd
storage-type: permanent
row status: active
groupname: network-operator
security model: any
security level: noAuthNoPriv
readview: network-operator-rd
writeview: network-operator-wr
notifyview: network-operator-rd
storage-type: permanent
row status: active
groupname: network-operator
security model: any
```

```
security level: authNoPriv
readview: network-operator-rd
writeview: network-operator-wr
notifyview: network-operator-rd
storage-type: permanent
row status: active
```

# その他の参考資料

SNMP の実装に関する詳細情報については、次の各項を参照してください。

### MIB

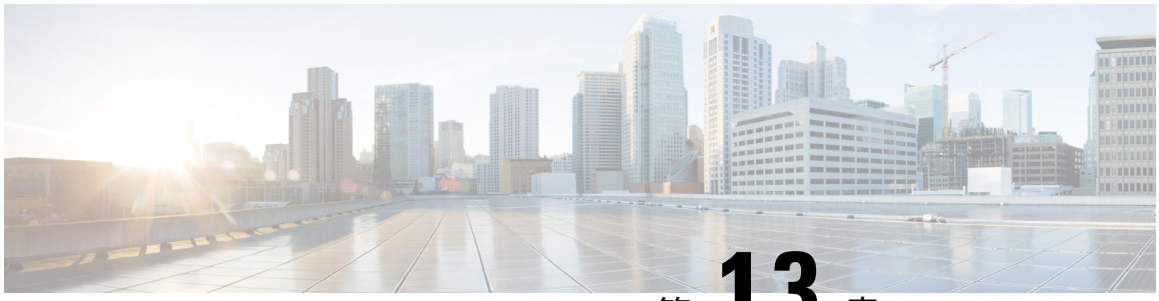
| MIB | MIB のリンク |
|---|---|
| • CISCO-SNMP-TARGET-EXT-MIB<br>• CISCO-SNMP-VACM-EXT-MIB | MIB を検索およびダウンロードするには、次の URL にアクセスしてください。<br>http://www.cisco.com/en/US/products/ps5989/prod_technical_reference_list.html |

# SNMP の機能の履歴

表 36 : SNMP の機能の履歴 （276 ページ） に、この機能のリリース履歴を示します。リリース 3.x 以降のリリースで導入または変更された機能のみが表に記載されています。

**表 *36 : SNMP* の機能の履歴**

| 機能名 | リリース | 機能情報 |
|---|---|---|
| 中央インフラ SNMP 機能 | 4.2(1) | 新しい中央インフラ SNMP 機能詳細を追加します。 |
| CLI から SNMP ユーザーの設定 | 3.3(1a) | 作成または CLI からの SNMP ユーザのパスワードを変更するために、コマンド switch (config) # snmp サーバ user user1: role1 auth md5 0xab0211gh priv 0x45abf342 localizedkey でから des を削除します。 |



第 13 章

# ドメイン パラメータの設定

ファイバ チャネル ドメイン（fcdomain）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。



## ファイバ チャネル ドメインについて

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

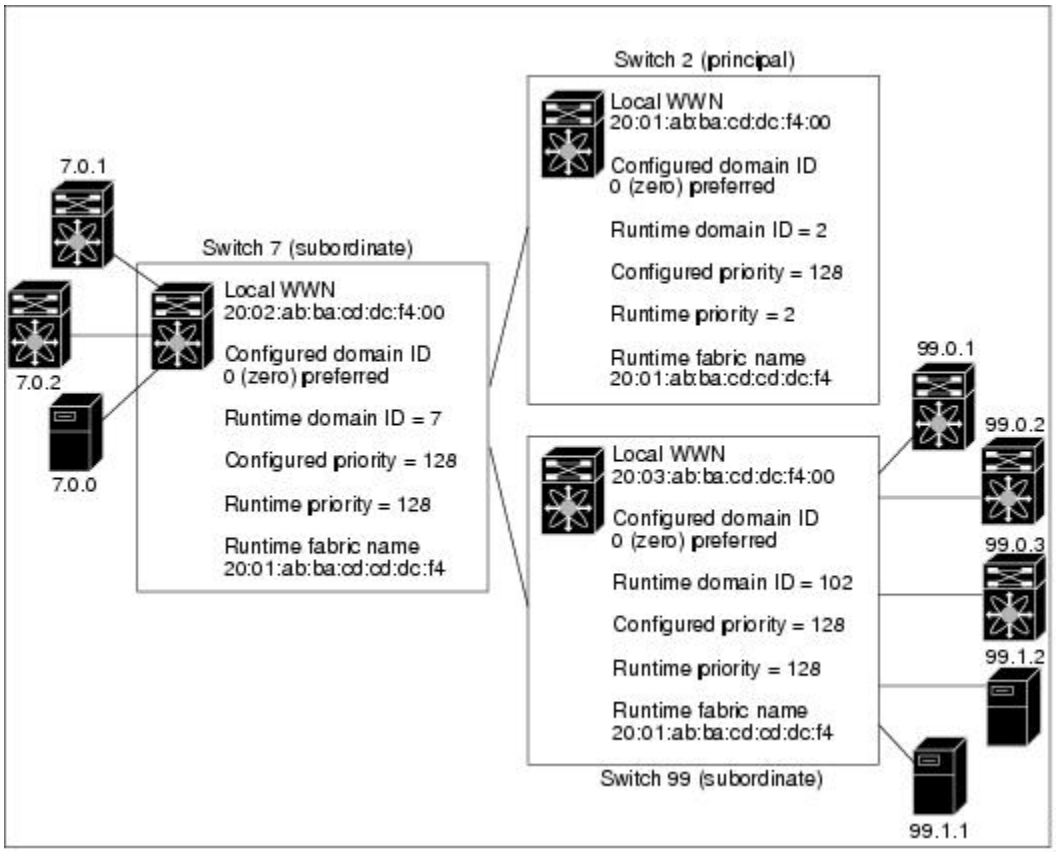
ここでは、fcdomain の各フェーズについて説明します。

- 主要スイッチの選択：このフェーズでは、ファブリック内で一意の主要スイッチを選択できます。
- ドメイン ID の配信：このフェーズでは、ファブリック内のスイッチごとに、一意のドメイン ID を取得できます。
- FC ID の割り当て：このフェーズでは、ファブリック内の対応するスイッチに接続された各デバイスに、一意の FC ID を割り当てることができます。
- ファブリックの再設定：このフェーズでは、ファブリック内のすべてのスイッチを再同期化して、新しい主要スイッチ選択フェーズを同時に再開できるようにします。

**注意** fcdomain パラメータは、通常変更しないでください。これらの変更は、管理者が行うか、スイッチ操作を熟知している人が行ってください。

図 12 : fcdomain の設定例 （278 ページ） に fcdomain の設定例を示します。

**図 *12 : fcdomain* の設定例**




# ドメインの再起動

ファイバ チャネル ドメインは、中断を伴う方法または中断を伴わない方法で起動できます。中断再起動を実行した場合は、Reconfigure Fabric（RCF）フレームがファブリック内のその他のスイッチに送信され、VSAN（リモートでセグメント化された ISL を含む）内のすべてのスイッチでデータ トラフィックは中断されます。非中断再起動を実行した場合は、Build Fabric（BF）フレームがファブリック内のその他のスイッチに送信され、該当スイッチでだけデータ トラフィックは中断されます。

ドメイン ID の競合を解消するには、手動でドメイン ID を割り当てる必要があります。ドメイン ID を手動で割り当てるなど、ほとんどの設定変更では中断再起動が必要になります。ドメインの非中断再起動は、優先ドメイン ID をスタティック ドメイン ID（実ドメイン ID は変更なし）に変更する場合にかぎり実行できます。

（注） 通常の再起動は問題を解決していないときにリカバリの目的のみに使用されるため、VSAN を中断/継続するのに従い、悪影響を及ぼす再起動を使用することは推奨されません。

（注） スタティック ドメインはユーザによって固有に設定されるため、実行時のドメインと異なることがあります。ドメイン ID が異なる場合は、次回の中断または非中断再起動後にスタティック ドメイン ID を使用するように、実行時のドメイン ID が変更されます。

ヒント VSAN が INTEROP モードである場合は、その VSAN の fcdomain で中断を伴う再起動を実行できません。

ほとんどの設定は、対応する実行時の値に適用できます。ここでは、実行時の値に fcdomain パラメータを適用する方法について詳細に説明します。

The **fcdomain restart** command applies your changes to the runtime settings. Use the **disruptive** option to apply most of the configurations to their corresponding runtime values, including preferred domain IDs (see the ドメイン ID （281 ページ）).

# ドメイン マネージャの全最適化

ドメインマネージャの全最適化機能は、最適化モードのすべてを有効または無効にするために使用できます。

（注） Interop モードが有効になっている（非ネイティブ モード） VSAN では、選択対象再起動、高速再起動、スケール再起動など、すべての最適化を有効にすることはできません。また、最適化が Interop モード 1 ～ 4.で有効になっている VSAN を移動することはできません。

# ドメイン マネージャの高速再起動

Cisco MDS SAN-OS Release 3.0(2) からは、主要リンクに障害が発生したときに、ドメイン マネージャが新しい主要リンクを選択する必要があります。デフォルトでは、ドメイン マネージャは Build Fabric フェーズを開始し、その後主要スイッチ選択フェーズが続きます。これらのフェーズは両方とも VSAN 内のすべてのスイッチに影響を及ぼし、完了するまで合計 15 秒以上かかります。ドメインマネージャが新しい主要リンクの選択に必要な時間を短縮するために、ドメイン マネージャの高速再起動機能をイネーブルにできます。

高速再起動がイネーブルで、バックアップ リンクを利用できる場合、ドメイン マネージャはわずか数ミリ秒で新しい主要リンクを選択し、障害が発生したリンクを交換します。また、新しい主要リンクの選択に必要な再設定は、VSAN 全体ではなく、障害が発生したリンクに直接

接続した2つのスイッチにだけ影響します。バックアップ リンクが利用できない場合、ドメイン マネージャはデフォルトの動作に戻り、ビルド ファブリック フェーズを開始します。その後、主要スイッチ選択フェーズが続きます。大部分のファブリックでは、特に多数の論理ポート（3200 以上）を使用する場合、高速再起動を使用することを推奨します。論理ポートは VSAN の物理ポートのインスタンスであるためです。

# ドメイン マネージャ スケールの再起動

ファブリックの再設定時とプリンシパル スイッチがドメイン ID をスイッチ（それ自体を含む）に割り当てるとき、Exchange Fabric Parameter（EFP）を送信します。この要求は、基本的にファブリックのドメイン リスト情報を送信します。そのため、ドメイン リストが成長するたび、ファブリックに Exchange Fabric Parameter がフラッディングされます。この機能の最適化が有効になっている状態で、単一の統合 Exchange Fabric Parameter 要求は、ドメイン識別子割り当て段階が完了すると、プリンシパル スイッチによってフラッディングされます。相互運用モードでは、この機能の最適化をサポートすることはできません。

すべてのネイティブVSANでスケール再起動がデフォルトで有効になります。相互運用VSANでは有効になりません。

# ドメイン マネージャの選択対象再起動

ファイバ チャネルのプロトコルで、ファブリック再設定はビルド ファブリック フレーム フラッディングから開始し、これはファブリックが変更されるファブリックのすべてのスイッチを示しています。このプロセスは、主要なスイッチの選択およびドメインIDの割り当てフェーズの後に行います。ビルド ファブリックのフラッディング フェーズ中に、すべてのリンクのビルド ファブリック フレームがフラッディングされます。スイッチには、ピア スイッチへの複数のリンクがあります。このような場合は、ピア スイッチへのリンクの 1 つだけにビルド ファブリック フレームを送信できます。この状況では、ファブリック再設定のビルド ファブリック フェーズ中に、ビルド ファブリック フレームの数を減らします。この機能の最適化を有効にすると、スケーリングのメリットがあるピア スイッチ リンクの1つのみにビルドフレームを送信します。

# Switch Priority

新しいスイッチは、安定したファブリックに参加する場合、主要スイッチになることがあります。主要スイッチ選択フェーズ中に、最高のプライオリティを持つスイッチが主要スイッチになります。2 つのスイッチに同じプライオリティが設定されている場合は、WWN が小さいスイッチが主要スイッチになります。

プライオリティ設定は、fcdomain の再起動の実行時に適用されます（ドメインの再起動 （278 ページ）を参照）。この設定は、中断再起動および非中断再起動のどちらにも適用できます。

# fcdomain の開始

デフォルトでは、fcdomain 機能は各スイッチ上でイネーブルになっています。スイッチ内で fcdomain 機能をディセーブルにすると、そのスイッチはファブリック内のその他のスイッチと共存できなくなります。fcdomain 設定は中断再起動の実行時に適用されます。

# 着信 RCF

インターフェイス単位、VSAN 単位で RCF 要求フレームを拒否するように選択できます。RCF 拒否オプションはデフォルトでディセーブルになっています（つまり、RCF 要求フレームは自動的に拒否されません）。

RCF 拒否オプションは、中断を伴う再起動によって、実行時にすぐに有効になります（ドメインの再起動 （278 ページ） を参照）。

rcf-reject オプションはインターフェイス単位、VSAN 単位で設定できます。デフォルトでは、rcf-reject オプションはディセーブルです（つまり、RCF 要求フレームは自動的に拒否されません）。

rcf-reject オプションは即座に有効になります。fcdomain の再起動は不要です。

# マージされたファブリックの自動再構成

デフォルトでは、autoreconfigure オプションはディセーブルです。ドメインが重なる別々の安定ファブリックに属する 2 つのスイッチを結合する場合は、次のような状況になる可能性があります。

- 両方のスイッチで autoreconfigure オプションがイネーブルの場合、中断再設定フェーズが開始します。
- いずれかまたは両方のスイッチで autoreconfigure オプションがディセーブルの場合は、2 つのスイッチ間のリンクが隔離されます。
- ファブリック全体で自動再設定が有効になっている場合にのみ、RCF が必要です。

autoreconfigure オプションは実行時に即座に有効になります。fcdomain を再起動する必要はありません。ドメインが重複によって現在隔離されており、後で両方のスイッチの autoreconfigure オプションをイネーブルにする場合は、ファブリックは隔離状態のままです。ファブリックを接続する前に両方のスイッチで autoreconfigure オプションをイネーブルにした場合、中断再設定（RCF）が発生します。中断再設定が発生すると、データ トラフィックが影響を受けることがあります。fcdomain に非中断再設定を行うには、重複リンク上の設定済みドメインを変更し、ドメインの重複を排除します。

# ドメイン ID

ドメイン ID は VSAN 内のスイッチを一意に識別します。スイッチは異なる VSAN に異なるドメイン ID を持つことがあります。ドメイン ID は FC ID 全体の一部です。

設定済みドメイン ID のタイプは優先またはスタティックになります。デフォルトで、設定済みドメイン ID は 0（ゼロ）、設定タイプは優先です。

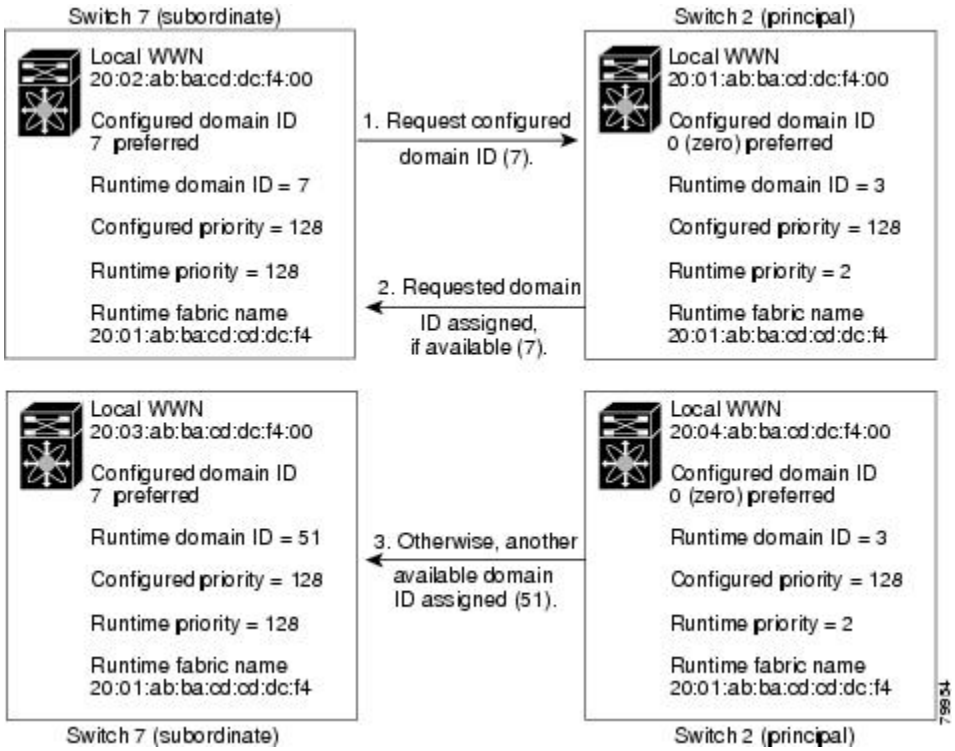
（注） 値 0（ゼロ）を設定できるのは、優先オプションを使用した場合だけです。

ドメイン ID を設定しない場合、ローカル スイッチは要求内でランダムな ID を送信します。スタティック ドメイン ID を使用することを推奨します。

下位スイッチがドメインを要求する場合は、次のプロセスが実行されます（図 13 : 基本設定オプションを使用した設定プロセス （282 ページ）を参照）。

1. ローカル スイッチは主要スイッチに設定済みドメイン ID 要求を送信します。
2. 要求されたドメイン ID が使用可能な場合、主要スイッチはこの ID を割り当てます。使用不可能な場合は、使用可能な別のドメイン ID を割り当てます。

図 *13 :* 基本設定オプションを使用した設定プロセス




下位スイッチの動作は、次の要因によって変化します。

- 許可ドメイン ID リスト。
- 設定済みドメイン ID。
- 主要スイッチが要求元スイッチに割り当てたドメイン ID。

状況に応じて、次のように変更されます。

- 受信されたドメイン ID が許可リストに含まれない場合は、要求されたドメイン ID が実行時ドメイン ID になり、該当する VSAN のすべてのインターフェイスが隔離されます。
- 割り当てられたドメイン ID と要求されたドメイン ID が同じである場合は、優先およびスタティック オプションは関係せず、割り当てられたドメイン ID が実行時ドメイン ID になります。
- 割り当てられたドメイン ID と要求されたドメイン ID が異なる場合は、次のようになります。
  - 設定タイプがスタティックの場合は、割り当てられたドメイン ID が廃棄され、すべてのローカル インターフェイスは隔離され、ローカル スイッチには設定済みのドメイン ID が自動的に割り当てられます（この ID が実行時ドメイン ID になります）。
  - 設定タイプが preferred 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、割り当てられた ID が実行時ドメイン ID になります。

設定済みドメイン ID を変更したときに、変更が受け入れられるのは、新しいドメイン ID が、VSAN 内に現在設定されているすべての許可ドメイン ID リストに含まれている場合だけです。または、ドメイン ID を 0 の優先に設定することもできます。

**ヒント** 特定の VSAN で FICON 機能がイネーブルになっている場合、その VSAN のドメイン ID はスタティックな状態のままになります。スタティック ID 値は変更できますが、優先オプションには変更できません。

**（注）** NAT 構成のない IVR では、IVR トポロジ内の 1 つの VSAN でスタティック ドメイン ID が設定されている場合、トポロジ内の他の VSAN（エッジまたは中継）にもスタティック ドメイン ID を設定する必要があります。IVR NAT 設定で、IVR トポロジ内の 1 つの VSAN に静的ドメイン ID が設定されている場合は、その VSAN にエクスポート可能な IVR ドメインにも静的ドメインを割り当てる必要があります。

**注意** 設定済みドメインの変更を実行時ドメインに適用する場合は、fcdomain 再起動コマンドを入力する必要があります。

**注意** You must restart the **fcdomain** if you want to apply the configured domain changes to the runtime domain.

（注） 許可ドメイン ID リストを設定した場合、追加するドメイン ID は VSAN でその範囲に収まっている必要があります。許可ドメイン ID リストの設定 （294 ページ）を参照してください。

## スタティック ドメイン ID または優先ドメイン ID の指定

スタティック ドメイン ID タイプを割り当てる場合、特定のドメイン ID を要求します。スイッチは、要求したアドレスを取得できなかった場合、自分自身をファブリックから分離します。優先ドメイン ID を指定した場合も特定のドメイン ID を要求しますが、要求したドメイン ID を取得できない場合スイッチは、別のドメイン ID を受け入れます。

スタティック オプションは、中断再起動または非中断再起動後の実行時に適用できますが、優先オプションは中断再起動後の実行時にだけ適用できます（ドメインの再起動 （278 ページ）を参照）。

## 許可ドメイン ID リスト

デフォルトでは、割り当て済みのドメイン ID リストの有効範囲は 1 ～ 239 です。許可ドメイン ID リストに複数の範囲を指定し、各範囲をカンマで区切れます。主要スイッチは、ローカルに設定された許可ドメイン リストで使用可能なドメイン ID を割り当てます。

重複しないドメイン ID で VSAN を設計するには、許可ドメイン ID リストを使用します。このリストは将来 NAT 機能を使用しない IVR を実装する必要がある場合に役立ちます。

## 許可ドメイン ID リストの CFS 配信

Cisco Fabric Service（CFS）インフラストラクチャを使用し、ファブリックのすべての Cisco MDS スイッチに許可ドメイン ID リストの設定情報を配信することをイネーブルにすることができます。この機能により、1 つの MDS スイッチのコンソールからファブリック全体の設定を同期できます。同じ設定が VSAN 全体に配信されるため、発生する可能性がある設定ミスや、同一 VSAN の 2 つのスイッチで互換性がない許可ドメインを設定する可能性を回避できます。

CFS を使用して許可ドメイン ID リストを配信し、VSAN 内のすべてのスイッチで許可ドメイン ID リストの整合性をとるようにします。

（注） 許可ドメイン ID リストを設定し、主要スイッチで確定することを推奨します。

CFS の詳細については、CFS インフラストラクチャの使用 （5 ページ）を参照してください。

## 連続ドメイン ID 割り当て

デフォルトでは、連続ドメイン割り当てはディセーブルです。下位スイッチが複数のドメインを主要スイッチに要求し、ドメインが連続していない場合は、次のような状況になる可能性があります。

- 主要スイッチで連続ドメイン割り当てがイネーブルの場合、主要スイッチは連続ドメインを特定し、それらを下位スイッチに割り当てます。連続ドメインが使用できない場合、NX-OS ソフトウェアはこの要求を却下します。
- 主要スイッチで連続ドメイン割り当てがディセーブルの場合、主要スイッチは使用可能なドメインを下位スイッチに割り当てます。

## ファブリックのロック

既存の設定を変更するときの最初のアクションによって、保留中の設定が作成され、ファブリック内の機能がロックされます。ファブリックをロックすると、次の条件が適用されます。

- 他のユーザがこの機能の設定に変更を加えることができなくなります。
- アクティブな設定をコピーすると保留中の設定が作成されます。これ以後の変更は保留設定に対して行われ、アクティブな設定（およびファブリック内の他のスイッチ）に変更をコミットするか、または変更を廃棄するまで、保留設定にとどまります。

## 変更のコミット

保留されているドメイン設定の変更を VSAN のその他の MDS スイッチに適用するには、変更を確定する必要があります。保留中の設定変更が配信され、正常に確定された時点で、設定変更は VSAN 全体の MDS スイッチでアクティブな設定に適用されて、ファブリックのロックが解除されます。

## ファブリックのロックのクリア

ドメイン設定作業を実行し、変更をコミットまたは廃棄してロックを解除していない場合、管理者はファブリック内の任意のスイッチからロックを解除できます。管理者がこのタスクを実行すると、保留中の変更は廃棄され、ファブリック ロックが解除されます。

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

## FC ID

Cisco MDS 9000 ファミリ スイッチに N または NL ポートがログインする場合、FC ID が割り当てられます。デフォルトでは、固定的FC ID機能はイネーブルです。この機能をディセーブルにした場合、次の結果になります。

- N ポートまたは NL ポートが Cisco MDS 9000 ファミリ スイッチにログインします。要求側の N ポートまたは NL ポートの WWN、および割り当てられた FC ID は保持され、揮発性キャッシュに保存されます。この揮発性キャッシュの内容は、再起動時に保存されません。
- スイッチは、FC ID と WWN のバインディングをベストエフォート方式で保持するように設計されています。たとえば、スイッチから 1 つの N ポートを切断したあとに、別のデバイスから FC ID が要求されると、この要求が許可されて、WWN と初期 FC ID の関連付けが解除されます。

- 揮発性キャッシュには、WWN と FC ID のバインディングのエントリを 4000 まで格納できます。このキャッシュが満杯になると、新しい（より最近の）エントリによって、キャッシュ内の最も古いエントリが上書きされます。この場合、最も古いエントリの対応する WWN と FC ID の関連付けが失われます。
- スイッチ接続動作は、N ポートと NL ポートで異なります。
  - N ポートを取り外し、同じスイッチの任意のポートに接続すると、（このポートが同じ VSAN に属するかぎり）この N ポートには同じ FC ID が割り当てられます。
  - NL ポートが同じ FC ID になるのは、スイッチ上の以前接続されていたポートと同じポートに再度接続された場合だけです。

## 永続的 FC ID

固定的 FC ID がイネーブルである場合は、次のようになります。

- The currently *in use* FC IDs in the fcdomain are saved across reboots.
- fcdomain は、デバイス（ホストまたはディスク）をポートインターフェイスに接続したあとに学習されたダイナミック エントリを、自動的にデータベースに入力します。

## 固定的 FC ID 設定

固定的 FC ID 機能をイネーブルにすると、固定的 FC ID サブモードを開始して、FC ID データベースにスタティックまたはダイナミックエントリを追加できるようになります。デフォルトでは、追加されたすべてのエントリはスタティックです。固定的 FC ID は VSAN 単位で設定します。固定的 FC ID を手動で設定するには、次の要件に従ってください。

- 必要な VSAN 内で固定的 FC ID 機能がイネーブルになっていることを確認します。
- 必要な VSAN がアクティブ VSAN であることを確認してください。固定的 FC ID は、アクティブな VSAN に対してだけ設定できます。
- FC ID のドメイン部分が必要な VSAN 内の実行時ドメイン ID と同じであることを確認します。ソフトウェアがドメインの不一致を検出した場合、コマンドは拒否されます。
- エリアを設定するときに、FC ID のポート フィールドが 0（ゼロ）であることを確認します。

（注） FICON は、前面パネルのポート番号に基づき、異なる方式を使用して FC ID を割り当てます。この方式は、FICON VSAN における FC ID の固定化よりも優先されます。

## HBA の固有エリア FC ID について

（注） HBA ポートおよびストレージ ポートを同一スイッチに接続している場合に限り、この項を読んでください。

HBA ポートとストレージ ポートを両方とも同一スイッチに接続している場合、一部の HBA ポートにはストレージ ポートとは別のエリア ID が必要となります。たとえば、ストレージ ポート FC ID が 0x6f7704 の場合、このポートのエリアは 77 です。この場合、HBA ポートのエリアには 77 以外の値を設定できます。HBA ポートの FC ID は、ストレージ ポートの FC ID と異なる値に手動で設定する必要があります。

Cisco MDS 9000 ファミリのスイッチでは、FC ID の固定化機能により、この要件への準拠が容易になります。この機能を使用すると、ストレージ ポートまたは HBA ポートに異なるエリアを持つ FC ID を事前に割り当てることができます。

## 固定的 FC ID の選択消去

固定的 FC ID は、選択的に消去できます。Static entries and FC IDs currently in use cannot be deleted. 表 37 : 消去される FC ID （287 ページ） identifies the FC ID entries that are deleted or retained when persistent FC IDs are purged.

**表 *37* : 消去される *FC ID***

| 固定的 FC ID の状態 | 固定的 FC ID の使用状態 | Action |
|---|---|---|
| スタティック | 使用中 | 削除されない |
| スタティック | 使用中でない | 削除されない |
| Dynamic | 使用中 | 削除されない |
| Dynamic | 使用中でない | 削除される。 |

# 注意事項と制約事項

- 設定を変更した場合は、必ず実行コンフィギュレーションを保存してください。次回にスイッチを再起動したときに、保存された設定が使用されます。設定を保存しない場合は、前回保存されたスタートアップ コンフィギュレーションが使用されます。
- すべての手順で使用されるドメイン ID および VSAN 値は、単なる例です。必ずご使用の設定に適用される ID および値を使用してください。

# デフォルト設定

表 38 : デフォルト fcdomain パラメータ （288 ページ） に、すべての fcdomain パラメータのデフォルト設定値を示します。

表 *38 :* デフォルト *fcdomain* パラメータ

| パラメータ | デフォルト |
|---|---|
| fcdomain 機能 | イネーブル |
| 設定済みドメイン ID | 0（ゼロ） |
| 設定済みドメイン | 優先 |
| **auto-reconfigure** オプション | ディセーブル |
| **contiguous-allocation** オプション | ディセーブル |
| プライオリティ | 128 |
| 許可リスト | 1 ～ 239 |
| ファブリック名 | 20:01:00:05:30:00:28:df |
| **rcf-reject** | ディセーブル |
| 固定的 FC ID | イネーブル |
| 許可ドメイン ID リスト設定の配信 | ディセーブル |

# ファイバ チャネル ドメインの設定

This section describes the fcdomain feature.

## ドメインの再起動

ドメイン設定シナリオ；

### スイッチの設定

VSAN 6 内のスイッチの設定方法に関係なく、fcdomain が中断 vsan 6 を再起動することで VSAN 6 のすべてのスイッチの全デバイスがログアウトし、データ トラフィックの中断が発生します。

### 設定されているドメインとランタイム ドメインが一致する

設定されたドメインとランタイム ドメインがすべてのスイッチ上にあることが前提の場合、fcdomain が vsan 6 を再起動しても VSAN 6 のデバイスがログアウトすることはありません。

### 設定されているドメインとランタイム ドメインが一致しない

VSAN 6 の一部のスイッチで設定されたドメインとランタイム ドメインが同じではないことが前提の場合、fcdomain が vsan 6 を再起動すると静的に設定されたドメインとランタイム ドメ

インを持つスイッチに接続された VSAN 6 のデバイスがログアウトに一致せず、データ トラフィックが中断します。

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。

**手順**

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **fcdomain restart vsan 1**

ネットワーク全体ではデータ トラフィックは中断しませんが、設定されたドメインが静的でランタイム ドメインと数字が同じではない場合、スイッチ上で中断が発生する可能性があります（たとえば、設定されたドメインが 11 スタティックでランタイム ドメインが 99 など）。

**ステップ 3** switch(config)# **fcdomain restart disruptive vsan1**

VSAN 内のすべてのスイッチでデータ トラフィックが中断します。

# ドメイン マネージャの全最適化の有効化

ドメイン マネージャの全最適化機能を有効にするには、次の手順を実行します。

**手順**

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **fcdomain optimize all vsan 3**

VSAN 3 ですべてのドメイン マネージャの最適化を有効にします（選択対象再起動、高速再起動、スケール再起動）。

**ステップ 3** switch(config)# **fcdomain optimize all vsan 7 - 10**

VSAN 7 ～ VSAN 10 の範囲の VSAN でドメイン マネージャの全最適化を有効にします。

**ステップ 4** switch(config)# **no fcdomain optimize all vsan 8**

VSAN 8 でドメイン マネージャの全最適化を無効にします。

# ドメイン マネージャの高速再起動のイネーブル化

Cisco SAN-OS リリース 3.0(2) 以降または MDS NX-OS リリース 4.1(1a) でドメイン マネージャの高速再起動を有効にするには、次の手順を実行します。

**手順**

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **fcdomain optimize fast-restart vsan 3**

VSAN 3 でドメイン マネージャの高速再起動を有効にします。

**ステップ 3** switch(config)# **fcdomain optimize fast-restart vsan 7 - 10**

VSAN 7 ～ VSAN 10 の範囲の VSAN でドメイン マネージャの高速再起動を有効にします。

**ステップ 4** switch(config)# **no fcdomain optimize fast-restart vsan 8**

VSAN 8 で ドメイン マネージャの高速再起動を無効（デフォルト）にします。

# ドメイン マネージャ スケール再起動の有効化

ドメイン マネージャ スケール再起動を有効にするには、これらの手順に従います。

**手順**

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **fcdomain optimize scale-restart vsan 3**

VSAN 3 でドメイン マネージャ スケールの再起動を有効にします。

**ステップ 3** switch(config)# **fcdomain optimize scale-restart vsan 7 - 10**

VSAN 7 から VSAN 10 までの範囲の VSANで、ドメイン マネージャ スケール再起動（デフォルト）を有効にします。

**ステップ 4** switch(config)# **no fcdomain optimize scale-restart vsan 8**

VSAN 8 のドメイン マネージャ スケール再起動を無効にします。

# ドメイン マネージャ選択的再起動の有効化

Cisco SAN-OS リリース 3.0(2) 以降、MDS NX-OS Release 4.1(1a) 以降でドメイン マネージャ選択的再起動機能を有効にするには、次の手順に従います。

**手順**

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **fcdomain optimize selective-restart vsan 3**

VSAN 3 でドメイン マネージャの選択的再起動を有効にします。

**ステップ 3** switch(config)# **fcdomain optimize selective-restart vsan 7 - 10**

VSAN7 から VSAN 10 の VSAN 範囲でドメイン マネージャ選択的再起動を有効にします。

**ステップ 4** switch(config)# **no fcdomain optimize selective-restart vsan 8**

VSAN 8 のドメイン マネージャの選択的再起動を無効にします（デフォルト）。

# スイッチ プライオリティの設定

（注） デフォルトでは、プライオリティは 128 に設定されます。プライオリティの有効設定範囲は 1 ～ 254 です。プライオリティ 1 が最高のプライオリティです。値 255 は、他のスイッチからは受け入れられますが、ローカルには設定できません。

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。

**手順**

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **fcdomain priority 25 VSAN 99**

VSAN 99 ローカル スイッチの 25 の優先順位を設定します。

**ステップ 3** switch(config)# **no fcdomain priority 25 VSAN 99**

VSAN 99.で優先順位を出荷時の設定（128）に戻します。

# ファブリック名の設定

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。

**手順**

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **fcdomain fabric-name 20:1:ac:16:5e:0:21:01 vsan 3**

VSAN 3 に設定済みファブリック名の値を割り当てます。

**ステップ 3** switch(config)# **no fcdomain fabric-name 20:1:ac:16:5e:0:21:01 vsan 3010**

VSAN 3010 のファブリック名の値を出荷時のデフォルト設定（20:01:00:05:30:00:28:df）に変更します。

# 着信 RCF の拒否

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。

**手順**

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **interface fc1/1**

switch(config-if)#

指定されたインターフェイスを設定します。

**ステップ 3** switch(config-if)# **fcdomain rcf-reject vsan 1**

VSAN 1 内の指定されたインターフェイス上で RCF フィルタを有効にします。

**ステップ 4** switch(config-if)# **no fcdomain rcf-reject vsan 1**

VSAN 1 内の指定されたインターフェイス上で RCF フィルタを無効（デフォルト）にします。

## 自動再設定のイネーブル化

特定の VSAN（または VSAN 範囲）で自動再構成をイネーブルにするには、次の手順を実行します。

**手順**

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **fcdomain auto-reconfigure vsan 10**

指定された VSAN 10 で自動再設定オプションをイネーブルにします。

**ステップ 3** switch(config)# **no fcdomain auto-reconfigure 69**

自動再設定オプションを無効にして、WBS 69 で出荷時のデフォルト設定に戻します。

# ドメイン ID の設定

ドメイン ID は VSAN 内のスイッチを一意に識別します。スイッチは異なる VSAN に異なるドメイン ID を持つことがあります。ドメイン ID は FC ID 全体の一部です。

設定済みドメイン ID のタイプは優先またはスタティックになります。デフォルトで、設定済みドメイン ID は 0（ゼロ）、設定タイプは優先です。

## スタティック ドメイン ID または優先ドメイン ID の指定

（注） 1 つの VSAN 内のスイッチは、すべて同じドメイン ID タイプ（スタティックまたは優先）を持っている必要があります。あるスイッチがスタティック ドメイン タイプで、別のスイッチが優先ドメイン タイプであるというように、設定が混在している場合は、リンクが分離されることがあります。

新しいドメイン ID が設定される場合、fcdomain 再起動コマンドを使用してドメインを手動で再起動することで新しい設定が適用され、後続のファブリック マージ中に設定されたドメイン ID およびランタイム ドメイン ID 間で不一致が検出されると、リンクが分離されます。

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。

### 手順

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **fcdomain domain 3 preferred vsan 8**

希望の ドメイン ID 3 を要求するために VSAN 8 内のスイッチを設定し、主要スイッチによって割り当てられた値をすべて受け入れます。ドメインの範囲は 1 ～ 239 です。

**ステップ 3** switch(config)# **no fcdomain domain 3 preferred vsan 8**

設定済みドメイン ID を、VSAN 8 内で 0（デフォルト）にリセットします。設定済みドメイン ID は 0 preferred になります。

**ステップ 4** switch(config)# **fcdomain domain 2 static vsan 237**

特定の値だけを受け入れるように VSAN 237 内のスイッチを設定し、要求されたドメイン ID が許可されない場合は、VSAN 237 内のローカル インターフェイスを隔離ステートに移行します。

**ステップ 5** switch(config)# **no fcdomain domain 18 static vsan 237**

設定済みドメイン ID を、VSAN 237 内の出荷時のデフォルト設定にリセットします。設定済みドメイン ID は 0 preferred になります。

# 許可ドメイン ID リストの設定

ファブリック内の 1 つのスイッチに許可リストを設定する場合は、整合性を保つために、ファブリック内のその他のすべてのスイッチに同じリストを設定するか、CFS を使用して設定を配信することを推奨します。

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。

### 始める前に

許可ドメイン ID リストは、次の条件を満たす必要があります。

- スイッチが主要スイッチである場合は、現在割り当てられているすべてのドメイン ID が許可リストに含まれている必要があります。
- このスイッチが下位スイッチである場合は、ローカル実行時ドメイン ID が許可リストに含まれている必要があります。
- ローカルに設定されたスイッチのドメイン ID が許可リスト内に含まれている必要があります。

- 割り当てられたドメイン ID の一部が、その他の設定済みドメイン ID のリストのいずれかに含まれている必要があります。

**手順**

| | コマンドまたはアクション | 目的 |
|---|---|---|
| **ステップ 1** | switch# **configure terminal** | コンフィギュレーション モードに入ります。 |
| **ステップ 2** | switch# **fcdomain allowed 50-110 vsan 4** | VSAN 4 で ドメイン ID 50 ～ 110 を持つスイッチを許可するリストを作成します。<br>switch# **no fcdomain allowed 50-110 vsan 4**<br>VSAN 5 で 1 ～ 239 までのドメイン ID を許可する出荷時のデフォルト設定に戻します。 |

# 許可ドメイン ID 配信の有効化

許可ドメイン ID リストの CFS 配信はデフォルトではディセーブルになっています。許可ドメイン ID リストを配信するすべてのスイッチで配信をイネーブルにする必要があります。

許可ドメイン ID リスト設定の配信をイネーブル（またはディセーブル）にするには、次の手順を実行します。

### 始める前に

CFS を使用して許可ドメイン ID リストを配信するには、ファブリック内のすべてのスイッチは Cisco SAN-OS Release 3.0(1) 以降を実行している必要があります。

### 手順

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **fcdomain distribute**

ドメイン設定の配信をイネーブルにします。

**ステップ 3** switch(config)# **no fcdomain distribute**

ドメイン設定の配信をディセーブル（デフォルト）にします。

## 変更のコミット

保留中のドメイン設定変更をコミットし、ロックを解除するには、次の手順を実行します。

**手順**

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **fcdomain commit vsan 10**

保留中のドメイン設定変更をコミットします。

## 変更の破棄

いつでもドメイン設定への保留変更を廃棄して、ファブリックのロックを解除できます。保留中の変更を廃棄（中断）する場合、設定には影響せずに、ロックが解除されます。

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。

**手順**

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **fcdomain abort vsan 10**

保留中のドメイン設定変更を廃棄します。

# 連続ドメイン ID 割り当てのイネーブル化

特定のVSAN（またはVSAN範囲）で連続ドメインをイネーブルにするには、次の手順を実行します。

**手順**

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **fcdomain contiguous-allocation vsan 81-83**

VSAN 81～ 83 まで継続した割り当てオプションを有効にします。

（注） The **contiguous-allocation** option takes immediate effect at runtime. fcdomain を再起動する必要はありません。

**ステップ 3** switch(config)# **no fcdomain contiguous-allocation vsan 1030**

VSAN 1030 で連続割り当てオプションを無効にし、出荷時の設定に戻します。

# FC ID の設定

Cisco MDS 9000 ファミリ スイッチに N または NL ポートがログインする場合、FC ID が割り当てられます。

## 永続的 FC ID 機能のイネーブル化

AIX または HP-UX ホストからスイッチに接続する場合は、それらのホストに接続する VSAN で固定的 FC ID 機能をイネーブルにする必要があります。

F ポートに割り当てられた固定的 FC ID は、インターフェイス間を移動させることができ、同じ固定的 FC ID をそのまま維持することができます。

（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。
- ループ接続デバイス（FL ポート）を使用した固定的 FC ID は、設定されたポートと同じポートに接続され続ける必要があります。
- デバイス上の Arbitrated Loop Physical Address（ALPA）のサポートの違いにより、ループ接続デバイスの FC ID の固定化は保証されません。
- Cisco MDS 9124、9134、9148、9148S、および 9250i スイッチでは、インターフェイスごとに完全な FCID 領域を割り当て、FCID（port_id）の右側の最後のバイトがこれらのプラットフォームで常に 0 であるようにします(NPV スイッチに接続されている NPIV で実行されている MDS 9148 を除く)。したがって、ゼロ以外の port_id でスタティック FCID を設定することはできません。たとえば、次は MDS 9124 で 9134、9148、9148S、および 9250i: では機能しません。

  **vsan**1000 **wwn** 33: e8:00:05:30:00:16: df **fcid** 0x070128

  1000 **vsanwwn** 33: e8:00:05:30:00:16: df **fcid** 0x070100 に変更する必要があります。

固定的 FC ID 機能をイネーブルにするには、次の手順を実行します。

手順

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **fcdomain fcid persistent vsan** *1000*

```
FCID(s) persistent feature is enabled.
```

VLAN 1000 で FC ID の永続性を有効（デフォルト）にします。

ステップ 3 switch(config)# **no fcdomain fcid persistent vsan** *20*

VLAN 20 で FC ID 永続性機能を無効にします。

# 永続的 FC ID の設定

固定的 FC ID を設定するには、次の手順を実行します。

手順

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **fcdomain fcid database**

switch(config-fcid-db)#

FC ID データベース コンフィギュレーション サブモードを開始します。

ステップ 3 switch(config-fcid-db)# **vsan 1000 wwn 33:e8:00:05:30:00:16:df fcid 0x070128**

Configures a device WWN (33:e8:00:05:30:00:16:df) with the FC ID 0x070128 in VSAN 1000.

（注） To avoid assigning a duplicate FC ID, use the **show fcdomain address-allocation vsan** command to display the FC IDs in use.

ステップ 4 switch(config-fcid-db)# **vsan 1000 wwn 11:22:11:22:33:44:33:44 fcid 0x070123 dynamic**

Configures a device WWN (11:22:11:22:33:44:33:44) with the FC ID 0x070123 in VSAN 1000 in dynamic mode.

ステップ 5 switch(config-fcid-db)# **vsan 1000 wwn 11:22:11:22:33:44:33:44 fcid 0x070100 area**

Configures a device WWN (11:22:11:22:33:44:33:44) with the FC IDs 0x070100 through 0x701FF in VSAN 1000.

（注） この fcdomain のエリア全体を保護するには、FC ID の末尾 2 文字に 00 を割り当てます。

# HBA の固有エリア FC ID の設定

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。

（注） 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。

**手順**

**ステップ 1** Obtain the port WWN (Port Name field) ID of the HBA using the **show flogi database** command.

```
switch# show flogi database
--------------------------------------------------------------------------------
INTERFACE   VSAN    FCID        PORT NAME                NODE NAME
--------------------------------------------------------------------------------

 fc1/9      3       0x6f7703    50:05:08:b2:00:71:c8:c2     50:05:08:b2:00:71:c8:c0
 fc1/10     3       0x6f7704    50:06:0e:80:03:29:61:0f     50:06:0e:80:03:29:61:0f
```

（注） この設定では、両方の FC ID に同じエリア 77 が割り当てられています。

**ステップ 2** MDS スイッチの HBA インターフェイスをシャットダウンします。

```
switch# configure terminal
switch(config)# interface fc1/9
switch(config-if)# shutdown
switch(config-if)# end
switch#
```

**例**：

**ステップ 3** Verify that the FC ID feature is enabled using the **show fcdomain vsan** command.

```
switch# show fcdomain vsan 1
Local switch run time information:
        State: Stable
        Local switch WWN:    20:01:54:7f:ee:de:b3:01
        Running fabric name: 20:01:00:05:9b:2c:1c:71
        Running priority: 128
        Current domain ID: 0xee(238)
Local switch configuration information:
        State: Enabled
        FCID persistence: Disabled
```

```
        Auto-reconfiguration: Disabled
        Contiguous-allocation: Disabled
        Configured fabric name: 20:01:00:05:30:00:28:df
        Optimize Mode: Disabled
        Configured priority: 128
        Configured domain ID: 0x00(0) (preferred)
Principal switch run time information:
        Running priority: 2
Interface              Role          RCF-reject
----------------    -------------    ------------
fc1/1               Non-principal    Disabled
fc1/2               Upstream         Disabled
fc1/11              Non-principal    Disabled
fc1/37              Non-principal    Disabled
port-channel 1      Downstream       Disabled
----------------    -------------    ------------
```

この機能がディセーブルの場合は、この手順を継続して、固定的 FC ID をイネーブルにします。

この機能がすでに有効になっている場合は、手順 7 に進みます。

**ステップ 4** Cisco MDS スイッチで永続的 FC ID 機能を有効にします。

```
switch# configure terminal
switch(config)# fcdomain fcid persistent vsan 1
switch(config)# end
switch#
```

**ステップ 5** 異なるエリアの新しい FC ID を割り当てます。この例では、*77* を *ee* に置き換えます。

```
switch# configure terminal
switch(config)# fcdomain fcid database
switch(config-fcid-db)# vsan 3 wwn 50:05:08:b2:00:71:c8:c2 fcid 0x6fee00 area
```

**ステップ 6** Cisco MDS スイッチの HBA インターフェイスを有効にします。

```
switch# configure terminal
switch(config)# interface fc1/9
switch(config-if)# no shutdown
switch(config-if)# end
switch#
```

**ステップ 7** Verify the pWWN ID of the HBA using the **show flogi database** command.

```
switch# show flogi database
--------------------------------------------------------------------------------
INTERFACE   VSAN    FCID        PORT NAME                 NODE NAME
--------------------------------------------------------------------------------
fc1/9       3       0x6fee00    50:05:08:b2:00:71:c8:c2   50:05:08:b2:00:71:c8:c0
fc1/10      3       0x6f7704    50:06:0e:80:03:29:61:0f   50:06:0e:80:03:29:61:0f
```

（注） これで、両方の FC ID にそれぞれ異なるエリアが割り当てられました。

# 永続的 FC ID の消去

固定的 FC ID を消去するには、次の手順を実行します。

**手順**

**ステップ 1** switch# **purge fcdomain fcid vsan 4**

VSAN 4 の未使用のダイナミック FC ID をすべて消去します。

**ステップ 2** switch# **purge fcdomain fcid vsan 3-5**

VSAN 3、4、および 5 の未使用のダイナミック FC ID を削除します。

# ファブリックのロックのクリア

To release a fabric lock, issue the **clear fcdomain session vsan** command in EXEC mode using a login ID that has administrative privileges.

```
switch# clear fcdomain session vsan 10
```

# FC ドメイン設定の確認

ドメイン ID の設定情報を表示するには、次の作業を行います。

| コマンド | 目的 |
|---|---|
| **show fcdomain status** | 許可済みドメイン ID リストの CFS 配信のステータスを表示します。 |
| **show fcdomain pending** | 保留中に設定変更を表示します。 |
| **show fcdomain session-status vsan** | 配信セッションのステータスを表示します。 |
| **show fcdomain** | グローバルについて fcdomain 設定を表示します。 |
| **show fcdomain domain-list** | ドメインのすべてのスイッチの Id のリストが表示されます。 |
| **show fcdomain allowed vsan** | 許可されているドメインこのスイッチに設定されている Id のリストが表示されます。 |
| **show fcdomain fcid persistent** | 指定した VSAN のすべての既存の永続的な FC Id を表示します。 |

| コマンド | 目的 |
|---|---|
| **show fcdomain statistics** | 指定した VSAN またはポート チャネルのフレームとその他の fcdomain 統計情報を表示します。 |
| **show fcdomain address-allocation** | 割り当てられたと free の FC Id のリストを含む FC ID の割り当ての統計情報を表示します。 |
| **show fcdomain address-allocation cache** | 有効なアドレス割り当てキャッシュを表示します。 |

For detailed information about the fields in the output from these commands, refer to the *Cisco MDS 9000 Family Command Reference* .

# CFS 配信ステータスの表示

You can display the status of CFS distribution for allowed domain ID lists using the **show fcdomain status** command.

```
switch# show fcdomain status
CFS distribution is enabled
```

# 保留中の変更の表示

保留中の設定変更は show fcdomain pending コマンドを使用して表示できます。

```
switch# show fcdomain pending vsan 10
Pending Configured Allowed Domains
---------------------------------
VSAN 10
Assigned or unallowed domain IDs: 1-9,24,100,231-239.
[User] configured allowed domain IDs: 10-230.
```

保留中の設定と現在の設定の違いは、show fcdomain pending-diff コマンドを使用して表示できます。

```
switch#show fcdomain pending-diff vsan 10
Current Configured Allowed Domains
---------------------------------
VSAN 10
Assigned or unallowed domain IDs: 24,100.
[User] configured allowed domain IDs: 1-239.
Pending Configured Allowed Domains
---------------------------------
VSAN 10
Assigned or unallowed domain IDs: 1-9,24,100,231-239.
[User] configured allowed domain IDs: 10-230.
```

# セッション ステータスの表示

You can display the status of the distribution session using the **show fcdomain session-status vsan** command.

```
switch# show fcdomain session-status vsan 1
Last Action: Distribution Enable
Result: Success
```

# Fcdomain 情報の表示

### グローバル fcdomain 情報

Use the **show fcdomain** command to display global information about fcdomain configurations. 次の例を参照してください。

（注） 次の例では、fcdomain 機能は無効です。その結果、ランタイム ファブリック名は設定済みファブリック名と同じです。

```
switch# show fcdomain vsan 2
The local switch is the Principal Switch.
Local switch run time information:
        State: Stable
        Local switch WWN:    20:01:00:0b:46:79:ef:41
        Running fabric name: 20:01:00:0b:46:79:ef:41
        Running priority: 128
        Current domain ID: 0xed(237)
Local switch configuration information:
        State: Enabled
        FCID persistence: Disabled
        Auto-reconfiguration: Disabled
        Contiguous-allocation: Disabled
        Configured fabric name: 20:01:00:05:30:00:28:df
        Optimize Mode: Disabled
        Configured priority: 128
        Configured domain ID: 0x00(0) (preferred)
Principal switch run time information:
        Running priority: 128
No interfaces available.
switch# show fcdomain vsan 1
The local switch is the Principal Switch.
Local switch run time information:
State: Stable
Local switch WWN: 20:01:54:7f:ee:46:5b:41
Running fabric name: 20:01:54:7f:ee:46:5b:41
Running priority: 128
Current domain ID: 0xe9(233)
Local switch configuration information:
State: Enabled
FCID persistence: Enabled
Auto-reconfiguration: Disabled
Contiguous-allocation: Disabled
Configured fabric name: 20:01:00:05:30:00:28:df
```

```
Optimize Mode: Enabled (Fast Restart, Selective Restart, Scale Restart)
Configured priority: 128
Configured domain ID: 0xe9(233) (static)
Principal switch run time information:
Running priority: 128
No interfaces available.
switch#
```

（注） Cisco MDS 6.2(9) リリース以降から 6.2(7) 以前のリリースにダウングレードしたときに、スケール再起動機能が有効になっており、その他の最適化モードが無効になっている場合、最適化モードは無効の代わりに空になります。

### Fcdomain リスト

Use the **show fcdomain domain-list** command to display the list of domain IDs of all switches belonging to a specified VSAN. このリストには、各ドメイン ID を所有するスイッチの WWN が記載されています。次の例では以下を表示します。

- 20:01:00:05:30:00:47:df の WWN を持つスイッチが主要スイッチで、ドメインは 200 です。
- 20:01:00:0d:ec:08:60:c1 の WWN を持つスイッチはローカル スイッチ（CLI コマンドを入力してドメイン リストを表示したスイッチ）で、ドメインは 99 です。
- IVR マネージャは 20:01:00:05:30:00:47:df を仮想スイッチの WWN として使用して仮想ドメイン 97 を取得しました。

```
switch# show fcdomain domain-list vsan 76
Number of domains: 3
Domain ID              WWN
---------    -----------------------
0xc8(200)    20:01:00:05:30:00:47:df [Principal]
 0x63(99)    20:01:00:0d:ec:08:60:c1 [Local]
 0x61(97)    50:00:53:0f:ff:f0:10:06 [Virtual (IVR)]
```

### 許可ドメイン ID リスト

Use the **show fcdomain allowed vsan** command to display the list of allowed domain IDs configured on this switch. 次の例を参照してください。

```
switch# show fcdomain allowed vsan 1

Assigned or unallowed domain IDs: 1-96,100,111-239.
[Interoperability Mode 1] allowed domain IDs: 97-127.
[User] configured allowed domain IDs: 50-110.
```

ヒント Ensure that the requested domain ID passes the Cisco NX-OS software checks, if **interop 1** mode is required in this switch.

### 指定された VSAN の永続的な FC ID

Use the **show fcdomain fcid persistent** command to display all existing, persistent FC IDs for a specified VSAN. You can also specify the **unused** option to view only persistent FC IDs that are still not in use. 次の例を参照してください。

```
switch# show fcdomain fcid persistent vsan 1000
Total entries 2.
Persistent FCIDs table contents:
VSAN              WWN                FCID         Mask         Used    Assignment
----    ----------------------    --------    -----------    ----    ----------
1000    11:11:22:22:11:11:12:23    0x700101    SINGLE FCID      NO    STATIC
1000    44:44:33:33:22:22:11:11    0x701000    ENTIRE AREA      NO    DYNAMIC
```

### Fcdomain 内のすべての永続的 ID

次の例では、fcdomain の永続的な FC ID がすべて表示されます。

```
switch# show fcdomain fcid persistent
Total entries 2.
Persistent FCIDs table contents:
VSAN              WWN                FCID         Mask         Used    Assignment
----    ----------------------    --------    -----------    ----    ----------
1000    11:11:22:22:11:11:22:22    0x700501    SINGLE FCID      NO    STATIC
1003    44:44:33:33:22:22:11:11    0x781000    ENTIRE AREA     YES    DYNAMIC
```

### 指定の VSAN の fcdomain 統計

Use the **show fcdomain statistics** command to display frame and other fcdomain statistics for a specified VSAN or PortChannel. 次の例と ドメイン マネージャの選択対象再起動 （280 ページ） を参照してください。

```
switch# show fcdomain statistics vsan1

VSAN Statistics
        Number of Principal Switch Selections: 5
        Number of times Local Switch was Principal: 0
        Number of 'Build Fabric's: 3
        Number of 'Fabric Reconfigurations': 0
```

### 指定の PortChannel の fcdomain 統計

次の例では、指定 PortChannel の fcdomain 統計を表示する例を示します。

```
switch# show fcdomain statistics interface port-channel 10 vsan 1

        Interface Statistics:
                Transmitted      Received
                -----------      --------
                EFPs      13       9
                DIAs      7        7
```

```
                RDIs      0         0
                ACCs      21        25
                RJTs      1         1
                BFs       2         2
                RCFs      4         4
                Error     0         0
                Total     48        48
        Total Retries: 0
        Total Frames: 96
                -----------       --------
```

### FC ID 情報

Use the **show fcdomain address-allocation** command to display FC ID allocation statistics including a list of assigned and free FC IDs. 次の例を参照してください。

```
switch# show fcdomain address-allocation vsan 1
Free FCIDs: 0x020000 to 0x02fdff
            0x02ff00 to 0x02fffe

Assigned FCIDs: 0x02fe00 to 0x02feff
                0x02ffff

Reserved FCIDs: 0x020100 to 0x02f0ff
                0x02fe00 to 0x02feff
                0x02ffff


Number free FCIDs: 65279
Number assigned FCIDs: 257
Number reserved FCIDs: 61697
```

### アドレス割り当て情報

Use the **show fcdomain address-allocation cache** command to display the valid address allocation cache. ファブリックから取り除かれたデバイス（ディスクやホスト）を元のファブリックに戻す場合、主要スイッチはキャッシュを使用して FC ID を再度割り当てます。キャッシュ内では、VSAN はこのデバイスを含む VSAN を、WWN は FC ID を所有していたデバイスを、マスクは FC ID に対応する 1 つのエリアまたはエリア全体を表します。次の例を参照してください。

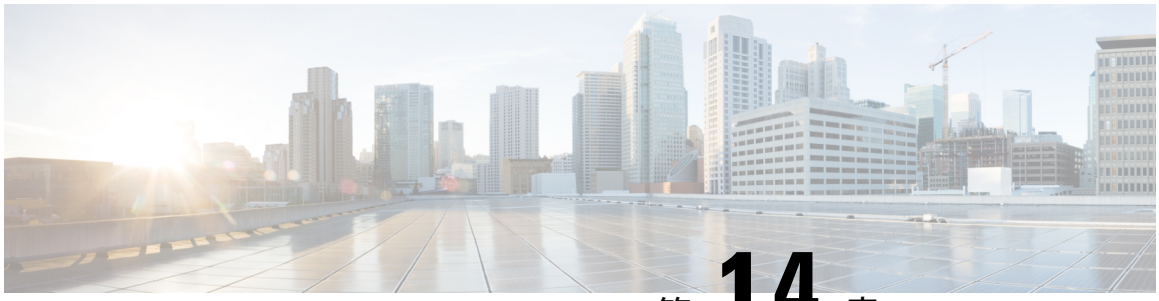
```
switch# show fcdomain address-allocation cache
Cache content:
line#    VSAN              WWN                 FCID        mask
-----    ----    ----------------------    --------    -----------
   1.      12    21:00:00:e0:8b:08:a2:21    0xef0400    ENTIRE AREA
   2.       6    50:06:04:82:c3:a1:2f:5c    0xef0002    SINGLE FCID
   3.       8    20:4e:00:05:30:00:24:5e    0xef0300    ENTIRE AREA
   4.       8    50:06:04:82:c3:a1:2f:52    0xef0001    SINGLE FCID
```

# ドメイン パラメータの機能履歴

表 39 : ドメイン パラメータの機能履歴 （307 ページ） に、この機能のリリース履歴を示します。リリース 3.x 以降のリリースで導入または変更された機能のみが表に記載されています。

**表 *39 :* ドメイン パラメータの機能履歴**

| 機能名 | リリース | 機能情報 |
|---|---|---|
| Domain Manager のターボ モード | 4.2(1) | Domain Manager のターボ モードの設定手順を追加。 |
| 許可ドメイン ID リストの CFS サポート | 3.0(1) | CFS インフラストラクチャを使用して許可ドメイン ID リストをファブリック内で配信できます。 |
| ドメイン マネージャの高速再起動 | 3.0(2) | バックアップ リンクが使用可能な場合、ドメイン マネージャで重大なリンクの障害を素早く回復できます。 |
| ドメインは 60 から 80 に増えます。 | 6.2(11) | スケール ファブリックでドメイン マネージャ保持できるスケーラビリティを最大 80 個に向上します。 |



第 14 章

# SPAN を使用したネットワーク トラフィックのモニタリング

この章では、Cisco MDS 9000 ファミリ スイッチに提供されるスイッチド ポート アナライザ（SPAN）機能について説明します。

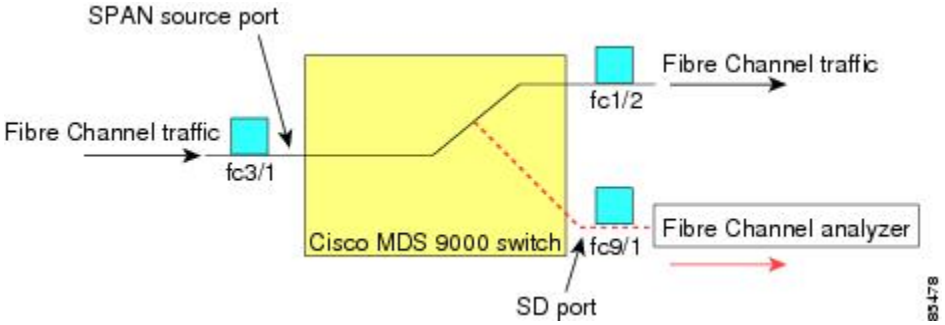


## SPAN について

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

SD ポートはフレームを受信しませんが、SPAN 送信元トラフィックのコピーを送信します。SPAN 機能は他の機能に割り込むことなく、SPAN 送信元ポートのネットワーク トラフィックのスイッチングに影響しません（図 14 : SPAN の送信 （310 ページ） を参照）。

図 *14 : SPAN* の送信

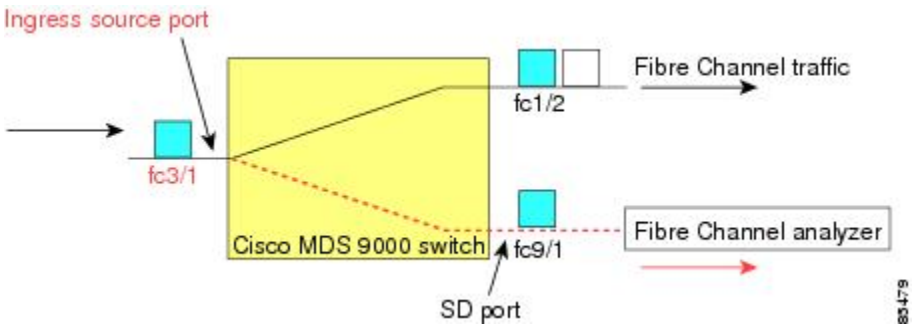



# SPAN ソース

SPAN 送信元とは、トラフィックをモニタリングできるインターフェイスを表します。VSAN を SPAN 送信元として指定することもできます。この場合は、指定された VSAN でサポートされているすべてのインターフェイスが、SPAN 送信元に含まれます。送信元として VSAN が指定されている場合は、この VSAN 内のすべての物理ポートおよび PortChannel が SPAN 送信元として含まれます。任意の送信元インターフェイスで、入力方向、出力方向、または両方向の SPAN トラフィックを選択できます。

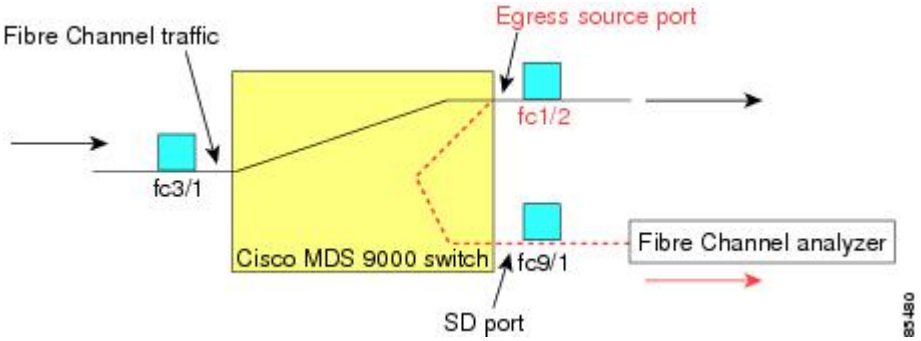
- 入力送信元（Rx）：この送信元インターフェイスを介してスイッチ ファブリックに入るトラフィックは、SD ポートにスパン（コピー）されます（図 15 : 入力方向からの SPAN トラフィック （310 ページ） を参照）。

図 *15 :* 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 16 : 出力方向からの SPAN トラフィック （311 ページ） を参照）。

図 *16* : 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）
  - インターフェイスを介してスーパーバイザ モジュールからスイッチ ファブリックに送信されるファイバ チャネル トラフィックを、入力トラフィックと言います。入力送信元ポートとして sup-fc0 が選択されている場合は、このトラフィックがスパンされます。
  - sup-fc0 インターフェイスを介してスイッチ ファブリックからスーパーバイザ モジュールに送信されるファイバ チャネル トラフィックを、出力トラフィックと言います。出力送信元ポートとして sup-fc0 が選択されている場合は、このトラフィックがスパンされます。
- ポートチャネル
  - PortChannel 内のすべてのポートが含まれ、送信元としてスパンされます。
  - PortChannel 内のポートを SPAN 送信元として個別に指定できません。設定済みの SPAN 固有のインターフェイス情報は廃棄されます。

- IPS モジュール固有のファイバ チャネル インターフェイス
  - iSCSI インターフェイス
  - FCIP インターフェイス

（注） Cisco MDS 9700 シリーズ スイッチで、iSCSI ポートは使用可能な送信元インターフェイス タイプに適用されません。

# 送信元としての VSAN

SPAN 送信元とは、トラフィックをモニタリングできるインターフェイスを表します。送信元としてVSANが指定されている場合は、このVSAN内のすべての物理ポートおよびPortChannelがSPAN送信元として含まれます。TEポートが含まれるのは、TEポートのポートVSANが送信元 VSAN と一致する場合だけです。設定済みの許可 VSAN リストに送信元 VSAN が含まれている場合でも、ポート VSAN が異なっていれば、TE ポートは除外されます。

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

# SPAN セッション

各SPANセッションは、1つの宛先と複数の送信元の対応関係、およびネットワーク トラフィックをモニタするために指定されたその他のパラメータを表します。1 つの宛先を 1 つ以上の SPAN セッションで使用することができます。スイッチには最大 16 個の SPAN セッションを設定できます。各セッションには複数の送信元ポートおよび 1 つの宛先ポートを設定できます。

SPAN セッションをアクティブにするには、少なくとも 1 つの送信元および SD ポートを起動して、機能させる必要があります。このようにしないと、トラフィックが SD ポートに転送されません。

ヒント 1 つの送信元を 2 つのセッションで共有することは可能です。ただし、各セッションはそれぞれ異なる方向（1 つは入力、1 つは出力）でなければなりません。

SPAN セッションを一時的に非アクティブ（一時停止）にできます。この期間中、トラフィック モニタリングは停止します。

（注） Cisco MDS 9250i マルチ サービス ファブリック スイッチでは、SPAN ポートが着信フレームのバーストを維持できない場合にパケットのドロップが発生します。これらのパケットのドロップを回避するには、SPAN 配信ポートの速度が送信元ポートの最高速度と等しくなる必要があります。ただし、送信元が FCIP インターフェイスの場合は、FCIP インターフェイスが 10 G のイーサネット物理インターフェイス上で実行されているため、SPAN宛先ポートの速度は10 G 以上にする必要があります。

# フィルタの指定

VSANベースのフィルタリングを実行すると、指定されたVSAN上でネットワーク トラフィックを選択的にモニタできます。このVSANフィルタは、セッション内のすべての送信元に適用できます（を参照）。スパンされるのは、このフィルタ内の VSAN だけです。

指定されたセッション内のすべての送信元に適用されるセッションVSANフィルタを指定できます。これらのフィルタは双方向であり、セッションに設定されたすべての送信元に適用されます。各 SPAN セッションは、1 つの宛先と複数の送信元の対応関係、およびネットワーク トラフィックをモニタするために指定されたその他のパラメータを表します。

# SD ポートの特性

SD ポートには、次の特性があります。

- BB_credits を無視します。
- 出力（Tx）方向のデータ トラフィックだけを許可します。
- デバイスまたはアナライザを物理的に接続する必要はありません。
- 1 Gbps または 2 Gbps の速度だけをサポートします。自動速度オプションは使用できません。
- 複数のセッションで同じ宛先ポートを共有できます。
- SDポートがシャットダウンされると、共有されたすべてのセッションがSPANトラフィックの生成を停止します。
- 発信フレームは、Extended Inter-Switch Link（EISL）フォーマットでカプセル化することができます。
- SD ポートにはポート VSAN がありません。
- Storage Services Module（SSM）を使用した SD ポートの設定はできません。
- SPAN セッションで使用中のポート モードは、変更できません。

（注）
- If you need to change an SD port mode to another port mode, first remove the SD port from all sessions and then change the port mode using the **switchport mode** command.
- Cisco MDS 9700 シリーズ スイッチ、SD ポートには、2 のみ Gbps、4 Gbps、8 Gbps、および 16 Gbps の速度がサポートされています。The auto speed option is not allowed

# 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,
```

Cisco MDS 9700 シリーズ スイッチ：

```
switch(config-if)# monitor session 1
switch(config-monitor)# source interface fc5/1
switch(config-monitor)# destination interface fc2/9
switch(config-monitor)# no shut
switch(config-monitor)# show monitor session all
session 1
---------------
ssn direction : both
state : up
source intf :
rx : fc5/1
tx : fc5/1
both : fc5/1
source VLANs :
rx :
tx :
both :
source exception :
rate-limit : Auto
filter VLANs : filter not specified
destination ports : fc2/9
```

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

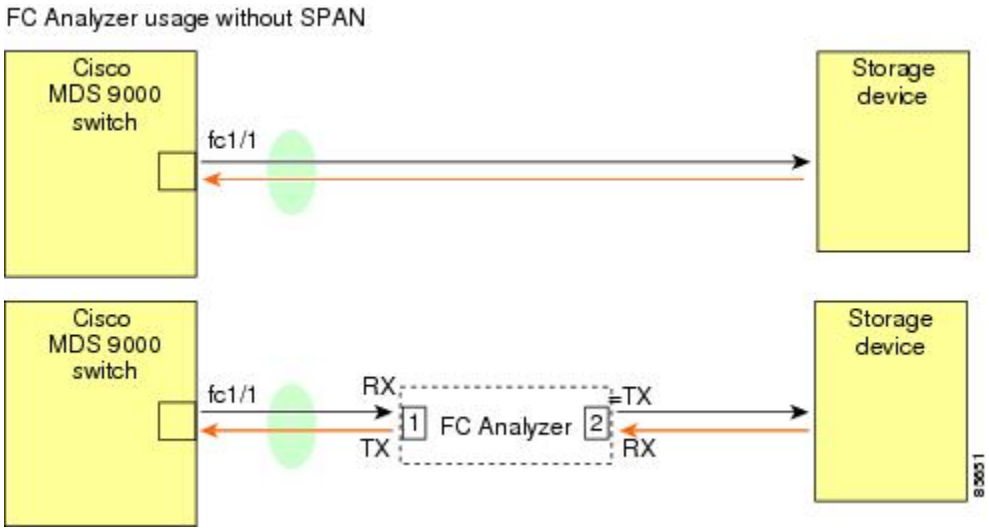
SPAN を使用すると、トラフィックを中断することなく、インターフェイス上でトラフィックをモニタできます。トラブルシューティング時においてトラフィックを中断することによって問題の環境が変更され、問題の再現が困難になる場合には、この機能が特に役立ちます。次の 2 つの方法のいずれかでトラフィックをモニタできます。

- SPAN を使用しない場合
- SPAN を使用する場合

# SPAN を使用しないモニタリング

別のスイッチまたはホストに接続された Cisco MDS 9000 ファミリ スイッチのインターフェイス fc1/1 を使用して、トラフィックをモニタできます。インターフェイス fc1/1 を通るトラフィックを分析するには、スイッチとストレージ デバイスをファイバ チャネル アナライザで物理的に接続する必要があります（図 17 : 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 （316 ページ） を参照）。

**図 *17 : SPAN* を使用しない場合のファイバ チャネル アナライザの使用方法**




この接続タイプには、次のような制約があります。

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

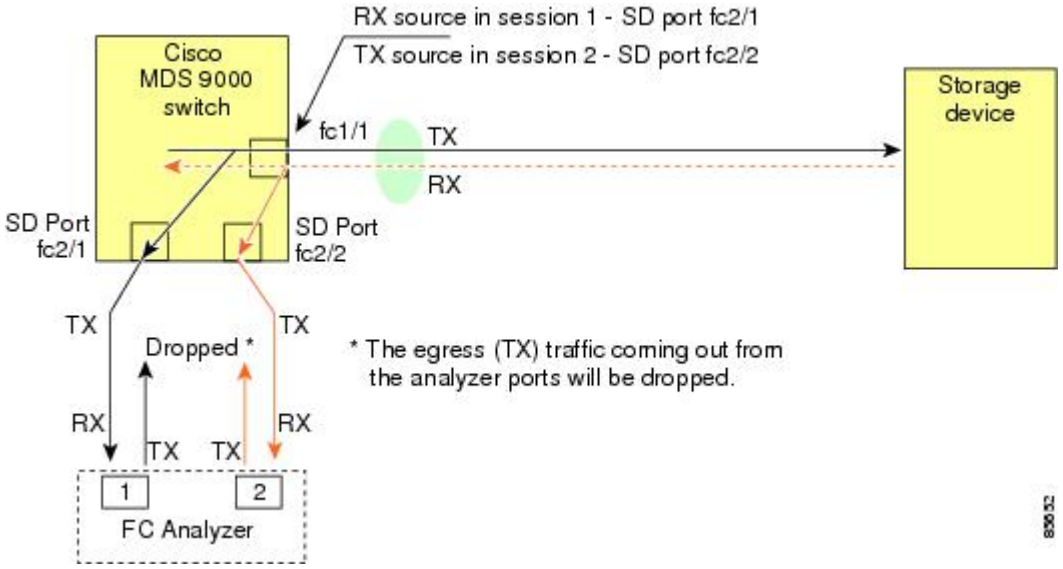
# SPAN を使用するモニタリング

SPAN を使用すると、前述のトラフィック（図 17 : 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 （316 ページ） を参照）をトラフィックの中断なしでキャプチャできます。ファイバ チャネル アナライザはポート 1 の入力（Rx）リンクを使用して、インターフェイス fc1/1 から送信されるすべてのフレームをキャプチャします。また、ポート 2 の入力リンクを使用して、インターフェイス fc1/1 へのすべての入力トラフィックをキャプチャします。

SPAN を使用すると、SD ポート fc2/2 で fc1/1 の入力トラフィックをモニタしたり、SD ポート fc2/1 の出力トラフィックをモニタすることができます。このトラフィックは、FC アナライザ

でシームレスにキャプチャされます（図 18 : 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 （317 ページ） を参照）。

図 *18 : SPAN* を使用した場合のファイバ チャネル アナライザの使用方法

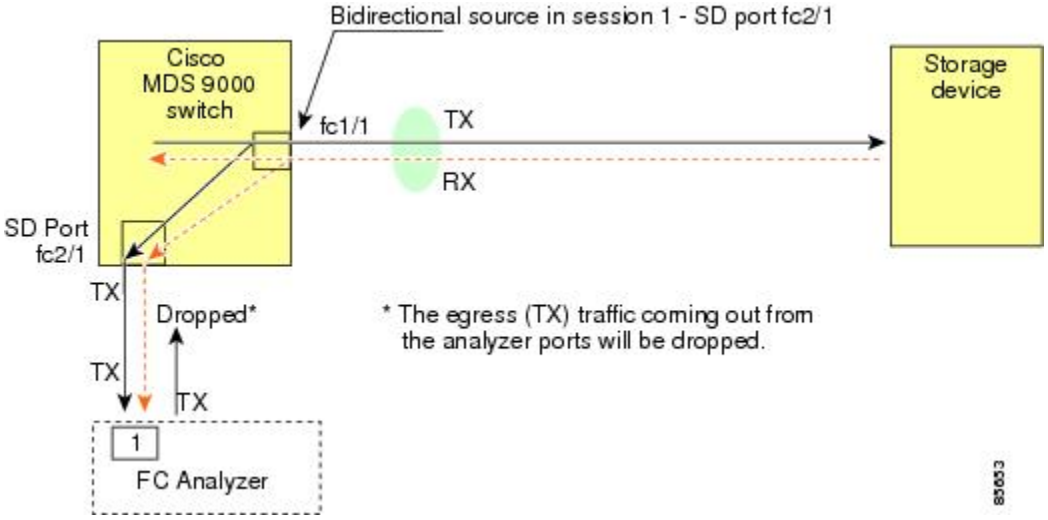



# 単一 SD ポートによるトラフィックのモニタ

任意のインターフェイス上で双方向トラフィックをモニタする場合、SD ポートを 2 つ使用する必要はありません（図 18 : 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 （317 ページ） を参照）。同じ SD ポート fc2/1 でこのインターフェイスのトラフィックをモニタすることにより、SD ポートおよびファイバ チャネル アナライザ ポートを 1 つずつ使用することができます。

図 19 : 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 （318 ページ） に、宛先ポート fc2/1 および送信元インターフェイス fc1/1 を含む 1 つのセッションを使用して、入力および出力方向のトラフィックをキャプチャする SPAN 設定を示します。この設定には、図 18 : 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 （317 ページ） に示された設定よりも多くの利点があり、費用対効果に優れています。完全な 2 ポート アナライザを使用する代わりに、1 つの SD ポートとアナライザ上の 1 つのポートが使用されます。

図 *19 : 単一 SD* ポートを使用した場合のファイバ チャネル アナライザ

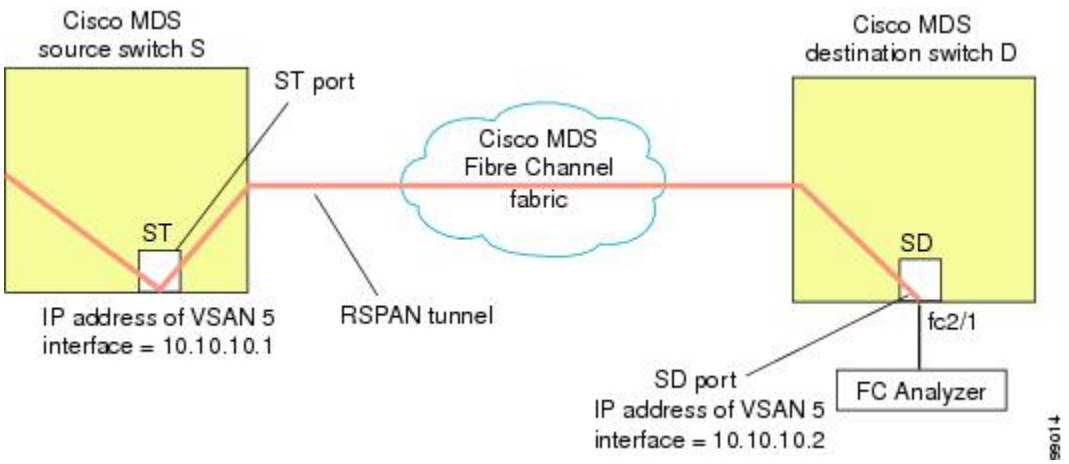



この設定を使用するには、キャプチャされたすべてのフレームの入出力トラフィックを区別する機能がアナライザに必要です。

# SD ポート設定

The SD port in the destination switch enables the FC analyzer to receive the RSPAN traffic from the Fibre Channel tunnel. 図 20 : RSPAN トンネル設定 （318 ページ） depicts an RSPAN tunnel configuration, now that tunnel destination is also configured.

図 *20 : RSPAN* トンネル設定

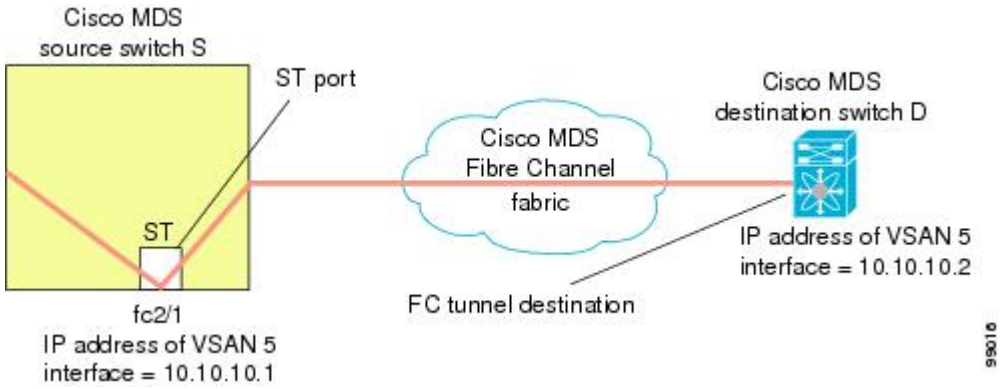



（注） Storage Services Module（SSM）を使用した SD ポートの設定はできません。

# FC トンネルのマッピング

The **tunnel-id-map** option specifies the egress interface of the tunnel at the destination switch (see 図 21 : FC トンネル設定 （319 ページ）).

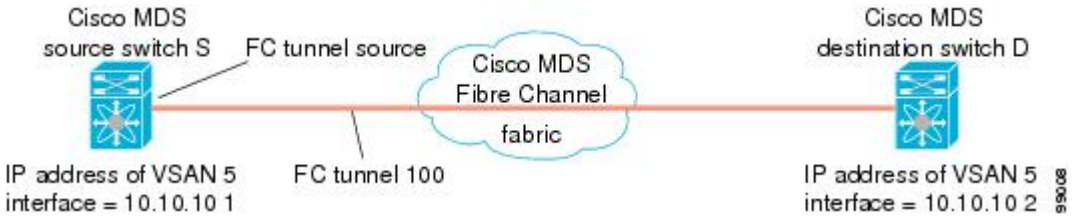
図 *21 : FC* トンネル設定




# VSAN インターフェイスの作成

図 22 : FC トンネル設定 （319 ページ） に、基本的な FC トンネル設定を示します。

図 *22 : FC* トンネル設定




（注） この例では、VSAN 5 が VSAN データベースですでに設定されているものとします。

# リモート SPAN

（注） リモート SPAN は HP c クラス BladeSystem の Cisco ファブリック スイッチ、IBM BladeSystem の Cisco ファブリック スイッチ、Cisco ファブリック スイッチ 9250i、および Cisco ファブリック スイッチ 9100S ではサポートされていません。

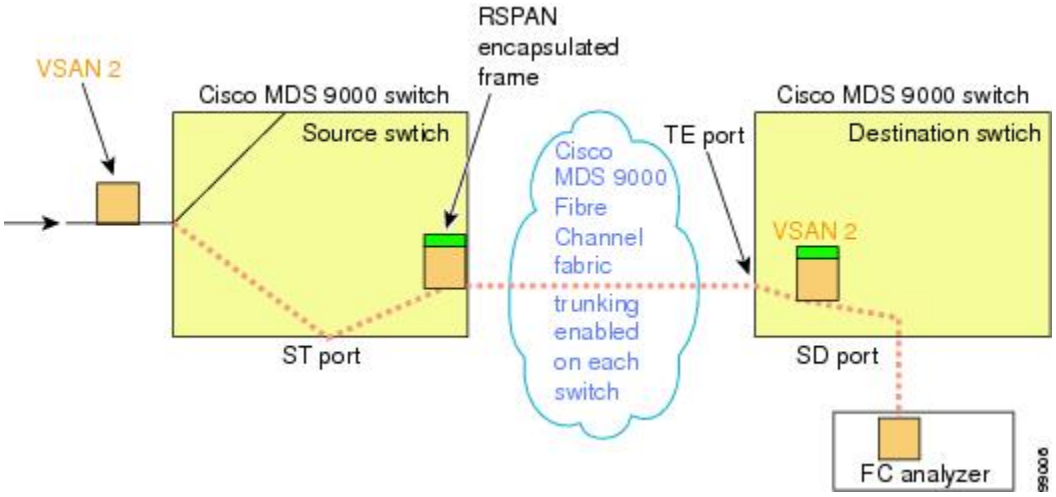
リモート SPAN（RSPAN）機能により、ファイバ チャネル ファブリック内の 1 台以上の送信元スイッチで配信される 1 つ以上の SPAN 送信元のトラフィックをリモートでモニタできるよ

うになります。SPAN 宛先（SD）ポートは、宛先スイッチ内でリモート モニタリング用に使用されます。宛先スイッチは、一般に送信元スイッチとは別に用意されますが、同じファイバ チャネル ファブリックに接続されます。Cisco MDS 送信元スイッチでトラフィックをモニタするのと同様に、任意のリモートの Cisco MDS 9000 ファミリ スイッチまたはディレクタでトラフィックを複製し、モニタすることができます。

RSPAN 機能は他の機能に割り込むことなく、SPAN 送信元ポートのネットワーク トラフィックのスイッチングに影響しません。リモート スイッチ上でキャプチャされたトラフィックは、送信元スイッチから宛先スイッチに至るまでの経路上にあるすべてのスイッチ上でトランキングがイネーブルにされているファイバ チャネル ファブリック上をトンネリングされます。ファイバ チャネル トンネルは、トランク化された ISL（TE）ポートを使用して構造化されます。TE ポート以外にも、RSPAN 機能では他に 2 つのインターフェイス タイプが使用されます（図 23 : RSPAN の送信 （320 ページ） を参照）。

- SD ポート：FC アナライザがリモート SPAN トラフィックを取得するために使用できるパッシブ ポート。
- ST ポート：SPAN トンネル（ST）ポートは、RSPAN ファイバ チャネル トンネル用の送信元スイッチ内の入口ポートです。ST ポートは、特別な RSPAN ポートであり、通常のファイバ チャネル トラフィックに使用することはできません。

**図 *23 : RSPAN* の送信**




# RSPAN の使用の利点

RSPAN 機能には、次の利点があります。

- 遠隔地での中断のないトラフィック モニタリングが可能になります。
- 複数のスイッチ上でリモート トラフィックをモニタするために 1 つの SD ポートを使用することにより、費用対効果に優れたソリューションを提供します。
- 任意のファイバ チャネル アナライザで動作します。
- Cisco MDS 9000 ポート アナライザ アダプタと互換性があります。

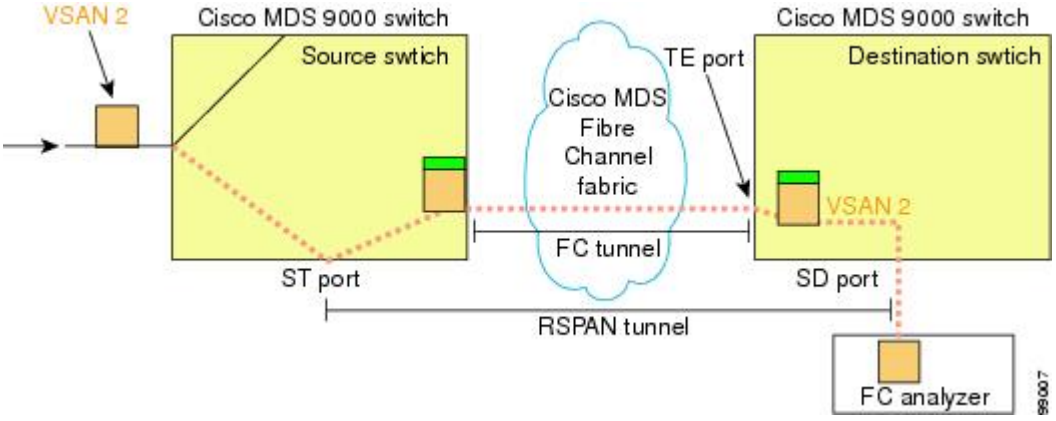
- 送信元スイッチ内のトラフィックに影響を与えません。ただし、ファブリック内の他のポートと ISL 帯域幅を共有します。

# FC トンネルと RSPAN トンネル

FC トンネルは、送信元スイッチと宛先スイッチの間の論理的なデータ パスです。FC トンネルは、送信元スイッチから開始し、離れた場所にある宛先スイッチで終端します。

RSPAN では、送信元スイッチ内の ST ポートから開始し、宛先スイッチ内の SD ポートで終端する特別なファイバ チャネル トンネル（FC トンネル）が使用されます。FC トンネルを送信元スイッチ内の ST ポートにバインドし、それと同じ FC トンネルを宛先スイッチ内の SD ポートにマッピングする必要があります。マッピングとバインディングが設定されると、その FC トンネルは RSPAN トンネルと呼ばれます（図 24 : FC トンネルと RSPAN トンネル （321 ページ） を参照）。

**図 *24 : FC* トンネルと *RSPAN* トンネル**



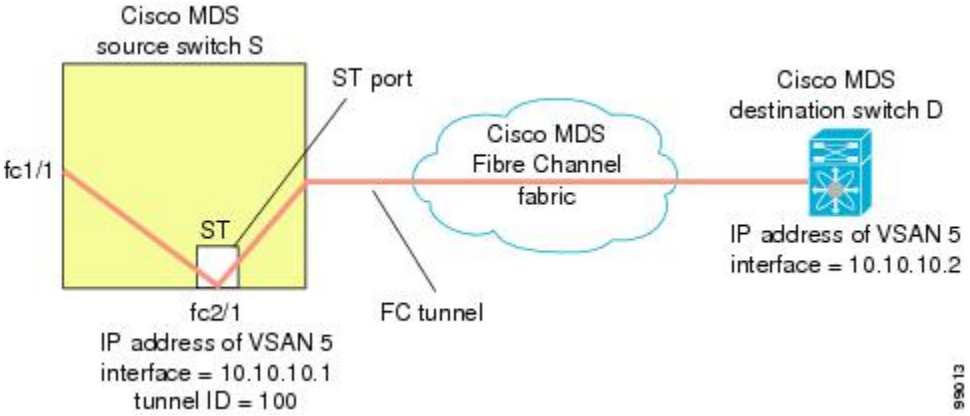

# ST ポート設定

（注） Cisco MDS 9700 シリーズ スイッチで、SPAN トンネル ポート（ST ポート）はサポートされていません。

FC トンネルを作成した後、送信元スイッチにおいて、その FC トンネルにバインドされるように ST ポートを設定する必要があります。バインディングとマッピングが完了すると、その FC トンネルは RSPAN トンネルになります。

図 25 : FC トンネルのバインディング （322 ページ） に、基本的な FC トンネル設定を示します。

図 *25 : FC* トンネルのバインディング




# ST ポートの特性

ST ポートには、次の特性があります。

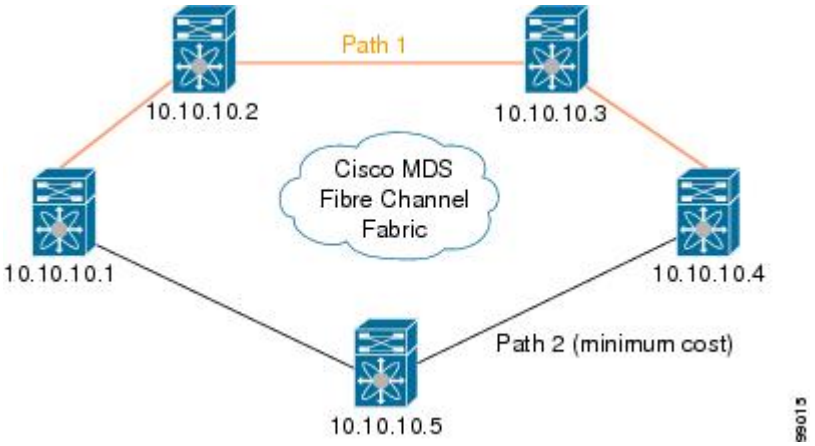
- ST ポートは、FC フレームの RSPAN カプセル化を実行します。
- ST ポートは、BB_credit を使用しません。
- 1 つの ST ポートは、1 つの FC トンネルにしかバインドできません。
- ST ポートは、RSPAN トラフィックの伝送以外には使用できません。
- ST ポートは、Storage Services Module（SSM）を使用して設定することはできません。

# 明示的なパスの作成

You can specify an explicit path through the Cisco MDS Fibre Channel fabric (source-based routing), using the **explicit-path** option. たとえば、トンネル宛先に対して複数のパスがある場合、このオプションを使用して、FC トンネルが宛先スイッチまで常に 1 つのパスを使用するように指定できます。この場合、ソフトウェアは、他のパスが使用可能であっても、この指定されたパスを使用します。

このオプションが特に役立つのは、使用可能なパスが他にあるときでも特定のパスにトラフィックを誘導したい場合です。RSPAN の場合、RSPAN トラフィックが既存のユーザ トラフィックの妨げにならないように、明示的なパスを指定できます。1 台のスイッチ内で作成できる明示的なパスの数に制限はありません（図 26 : 明示的なパスの設定 （323 ページ） を参照）。

図 *26 :* 明示的なパスの設定




# 注意事項と制約事項

## Cisco MDS 9700 シリーズ スイッチのガイドライン

次の注意事項と制約事項は、Cisco MDS 9700 シリーズ スイッチに適用されます。

- Cisco MDS 9700 シリーズ スイッチで SPAN はモニタに置き換えられます。
- Cisco MDS 9700 シリーズ スイッチで SPAN トンネル ポート（ST ポート）はサポートされていません。
- Cisco MDS 9700 シリーズ スイッチで RSPAN はリモート モニタに置き換えられます。
- Cisco MDS 9700 シリーズ スイッチの第二世代ファブリック スイッチはサポートされていません

## SPAN 設定時の注意事項

SPAN を設定する場合は、次の注意事項と制限が適用されます。

- 複数の入力（Rx）送信元には、最大 16 個の SPAN セッションを設定できます。
- 送信元ポートの数は16以下にする必要があります。ただし、SPANまたはモニタセッションあたり 2 つの送信元ポートのみ最大数を設定することをお勧めします。
- 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。

（注） これは Cisco MDS 9700 シリーズ スイッチには適用されません。

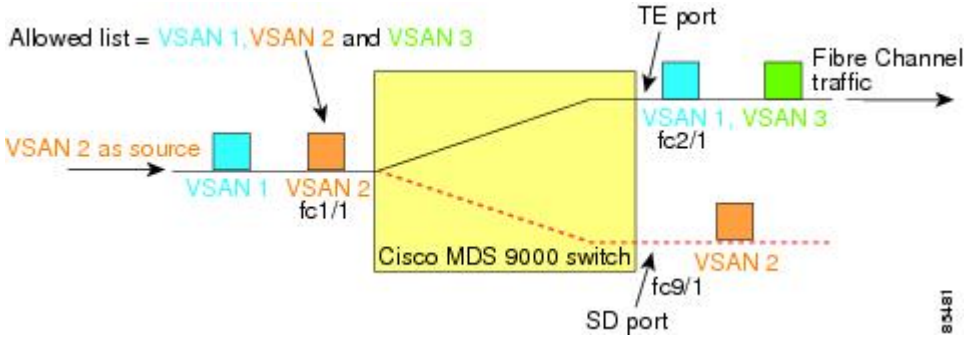
- 送信元の合計帯域幅が宛先ポートの速度を超えると、SPAN フレームは廃棄されます。
- 送信元ポートで廃棄されたフレームは、スパンされません。
- SPAN は、Fibre Channel over Ethernet（FCoE）ネットワーク内のポーズ フレームをキャプチャしません。仮想拡張（VE）ポートから送信されるポーズ フレームは、最も外側の MAC レイヤで生成および終端が行われるためです。FCoE の詳細については、『Cisco NX-OS FCoE Configuration Guide for Cisco Nexus 7000 and Cisco MDS 9500』を参照してください。

# VSAN を送信元として設定する場合の注意事項

VSAN を送信元として設定する場合は、次の注意事項に従ってください。

- 送信元 VSAN に含まれるすべてのインターフェイスのトラフィックは、入力方向の場合にだけスパンされます。
- VSAN が送信元として指定されている場合は、VSAN に含まれるインターフェイス上でインターフェイスレベルの SPAN 設定を実行することができません。設定済みの SPAN 固有のインターフェイス情報は廃棄されます。
- VSAN 内のインターフェイスが送信元として設定されている場合は、この VSAN を送信元として設定できません。VSAN を送信元として設定する前に、まずこのようなインターフェイス上の既存の SPAN 設定を削除する必要があります。
- Interfaces are only included as sources when the port VSAN matches the source VSAN. 図 27 : 送信元としての VSAN （325 ページ） displays a configuration using VSAN 2 as a source:
  - 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 *27*：送信元としての *VSAN*




この設定では、次のようになります。

- 送信元としての VSAN 2 には、ポート VSAN 2 を持つ TE ポート fc1/1 だけが含まれます。
- ポート VSAN が VSAN 1 と一致しないため、送信元としての VSAN 1 には TE ポート fc1/1 が含まれません。

# フィルタを指定する場合の注意事項

SPAN フィルタには、次の注意事項が適用されます。

- PortChannel 設定は、PortChannel 内にあるすべてのポートに適用されます。
- フィルタが指定されていない場合は、該当するインターフェイスのすべてのアクティブ VSAN からのトラフィックがデフォルトでスパンされます。
- セッションでは任意の VSAN フィルタを指定できますが、トラフィックをモニタできるのは、該当するポート VSAN 上、または該当するインターフェイスで許可されているアクティブ VSAN 上だけです。

# RSPAN 設定時の注意事項

SPAN を設定する場合は、次の注意事項が適用されます。

- RSPAN トンネルのエンドツーエンドのパス上にあるすべてのスイッチは、Cisco MDS 9000 ファミリに属している必要があります。
- RSPAN トラフィックが含まれるすべての VSAN がイネーブルになっている必要があります。RSPAN トラフィックが含まれる VSAN がイネーブルになっていないと、そのトラフィックはドロップされます。
- RSPAN が実装されるファイバ チャネル トンネルのエンドツーエンドのパス内にある各 スイッチ上で次の設定を実行する必要があります。
  - トランキングをイネーブルにし（デフォルトではイネーブル）、トランク対応リンクをパス内の最低コスト リンクにする必要があります。
  - VSAN インターフェイスを設定する必要があります。

- ファイバ チャネル トンネル機能をイネーブルにする必要があります（デフォルトではディセーブル）。
- IP ルーティングをイネーブルにする必要があります（デフォルトではディセーブル）。

（注） IP アドレスが VSAN と同じサブネット内である場合は、トラフィックがスパンされるすべての VSAN に対して VSAN インターフェイスを設定する必要はありません。

- 単一のファイバ チャネル スイッチ ポートを ST ポート機能専用にする必要があります。
- モニタ対象のポートを ST ポートとして設定してはなりません。
- FC トンネルの IP アドレスは、VSAN インターフェイスと同じサブネット内に存在する必要があります。

# SPAN および RSPAN のデフォルト設定

表 40 : SPAN パラメータのデフォルト設定値 （326 ページ） に、SPAN パラメータのデフォルト設定を示します。

**表 *40 : 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<br>（注） Cisco MDS 9700 シリーズ スイッチでのモニタ セッションのデフォルト値がシャット ダウンします。 |
| フィルタが指定されていない場合 | SPAN トラフィックには、すべてのアクティブ VSAN から特定のインターフェイスを経由するトラフィックが含まれます。 |
| カプセル化 | ディセーブル |
| SD ポート | 出力フレーム形式はファイバ チャネルです。 |

表 41 : RSPAN パラメータのデフォルト設定値 （326 ページ） RSPAN パラメータのデフォルト設定を示します。

**表 *41 : RSPAN* パラメータのデフォルト設定値**

| パラメータ | デフォルト |
|---|---|
| FC トンネル | 無効 |
| 明示パス | Not configured |

| パラメータ | デフォルト |
|---|---|
| 最小コスト パス | 明示パスが設定されていない場合に使用されます |

# SPAN の設定

SPAN 機能は、Cisco MDS 9000 ファミリ スイッチに特有の機能です。SPAN は、ファイバ チャネル インターフェイスを通じてネットワーク トラフィックをモニタします。

# SPAN の SD ポートの設定

## SPAN モニタリング用 SD ポートの設定

SPAN モニタリングに SD ポートを設定するには、次の手順を実行します。

**手順**

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **interface fc9/1**

指定されたインターフェイスを設定します。

**ステップ 3** switch(config-if)# **switchport mode SD**

インターフェイス fc9/1 の SD ポート モードを設定します。

**ステップ 4** switch(config-if)# **switchport speed 1000**

ST ポート速度を 1000 Mbps に設定します。

（注） Cisco MDS 9700 シリーズ スイッチでは、スイッチ ポート速度は 8000 Mbps です。

**ステップ 5** switch(config-if)# **no shutdown**

このインターフェイスを介してトラフィック フローを有効にします。

## SPAN セッション設定

SPAN セッションを設定する手順は、次のとおりです。

手順

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **span session 1**

switch(config-span) #

Configures the specified SPAN session (1). セッションが存在しない場合は、作成されます。

（注） Cisco MDS 9700 シリーズ スイッチでの SPAN は、モニタに置き換えられます。

**ステップ 3** switch(config)# **no span session 1**

指定された SPAN セッション (1) を削除します。

**ステップ 4** switch(config-span) # **destination interface fc9/1**

Configures the specified destination interface (fc 9/1) in a session.

**ステップ 5** switch(config-span) # **no destination interface fc9/1**

指定の接続先インターフェイス (fc 9/1) を削除します。

**ステップ 6** switch(config-span) # **source interface fc7/1**

両方向で送信元 (fc7/1) インターフェイスを設定します。

（注） Cisco MDS 9124 ファブリック スイッチの SPAN ソースを設定する際、方向 (Rx および Tx) は、明示的に言及する必要があります。

**ステップ 7** switch(config-span) # **no source interface fc7/1**

このセッションから、指定の接続先インターフェイス (fc 7/1) を削除します。

**ステップ 8** switch(config-span) # **source interface sup-fc0**

セッションの送信元インターフェイス (sup fc0) を設定します。

**ステップ 9** switch(config-span) # **source interface fc1/5 - 6, fc2/1 -3**

セッションで指定したインターフェイスの範囲を設定します。

**ステップ 10** switch(config-span) # **source vsan 1-2**

セッションのソース Vsan 1 および 2 を設定します。

**ステップ 11** switch(config-span) # **source interface port-channel 1**

送信元ポート チャネル (ポート チャネル 1) を設定します。

**ステップ 12** switch(config-span) # **source interface fcip 51**

セッションの送信元 FCIP インターフェイスを設定します。

**ステップ 13** switch(config-span) # **source interface iscsi 4/1**

セッションの送信元 iSCSI インターフェイスを設定します。

（注） これは MDS 9700 シリーズ スイッチの適用されません。

**ステップ 14** switch(config-span) # **source interface svc1/1 tx traffic-type initiator**

イニシエータ トラフィック タイプの Tx 方向で送信元 SVC インターフェイスを設定します。

（注） これは MDS 9700 シリーズ スイッチの適用されません。

**ステップ 15** switch(config-span) # **no source interface port-channel 1**

指定された送信元インターフェイス (ポート チャネル 1) を削除します。

**ステップ 16** switch(config-span) # **shutdown**

セッションが一時的に中断します。

（注） これは、MDS 9700 シリーズ スイッチに適用されます。

## SPAN フィルタの設定

To configure a SPAN filter, follow these steps:

**手順**

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **span session 1**

switch(config-span)#

指定したセッション（1）を設定します。

（注） Cisco MDS 9700 シリーズ スイッチでの SPAN は、モニタ セッション 1 に置き換えられます。

**ステップ 3** switch(config-span) # **source interface fc9/1 tx**

出力 (Tx) 方向で送信元 fc9/1 インターフェイスを設定します。

**ステップ 4** switch(config-span) # **source filter vsan 1-2**

セッションのフィルタとして Vsan 1 および 2 を設定します。

**ステップ 5** switch(config-span) # **source interface fc7/1 rx**

入力 (Rx) 方向には、送信元 fc7/1 インターフェイスを設定します。

# 第 2 世代ファブリック スイッチ用の SPAN の設定

シスコの第 2 世代ファブリック スイッチ（MDS 9124 など）では、SPAN セッションが両方向（Rx と Tx）でサポートされます。

（注） 第 2 世代ファブリック スイッチを使用する場合、アクティブな SPAN セッションは 1 つしか作成できません。

複数の SPAN 送信元インターフェイスを Rx 方向と Tx 方向で指定できます。ただし、コマンドの最後に、方向を明示的に記載する必要があります。SPAN は、方向を指定するに失敗した送信元インターフェイス コンフィギュレーションを拒否します。

## 入力 SPAN セッションの設定

入力 SPAN セッションを設定するには、これらの手順に従います。

**手順**

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **span session 1**

switch(config-span)#

指定したセッション（1）を設定します。

**ステップ 3** switch(config-span)# **destination interface fc1/1**

インターフェイス fc1/1 を宛先として設定します。

**ステップ 4** switch(config-span)# **source interface fc1/2 rx**

入力方向のソース インターフェイス fc1/2 を設定します。

## SPAN セッション出力設定

SPAN セッション出力を設定する手順は、次のとおりです。

手順

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **span session 1**

switch(config-span)#

指定したセッション（1）を設定します。

**ステップ 3** switch(config-span)# **destination interface fc1/1**

インターフェイス fc1/1 を宛先として設定します。

**ステップ 4** switch(config-span)# **source interface fc1/2 tx**

送信元インターフェイス fc1/2 を出力方向に設定します。

## 例

この例は、複数の SPAN インターフェイスの Cisco MDS 9124 を設定する方法を示しています。

```
switch(config-span)# span session 1
switch(config-span)# destination interface fc1/1
switch(config-span)# source interface fc1/2 rx
switch(config-span)# source interface fc1/2 tx
```

第 2 世代ファブリック スイッチでは、出力方向において 1 つの VSAN に対してのみ VSAN フィルタがサポートされます。この制限は、入力方向には適用されません。たとえば、TE ポートのインターフェイスで 1 ～ 5 のアクティブな VSAN が存在する場合、VSAN 2 に対して VSAN フィルタを指定すると、VSAN 2 上のトラフィックのみがフィルタリングされます。

```
switch(config-span)# span session 1
switch(config-span)# source filter vsan 2
switch(config-span)# destination interface fc1/1
switch(config-span)# source interface fc1/2 tx
```

ただし、VSAN 1 ～ 2 の VSAN フィルタを指定する場合、すべての VSAN のトラフィック（1 ～ 5）がフィルタリングされ、フィルタが不要になります。

```
switch(config-span)# span session 1
switch(config-span)# source filter vsan 1-2
switch(config-span)# destination interface fc1/1
switch(config-span)# source interface fc1/2 tx
```

# SPAN セッションの中断と再アクティブ化

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。

SPANセッション フィルタを一時的に中断または再アクティブ化するには、次の手順に従います。

**手順**

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **span session 1**

switch(config-span)#

指定したセッション（1）を設定します。

**ステップ 3** switch(config-span)# **suspend**

セッションが一時的に中断します。

**ステップ 4** switch(config-span)# **no suspend**

セッションを再アクティブ化します。

# フレームのカプセル化

フレームのカプセル化機能は、デフォルトでは無効です。カプセル化機能を有効にすると、すべての発信フレームがカプセル化されます。

The **switchport encap eisl** command only applies to SD port interfaces. If encapsulation is enabled, you see a new line ( Encapsulation is eisl ) in the **show interface** *SD_port_interface* command output.

発信フレーム（オプション）をカプセル化するには、次の手順を実行します。

**手順**

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **interface fc9/32**

指定されたインターフェイスを設定します。

**ステップ 3** switch(config-if)# **switchport mode SD**

インターフェイス fc9/32 の SD ポート モードを設定します。

**ステップ 4** switch(config-if)# **switchport encap eisl**

この SD ポートのカプセル化のオプションを有効にします。

**ステップ 5** switch(config-if)# **no switchport encap eisl**

カプセル化オプションを無効（デフォルト）にします。

# SPAN を使用したファイバ チャネル アナライザの設定

送信元と宛先インターフェイスでの SPAN の設定、次の手順に従います。

**手順**

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **span session 1**

switch(config-span) #

SPAN セッションの 1 を作成します。

**ステップ 3** switch(config-span) ## **destination interface fc2/1**

宛先インターフェイス fc2/1 を設定します。

**ステップ 4** switch(config-span) # **source interface fc1/1 rx**

Configures the source interface fc1/1 in the ingress direction.

**ステップ 5** switch(config)# **span session 2**

switch(config-span) #

SPAN セッション 2 を作成します。

**ステップ 6** switch(config-span) ## **destination interface fc2/2**

宛先インターフェイス fc2/2 を設定します。

**ステップ 7** switch(config-span) # **source interface fc1/1 tx**

送信元インターフェイス fc1/1 を出力方向に設定します。

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（ の例を使用）、次の手順を実行します。

手順

**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。

## 構成単一 SD ポートによるトラフィックのモニタの設定

To configure SPAN on a single SD port, follow these steps:

手順

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **span session 1**

switch(config-span) #

SPAN セッションの 1 を作成します。

**ステップ 3** switch(config-span) ## **destination interface fc2/1**

宛先インターフェイス fc2/1 を設定します。

**ステップ 4** switch(config-span) # **source interface fc1/1**

同じ SD ポートで送信元インターフェイス fc1/1 を設定します。

# 送信元スイッチの設定

ここでは、送信元スイッチ（スイッチ S）で実行する必要のある作業を示します。

## VSAN インターフェイスの作成

のシナリオで送信元スイッチのVSANインターフェイスを作成するには、次の手順を実行します。

手順

**ステップ 1** switchS# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switchS(config)# **interface vsan 5**

switchS(config-if)#

送信元スイッチ（スイッチ S）で指定した VSAN インターフェイス（VSAN 5）を設定します。

**ステップ 3** switchS(config-if)# **ip address 10.10.10.1 255.255.255.0**

送信元スイッチ（スイッチ S）で IPv4 アドレスおよび VSAN インターフェイス 5 のサブネットを設定します。

**ステップ 4** switchS(config-if)# **no shutdown**

このインターフェイスを介してトラフィック フローを有効にします。

# FC トンネルの有効化

（注）
- FC トンネルは、非トランキング Isl では機能しません。
- インターフェイスは、FC トンネル マッピングは宛先スイッチで設定されるまで、運用することはできません。

FC トンネル機能を有効にするには、次の手順を実行します。

手順

**ステップ 1** スイッチ # **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switchS(config)# **fc-tunnel enable**

FC トンネル機能をイネーブルにします（デフォルトではディセーブル）。

（注） ファブリックのエンドツー エンド パス内の各スイッチでは、この機能を有効にすることを確認します。

# FC トンネルの開始

のシナリオで送信元スイッチの FC トンネルを開始するには、次の手順を実行します。

**手順**

**ステップ 1** switchS# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switchS(config)# **interface fc-tunnel 100**

switchS(config-if)#

送信元スイッチ（S）で、FC トンネル（100）を開始します。トンネル ID の範囲は、1 ～ 255 です。

**ステップ 3** switchS(config-if)# **source 10.10.10.1**

送信元スイッチ（スイッチ S）の IPv4 アドレスを FC トンネル（100）にマッピングします。

**ステップ 4** switchS(config-if)# **destination 10.10.10.2**

宛先スイッチ（スイッチ D）の IPv4 アドレスを FC トンネル（100）にマッピングします。

**ステップ 5** switchS(config-if)# **no shutdown**

このインターフェイスを介してトラフィック フローを有効にします。

# ST ポートの設定

（注） ST ポートは、Storage Services Module（SSM）を使用して設定することはできません。

To configure an ST port, follow these steps:

**手順**

**ステップ 1** スイッチ # **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switchS(config)# **interface fc2/1**

指定されたインターフェイスを設定します。

**ステップ 3** switchS(config-if)# **switchport mode ST**

インターフェイス fc2/1 の ST ポート モードを設定します。

**ステップ 4** switchS(config-if)# **switchport speed 2000**

ST ポート速度を 2000 Mbps に設定します。

**ステップ 5** switchS(config-if)# **rspan-tunnel interface fc-tunnel 100**

関連付け、RSPAN トンネル (100) ST ポートにバインドします。

**ステップ 6** switchS(config-if)# **no shutdown**

このインターフェイスを介してトラフィック フローを有効にします。

# FRSPAN セッションの設定

RSPAN セッションは、RSPAN トンネルをされている宛先インターフェイスでの SPAN セッションに似ています。

のシナリオで送信元スイッチに RSPAN セッションを設定するには、次の手順を実行します。

**手順**

**ステップ 1** スイッチ # **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switchS(config)# **span session 2**

switchS(config-span) #

指定された SPAN セッション（2）を設定します。セッションが存在しない場合は、作成されます。セッション ID の範囲は、1 ～ 16 です。

**ステップ 3** switchS(config-span) # **destination interface fc-tunnel 100**

指定された RSPAN トンネル（100）をセッション内で設定します。

**ステップ 4** switchS(config-span) # **source interface fc1/1**

このセッションの送信元インターフェイス（fc1/1）を設定し、インターフェイス fc1/1 から RSPAN トンネル 100 にトラフィックをスパンします。

# すべての中間スイッチの設定

ここでは、RSPAN トンネルのエンドツーエンドのパス内にあるすべての中間スイッチで実行する必要のある作業を示します。

## VSAN インターフェイスの設定

に、宛先スイッチ（スイッチ D）で終端している RSPAN トンネル設定を示します。

（注） この例では、VSAN 5 が VSAN データベースですでに設定されているものとします。

のシナリオで宛先スイッチの VSAN インターフェイスを作成するには、次の手順を実行します。

**手順**

**ステップ 1** switchD# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switchD(config)# **interface vsan 5**

switchD(config-if)#

宛先スイッチ (スイッチ D) で指定した VSAN インターフェイス (VSAN 5) を設定します。

**ステップ 3** switchD(config-if)# **ip address 10.10.10.2 255.255.255.0**

宛先スイッチ (スイッチ D) で VSAN インターフェイスの IPv4 アドレスとサブネットを設定します。

**ステップ 4** switchD(config-if)# **no shutdown**

トラフィック フローを有効にすることで、管理上トラフィックトラフィックを許可します (動作状態は up)。

## IP ルーティングの有効化

IP ルーティング機能は、デフォルトではディセーブルになっています。ファブリック内のエンドツーエンドのパス内にある各スイッチ（送信元スイッチと宛先スイッチを含む）において IP ルーティングをイネーブルにする必要があります。この手順は、FC トンネルをセットアップするために必要です。

# 宛先スイッチの設定

ここでは、宛先スイッチ（スイッチ D）で実行する必要のある作業を示します。

## VSAN インターフェイスの設定

に、宛先スイッチ（スイッチ D）で終端している RSPAN トンネル設定を示します。

（注） この例では、VSAN 5 が VSAN データベースですでに設定されているものとします。

## SD ポートの設定

（注） Storage Services Module（SSM）を使用した SD ポートの設定はできません。

のシナリオで SD ポートを設定するには、次の手順を実行します。

**手順**

**ステップ 1** switchD# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switchD(config)# **interface fc2/1**

指定されたインターフェイスを設定します。

**ステップ 3** switchD(config-if)# **switchport mode SD**

インターフェイス fc2/1 の SD ポート モードを設定します。

**ステップ 4** switchD(config-if)# **switchport speed 2000**

ST ポート速度を 2000 Mbps に設定します。

**ステップ 5** switchD(config-if)# **no shutdown**

このインターフェイスを介してトラフィック フローを有効にします。

# FC トンネルのマッピング

のシナリオの宛先スイッチで FC トンネルを修了するには、これらの手順に従います。

### 手順

**ステップ 1** switchD# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switchD(config)# **fc-tunnel tunnel-id-map 100 interface fc2/1**

宛先スイッチ（スイッチ D）で FC トンネル（100）を終了します。トンネル ID の範囲は 1 ～ 255 です。

# 明示的なパスの作成

でのシナリオの明示的なパスを作成するには、次の手順を実行します。

### 始める前に

明示的なパスは送信元スイッチに作成する必要があります。明示的なパスを設定するには、最初にパスを作成し、次にいずれか1つのパスを使用するように設定します。明示的なパスが設定されていない場合は、by default(デフォルトで、デフォルトでは) 最小コストパスが使用されます。明示的なパスが設定されていて、機能している場合は、指定されたパスが使用されます。

### 手順

**ステップ 1** スイッチ # **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switchS(config)# **fc-tunnel explicit-path Path1**

switch(config-explicit-path) #

パス Path 1 に関する明示的なパスのプロンプトが表示されます。

**ステップ 3** switchS(config-explicit-path) # **next-address 10.10.10.2 strict**

switchS(config-explicit-path) # **next-address 10.10.10.3 strict**

switchS(config-explicit-path) # **next-address 10.10.10.4 strict**

VSAN のネクスト ホップのインターフェイスの IPv4 アドレスと、明示的なパスで指定された前のホップに直接接続が必要としないことを指定します。

**ステップ 4** switchS(config)# **fc-tunnel explicit-path Path2**

switch(config-explicit-path) #

Path 2 に関する明示的なパスのプロンプトが表示されます。

**ステップ 5** switchS(config-explicit-path) # **next-address 10.10.10.5 strict**

**例**：

```
switchS(config-explicit-path)# next-address 10.10.10.4 strict
```

VSAN のネクスト ホップのインターフェイスの IPv4 アドレスと、明示的なパスで指定された前のホップに直接接続が必要としないことを指定します。

**ステップ 6** switchS(config)# **fc-tunnel explicit-path Path3**

switch(config-explicit-path) #

Path 3 に関する明示的なパスのプロンプトが表示されます。

**ステップ 7** switchS(config-explicit-path) # **next-address 10.10.10.3 loose**

最小コスト パスを設定 10.10.10.3 IPv4アドレスが存在します。

（注） 、パス 3 は、パス 1 と同じ: パス 1 で 10.10.10.3 が存在します。Using the **loose** option, you can achieve the same effect with one command instead of issuing three commands (using the **strict** option) in Step 3.

## 明示パスの参照

明示パスを参照するには、次の手順を実行します。

**手順**

**ステップ 1** switchS# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switchS(config)# **interface fc-tunnel 100**

パス 1 のトンネル ID を参照します。

**ステップ 3** switchS(config)# **explicit-path Path1**

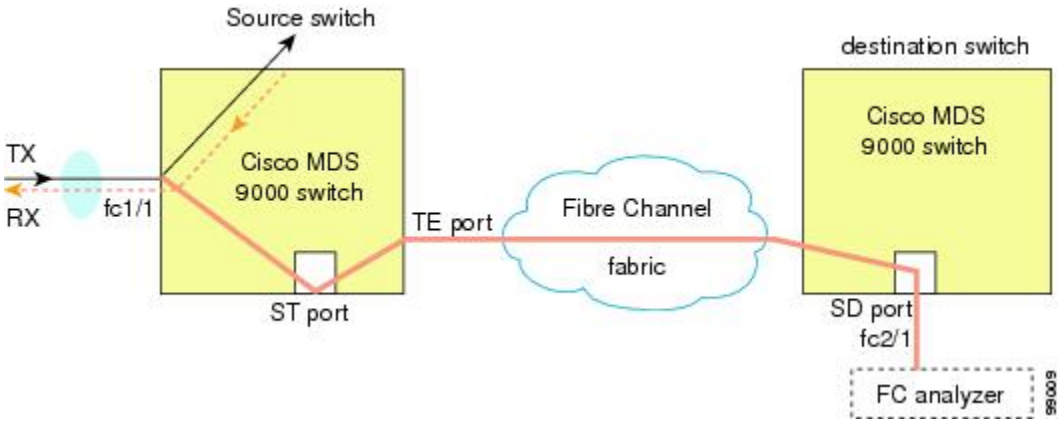
Path1 をトンネル ID にリンクします。

この設定は、RSPANトラフィックで使用されるPath1を明示的に指定します。明示パスおよび送信元ベース ルーティングの詳細については、RFC 3209 を参照してください。

# RSPAN トラフィックのモニタリング

Once the session is configured, other SPAN sources for this session can also be configured as required. 図 28 : 単一の SD ポートを使用して RSPAN トラフィックをモニタするファイバ チャネル アナライザ （342 ページ） shows an RSPAN setup where one session with destination port fc2/1 and source interface fc1/1 is used to capture traffic in both ingress and egress directions.

図 *28 :* 単一の *SD* ポートを使用して *RSPAN* トラフィックをモニタするファイバ チャネル アナライザ




この設定を使用するには、キャプチャされたすべてのフレームの入出力トラフィックを区別する機能がアナライザに必要です。

# SPAN 設定の確認

SPAN の設定情報を表示するには、次のいずれかの作業を行います。

| コマンド | 目的 |
|---|---|
| **show span** | ブリーフ形式で SPAN セッションを表示する<br>（注） In Cisco MDS 9700 Series Switches, **show span** command is replaced by **show monitor** command. |
| **show span session 7** | 特定の SPAN セッションの詳細が表示されます。<br>（注） In Cisco MDS 9700 Series Switches, **show span session 7** command is replaced by **show monitor session 7** command. |
| **show span session** | すべての SPAN セッションを表示します<br>（注） In Cisco MDS 9700 Series Switches, **show span session** command is replaced by **show monitor session all** command. |
| **show int fc9/32** | カプセル化を有効になっている状態で SD ポート インターフェイスが表示されます。 |

| コマンド | 目的 |
|---|---|
| **show interface brief** | ST ポート インターフェイス情報の表示 |
| **show interface fc1/11** | ST ポート インターフェイスの詳細情報を表示します |
| **show fc-tunnel** | FC トンネル ステータスを表示します |
| **show fc-tunnel tunnel-id-map** | FC トンネル出力マッピング情報の表示 |
| **show fc-tunnel explicit-path** | FC トンネルの明示的なマッピング情報の表示 |
| **show interface fc-tunnel 200** | FC トンネル インターフェイスの表示 |

For detailed information about the fields in the output from these commands, refer to the *Cisco MDS 9000 Family Command Reference* .

# SPAN 情報の表示

Use the **show span** command to display configured SPAN information. 次の例を参照してください。

### 簡単な形式での SPAN セッション

次の例では、簡単な形式での SPAN セッションが表示されます。

```
switch# show span session brief
-------------------------------------------------------
 Session  Admin          Oper           Destination
          State          State          Interface
-------------------------------------------------------
 7        no suspend     active         fc2/7
 1        suspend        inactive       not configured
 2        no suspend     inactive       fc3/1
```

### 詳細に指定された SPAN セッション

次の例では、詳細に指定された SPAN セッションが表示されます。

```
switch# show span session 7
Session 7 (active)
   Destination is fc2/7
   No session filters configured
   No ingress (rx) sources
   Egress (tx) sources are
     port-channel 7,
```

### すべての SPAN セッション

次の例では、すべての SPAN セッションが表示されます。

```
switch# show span session
Session 1 (inactive as no destination)
Destination is not specified
   Session filter vsans are 1
   No ingress (rx) sources
   No egress (tx) sources
Session 2 (active)
   Destination is fc9/5
   No session filters configured
   Ingress (rx) sources are
      vsans 1
   No egress (tx) sources
Session 3 (admin suspended)
   Destination is not configured
   Session filter vsans are 1-20
   Ingress (rx) sources are
     fc3/2, fc3/3, fc3/4, fcip 51,
     port-channel 2, sup-fc0,
   Egress (tx) sources are
     fc3/2, fc3/3, fc3/4, sup-fc0,
```

### カプセル化が有効になっている SD ポート インターフェイス

次の例には、カプセル化が有効になっている SD ポート インターフェイスが表示されます。

```
switch# show int fc9/32
fc9/32 is up
    Hardware is Fibre Channel
    Port WWN is 22:20:00:05:30:00:49:5e
    Admin port mode is SD
    Port mode is SD
    Port vsan is 1
    Speed is 1 Gbps
    Receive Buffer Size is 2112
    Encapsulation is eisl
<----------------
Displays the enabled encapsulation status
    Beacon is turned off
    5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
      0 frames input, 0 bytes, 0 discards
        0 CRC,  0 unknown class
        0 too long, 0 too short
      0 frames output, 0 bytes, 0 discards
      0 input OLS, 0 LRR, 0 NOS, 0 loop inits
```

0 output OLS, 0 LRR, 0 NOS, 0 loop inits

# RSPAN 情報の表示

Use the **show** commands to display configured RSPAN information. 次の例を参照してください。

### ST ポート インターフェイス情報

次の例では、ST ポート インターフェイス情報を示します。

```
switch# show interface brief
--------------------------------------------------------------------------------
Interface   Vsan    Admin   Admin   Status      Oper    Oper    Port-channel
                    Mode    Trunk               Mode    Speed
                            Mode                        (Gbps)
--------------------------------------------------------------------------------
fc1/1       1       auto    on      trunking    TE          2       --
...
fc1/14      1       auto    on      trunking    TE          2       --
fc1/15      1       ST      on      up          ST          2       --
...
fc2/9       1       auto    on      trunking    TE          2       port-channel 21
fc2/10      1       auto    on      trunking    TE          2       port-channel 21
...
fc2/13      999     auto    on      up          F           1       --
fc2/14      999     auto    on      up          FL          1       --
fc2/15      1       SD      --      up          SD          2       --
fc2/16      1       auto    on      trunking    TE          2       --
--------------------------------------------------------------------------------
Interface           Status      Speed
                                (Gbps)
--------------------------------------------------------------------------------
sup-fc0             up          1
--------------------------------------------------------------------------------
Interface           Status      IP Address              Speed       MTU
--------------------------------------------------------------------------------
mgmt0               up        172.22.36.175/22          100 Mbps    1500
--------------------------------------------------------------------------------
Interface           Status      IP Address              Speed       MTU--
--------------------------------------------------------------------------------
vsan5               up          10.10.10.1/24           1 Gbps      1500
--------------------------------------------------------------------------------
Interface           Vsan        Admin           Status      Oper    Oper
                                Trunk                       Mode    Speed
                                Mode                                (Gbps)
--------------------------------------------------------------------------------
port-channel 21     1           on              trunking    TE      4
--------------------------------------------------------------------------------
Interface           Status      Dest IP Addr    Src IP Addr     TID    Explicit Path
--------------------------------------------------------------------------------
fc-tunnel 100       up          10.10.10.2      10.10.10.1      100
```

### ST ポート インターフェイスの詳細情報

次の例では、ST ポート インターフェイスの詳細情報を示します。

```
switch# show interface fc1/11
fc1/11 is up
    Hardware is Fibre Channel
    Port WWN is 20:0b:00:05:30:00:59:de
   Admin port mode is ST
    Port mode is ST
    Port vsan is 1
    Speed is 1 Gbps
   Rspan tunnel is fc-tunnel 100
```

```
    Beacon is turned off
    5 minutes input rate 248 bits/sec, 31 bytes/sec, 0 frames/sec
    5 minutes output rate 176 bits/sec, 22 bytes/sec, 0 frames/sec
      6862 frames input, 444232 bytes
        0 discards, 0 errors
        0 CRC, 0 unknown class
        0 too long, 0 too short
      6862 frames output, 307072 bytes
        0 discards, 0 errors
      0 input OLS, 0 LRR, 0 NOS, 0 loop inits
      0 output OLS, 0 LRR, 0 NOS, 0 loop inits
```

### FC トンネル ステータス

次の例では、FC トンネル ステータスを示します。

```
switch# show fc-tunnel
fc-tunnel is enabled
```

### FC トンネル出力マッピング情報

次の例では、FC トンネル出力マッピング情報を示します。

```
switch# show fc-tunnel tunnel-id-map
tunnel id egress interface
    150     fc3/1
    100     fc3/1
```

（注） 複数のトンネル ID を同じインターフェイスで終端させることができます。

### FC トンネルの明示的なマッピング情報

次の例では、FC トンネル マッピング情報を示します。

```
switch# show fc-tunnel explicit-path
Explicit path name: Alternate1
       10.20.1.2 loose
       10.20.1.3 strict
Explicit path name: User2
       10.20.50.1 strict
       10.20.50.4 loose
```

### SPAN マッピング情報

次の例では、SPAN マッピング情報を示します。

```
switch# show span session
Session 2 (active)
```

```
  Destination is fc-tunnel 100
  No session filters configured
  Ingress (rx) sources are
    fc2/16,
  Egress (tx) sources are
    fc2/16,
```

### FC トンネル インターフェイス

次の例では、FC トンネル インターフェイスを示します。

```
switch# show interface fc-tunnel 200
fc-tunnel 200 is up
Dest   IP Addr: 200.200.200.7   Tunnel ID: 200
Source IP Addr: 200.200.200.4   LSP ID: 1
Explicit Path Name:
```

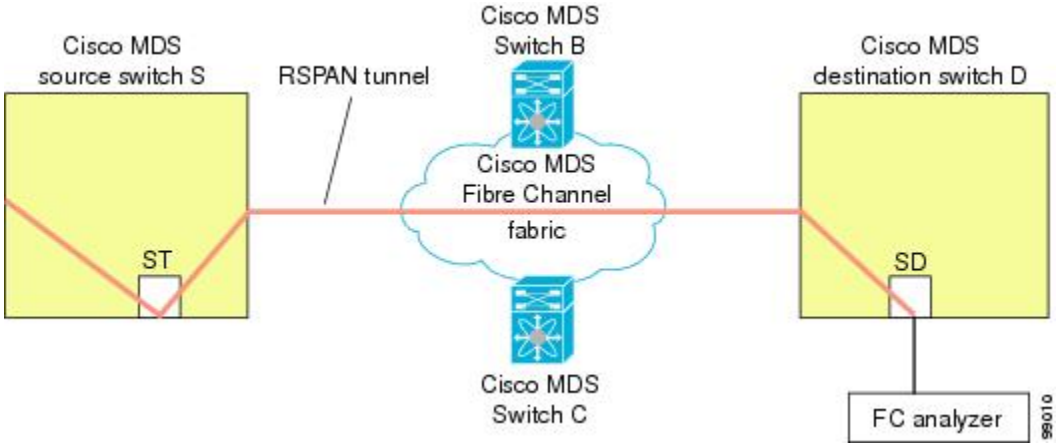
# RSPAN の設定例

（注） RSPAN は、SD ポートがローカル SPAN トラフィックをリモート SPAN トラフィックと一緒に転送するように、ローカル SPAN 機能と組み合わせることができます。ここでは、さまざまな SPAN 送信元とトンネルのシナリオが説明されます。

## 単一の送信元と 1 本の RSPAN トンネル

送信元のスイッチ S と宛先のスイッチ D がファイバ チャネル ファブリックを介して相互接続されます。RSPAN トンネルは SPAN セッションの宛先インターフェイスとして設定され、ST ポートは SPAN トラフィックを RSPAN トンネル経由で転送します（図 29 : 送信元スイッチが 1 台、宛先スイッチが 1 台、トンネルが 1 本の場合の RSPAN シナリオ （348 ページ） を参照）。

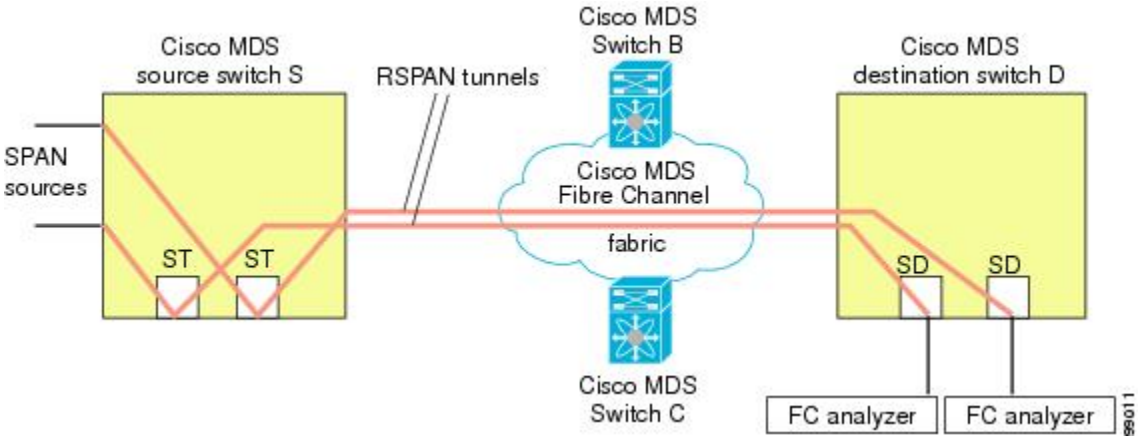
図 29 : 送信元スイッチが 1 台、宛先スイッチが 1 台、トンネルが 1 本の場合の RSPAN シナリオ




# 複数の RSPAN トンネルによる単一の送信元

複数の RSPAN トンネルによる単一の送信元 （348 ページ） スイッチ S および N 間に設定されている異なる 2 個の RSPAN トンネルを表示します。各トンネルは送信元スイッチに関連付けられた ST ポートと、宛先スイッチに別の SD ポートがあります。この設定は、トラブルシューティングの場合に役立ちます。

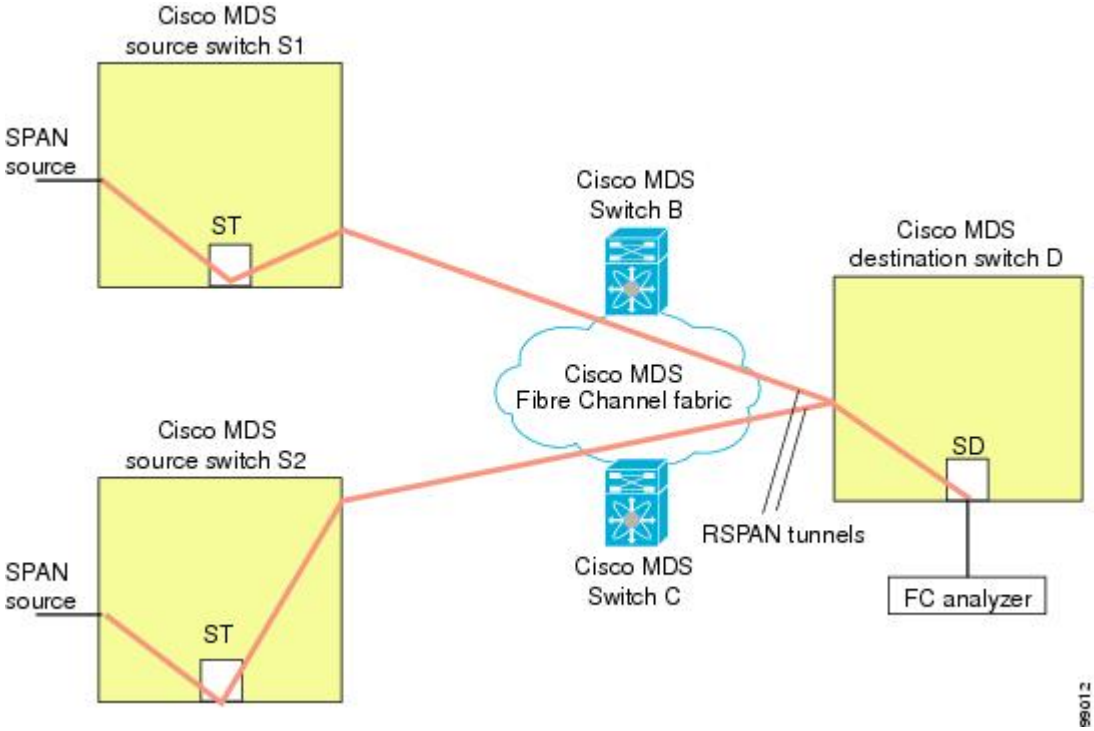
図 30 : 送信元スイッチが 1 台、宛先スイッチが 1 台、トンネルが複数の場合の RSPAN シナリオ



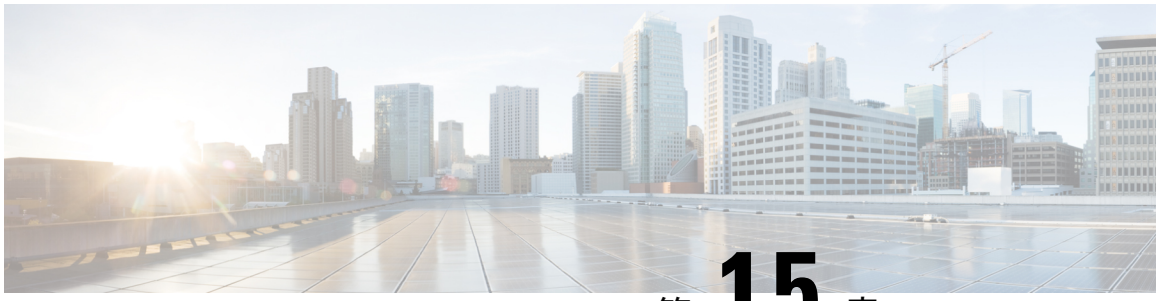

# 複数の送信元と複数の RSPAN トンネル

図 31 : 送信元スイッチが 2 台、宛先スイッチが 1 台、トンネルが複数の場合の RSPAN シナリオ （349 ページ） に、スイッチ S1 とスイッチ S2 の間に設定された 2 本の独立した RSPAN トンネルを示します。これらのトンネルは、関連 ST ポートがそれぞれ別々の送信元スイッチ内に存在し、両方とも宛先スイッチ内にある同じ SD ポートで終端します。

図 *31* : 送信元スイッチが *2* 台、宛先スイッチが *1* 台、トンネルが複数の場合の *RSPAN* シナリオ




この設定は、リモートモニタリングの場合に役立ちます。たとえば、管理者は宛先スイッチからリモートで 2 台の送信元スイッチをモニタできます。



第 15 章

# 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。



## FCS について

Fabric Configuration Server（FCS）を使用すると、トポロジ属性を検出したり、ファブリック要素の設定情報リポジトリを維持したりすることができます。通常、管理アプリケーションはNポートを通してスイッチの FCS に接続されます。FCS は次のオブジェクトに基づいて、ファブリック全体を表示します。

- Interconnect Element（IE）オブジェクト：ファブリック内の各スイッチは IE オブジェクトに対応しています。ファブリックは 1 つまたは複数の IE オブジェクトで構成されます。
- ポート オブジェクト：IE の各物理ポートはポート オブジェクトに対応しています。ポート オブジェクトにはスイッチ ポート（xE、Fx、および TL ポート）および接続された Nx ポートが含まれます。
- プラットフォーム オブジェクト：一連のノードをプラットフォーム オブジェクトとして定義して、管理可能な単一のエンティティにできます。これらのノードはファブリックに接続されたエンドデバイス（ホスト システム、ストレージ サブシステム）です。プラットフォーム オブジェクトは、ファブリックのエッジ スイッチ上にあります。

各オブジェクトには、それぞれ独自の属性および値のセットがあります。一部の属性にはヌル値も定義できます。

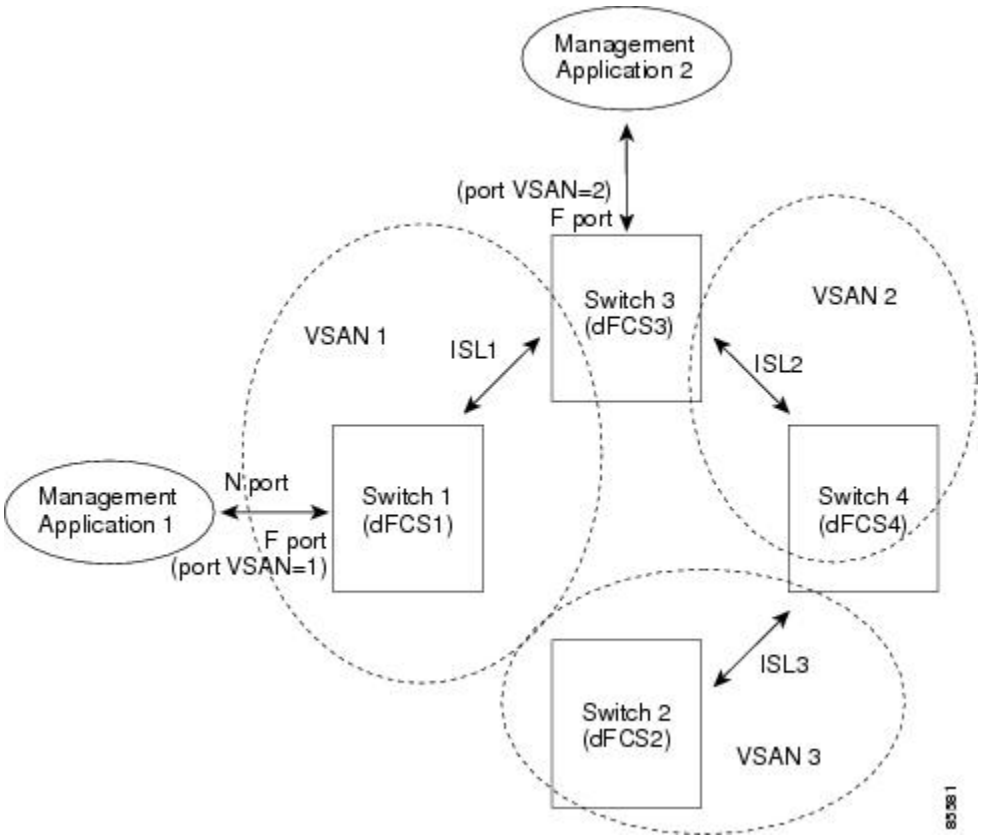
Cisco MDS 9000 ファミリ スイッチ環境では、複数の VSAN がファブリックを構成し、VSAN ごとに 1 つの FCS インスタンスが存在します。

Cisco NX-OS Release 4.1(1) から、FCS は仮想デバイスの検出をサポートしています。The **fcs virtual-device-add** command, issued in FCS configuration submode, allows you to discover virtual devices in a particular VSAN or in all VSANs. IVR 用にゾーン分割されたデバイスは、IVR ゾーン セットをアクティブ化する前に、このコマンドで検出し、Request Domain ID（RDI）をイネーブルにする必要があります。

スイッチに管理アプリケーションが接続されている場合、スイッチの FCS に転送されるすべてのフレームは、スイッチ ポート（Fx ポート）のポート VSAN に属します。管理アプリケーションの表示対象はこの VSAN に限定されます。ただし、このスイッチが属する他の VSAN に関する情報は、SNMP または CLI を使用して取得できます。

図 32 : VSAN 環境における FCS （352 ページ） では、管理アプリケーション 1（M1）は、ポート VSAN ID が 1 の F ポートを介して接続され、管理アプリケーション 2（M2）はポート VSAN ID が 2 の F ポートを介して接続されています。M1 はスイッチ S1 および S3 の FCS 情報を、M2 はスイッチ S3 および S4 の FCS 情報をそれぞれ問い合せることができます。スイッチ S2 の情報はどちらにも提供されません。FCS は、VSAN で表示可能なこれらのスイッチ上でだけ動作します。なお、S3 は VSAN 1 にも属していますが、M2 は VSAN 2 にだけ FCS 要求を送信できます。

**図 *32 : VSAN* 環境における *FCS***



# FCS の重要性

ここでは、FCS の重要性について説明します。

- FCS は次のようなネットワーク管理をサポートします。
  - N ポート管理アプリケーションはファブリック要素に関する情報を問い合せて、取得できます。
  - SNMP マネージャは FCS 管理情報ベース（MIB）を使用して、ファブリック トポロジ情報の検出を開始して、取得できます。
- FCS は、標準の F ポートおよび E ポートだけでなく、TE ポートと TL ポートもサポートします。
- FCS は、プラットフォームに登録された論理名および管理アドレスを使用して、一連のモードを維持することができます。FCS はすべての登録情報のバックアップをセカンダリ ストレージに維持し、変更があるたびに更新します。再起動またはスイッチオーバーが発生すると、FCS はセカンダリ ストレージ情報を取得し、データベースを再構築します。
- SNMP マネージャは FCS に、ファブリック内のすべての IE、ポート、およびプラットフォームについて問い合せることができます。

# デフォルト設定

表 42 : FCS のデフォルト設定 （353 ページ） に、FCSの デフォルト設定値を示します。

**表 *42 : FCS* のデフォルト設定**

| パラメータ | デフォルト |
|---|---|
| プラットフォーム名のグローバルチェック | ディセーブル |
| プラットフォームのノード タイプ | 不明。 |

# FCS の設定

Fabric Configuration Server（FCS）を使用すると、トポロジ属性を検出したり、ファブリック要素の設定情報リポジトリを維持したりすることができます。

# FCS 名を指定します。

一意の名前の確認をファブリック全体（グローバル）に行うのか、または登録されたプラットフォームにローカル（デフォルト）に行うのかを指定できます。

（注） このコマンドのグローバル設定は、ファブリック内のすべてのスイッチが Cisco MDS 9000 ファミリまたは である場合にかぎり実行してください。

プラットフォーム名のグローバルチェックをイネーブルにするには、次の手順を実行します。

**手順**

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **fcs plat-check-global vsan 1**

プラットフォーム名のグローバル チェックをイネーブルにします。

**ステップ 3** switch(config)# **no fcs plat-check-global vsan 1**

プラットフォーム名のグローバル チェックをディセーブル（デフォルト）にします。

## プラットフォームの属性を登録

プラットフォーム属性を登録するには、次の手順を実行します。

**手順**

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch(config)# **fcs register**

switch(config-fcs-register)#

FCS 登録サブモードを開始します。

**ステップ 3** switch(config-fcs-register)# **platform name SamplePlatform vsan 1**

switch(config-fcs-register-attrib)#

FCS 登録属性サブモードを開始します。

**ステップ 4** switch(config-fcs-register)# **no platform name SamplePlatform vsan 1**

switch(config-fcs-register)#

登録されたプラットフォームを削除します。

**ステップ 5** switch(config-fcs-register-attrib)# **mgmt-addr 1.1.1.1**

プラットフォーム管理 IPv4 アドレスを設定します。

**ステップ 6** switch(config-fcs-register-attrib)# **no mgmt-addr 1.1.1.1**

プラットフォーム管理 IPv4 アドレスを削除します。

**ステップ 7** switch(config-fcs-register-attrib)# **mgmt-addr 2001:0DB8:800:200C::417A**

プラットフォーム管理 IPv6 アドレスを設定します。

**ステップ 8** switch(config-fcs-register-attrib)# **no mgmt-addr 2001:0DB8:800:200C::417A**

プラットフォーム管理 IPv6 アドレスを削除します。

**ステップ 9** switch(config-fcs-register-attrib)# **nwwn 11:22:33:44:55:66:77:88**

プラットフォーム ノード名を設定します。

**ステップ 10** switch(config-fcs-register-attrib)# **no nwwn 11:22:33:44:55:66:77:88**

プラットフォーム ノード名を削除します。

**ステップ 11** switch(config-fcs-register-attrib)# **type 5**

定義済みプラットフォーム タイプ fc-gs-3 を設定します。

**ステップ 12** switch(config-fcs-register-attrib)# **no type 5**

設定済みのタイプを削除し、スイッチを出荷時の設定（不明なタイプ）に戻します。

**ステップ 13** switch(config-fcs-register-attrib)# **exit**

FCS 登録属性サブモードを終了します。

**ステップ 14** switch(config-fcs-register)# **exit**

FCS 登録サブモードを終了します。

# FCS 設定の確認

FCS の設定情報を表示するには、次のいずれかの作業を行います。

| コマンド | 目的 |
|---|---|
| **show fcs database** | FCS ローカル データベース情報を表示します。 |
| **show fcs ie vsan 1** | 特定の VSAN のすべての Ie のリストを表示します。 |
| **show fcs ie nwwn 20:01:00:05:30:00:16:df vsan 1** | 特定の nWWN の Interconnect Element オブジェクト情報の表示 |

| コマンド | 目的 |
|---|---|
| **show fcs platform name SamplePlatform vsan 1** | 特定のプラットフォームの情報の表示 |
| **show fcs platform vsan 1** | 指定された VSAN のプラットフォームのリストの表示 |
| **show fcs port vsan 24** | 指定された VSAN のスイッチポートのリストの表示 |
| **show fcs port pwwn 20:51:00:05:30:00:16:de vsan 24** | 指定された pWWN のポート情報の表示 |
| **show fcs statistics** | FCS 統計情報の表示 |
| **show fcs vsan** | 各 VSAN のプラットフォーム設定の表示 |

For detailed information about the fields in the output from these commands, refer to the *Cisco MDS 9000 Family Command Reference* .

# FCS 要素の表示

Use the **show fcs** commands to display the status of the WWN configuration (see Example FCS Local Database Information （356 ページ） to Platform Settings for Each VSAN （359 ページ）).

### FCS Local Database Information

The following example displays FCS local database information:

```
switch# show fcs database
FCS Local Database in VSAN: 1
------------------------------
Switch WWN               : 20:01:00:05:30:00:16:df
Switch Domain Id         : 0x7f(127)
Switch Mgmt-Addresses    : snmp://172.22.92.58/eth-ip
                           http://172.22.92.58/eth-ip
Fabric-Name              : 20:01:00:05:30:00:16:df
Switch Logical-Name      : 172.22.92.58
Switch Information List  : [Cisco Systems*DS-C9509*0*20:00:00:05:30:00
Switch Ports:
--------------------------------------------------------------------
Interface  pWWN                      Type     Attached-pWWNs
--------------------------------------------------------------------
fc2/1      20:41:00:05:30:00:16:de  TE       20:01:00:05:30:00:20:de
fc2/2      20:42:00:05:30:00:16:de  Unknown  None
fc2/17     20:51:00:05:30:00:16:de  TE       20:0a:00:05:30:00:20:de
FCS Local Database in VSAN: 5
------------------------------
Switch WWN               : 20:05:00:05:30:00:12:5f
Switch Domain Id         : 0xef(239)
Switch Mgmt-Addresses    : http://172.22.90.171/eth-ip
                           snmp://172.22.90.171/eth-ip
                           http://10.10.15.10/vsan-ip
                           snmp://10.10.15.10/vsan-ip
Fabric-Name              : 20:05:00:05:30:00:12:5f
```

```
Switch Logical-Name      : 172.22.90.171
Switch Information List  : [Cisco Systems*DS-C9509**20:00:00:05:30:00:12:5e]
Switch Ports:
--------------------------------------------------------------------
Interface  pWWN                      Type     Attached-pWWNs
--------------------------------------------------------------------
fc3/1      20:81:00:05:30:00:12:5e  TE       22:01:00:05:30:00:12:9e
fc3/2      20:82:00:05:30:00:12:5e  TE       22:02:00:05:30:00:12:9e
fc3/3      20:83:00:05:30:00:12:5e  TE       22:03:00:05:30:00:12:9e
```

### 特定の VSAN のすべての Ie のリスト

The following example displays list of all IEs for a specific VSAN:

```
switch# show fcs ie vsan 1
IE List for VSAN: 1
--------------------------------------------------------------------
IE-WWN                   IE-Type                          Mgmt-Id
--------------------------------------------------------------------
20:01:00:05:30:00:16:df  Switch (Local)                   0xfffc7f
20:01:00:05:30:00:20:df  Switch (Adjacent)                0xfffc64
[Total 2 IEs in Fabric]
```

### Interconnect Element Object Information for a Specific nWWN

The following example displays interconnect element object information for a specific nWWN:

```
switch# show fcs ie nwwn 20:01:00:05:30:00:16:df vsan 1
IE Attributes
-------------
Domain-Id = 0x7f(127)
Management-Id = 0xfffc7f
Fabric-Name = 20:01:00:05:30:00:16:df
Logical-Name = 172.22.92.58
Management Address List =
        snmp://172.22.92.58/eth-ip
        http://172.22.92.58/eth-ip
Information List:
        Vendor-Name = Cisco Systems
        Model Name/Number = DS-C9509
        Release-Code = 0
```

### 特定のプラットフォームに関する情報

The following example displays information for a specific platform:

```
switch# show fcs platform name SamplePlatform vsan 1
Platform Attributes
-------------------
Platform Node Names:
        11:22:33:44:55:66:77:88
Platform Type = Gateway
Platform Management Addresses:
        1.1.1.1
```

### List of Platforms for a Specified VSAN

The following example displays list of platforms for a specified VSAN:

```
switch# show fcs platform vsan 1
Platform List for VSAN: 1
Platform-Names
--------------
SamplePlatform
[Total 1 Platforms in Fabric]
```

### List of Switch Ports in a Specified VSAN

The following example displays a list of switch ports in a specified VSAN:

```
switch# show fcs port vsan 24
Port List in VSAN: 24
                -- IE WWN: 20:18:00:05:30:00:16:df  --
------------------------------------------------------------------------
Port-WWN                 Type      Module-Type            Tx-Type
------------------------------------------------------------------------
20:41:00:05:30:00:16:de  TE_Port   SFP with Serial Id      Shortwave Laser
20:51:00:05:30:00:16:de  TE_Port   SFP with Serial Id      Shortwave Laser
[Total 2 switch-ports in IE]
                -- IE WWN: 20:18:00:05:30:00:20:df  --
------------------------------------------------------------------------
Port-WWN                 Type      Module-Type            Tx-Type
------------------------------------------------------------------------
20:01:00:05:30:00:20:de  TE_Port   SFP with Serial Id      Shortwave Laser
20:0a:00:05:30:00:20:de  TE_Port   SFP with Serial Id      Shortwave Laser
[Total 2 switch-ports in IE]
```

### Port Information for a Specified pWWN

The following example displays port information for a specified pWWN:

```
switch# show fcs port pwwn 20:51:00:05:30:00:16:de vsan 24
Port Attributes
---------------
Port Type = TE_Port
Port Number = 0x1090000
Attached-Port-WWNs:
        20:0a:00:05:30:00:20:de
Port State = Online
```

### FCS 統計情報

The following example displays FCS statistics:

```
switch# show fcs statistics
FCS Statistics for VSAN: 1
--------------------------
FCS Rx Get Reqs   :2
FCS Tx Get Reqs   :7
```

```
FCS Rx Reg Reqs   :0
FCS Tx Reg Reqs   :0
FCS Rx Dereg Reqs :0
FCS Tx Dereg Reqs :0
FCS Rx RSCNs      :0
...
FCS Statistics for VSAN: 30
---------------------------
FCS Rx Get Reqs   :2
FCS Tx Get Reqs   :2
FCS Rx Reg Reqs   :0
FCS Tx Reg Reqs   :0
FCS Rx Dereg Reqs :0
FCS Tx Dereg Reqs :0
FCS Rx RSCNs      :0
FCS Tx RSCNs      :0
...
```

### Platform Settings for Each VSAN

The following example displays platform settings for each VSAN:

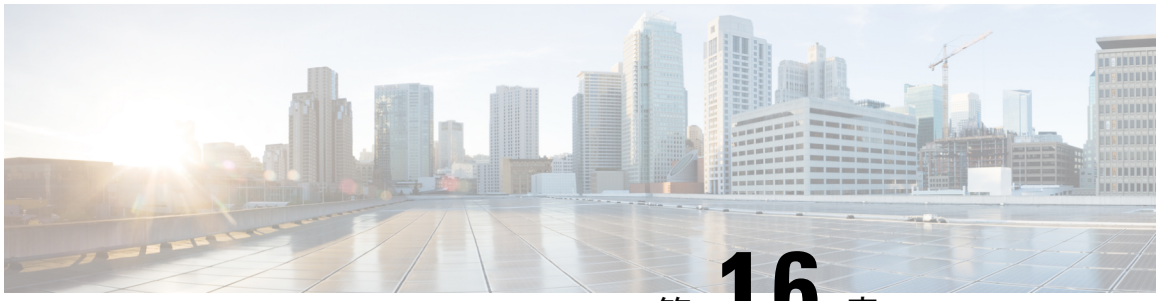
```
switch# show fcs vsan
------------------------------
VSAN    Plat Check fabric-wide
------------------------------
0001    Yes
0010    No
0020    No
0021    No
0030    No
```

# その他の参考資料

FCS の実装に関する詳細情報については、次の項を参照してください。

**表 *43 : MIB***

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



第 16 章

# ポート ペーシングの設定

この章では、ポート ペーサの設定方法を説明します。



## Information About Port Pacing

ファイバ チャネル ポート Pacer は Cisco MDS 9513 でのみサポートし、MDS 9710 スイッチします。ポート Pacer は、ポートは段階的に状態になるように同時にアップ モード F ポートの数をペースに設計されています。

F でポートの起動時に、時に、ポート Pacer は、ポートが始動 F ポート サーバを通知します。ポート Pacer F ポート サーバ FLOGIs と FDISCs ポートで受信するまで待機します。ポート Pacer は、ポートの同時ポート数を同時に起動を試みます。ただし、F ポート サーバことを通知ポート Pacer FLOGI および FDISC をそのポートの受信したポート Pacer が完了した後、ポートは起動しと最大ポートのステータスを更新します。その後、始動の次のポートが試行されました。

By default, F port pacing is disabled. ポートのペーシング有効にすると、FLOGI またはポートで受信した FDISC の数を追跡されています。すべての FLOGI または数秒がかかりが正常にログイン FDISC 時別の一連の同時ポートが開かれます。任意の時点での同時ポートで設定されているのみ FLOGI が処理されます。この機能は、ホストにゼロ FLOGI 再試行回数が発生した場合に便利です。

## 注意事項と制約事項

以下は、推奨されるガイドラインとポート Pacer を有効にするための要件です。

- ポートのペーシング設定が admin ポート モード F. でのみサポートされます。
- 電話機のトポロジを設定し、この値はどれくらいの数の F ポートで設定するポート番号ニーズを同時ポートは、同時に 15/255 = 6 ことができます。

# Configuring Port Pacer

## ポート ペーシングの有効化

（注） 管理ポート モード F. についてのみポート ペーシング設定がサポートされています。

ポート ペーシング コマンドは、すべての管理ポート モード F に適用されるシステム全体コマンドです。

ポート ペーサーを有効にするには、次の手順を実行します。

**手順**

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch# (config)# **system port pacer mode F interface-login-threshold 10 concurrent-ports 1**

同時並行を 1、しきい値を 10 として設定して F ポートの pacer モードを有効にします。

interface-login-threshold では、ポートで想定される FLOGI または FDISC の数を指定します。

Concurrent-ports は、同時にアップ状態にできる管理ポート モード F ポートの数を指定します。

## ポート ペーシング設定の無効化

ポート ペーシン設定を無効にする手順は、次のとおりです。

**手順**

**ステップ 1** switch# **configure terminal**

コンフィギュレーション モードに入ります。

**ステップ 2** switch# (config)# **no system port pacer mode F interface-login-threshold 10 concurrent-ports 1**

Disables the pacer mode for F port.