Inter-VSAN ルーティング コンフィギュレーション ガイド、Cisco DCNM for SAN

Cisco DCNM for SAN リリース 5.x
2011 年 6 月

Text Part Number: OL-25134-01-J

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

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

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

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

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

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

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

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

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Inter-VSAN ルーティング コンフィギュレーション ガイド、*Cisco DCNM for SAN*
© 2011 Cisco Systems, Inc. All rights reserved.

Copyright © 2011, シスコシステムズ合同会社 .
All rights reserved.

CONTENTS

新機能および変更された機能に関する情報 vii

はじめに ix

対象読者 ix

マニュアルの構成 ix

表記法 ix

関連資料 x

リリース ノート x

適合規格および安全に関する情報 x

互換性に関する情報 xi

ハードウェアの設置 xi

ソフトウェアのインストールおよびアップグレード xi

Cisco NX-OS xi

Cisco DCNM for SAN xi

コマンドライン インターフェイス xii

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

トラブルシューティングおよび参考資料 xii

マニュアルの入手方法およびテクニカル サポート xii

CHAPTER 1

基本的な Inter-VSAN Routing の設定 1-1

基本的な Inter-VSAN Routing について 1-1

IVR の概要 1-2

IVR の機能 1-2

IVR の用語 1-3

IVR の設定制限 1-4

IVR CFS の配信 1-5

データベースの実装 1-5

ファブリックのロック 1-5

ファイバ チャネル ヘッダーの変更 1-5

IVR ネットワーク アドレス変換 1-6

IVR VSAN のトポロジ 1-6

IVR 仮想ドメイン 1-6

IVR ゾーン 1-7

IVR ゾーンの自動作成 1-7

IVR 相互運用性 1-8
注意事項と制限 1-9
IVR NAT の要件とガイドライン 1-9
中継 VSAN に関するガイドライン 1-10
境界スイッチに関するガイドライン 1-10
IVR ゾーンの制限とイメージ ダウングレードに関するガイドライン 1-11
データベース マージに関する注意事項 1-11
デフォルト設定 1-13
基本的な Inter-VSAN Routing の設定 1-14
基本的な Inter-VSAN Routing の設定のタスク フロー 1-14
IVR Zone Wizard を使用した IVR と IVR ゾーンの設定 1-15
IVR のイネーブル化 1-16
CFS を使用した IVR 設定の配信 1-16
変更のコミット 1-16
変更の廃棄 1-16
ロック済みセッションのクリア 1-16
IVR NAT と IVR 自動トポロジ モードのイネーブル化 1-17
IVR ゾーンと IVR ゾーン セットの設定 1-18
IVR CFS リージョンを使用した IVR ゾーンの設定 1-19
適用 IVR ゾーン セットを使用した IVR CFS リージョンの設定 1-20
ゾーン セットのアクティブ化および force オプションの使用 1-20
IVR ゾーン セットのアクティブ化または非アクティブ化 1-21
IVR ロギング重大度の設定 1-22
基本的な Inter-VSAN Routing 設定のモニタリング 1-22
IVR fcdomain データベースの消去 1-23
IVR フル ゾーン データベースの回復 1-23
IVR トポロジの回復 1-23
データベースのマージ障害の解決 1-24
関連情報 1-24

CHAPTER 2 **高度な Inter-VSAN Routing の設定 2-1**
高度な Inter-VSAN Routing について 2-1
IVR サービス グループ 2-1
デフォルト サービス グループ 2-1
サービス グループのアクティベーション 2-2
Autonomous Fabric ID 2-2
FC ID の機能とメリット 2-2
高度な IVR ゾーンと IVR ゾーン セット 2-2
IVR CFS リージョン 2-3

IVR フローにおける高度なファブリック サービス 2-3
注意事項と制限 2-3
サービス グループに関するガイドライン 2-4
Autonomous Fabric ID に関するガイドライン 2-4
IVR NAT または IVR 自動トポロジを使用しない IVR に関するガイドライン 2-5
ドメイン ID に関するガイドライン 2-5
中継 VSAN に関するガイドライン 2-6
境界スイッチに関するガイドライン 2-6
手動での IVR トポロジ設定に関するガイドライン 2-6
FC ID に関するガイドライン 2-7
IVR ゾーン設定に関するガイドライン 2-8
高度なファブリック サービスに関する注意事項および制約事項 2-8
高度な Inter-VSAN Routing の設定 2-8
高度な Inter-VSAN Routing の設定のタスク フロー 2-9
IVR サービス グループの設定 2-10
デフォルト AFID の設定 2-10
個別の AFID の設定 2-11
NAT を使用しない IVR の設定 2-11
IVR トポロジの手動設定 2-11
手動で設定された IVR トポロジのアクティベーション 2-12
手動で設定された IVR トポロジ データベースの削除 2-13
IVR 自動トポロジ モードから IVR 手動トポロジ モードへの移行 2-13
IVR の永続的 FC ID の設定 2-13
IVR ゾーン分割における LUN の設定 2-14
IVR ゾーンの QoS の設定 2-14
IVR ゾーンと IVR ゾーン セットの名前の変更 2-15
IVR CFS リージョン ID の設定 2-15
読み取り専用ゾーン分割を使用した IVR の設定 2-15

INDEX

新機能および変更された機能に関する情報

Cisco DCNM Release 5.2 以降は、Cisco Fabric Manager と Cisco Data Center Network Manager for LAN が、LAN 環境と SAN 環境の両方を管理できる Cisco Data Center Network Manager（DCNM）という 1 つの製品に統合されています。この製品統合の一環として、Cisco Fabric Manager という名前は Cisco DCNM for SAN に変更されました。

次の文書変更によって、統合された Cisco DCNM 製品がサポートされます。

- Cisco DCNM Release 5.2 に対応する Cisco DCNM 製品のマニュアルのタイトルが、Cisco DCNM for LAN に変更されました。
- Cisco DCNM Release 5.2 に対応する Cisco Fabric Manager 製品のマニュアルのタイトルが、Cisco DCNM for SAN に変更されました。
- Cisco DCNM for SAN 製品のマニュアルが、次の URL にある Cisco.com の Data Center Network Manager リスト ページで公開されました。
  http://www.cisco.com/en/US/products/ps9369/tsd_products_support_configure.html

  この URL は、Cisco DCNM for LAN 製品マニュアルのリスト ページと同じです。
- Cisco DCNM Release 5.2 以前のソフトウェア リリースに対応する Cisco Fabric Manager のマニュアルは、Cisco Fabric Manager という名前を使用し続けており、次の URL にある現在の Cisco.com リスト ページで入手できます。
  http://www.cisco.com/en/US/products/ps10495/tsd_products_support_configure.html

  Cisco DCNM Release 5.2 以前のリリースの Cisco Fabric Manager ソフトウェアを使用する場合は、引き続き、Cisco Fabric Manager のマニュアルを使用する必要があります。
- DCNM-SAN という名前は、Cisco Data Center Network Manager のユーザ インターフェイスで、Cisco DCNM for SAN の代わりに使用されます。同様に、DCNM-LAN という名前は、ユーザ インターフェイスで、Cisco DCNM for LAN の代わりに使用されます。ユーザ インターフェイスと合わせるために、製品マニュアルでも DCNM-SAN および DCNM-LAN という名前を使用します。
- 次の新しい資料では、Cisco DCNM for LAN と DCNM for SAN の両方をサポートし、新しいライセンス モデル、新しいインストール手順、および Cisco DCNM の新機能を取り扱います。
  - 『*Cisco DCNM Installation and Licensing Guide*』
  - 『*Cisco DCNM Release Notes*』
- Cisco DCNM のマニュアルの全リストについては、「はじめに」の「関連資料」を参照してください。

Cisco Fabric Manager Release 4.2(1) 以降は、ソフトウェアの設定情報が、次の情報に関する新機能固有のコンフィギュレーション ガイドに記載されています。

- システム管理
- インターフェイス

- ファブリック
- Quality of service
- セキュリティ
- IP サービス
- ハイ アベイラビリティおよび冗長性

これらの新しいガイドの情報は、以前は『*Cisco MDS 9000 Family CLI Configuration Guide*』および『*Cisco MDS 9000 Family Fabric Manager Configuration Guide*』に記載されていました。これらのコンフィギュレーション ガイドはまだ Cisco.com から入手できますが、Cisco Fabric Manager Release 5.0(1) よりも前のソフトウェア リリースに対してのみ使用するようにしてください。各ガイドには、特定のリリースで導入された機能や使用可能な機能が記載されています。ご使用のスイッチにインストールされているソフトウェアに対応したコンフィギュレーション ガイドを選択して参照してください。

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

Cisco Fabric Manager Release 5.0(1) に関する追加情報については、次の Cisco Systems の Web サイトから入手可能な『*Cisco MDS 9000 Family Release Notes*』を参照してください。

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

このマニュアルについて

この新しい『*Inter-VSAN ルーティング コンフィギュレーション ガイド、Cisco DCNM for SAN*』内の情報は、『*Cisco MDS 9000 Family Fabric Manager Configuration Guide, Release 5.0(1)*』の「Fabric Configuration」の項に記載されていたものです。

表 i-1 は、Cisco Fabric Manager Release 4.2(1) で導入された新しい機能と変更された機能を示しています。

表 i-1　新機能および変更された機能

機能	追加または変更された内容	変更されたリリース	参照先
IVR CFS リージョンを使用した IVR ゾーンの設定	IVR CFS リージョンを使用した IVR ゾーン設定情報を追加	5.2(1)	第 1 章「基本的な Inter-VSAN Routing の設定」
適用 IVR ゾーン セットを使用した IVR CFS リージョンの設定	適用 IVR ゾーン セットを使用した IVR CFS リージョン設定情報を追加	5.2(1)	第 1 章「基本的な Inter-VSAN Routing の設定」
IVR CFS リージョン ID の設定	IVR CFS リージョン ID 設定情報を追加	5.2(1)	第 2 章「高度な Inter-VSAN Routing の設定」
基本的な IVR 設定	基本的な IVR 設定情報を再編集	4.2(1)	第 1 章「基本的な Inter-VSAN Routing の設定」
高度な IVR 設定	高度な IVR 設定情報を再編集 「既存の IVR トポロジの操作」を追加 「高度な設定タスク リスト」を追加 IVR ゾーンの設定に関するガイドラインを追加	4.2(1)	第 2 章「高度な Inter-VSAN Routing の設定」 「IVR トポロジの手動設定」（P.11） 「高度な Inter-VSAN Routing の設定のタスク フロー」（P.9） 「IVR ゾーン設定に関するガイドライン」（P.8）

はじめに

ここでは、『*Inter-VSAN ルーティング コンフィギュレーション ガイド、Cisco DCNM for SAN*』の対象読者、構成、および表記法について説明します。さらに、関連資料の入手方法についても説明します。

対象読者

このマニュアルは、Cisco Inter-VSAN Routing の計画、インストール、設定、および保守を担当する、経験豊富なネットワーク管理者を対象とします。

マニュアルの構成

このマニュアルの構成は、次のとおりです。

章	タイトル	説明
第 1 章	「基本的な Inter-VSAN Routing の設定」	基本的な IVR 設定に関する概念と手順について説明します。
第 2 章	「高度な Inter-VSAN Routing の設定」	高度な IVR 設定に関する概念と手順について説明します。

表記法

コマンドの説明では、次の表記法を使用しています。

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

出力例では、次の表記法を使用しています。

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

このマニュアルでは、次の表記法を使用しています。

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

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

関連資料

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

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

リリース ノート

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

適合規格および安全に関する情報

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

互換性に関する情報

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

ハードウェアの設置

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

ソフトウェアのインストールおよびアップグレード

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

Cisco NX-OS

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

Cisco DCNM for SAN

- 『*Cisco DCNM Fundamentals Guide, Release 5.x*』
- 『*System Management Configuration Guide, Cisco DCNM for SAN, Release 5.x*』
- 『*Interfaces Configuration Guide, Cisco DCNM for SAN, Release 5.x*』
- 『*Fabric Configuration Guide, Cisco DCNM for SAN, Release 5.x*』
- 『*Quality of Service Configuration Guide, Cisco DCNM for SAN, Release 5.x*』

- 『*Security Configuration Guide, Cisco DCNM for SAN, Release 5.x*』
- 『*IP Services Configuration Guide, Cisco DCNM for SAN, Release 5.x*』
- 『*Intelligent Storage Services Configuration Guide, Cisco DCNM for SAN, Release 5.x*』
- 『*High Availability and Redundancy Configuration Guide, Cisco DCNM for SAN, Release 5.x*』
- 『*Inter-VSAN Routing Configuration Guide, Cisco DCNM for SAN, Release 5.x*』
- 『*SMI-S and Web Services Programming Guide, Cisco DCNM for SAN, Release 5.x*』

コマンドライン インターフェイス

- 『*Cisco MDS 9000 Family Command Reference*』

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

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

トラブルシューティングおよび参考資料

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

マニュアルの入手方法およびテクニカル サポート

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

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

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

CHAPTER 1

基本的な Inter-VSAN Routing の設定

この章では、基本的な Inter-VSAN Routing（IVR）機能の設定方法について説明し、IVR 管理インターフェイスを使用して VSAN 上でリソースを共有するための手順を紹介します。

この章では、次の事項について説明します。

- 「基本的な Inter-VSAN Routing について」（P.1-1）
- 「注意事項と制限」（P.1-9）
- 「デフォルト設定」（P.1-13）
- 「基本的な Inter-VSAN Routing の設定」（P.1-14）
- 「基本的な Inter-VSAN Routing 設定のモニタリング」（P.1-22）
- 「関連情報」（P.1-24）

基本的な Inter-VSAN Routing について

ここでは、次の内容について説明します。

- 「IVR の概要」（P.1-2）
- 「IVR の機能」（P.1-2）
- 「IVR の用語」（P.1-3）
- 「IVR の設定制限」（P.1-4）
- 「IVR CFS の配信」（P.1-5）
- 「ファイバ チャネル ヘッダーの変更」（P.1-5）
- 「IVR ネットワーク アドレス変換」（P.1-6）
- 「IVR VSAN のトポロジ」（P.1-6）
- 「IVR 仮想ドメイン」（P.1-6）
- 「IVR ゾーン」（P.1-7）
- 「IVR ゾーンの自動作成」（P.1-7）
- 「IVR 相互運用性」（P.1-8）

IVR の概要

Virtual SAN（VSAN; 仮想 SAN）は複数のファイバ チャネル SAN でスイッチおよび Inter-Switch Link（ISL; スイッチ間リンク）の共通物理インフラストラクチャを共有可能にすることによって、Storage Area Network（SAN; ストレージ エリア ネットワーク）のスケーラビリティ、可用性、およびセキュリティを改善します。これらのメリットは、各 VSAN 上のファイバ チャネル サービスが分離され、VSAN 間のトラフィックが隔離されることから得られます。VSAN 間のデータ トラフィックが隔離されることによって、自動テープ ライブラリなどの VSAN に接続されたリソースの共有を本質的に防ぐことができます。IVR を使用すると、他の VSAN のメリットを損ねることなく、VSAN を越えてリソースにアクセスできます。

IVR の機能

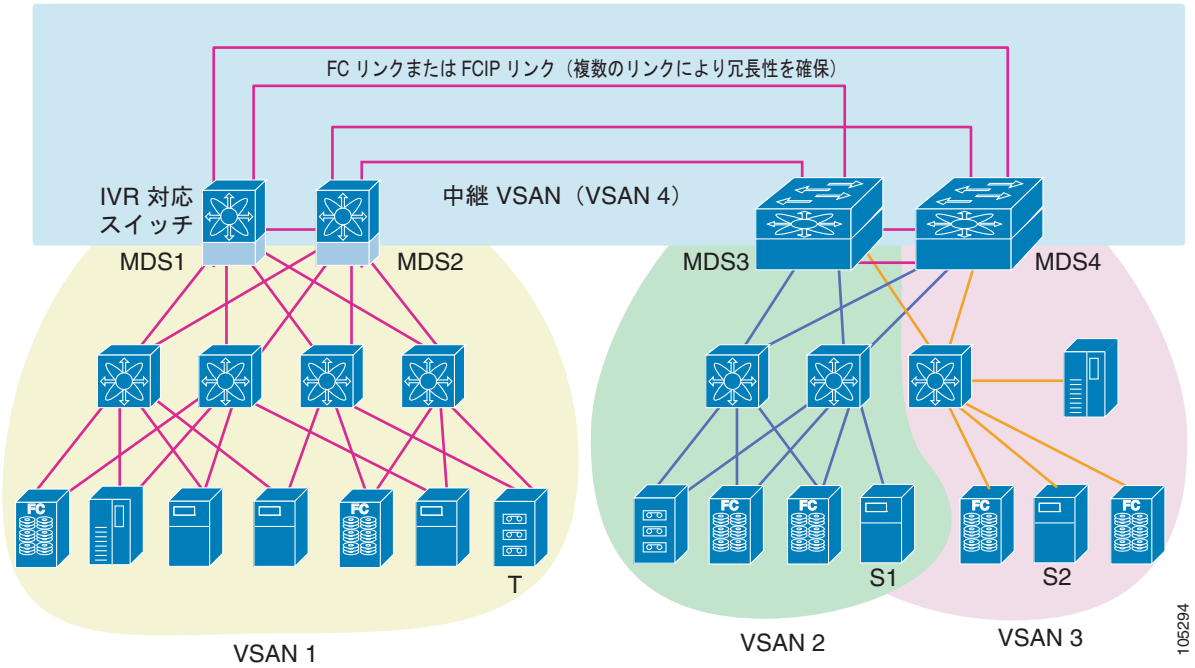
IVR は次の機能をサポートします。

- 他の VSAN のメリットを損ねることなく、VSAN を越えてリソースにアクセスします。
- VSAN を単一の論理ファブリックにマージせずに、複数の VSAN 上の特定の発信側とターゲット間でデータ トラフィックを転送します。
- 複数のスイッチをまたいで 1 つ以上の VSAN を接続する、正しい相互接続経路を確立します。IVR は、共通のスイッチ上に存在する VSAN に制限されません。
- 何も犠牲にすることなく、VSAN を越えて貴重なリソース（テープ ライブラリなど）を共有します。ファイバ チャネル トラフィックは VSAN 間で転送されません。また、発信側は、指定された VSAN 以外の VSAN 上のリソースにはアクセスできません。
- FCIP と併用した場合に、効果的なビジネス継続ソリューションまたはディザスタ リカバリ ソリューションを提供します（図 1-1 を参照）。
- ファイバ チャネル標準に準拠しています。
- サードパーティ製スイッチとの連携が可能です。ただし、IVR 対応 VSAN を interop モードのいずれかに設定する必要があります。

（注）Cisco MDS 9124 ファブリック スイッチ、Cisco MDS 9134 ファブリック スイッチ、Cisco MDS 9148 ファブリック スイッチ、HP c-Class BladeSystem 用 Cisco ファブリック スイッチ、IBM BladeCenter 用 Cisco ファブリック スイッチでは、IVR がサポートされません。

第 1 世代スイッチング モジュールでは、IVR 対応スイッチからの IVR トラフィックの Originator Exchange ID（OX ID）ロード バランシングがサポートされません。一部の環境では、非 IVR MDS スイッチからの IVR トラフィックの OX ID ベース ロード バランシングが機能します。第 2 世代スイッチング モジュールは、IVR 対応スイッチからの IVR トラフィックの OX ID ベース ロード バランシングをサポートします。

図 1-1　IVR と FCIP を使用したトラフィックの連続性



IVR の用語

IVR に関するマニュアルでは、次の IVR 関連用語が使用されます。

- ネイティブ VSAN - エンド デバイスがログインしている VSAN が、そのエンド デバイスのネイティブ VSAN です。
- 現在の VSAN - IVR 用に設定されている VSAN
- Inter-VSAN Routing ゾーン（IVR ゾーン）: 相互接続された SAN ファブリック内の VSAN 経由で通信可能なエンド デバイスの集合。この定義は port World Wide Name（pWWN）とネイティブ VSAN の関係に基づきます。Cisco SAN-OS Release 3.0(3) よりも前のリリースでは、ネットワーク内のスイッチ上に最大 2,000 の IVR ゾーンと 10,000 の IVR ゾーン メンバーを設定できます。Cisco SAN-OS Release 3.0(3) 以降では、ネットワーク内のスイッチ上に最大 8,000 の IVR ゾーンと 20,000 の IVR ゾーン メンバーを設定できます。
- Inter-VSAN Routing ゾーン セット（IVR ゾーン セット）: IVR ゾーン セットは 1 つ以上の IVR ゾーンで構成されます。Cisco MDS 9000 ファミリに属するスイッチの場合は、最大 32 の IVR ゾーン セットを設定できます。アクティブにできるのは、常に 1 つの IVR ゾーン セットだけです。
- IVR パス - ある VSAN 上のエンド デバイスから別の VSAN 上のエンド デバイスにフレームを到達させることが可能なスイッチと ISL の集合です。このような 2 つのエンド デバイス間に複数のパスを存在させることができます。
- IVR 対応スイッチ - IVR 機能がイネーブルになっているスイッチ
- エッジ VSAN - IVR パスを開始する VSAN（送信元エッジ VSAN）または終了する VSAN（送信先エッジ VSAN）。エッジ VSAN は、隣接させることも、1 つ以上の中継 VSAN で接続することもできます。VSAN 1、2、および 3（図 1-1 を参照）がエッジ VSAN です。

（注）　ある IVR パスのエッジ VSAN を別の IVR パスの中継 VSAN にすることができます。

- 中継 VSAN - IVR パスの送信元エッジ VSAN から送信先エッジ VSAN までの間に存在する VSAN。VSAN 4 が中継 VSAN（図 1-1 を参照）です。

（注）　送信元と送信先のエッジ VSAN が隣接している場合は、その間に中継 VSAN は必要ありません。

- 境界スイッチ - 複数の VSAN のメンバーになっている IVR 対応スイッチ。VSAN 1 と VSAN 4 の間に存在する IVR 対応スイッチなどの境界スイッチ（図 1-1 を参照）は、色分けされた複数の VSAN にまたがっています。
- エッジ スイッチ - IVR ゾーンのメンバーがログインしているスイッチ。エッジ スイッチは、境界スイッチ上の IVR 設定を認識できません。また、エッジ スイッチは IVR に対応している必要はありません。
- Autonomous Fabric 識別番号（AFID）：ネットワーク内の複数の VSAN を同じ VSAN ID に設定することによって、ID が同じ VSAN を含むファブリック間の IVR を設定するときのダウンタイムを回避できます。
- サービス グループ - トラフィックを IVR 対応 VSAN に制限する 1 つ以上のサービス グループを設定することによって、非 IVR 対応 VSAN への IVR トラフィック量を減らすことができます。

IVR の設定制限

表 1-1 は、IVR の設定制限を要約したものです。

表 1-1　IVR の設定制限

IVR の機能	最大制限
IVR VSAN	128
IVR ゾーン メンバー	Cisco SAN-OS Release 3.0(3) 以降では、物理ファブリックごとに 20,000 の IVR ゾーン メンバー Cisco SAN-OS Release 3.0(3) よりも前のリリースでは、物理ファブリックごとに 10,000 の IVR ゾーン メンバー
IVR ゾーン	Cisco SAN-OS Release 3.0(3) 以降では、物理ファブリックごとに 8,000 の IVR ゾーン Cisco SAN-OS Release 3.0(3) よりも前のリリースでは、物理ファブリックごとに 2,000 の IVR ゾーン
IVR ゾーン セット	物理ファブリックごとに 32 の IVR ゾーン セット
IVR サービス グループ	物理ファブリックごとに 16 のサービス グループ
IVR スイッチ	25（IVR 自動トポロジ モード） （注）　25 を超える IVR スイッチがある場合は、IVR 手動トポロジ モードをお勧めします。「IVR トポロジの手動設定」（P.2-11）を参照してください。

IVR CFS の配信

IVR 機能は Cisco Fabric Services（CFS）インフラストラクチャを使用して、効率のよい設定管理を行い、VSAN 内のファブリック全体においてシングル ポイントの設定を提供します。CFS の詳細については、『*Cisco MDS 9000 Family NX-OS System Management Configuration Guide*』を参照してください。

次の設定が配信されます。

- IVR ゾーン
- IVR ゾーン セット
- IVR VSAN トポロジ
- IVR のアクティブ トポロジおよびゾーン セット（あるスイッチでこれらの機能をアクティブにすると、ファブリック内で配信がイネーブルになっている他のすべてのスイッチに対して設定が伝播されます）。
- AFID データベース

データベースの実装

IVR 機能は、次の 3 つのデータベースを使用して、設定を受け入れ、実装します。

- 設定済みのデータベース：データベースはユーザにより手動で設定されています。
- アクティブ データベース：データベースはファブリックで実行されています。
- 保留データベース：設定を変更する場合は、設定済みデータベースの変更内容を保留データベースへコミットするか、または破棄する必要があります。その間、ファブリックはロックされた状態になります。保留データベースに対する変更は、変更内容を CFS へコミットするまで、アクティブ データベースには反映されません。

ファブリックのロック

データベースを変更するときの最初のアクションによって、保留中のデータベースが作成され、VSAN 内の機能がロックされます。ファブリックがロックされると、次のような状況になります。

- 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。
- コンフィギュレーション データベースのコピーが、最初のアクティブ変更と同時に保留中のデータベースになります。

ファイバ チャネル ヘッダーの変更

IVR は、仮想ドメインを使用して、ネイティブ VSAN 内のリモート エンド デバイスを仮想化します。2 つの異なる VSAN 内のエンド デバイスをリンクするように IVR が設定されている場合は、IVR 境界スイッチがエンド デバイス間のすべての通信に関するファイバ チャネル ヘッダーを変更する責任を負います。変更されるファイバ チャネル フレーム ヘッダーのセクションは、次のとおりです。

- VSAN 番号
- 送信元 FCID
- 送信先 FCID

発信側からターゲットへのフレームの送信時に、発信側 VSAN 番号がターゲット VSAN 番号になるようにファイバ チャネル フレーム ヘッダーが変更されます。IVR Network Address Translation（NAT; ネットワーク アドレス変換）がイネーブルの場合は、エッジ境界スイッチで送信元と送信先の FCID も変換されます。IVR NAT がイネーブルでない場合は、IVR パスに関与するすべてのスイッチに対して一意のドメイン ID を設定する必要があります。

IVR ネットワーク アドレス変換

IVR ネットワーク アドレス変換（NAT）をイネーブルにすれば、一意でないドメイン ID を使用できます。ただし、NAT を使用しない場合は、IVR 用に、ファブリック内のすべてのスイッチに対して一意のドメイン ID を設定する必要があります。IVR NAT は、一意でないドメイン ID が存在する可能性のある既存のファブリックへの IVR 展開を容易にします。

IVR NAT を使用するには、ファブリック内のすべての IVR 対応スイッチで NAT をイネーブルにする必要があります。Cisco MDS 9000 ファミリに属するすべてのスイッチで、IVR NAT と IVR 設定の配信がデフォルトでディセーブルになっています。

IVR の要件とガイドラインに関する情報と設定情報については、「IVR NAT と IVR 自動トポロジ モードのイネーブル化」（P.1-17）を参照してください。

IVR VSAN のトポロジ

IVR では、設定された IVR VSAN トポロジを使用して、ファブリック内の発信側とターゲット間のトラフィックのルーティング方法が判別されます。

IVR 自動トポロジ モードでは、ファブリックが再設定されると、自動的に、IVR VSAN トポロジが構築され、トポロジ データベースがメンテナンスされます。また、IVR 自動トポロジ モードでは、CFS を使用して、IVR VSAN トポロジが IVR 対応スイッチに配信されます。

IVR 自動トポロジ モードを使用すれば、ファブリックが再設定されても、IVR VSAN トポロジを手動で更新する必要がありません。IVR 手動トポロジ データベースが存在する場合は、IVR 自動トポロジ モードで最初にそのトポロジ情報が使用されます。自動的な更新では、ユーザ指定のトポロジ データベースから、自動学習されたトポロジ データベースへの移行が段階的に進み、ネットワーク中断が削減されます。ネットワークに属さないユーザ設定のトポロジ エントリは、約 3 分間で期限切れになります。ユーザ設定のデータベースに属さない新しいエントリは、ネットワーク上で検出された時点で追加されます。

IVR 自動トポロジ モードがイネーブルの場合は、以前アクティブだった IVR 手動トポロジが存在すれば、そこから開始され、検出プロセスが開始されます。新規パス、代替パス、またはより良いパスが検出されます。トラフィックが代替パスまたはより良いパスに切り替えられると、パスの切り替え時に発生することが多い一時的なトラフィック中断が起きる可能性があります。

（注）　IVR 自動トポロジ モードで IVR トポロジを使用する場合は、ファブリック内のすべてのスイッチに Cisco MDS SAN-OS Release 2.1(1a) 以降をインストールし、IVR に対して CFS をイネーブルにする必要があります。

IVR 仮想ドメイン

リモート VSAN では、割り当て済みドメイン リストに仮想ドメインが自動的に追加されることはありません。一部のスイッチ（Cisco SN5428 スイッチなど）は、ファブリック内の割り当て済みドメイン リストにリモート ドメインが追加されるまで、リモート ネーム サーバに問い合わせません。このよう

な場合は、VSAN 内の割り当て済みドメイン リストに、特定の VSAN 内の IVR 仮想ドメインを追加します。IVR ドメインを追加すると、ファブリック内に存在する IVR 仮想ドメイン（および今後作成される仮想ドメイン）がすべて、その VSAN の割り当て済みドメイン リストに追加されます。

ヒント　Cisco SN5428 スイッチまたは Cisco MDS 9020 スイッチが VSAN 上に存在する場合は、必ず IVR 仮想ドメインを追加してください。

IVR 仮想ドメインがイネーブルの場合は、仮想ドメイン ID の重複が原因でリンクを起動できないことがあります。この現象が起きたときは、その VSAN から重複する仮想ドメインを一時的に削除します。

（注）　IVR VSAN から重複する仮想ドメインを削除すると、そのドメインに対する IVR トラフィックが中断します。

ヒント　IVR ドメインは、エッジ VSAN にだけ追加し、中継 VSAN には追加しないでください。

IVR ゾーン

IVR 設定の一部として、1 つ以上の IVR ゾーンを設定して、VSAN 間通信をイネーブルにする必要があります。そのためには、各 IVR ゾーンを（pWWN、VSAN）エントリの集合として指定する必要があります。ゾーンと同様に、複数の IVR ゾーン セットが 1 つの IVR ゾーンに属するように設定できます。複数の IVR ゾーン セットを定義して、そのうちの 1 つだけをアクティブにできます。

（注）　同じ IVR ゾーン セットは、すべての IVR 対応スイッチ上でアクティブにする必要があります。

表 1-2 は、IVR ゾーンとゾーンの主な違いをまとめたものです。

表 1-2　IVR ゾーンとゾーンの主な相違点

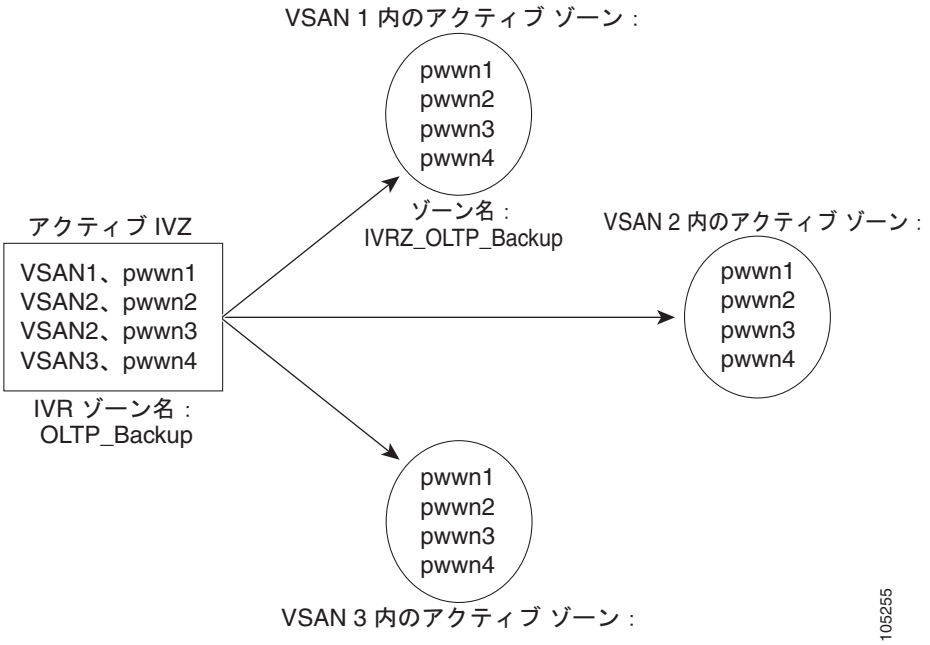
IVR ゾーン	ゾーン
IVR ゾーン メンバーシップは、VSAN と pWWN の組み合わせを使用して指定します。	ゾーン メンバーシップは、pWWN、ファブリック WWN、sWWN、または AFID を使用して指定します。
デフォルト ゾーン ポリシーは常に deny です（変更不可）。	デフォルト ゾーン ポリシーは deny です（変更可能）。

IVR ゾーンの自動作成

図 1-2 は、4 つのメンバーで構成された IVR ゾーンを示しています。pwwn1 と pwwn2 が通信できるようにするには、これらのメンバーが VSAN 1 と VSAN 2 で同じゾーンに属している必要があります。同じゾーンに属していない場合は、ハード ゾーン分割 ACL エントリによって、pwwn1 と pwwn2 の通信が禁止されます。

アクティブ IVR ゾーンで指定されたエッジ VSAN ごとに、アクティブ IVR ゾーンに対応するゾーンが自動的に作成されます。IVR ゾーン内のすべての pWWN が、各 VSAN 内のゾーンのメンバーです。

図 1-2　IVR ゾーンのアクティベーション時のゾーン作成



IVR ゾーン セットがアクティブになると、IVR プロセスによって自動的にゾーンが作成されます。作成されたゾーンはフル ゾーン セット データベースに格納されないため、スイッチを再起動するか、新規ゾーン セットがアクティブになると失われます。IVR 機能がこれらのイベントをモニタして、新規ゾーン セットがアクティブになると、アクティブ IVR ゾーン セット設定に対応するゾーンを追加します。ゾーン セットと同様に、IVR ゾーン セットも中断することなくアクティブになります。

（注）pwwn1 と pwwn2 が現在の IVR ゾーン セットと新規 IVR ゾーン セット内の IVR ゾーンに含まれている場合は、新規 IVR ゾーン セットがアクティブになっても、これらの間のトラフィックは中断されません。

IVR ゾーンと IVR ゾーン セットの名前は、64 文字までの英数字に制限されています。

注意　Cisco SAN-OS Release 3.0(3) よりも前のリリースでは、ネットワーク内のスイッチ上に最大 2,000 の IVR ゾーンと 32 の IVR ゾーン メンバーしか設定できません。Cisco SAN-OS Release 3.0(3) 以降では、ネットワーク内のスイッチ上に最大 8,000 の IVR ゾーンと 32 の IVR ゾーン メンバーを設定できます。「データベース マージに関する注意事項」（P.1-11）を参照してください。

IVR 相互運用性

IVR 機能を使用する場合は、ファブリック内のすべての境界スイッチを Cisco MDS スイッチにする必要があります。ただし、ファブリック内の他のスイッチは非 MDS スイッチにすることができます。たとえば、アクティブ IVR ゾーン セットのメンバーになっているエンド デバイスを非 MDS スイッチに接続することができます。interop モードの 1 つがイネーブルである場合は、中継 VSAN またはエッジ VSAN 上に、MDS 以外のスイッチが存在することも可能です。

スイッチの相互運用性の詳細については、『*Cisco Data Center Interoperability Support Matrix*』を参照してください。

注意事項と制限

ここでは、次の内容について説明します。

- 「IVR NAT の要件とガイドライン」（P.1-9）
- 「IVR ゾーンの制限とイメージ ダウングレードに関するガイドライン」（P.1-11）
- 「データベース マージに関する注意事項」（P.1-11）

IVR NAT の要件とガイドライン

IVR NAT には、次の要件およびガイドラインがあります。

- IVR 対応スイッチは、Cisco MDS SAN-OS Release 2.1(1a) 以降を実行する必要があります。
- ホストから送信される IVR NAT ポート ログイン（PLOGI）要求は、FC ID アドレスへの再書き込みを実行するために数秒遅れます。 ホストの PLOGI タイムアウト値が 5 秒未満に設定されている場合は、必要な PLOGI が破棄され、ホストがターゲットにアクセスできなくなる可能性があります。ホスト バス アダプタは 10 秒以上のタイムアウトに設定することをお勧めします（ほとんどの HBA はデフォルトで 10 ～ 20 秒に設定されています）。
- IVR NAT を使用するには、ファブリック内のすべての IVR スイッチ上に Cisco MDS SAN-OS Release 2.1(1a) 以降をインストールする必要があります。トポロジ内で設定され、古いリリースがインストールされたスイッチが隔離されている場合は、隔離されたすべてのファブリックを DCNM-SAN のモニタ対象から外してから、ファブリックをもう一度開いて IVR NAT を使用する必要があります。継続的に管理するファブリックの選択方法については、『*Cisco DCNM Fundamentals Guide*』を参照してください。
- IVR 対応スイッチからの等コスト パスをまたぐ IVR NAT トラフィックのロード バランシングはサポートされません。ただし、PortChannel リンク上の IVR NAT トラフィックのロード バランシングはサポートされます。第 1 世代のモジュールを使用した PortChannel 上の IVR NAT トラフィックのロード バランシング アルゴリズムは SRC/DST だけです。第 2 世代のモジュールは、PortChannel 上で IVR NAT トラフィックの SRC/DST/OXID ベースのロード バランシングをサポートします。
- 第 1 世代のモジュール インターフェイス上では、IVR NAT と推奨ファイバ チャネル ルートは設定できません。
- IVR NAT を使用すると、IVR パス上のすべてのスイッチに一意のドメイン ID を設定しなくても、ファブリック内に IVR をセットアップできます。IVR NAT は、ファイバ チャネル ヘッダー内の送信先 ID に指定されたローカル VSAN を使用して、他の VSAN 内のスイッチを仮想化します。一部の Extended Link Service メッセージ タイプでは、送信先 ID がパケット データに含まれています。このような場合は、IVR NAT が、実際の送信先 ID を仮想化された送信先 ID に置き換えます。IVR NAT は、表 1-3 に示す Extended Link Service メッセージ内の送信先 ID の置き換えをサポートします。

表 1-3　IVR NAT がサポートする Extended Link Service メッセージ

Extended Link Service メッセージ	リンク サービス コマンド（LS_COMMAND）	ニーモニック
Abort Exchange	0x06 00 00 00	ABTX
Discover Address	0x52 00 00 00	ADISC
Discover Address Accept	0x02 00 00 00	ADISC ACC

表 1-3　IVR NAT がサポートする Extended Link Service メッセージ （続き）

Extended Link Service メッセージ	リンク サービス コマンド（LS_COMMAND）	ニーモニック
Fibre Channel Address Resolution Protocol Reply	0x55 00 00 00	FARP-REPLY
Fibre Channel Address Resolution Protocol Request	0x54 00 00 00	FARP-REQ
Logout	0x05 00 00 00	LOGO
Port Login	0x30 00 00 00	PLOGI
Read Exchange Concise	0x13 00 00 00	REC
Read Exchange Concise Accept	0x02 00 00 00	REC ACC
Read Exchange Status Block	0x08 00 00 00	RES
Read Exchange Status Block Accept	0x02 00 00 00	RES ACC
Read Link Error Status Block	0x0F 00 00 00	RLS
Read Sequence Status Block	0x09 00 00 00	RSS
Reinstate Recovery Qualifier	0x12 00 00 00	RRQ
Request Sequence Initiative	0x0A 00 00 00	RSI
Scan Remote Loop	0x7B 00 00 00	RSL
Third Party Process Logout	0x24 00 00 00	TPRLO
Third Party Process Logout Accept	0x02 00 00 00	TPRLO ACC

- IVR NAT で認識されないメッセージが存在し、送信先 ID がパケット データに含まれている場合は、トポロジ内で IVR と NAT を併用できません。ただし、一意のドメイン ID を持つ IVR を使用することはできます。

中継 VSAN に関するガイドライン

中継 VSAN に関する次のガイドラインを考慮してください。

- IVR ゾーン メンバーシップを定義するほかに、一連の中継 VSAN を指定して 2 つのエッジ VSAN を接続することもできます。
  - IVR ゾーン内の 2 つのエッジ VSAN が重複している場合は、中継 VSAN がなくても接続できます（ただし、禁止されるわけではありません）。
  - IVR ゾーン内の 2 つのエッジ VSAN が重複していない場合は、1 つ以上の中継 VSAN がなければ接続できません。送信元と送信先の両方のエッジ VSAN に属しているスイッチ上で IVR がイネーブルになっていない場合は、IVR ゾーン内の 2 つのエッジ VSAN が重複することはありません。
- エッジ VSAN 間のトラフィックは、必ず最短の IVR パスを経由します。
- 中継 VSAN 情報は、すべての IVR ゾーン セットで共通です。場合によっては、中継 VSAN が別の IVR ゾーン内のエッジ VSAN として機能することもできます。

境界スイッチに関するガイドライン

境界スイッチを設定する前に、次のガイドラインを考慮してください。

- 境界スイッチには Cisco MDS SAN-OS Release 2.1(1a) 以降をインストールする必要があります。
- 境界スイッチは複数の VSAN のメンバーにする必要があります。
- IVR 通信を実行する境界スイッチは IVR に対応している必要があります。
- 追加の境界スイッチ上で IVR をイネーブルにして（オプション）、アクティブ IVR ゾーン メンバー間に冗長パスを提供することもできます。
- 境界スイッチを追加または削除すると、VSAN トポロジ設定が自動的に更新されます。

IVR ゾーンの制限とイメージ ダウングレードに関するガイドライン

表 1-4 は、物理ファブリック別に IVR ゾーンの制限をまとめたものです。

表 1-4　IVR ゾーンの制限

Cisco リリース	IVR ゾーンの制限	IVR ゾーン メンバーの制限	IVR ゾーン セットの制限
SAN-OS Release 3.0(3) 以降	8000	20,000	32
SAN-OS Release 3.0(2b) 以前	2000	10,000	32

（注） 1 つのゾーン メンバーが 2 つのゾーンに存在する場合は、2 回カウントされます。「データベース マージに関する注意事項」（P.1-11）を参照してください。

注意 Cisco SAN-OS Release 3.0(3) よりも前のリリースにダウングレードする場合は、IVR ゾーン数を 2,000 以下に、IVR ゾーン メンバーを 10,000 以下にする必要があります。

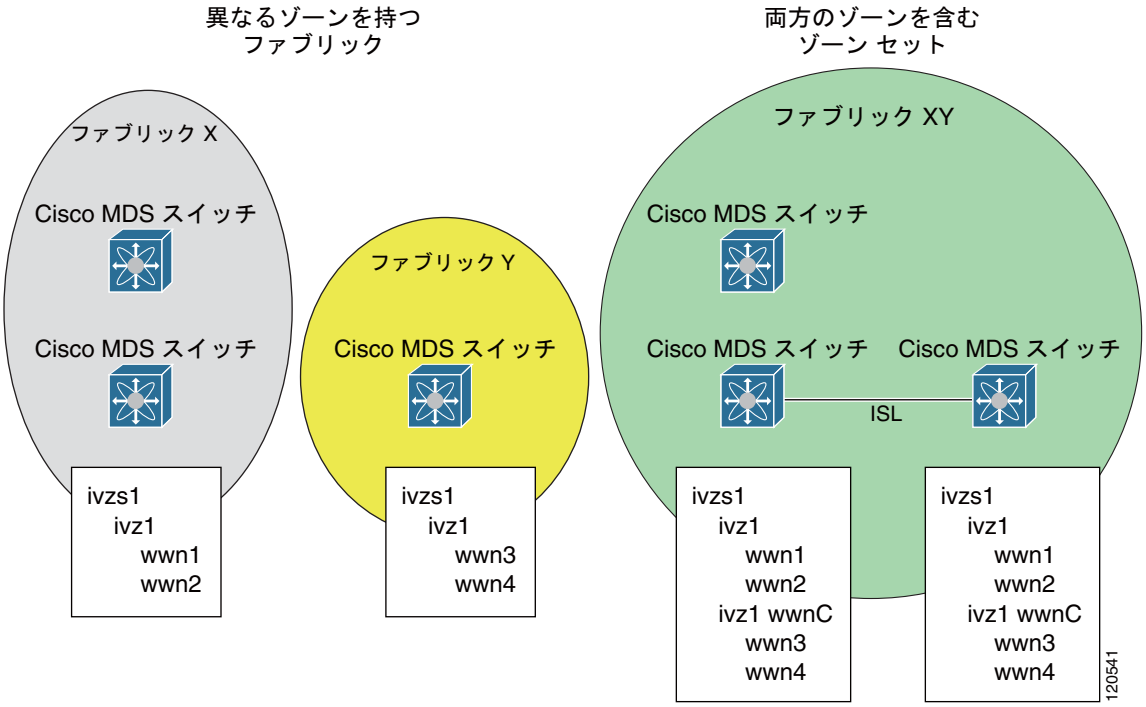
データベース マージに関する注意事項

データベースのマージとは、コンフィギュレーション データベースと、アクティブ データベース内の静的な（学習されていない）エントリの組み合わせを意味します。CFS マージ サポートの詳細については、『*Cisco MDS 9000 Family NX-OS System Management Configuration Guide*』または『*System Management Configuration Guide, Cisco DCNM for SAN*』を参照してください。

2 つの IVR ファブリックをマージする場合は、次のガイドラインを考慮してください。

- 2 つのファブリックの設定が異なる場合でも IVR 設定はマージされます。
- 2 つのマージされたファブリックに異なるゾーンが存在する場合は、それぞれのファブリック内のゾーンが適切な名前で配信ゾーン セットにコピーされます（図 1-3 を参照）。

図 1-3　ファブリック マージの結果



- Cisco MDS スイッチごとに IVR 設定を変えることができます。
- トラフィックの中断を避けるために、データベース マージの完了後の設定は、マージに関与した 2 つのスイッチ上の設定を組み合わせたものになります。
  - 両方のファブリックの設定が異なる場合でも設定はマージされます。
  - ゾーンとゾーン セットの組み合わせは、マージされたゾーンとゾーン セットを取得するために使用されます。2 つのファブリック内に異なるゾーンが存在する場合は、それぞれのゾーンが適切な名前でゾーン セットにコピーされるため、両方のゾーンが共存できます。
  - マージされたトポロジには、両方のファブリックのトポロジ エントリを組み合わせたものが格納されます。
  - マージするデータベースに最大許容数を超えるトポロジ エントリが含まれている場合は、マージが失敗します。
  - 2 つのファブリック全体の VSAN 数は 128 以下にする必要があります。

    （注）　VSAN ID は同じだが AFID が異なる VSAN は 2 つの異なる VSAN としてカウントされます。

  - 2 つのファブリック全体の IVR 対応スイッチ数は 128 以下にする必要があります。
  - 2 つのファブリック全体のゾーン メンバー数は 10,000 以下にする必要があります。Cisco SAN-OS Release 3.0(3) 以降では、2 つのファブリック全体のゾーン メンバー数を 20,000 以下にする必要があります。1 つのゾーン メンバーが 2 つのゾーンに存在する場合は、2 回カウントされます。

（注）　1 つ以上のファブリック スイッチが Cisco SAN-OS Release 3.0(3) 以降を実行しており、そのゾーン メンバー数が 10,000 を超えている場合は、ファブリック内のゾーン メンバー数を減らすか、両方のファブリック内の全スイッチを Cisco SAN-OS Release 3.0(3) 以降にアップグレードする必要があります。

– 2 つのファブリック全体のゾーン数は 2,000 以下にする必要があります。Cisco SAN-OS Release 3.0(3) 以降では、2 つのファブリック全体のゾーン数を 8,000 以下にする必要があります。

（注）　ファブリック内の一部のスイッチだけが Cisco SAN-OS Release 3.0(3) 以降を実行しており、そのゾーン数が 2,000 を超えている場合は、ファブリック内のゾーン数を減らすか、両方のファブリックのすべてのスイッチを Cisco SAN-OS Release 3.0(3) 以降にアップグレードする必要があります。

– 2 つのファブリック全体のゾーン セット数は 32 以下にする必要があります。

表 1-5 に、さまざまな条件下における 2 つの IVR 対応ファブリックの CFS マージ結果を示します。

表 1-5　2 つの IVR 対応ファブリックのマージ結果

IVR ファブリック 1	IVR ファブリック 2	マージ後
NAT イネーブル	NAT ディセーブル	マージが成功し、NAT がイネーブルになる
自動モードがイネーブルになる	自動モードがディセーブルになる	マージが成功し、IVR 自動トポロジ モードがイネーブルになる
AFID データベースの矛盾		マージが失敗する
IVR ゾーン セット データベースの矛盾		矛盾を解決するために作成された新しいゾーンでマージが成功する
結合設定が上限（ゾーンまたは VSAN の最大数など）を超過する		マージが失敗する
サービス グループ 1	サービス グループ 2	結合されたサービス グループでマージが成功する
矛盾のあるユーザ設定 VSAN トポロジ設定		マージが失敗する
矛盾のないユーザ設定 VSAN トポロジ設定		マージが成功する

注意　この条件に従わない場合は、マージが失敗します。次の配信がデータベースとファブリック内のアクティベーション ステートを強制的に同期化します。

デフォルト設定

表 1-6 に、IVR パラメータのデフォルト設定を示します。

表 1-6　デフォルト IVR パラメータ

パラメータ	デフォルト
IVR の機能	ディセーブル
IVR VSAN	仮想ドメインに追加されない
IVR NAT	ディセーブル
IVR ゾーンの QoS	Low
設定配信	ディセーブル

基本的な Inter-VSAN Routing の設定

ここでは、次の内容について説明します。

- 「基本的な Inter-VSAN Routing の設定のタスク フロー」（P.1-14）
- 「IVR Zone Wizard を使用した IVR と IVR ゾーンの設定」（P.1-15）
- 「IVR のイネーブル化」（P.1-16）
- 「CFS を使用した IVR 設定の配信」（P.1-16）
- 「IVR NAT と IVR 自動トポロジ モードのイネーブル化」（P.1-17）
- 「IVR ゾーンと IVR ゾーン セットの設定」（P.1-18）
- 「ゾーン セットのアクティブ化および force オプションの使用」（P.1-20）
- 「IVR ゾーン セットのアクティブ化または非アクティブ化」（P.1-21）
- 「IVR ロギング重大度の設定」（P.1-22）

基本的な Inter-VSAN Routing の設定のタスク フロー

基本的な IVR を設定するには、次の手順を実行します。

	作業	参照先
ステップ 1	すべての境界スイッチで IVR をイネーブルにします。	
ステップ 2	IVR 配信をイネーブルにします。	
（注）	ファブリック内の 1 つのスイッチで次の手順を実行する必要があります。	
ステップ 3	IVR NAT をイネーブルにします。	「IVR NAT と IVR 自動トポロジ モードのイネーブル化」(P.1-17) を参照してください。
ステップ 4	IVR 自動トポロジ モードをイネーブルにします。	「IVR NAT と IVR 自動トポロジ モードのイネーブル化」(P.1-17) を参照してください。
ステップ 5	IVR 仮想ドメインを設定します。	
ステップ 6	ゾーン セットを設定し、アクティブにします。	「IVR ゾーンと IVR ゾーン セットの設定」（P.1-18）を参照してください。
ステップ 7	IVR 設定をコミットします。	
ステップ 8	IVR 設定を確認します。	

IVR Zone Wizard を使用した IVR と IVR ゾーンの設定

IVR Zone Wizard を使用すれば、ファブリック内の IVR ゾーンの設定プロセスが容易になります。IVR Zone Wizard は次の条件を調べて、関連する問題を特定します。

- ファブリック内のすべてのスイッチをチェックして、スイッチ上で動作している Cisco SAN-OS または NX-OS のリリースを特定します。Cisco MDS SAN-OS Release 2.1(1a) 以降がスイッチ上で動作している場合は、IVR 自動トポロジ モードを使用した IVR NAT への移行を選択することができます。
- ファブリック内のすべてのスイッチをチェックして、スイッチ上で動作している Cisco SAN-OS または NX-OS のリリースを特定します。Cisco MDS SAN-OS Release 2.1(1a) 以降がスイッチ上で動作している場合は、必要なスイッチのアップグレードを選択したり、IVR NAT または IVR 自動トポロジ モードがイネーブルの場合にそれらのディセーブル化を選択したりすることができます。

手順の詳細

IVR Zone Wizard を使用して IVR と IVR ゾーンを設定するには、次の手順を実行します。

ステップ 1　Zone ツールバーにある [IVR Zone Wizard] アイコンをクリックします。

IVR NAT モードに移行するには [Yes] をクリックします。それ以外の場合は [No] をクリックします。[IVR Zone Wizard] ダイアログボックスが表示されます。

ステップ 2　IVR に関与するファブリック内の [VSAN] を選択します。[Next] をクリックします。

ステップ 3　IVR を使用して接続するエンド デバイスを選択します。

（注）　IVR NAT を使用していない場合は、IVR に関与するすべてのスイッチに一意のドメイン ID が設定されていなければ、エラー メッセージが表示されます。IVR を設定する前に、これらのスイッチを再設定する必要があります。ステップ 6 を参照してください。

ステップ 4　IVR NAT をイネーブルにした場合は、IVR NAT、IVR 用の CFS、および IVR 自動トポロジ モードを使用して DCNM-SAN でイネーブルにするスイッチを確認します。

ステップ 5　IVR ゾーン用に選択された VSAN 間の中継 VSAN として使用する VSAN の VSAN ID を入力します。[Next] をクリックします。

ステップ 6　（オプション）[Select AFID] ダイアログボックスで、VSAN ID が一意でないファブリック内のスイッチに一意の AFID を設定します。

ステップ 7　IVR NAT がディセーブルで、DCNM-SAN によって適切な中継 VSAN が検出されなかった場合は、中継 VSAN を確認するか、中継 VSAN を設定します。

ステップ 8　IVR ゾーンと IVR ゾーン セットを設定します。

ステップ 9　ファブリック内の IVR を設定するための DCNM-SAN の実行手順をすべて確認します。

ステップ 10　IVR NAT と IVR 自動トポロジ モードをイネーブルにして、対応する IVR ゾーンと IVR ゾーン セットを作成する場合は、[Finish] をクリックします。

[Save Configuration] ダイアログボックスが表示されます。他の IVR 対応スイッチにコピーするマスター スイッチの設定を保存できます。

ステップ 11　[Continue Activation] をクリックするか、[Cancel] をクリックします。

ステップ 12　[Finish] をクリックします。

（注）　IVR Zone Wizard を使用せずに IVR NAT と IVR 自動トポロジ モードを設定する場合は、これらを個別に設定できます。「基本的な Inter-VSAN Routing の設定」（P.1-14）を参照してください。

IVR のイネーブル化

IVR 機能は、IVR に関与しているファブリック内のすべての境界スイッチで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。ファブリック内の必要なすべてのスイッチで IVR を手動でイネーブルにすることも、IVR 設定のファブリック全体の配信を設定することもできます。「CFS を使用した IVR 設定の配信」（P.1-16）を参照してください。

IVR 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 IVR がイネーブルに設定されている場合だけです。この設定をディセーブルにした場合、関連するすべての設定は自動的に廃棄されます。

CFS を使用した IVR 設定の配信

IVR 設定配信は、デフォルトではディセーブルになっています。正しく機能するためには、ネットワーク内の IVR 対応のすべてのスイッチで、設定配信をイネーブルにしておく必要があります。

ここでは、次の内容について説明します。

- 「変更のコミット」（P.1-16）
- 「変更の廃棄」（P.1-16）
- 「ロック済みセッションのクリア」（P.1-16）

変更のコミット

アクティブ データベースに加えられた変更をコミットする場合、ファブリック内のすべてのスイッチに設定がコミットされます。コミットが正常に行われると、設定の変更がファブリック全体に適用され、ロックが解除されます。

変更の廃棄

保留中のデータベースに加えられた変更を廃棄（中断）する場合、コンフィギュレーション データベースは影響を受けないまま、ロックが解除されます。

ロック済みセッションのクリア

IVR タスクを実行し、変更の確定か破棄を行ってロックを解除していない場合、管理者はファブリックのスイッチからロックを解除できます。管理者がこの操作を行うと、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　保留データベースは、一時的なディレクトリだけで使用可能であり、スイッチが再起動されると破棄されることがあります。

IVR NAT と IVR 自動トポロジ モードのイネーブル化

ここでは、IVR NAT をイネーブルにする方法と IVR 自動トポロジ モードをイネーブルにする方法について説明します。

前提条件

IVR NAT と IVR 自動トポロジ モードを使用するように IVR SAN ファブリックを設定する前に、次のガイドラインを考慮してください。

- 関連するスイッチ以外で IVR を設定しないようにします。
- ファブリック内のすべてのスイッチ上で IVR 用の CFS をイネーブルにします。ダイアログボックスの他のタブを使用可能にするには、最初に [CFS] タブをクリックする必要があります。
- ファブリック内のすべてのスイッチで、Cisco MDS SAN-OS Release 2.1(1a) 以降が動作していることを確認します。
- Cisco MDS SAN-OS Release 2.1(1a) 以降がインストールされており、この機能に対応したアクティブな IPS カードが実装されている場合は、必須の Enterprise License Package または SAN-EXTENSION ライセンス パッケージを取得します。ライセンスの詳細については、『*Cisco MDS 9000 Family NX-OS Licensing Guide*』を参照してください。
- IVR 自動トポロジ モードを設定する前に、IVR 設定配信をイネーブルにします（「CFS を使用した IVR 設定の配信」（P.1-16）を参照）。IVR 自動トポロジ モードをイネーブルにした後は、IVR 設定配信をディセーブルにできなくなります。

制約事項

- FSPF リンク コストを変更した場合は、すべての IVR パスの FSPF パス距離（パスのリンク コストの合計）が 30,000 未満であるか確認します。
- IVR over FCIP 機能が Cisco MDS 9216i スイッチにバンドルされているため、スーパーバイザ モジュールの固定 IP ポート用の SAN Extension over IP パッケージが必要ありません。
- interop モードがイネーブル（いずれかの interop モード）またはディセーブル（interop モード以外）の場合に、IVR 対応 VSAN を設定できます。

手順の詳細

IVR NAT および IVR 自動トポロジ モードをイネーブルにするには、次の手順を実行します。

ステップ 1　[Logical Domains] ペインで、[All VSANs] を開き、[IVR] を選択します。

[Information] ペインに VSAN 間ルーティング設定が表示されます。

ステップ 2　プライマリ スイッチの [Admin] カラムのドロップダウン メニューで [Enable] を選択します。

ステップ 3　[Apply Changes] アイコンをクリックして、この変更をファブリック内のすべてのスイッチに配信します。

ステップ 4　[Action] タブをクリックします。

ステップ 5　[Enable IVR Nat] チェックボックスをオンにして、NAT モードで IVR をイネーブルにします。

ステップ 6　[Auto Discover Topology] チェックボックスをオンにして、IVR 自動トポロジ モードをイネーブルにします。

ステップ 7　[Apply Changes] アイコンをクリックし、スイッチの IVR をイネーブルにします。

IVR ゾーンと IVR ゾーン セットの設定

制約事項

- プレフィクスが IVRZ のゾーンまたは [nozonset] という名前のゾーン セットは作成しないでください。これらの名前はシステムで作成され、IVR ゾーンを識別するために使用されています。

手順の詳細

IVR ゾーンと IVR ゾーン セットを作成するには、次の手順を実行します。

ステップ 1　[Zone] > [IVR] > [Edit Local Full Zone Database] を選択します。

選択した VSAN の [Edit IVR Local Full Zone Database] ダイアログボックスが表示されます。

ゾーン メンバーシップ情報を表示する場合は、[Members] カラムを右クリックして、ポップアップ メニューで現在の行、またはすべての行の [Show Details] をクリックします。

ステップ 2　左側ペインの [Zones] をクリックし、[Insert] アイコンをクリックして、ゾーンを作成します。

[Create IVR Zone] ダイアログボックスが表示されます。

ステップ 3　IVR ゾーン名を入力します。

ステップ 4　次のチェックボックスのうち 1 つをオンにします。

a. **Read Only**：このゾーンでは読み込みを許可しますが、書き込みは拒否します。

b. **Permit QoS traffic with Priority**：ドロップダウン メニューでプライオリティを設定します。

ステップ 5　[OK] をクリックして IVR ゾーンを作成します。

ステップ 6　このゾーンにメンバーを追加するには、[Fabric] ペインから追加するメンバーを選択して、[Add to Zone] をクリックします。

ステップ 7　または、メンバーを追加するゾーンをクリックし、[Insert] アイコンをクリックします。

[Add Member to Zone] ダイアログボックスが表示されます。

ステップ 8　ゾーン セットを追加する場合は、新しいゾーン セットを選択し、[Activate] をクリックします。

[Save Configuration] ダイアログボックスが表示されます。

ステップ 9　[Save Running to Startup Configuration] チェックボックスをオンにして、すべての変更をスタートアップ コンフィギュレーションに保存します。

ステップ 10　[Continue Activation] をクリックして、ゾーン セットをアクティブにします。

（注）　論理ビューには、プレフィクス IVRZ で始まるゾーン名、および **nozoneset** という名前のゾーン セットが表示されることがあります。プレフィクスが IVRZ のゾーンは、標準アクティブ ゾーンに付加される IVR ゾーンです。アクティブ IVR ゾーンには、自動的にプレフィクスの IVRZ が付加されます。同様に、VSAN で使用可能なアクティブ ゾーン セットが存在しない場合と ivrZonesetActivateForce フラグがスイッチ上でイネーブルになっている場合は、nozoneset という名前のゾーン セットが、自動的に作成された IVR アクティブ ゾーン セットです。

server.properties ファイルで、プロパティの zone.ignoreIVRZones を [true] または [false] に設定することによって、標準アクティブ ゾーンとしての IVR ゾーンの表示 / 非表示を切り替えることができます。server.properties ファイルの詳細については、『*Cisco DCNM Fundamentals Configuration Guide*』を参照してください。

ステップ 11　[Information] ペインのリストで新しいゾーンまたはゾーン セットを選択して、[Distribute] をクリックします。

IVR CFS リージョンを使用した IVR ゾーンの設定

手順の詳細

IVR CFS リージョンを使用して IVR ゾーンを作成するには、次の手順を実行します。

ステップ 1　すべてのスイッチで IVR をイネーブルにします。

この時点では、IVR 対応スイッチに IVR CFS リージョンが設定されていない必要があります。

ステップ 2　[Zone] > [IVR] > [Edit Local Full Zone Database] を選択します。

選択した VSAN の [Edit IVR Local Full Zone Database] ダイアログボックスが表示されます。

ステップ 3　[Regions] ドロップダウン メニューから、[IVR Region ID] を選択します。

リージョンには、IVR 対応スイッチだけを含める必要があります。

ステップ 4　左側ペインの [Zones] をクリックし、[Insert] アイコンをクリックして、ゾーンを作成します。

[Create IVR Zone] ダイアログボックスが表示されます。

ステップ 5　IVR ゾーン名を入力します。

ステップ 6　次のチェックボックスのうち 1 つをオンにします。

a. **Read Only**：このゾーンでは読み込みを許可しますが、書き込みは拒否します。

b. **Permit QoS traffic with Priority**：ドロップダウン メニューでプライオリティを設定します。

ステップ 7　[OK] をクリックして IVR ゾーンを作成します。

ステップ 8　このゾーンにメンバーを追加するには、[Fabric] ペインから追加するメンバーを選択して、[Add to Zone] をクリックします。

ステップ 9　または、メンバーを追加するゾーンをクリックし、[Insert] アイコンをクリックします。

[Add Member to Zone] ダイアログボックスが表示されます。

ステップ 10　ゾーン セットを追加する場合は、新しいゾーン セットを選択し、[Activate] をクリックします。

[Save Configuration] ダイアログボックスが表示されます。

ステップ 11　[Save Running to Startup Configuration] チェックボックスをオンにして、すべての変更をスタートアップ コンフィギュレーションに保存します。

ステップ 12　[Continue Activation] をクリックして、ゾーン セットをアクティブにします。

（注）　CFS リージョンを使用するスイッチでアクティベーションが実行された場合、コミットによって単一スイッチのアクティベーションが完了します。アクティベーション ステータスは、SNMP トレースを通じて確認できます。

設定済みの IVR CFS リージョン内にあるスイッチが CFS 対応でなかった場合、アクティベーションのときにエラー メッセージが表示されます。

適用 IVR ゾーン セットを使用した IVR CFS リージョンの設定

手順の詳細

IVR CFS リージョンを使用して IVR ゾーンを作成するには、次の手順を実行します。

ステップ 1　すべてのスイッチで IVR をイネーブルにします。

この時点では、IVR 対応スイッチに IVR CFS リージョンが設定されていない必要があります。

ステップ 2　[Zone] > [IVR] > [Edit Local Full Zone Database] を選択します。

選択した VSAN の [Edit IVR Local Full Zone Database] ダイアログボックスが表示されます。

ステップ 3　[Regions] ドロップダウン メニューから、[IVR Region ID] を選択します。

リージョンには、IVR 対応スイッチだけを含める必要があります。

ステップ 4　左側ペインの [Zones] をクリックし、[Insert] アイコンをクリックして、ゾーンを作成します。

[Create IVR Zone] ダイアログボックスが表示されます。

ステップ 5　リージョンごとに、適用 IVR ゾーンを作成します。

論理ペインの VSAN ツリーで、IVR ツリー ノードの下に、リージョンごとに適用される各ゾーン セットのノードが表示されます。適用ゾーン ツリー ノードをクリックすると、右ペインの表に、関連する IVR CFS リージョンに適用されるゾーンおよびゾーン メンバーが表示されます。リージョンのゾーンがアクティブ化または非アクティブ化されると、VSAN ツリーは動的に更新されます。

ゾーン セットのアクティブ化および force オプションの使用

作成して設定したゾーン セットは、アクティブにする必要があります。IVR ゾーン セットをアクティブにすると、自動的に、各エッジ VSAN の標準アクティブ ゾーン セットに IVR ゾーンが追加されます。VSAN にアクティブ ゾーン セットが存在しない場合、IVR は force オプションを使用して IVR ゾーン セットをアクティブにすることしかできません。このとき、「nozoneset」という名前のアクティブ ゾーン セットが作成され、そのアクティブ ゾーン セットに IVR ゾーンが追加されます。

注意　VSAN 内の標準アクティブ ゾーン セットを非アクティブにすると、IVR ゾーン セットも非アクティブになります。これは、標準アクティブ ゾーン セット内の IVR ゾーンと、スイッチとの間でやり取りされるすべての IVR トラフィックが停止するために起こります。IVR ゾーン セットを再アクティブ化するには、標準ゾーン セットを再アクティブ化する必要があります。

（注）　同じファブリック内で IVR と iSLB がイネーブルになっている場合は、ファブリック内の少なくとも 1 つのスイッチで両方の機能をイネーブルにする必要があります。ゾーン分割関連のすべての設定またはアクティベーション操作（通常のゾーン、IVR ゾーン、または iSLB ゾーンに対して）をこのスイッチ上で実行する必要があります。そうしなければ、ファブリック内のトラフィックが中断される可能性があります。

IVR ゾーン セットをアクティブにするには、**force activate** オプションも使用できます。表 1-7 に、force activate オプションを使用する場合と使用しない場合の各種シナリオを示します。

表 1-7　Force Activate オプションを使用する場合と使用しない場合の IVR シナリオ

ケース	デフォルト ゾーン ポリシー	IVR ゾーンをアクティブにする前のアクティブ ゾーン セット	Force Activate オプションが使用されたか	IVR ゾーン セットのアクティベーション ステータス	アクティブ IVR ゾーンが作成されたか	トラフィックが中断する可能性があるか
1	Deny	アクティブ ゾーンセットが存在しない	No	Failure	No	No
2			Yes	Success	Yes	No
3[1]	Deny	アクティブ ゾーンセットが存在する	No/Yes	Success	Yes	No
4	Permit	アクティブ ゾーンセットが存在しない *または* アクティブ ゾーンセットが存在する	No	Failure	No	No
5			Yes	Success	Yes	Yes

1. ケース 3 のシナリオを使用することをお勧めします。

注意　IVR ゾーン セットのアクティベーションに **force activate** オプションを使用した場合は、IVR に関与しないデバイスについても、トラフィックが中断する可能性があります。たとえば、設定にアクティブ ゾーン セットが含まれておらず、デフォルト ゾーン ポリシーが permit の場合は、IVR ゾーン セットのアクティベーションが失敗します。ただし、**force activate** オプションを使用すれば、IVR ゾーン セットのアクティベーションが成功します。各 IVR ゾーンに対応するエッジ VSAN 上にゾーンが作成されるので、デフォルトのゾーン ポリシーが permit であるエッジ VSAN では、トラフィックが中断される可能性があります

IVR ゾーン セットのアクティブ化または非アクティブ化

制約事項

- トラフィックを中断せずに、アクティブな IVR ゾーン セットを新しい IVR ゾーン セットで置き換えるには、現在のアクティブな IVR ゾーン セットを非アクティブにすることなく、新しい IVR ゾーン セットをアクティブにします。

手順の詳細

既存の IVR ゾーン セットをアクティブまたは非アクティブにするには、次の手順を実行します。

ステップ 1　[Zone] をクリックして、[Edit Local Full Zone Database] を選択します。

[Edit Local Full Zone Database] ダイアログボックスが表示されます。

ステップ 2　[Zoneset] フォルダを選択してから [Activate] をクリックしてゾーン セットをアクティブにするか、[Deactivate] をクリックしてアクティブなゾーン セットを非アクティブにします。

[Save Configuration] ダイアログボックスが表示されます。

ステップ 3　（任意）[Save Running to Configuration] チェックボックスの 1 つをオンにして、これらの変更をスタートアップ コンフィギュレーションに保存します。

ステップ 4　ゾーン セットをアクティブにするには、[Continue Activation] をクリックします。ゾーン セットを非アクティブにしている場合は、[Yes] をクリックします。

（注）　フル ゾーン セットが変更された結果、アクティブ ゾーン セットとフル ゾーン セットの間に相違が生じた場合は、Edit Zone 内のアクティブ ゾーン セットが太字で表示されます。ゾーン セットがアクティブになると、太字が解除されます。

IVR ロギング重大度の設定

IVR 機能に関する Telnet または SSH ロギングを設定できます。たとえば、IVR ロギング レベルをレベル 4（warning）に設定した場合は、重大度が 4 以上のメッセージが表示されます。ここで紹介する手順を使用して、ロギング レベルを設定します。

手順の詳細

記録する IVR 機能のメッセージの重大度を設定するには、次の手順を実行します。

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

ステップ 2　[Severity Levels] タブをクリックします。

ステップ 3　[Facility] カラム ヘッダーをクリックし、ファシリティ名ごとにテーブルをソートします。

ステップ 4　[Severity] ドロップダウン メニューで IVR がシステム メッセージを記録する重大度を選択します。

ヒント　重大度を **warning** に設定することは、警告レベル以上のすべての IVR メッセージが DCNM-SAN に記録されることを意味します。

ステップ 5　[Apply Changes] アイコンをクリックして、これらの変更をローカルに保存します。

基本的な Inter-VSAN Routing 設定のモニタリング

ここでは、次の内容について説明します。

- 「IVR fcdomain データベースの消去」（P.1-23）
- 「IVR フル ゾーン データベースの回復」（P.1-23）
- 「IVR トポロジの回復」（P.1-23）
- 「データベースのマージ障害の解決」（P.1-24）

IVR fcdomain データベースの消去

手順の詳細

IVR 仮想ドメインを手動で設定するには、次の手順を実行します。

ステップ 1　[Logical Domains] ペインで、[All VSANs] を開き、[IVR] を選択します。

[Information] ペインに IVR 設定が表示されます。

ステップ 2　[Domains] タブをクリックして、既存の IVR トポロジを表示します。

ステップ 3　[Create Row] アイコンをクリックして、IVR トポロジに行を作成します。

ステップ 4　ダイアログボックスで、現在のファブリック、現在の VSAN、ネイティブ ファブリック、ネイティブ VSAN、およびドメイン ID を入力します。これらは、割り当て済みドメイン リストに IVR 仮想ドメインを追加する VSAN です。

ステップ 5　[Create] をクリックして新しい行を作成します。

IVR フル ゾーン データベースの回復

IVR ゾーン データベースを回復するには、別のスイッチから IVR フル ゾーン データベースをコピーします。

手順の詳細

IVR ゾーン データベースを回復するには、次の手順を実行します。

ステップ 1　[Zone] > [IVR] > [Edit Local Full Zone Database] を選択します。

[Edit IVR Local Full Zone Database] ダイアログボックスが表示されます。

ステップ 2　[Edit] > [Copy Full Zone Database] を選択します。

[Copy Full Zone Database] ダイアログボックスが表示されます。

ステップ 3　コピーする IVR データベースのタイプに応じて、[Active] または [Full] を選択します。

ステップ 4　ドロップダウン リストで、情報のコピー元のスイッチを選択します。

ステップ 5　ドロップダウン リストでコピー先のスイッチを選択します。

ステップ 6　[Copy] をクリックしてデータベースをコピーします。

IVR トポロジの回復

トポロジを回復するには、アクティブ ゾーン データベースまたはフル ゾーン データベースをコピーします。

手順の詳細

ゾーン トポロジを回復するには、次の手順を実行します。

ステップ 1　[Zone] > [IVR] > [Edit Local Full Zone Database] を選択します。

[Edit IVR Local Full Zone Database] ダイアログボックスが表示されます。

ステップ 2　[Edit] > [Copy Full Topology] を選択します。

[Copy Full Topology] ダイアログボックスが表示されます。

ステップ 3　コピーする IVR データベースのタイプに応じて、[Active] または [Full] を選択します。

ステップ 4　ドロップダウン リストで、情報のコピー元のスイッチを選択します。

ステップ 5　ドロップダウン リストでコピー先のスイッチを選択します。

ステップ 6　[Copy] をクリックしてトポロジをコピーします。

データベースのマージ障害の解決

マージの障害が発生した場合は、次の CLI コマンドを使用するとエラー状態が表示されます。

- **show ivr merge status**
- **show cfs merge status name ivr**
- **show logging last** *lines*（表示結果で MERGE 障害を調べます）

マージ障害を解決するには、**show** コマンドの出力に示された障害情報を確認し、障害に関連するこのリスト内のシナリオを見つけて、トラブルシューティングの指示に従います。

- スイッチが複数の Cisco SAN-OS または NX-OS リリースを実行しているファブリックで、最大設定の制限を超えたことによって障害が発生した場合は、以前のリリースを実行しているスイッチをアップグレードするか、またはより新しいリリースを実行しているスイッチで、IVR ゾーンおよび IVR ゾーン メンバーの数を減らします（「IVR の設定制限」（P.1-4）を参照）。
- すべてのスイッチが同じ Cisco SAN-OS or NX-OS リリースを実行しているファブリックで、最大制限を超えたことによって障害が発生した場合は、正しい設定のスイッチを特定し、CFS コミットを実行して IVR 設定を配信します。「CFS を使用した IVR 設定の配信」（P.1-16）および「Autonomous Fabric ID」（P.2-2）を参照してください。
- その他の障害の場合は、正しい設定を持つスイッチにおいてマージ障害の原因となっているエラーを解決し、CFS コミットを実行して IVR 設定を配信してください。「CFS を使用した IVR 設定の配信」（P.1-16）および「Autonomous Fabric ID」（P.2-2）を参照してください。

（注）　CFS コミットが正常終了すると、マージも成功します。

関連情報

基本的な IVR 設定のセットアップ後に高度な IVR 設定が必要な場合は、第 2 章「高度な Inter-VSAN Routing の設定」を参照してください。

CHAPTER 2

高度な Inter-VSAN Routing の設定

この章では、高度な設定に関する情報と手順について説明します。高度な IVR 設定をセットアップする前に、第 1 章「基本的な Inter-VSAN Routing の設定」で基本的な設定手順と IVR 機能の説明、制限事項、および用語を参照してください。

この章の内容は、次のとおりです。

- 「高度な Inter-VSAN Routing について」（P.2-1）
- 「注意事項と制限」（P.2-3）
- 「高度な Inter-VSAN Routing の設定」（P.2-8）

高度な Inter-VSAN Routing について

ここでは、次の内容について説明します。

- 「IVR サービス グループ」（P.2-1）
- 「デフォルト サービス グループ」（P.2-1）
- 「サービス グループのアクティベーション」（P.2-2）
- 「Autonomous Fabric ID」（P.2-2）
- 「FC ID の機能とメリット」（P.2-2）
- 「高度な IVR ゾーンと IVR ゾーン セット」（P.2-2）
- 「IVR フローにおける高度なファブリック サービス」（P.2-3）

IVR サービス グループ

複雑なネットワーク トポロジ内に、いくつかの IVR 対応 VSAN だけが存在するものとします。非 IVR 対応 VSAN へのトラフィック量を削らすには、IVR 対応 VSAN へのトラフィックを制限するサービス グループを設定する必要があります。ネットワーク上では、最大 16 個の IVR サービス グループが許可されます。新しい IVR 対応スイッチをネットワークに追加した場合は、新しい VSAN を含むようにサービス グループを更新する必要があります。

デフォルト サービス グループ

IVR VSAN トポロジの一部であるが、ユーザ定義のサービス グループの一部ではないすべての AFID と VSAN の組み合わせが、デフォルト サービス グループのメンバーです。デフォルト サービス グループの識別番号は 0 です。

デフォルトで、デフォルト サービス グループのメンバー間の IVR 通信が許可されます。デフォルト ポリシーを deny に変更できます。デフォルト ポリシーを変更するには、「IVR サービス グループの設定」（P.2-10）を参照してください。デフォルト ポリシーは ASCII 設定の一部ではありません。

サービス グループのアクティベーション

設定したサービス グループはアクティブにする必要があります。ゾーン セットのアクティベーションや VSAN トポロジのアクティベーションと同様に、設定したサービス グループをアクティブにすると、現在アクティブなサービス グループが、もしあれば、設定したサービス グループに置き換えられます。設定済みのサービス グループ データベースとアクティブなサービス グループ データベースは 1 つずつしか存在しません。これらのデータベースのそれぞれに最大 16 個のサービス グループを設定できます。

Autonomous Fabric ID

Autonomous Fabric ID（AFID）は、セグメント化された VSAN（たとえば、論理的にも物理的にも分離しているが、同じ VSAN 番号を持つ 2 つの VSAN）を区別するためのものです。Cisco Fabric Manager Release 4.2(1) は、AFID の 1 ～ 64 をサポートします。AFID を IVR 自動トポロジ モードと組み合わせて使用すれば、IVR VSAN トポロジ データベース内でセグメント化された VSAN を使用できます。

FC ID の機能とメリット

FC ID の永続性によって、IVR 管理を容易にする次の機能が提供されます。

- ネイティブ VSAN で使用する仮想ドメインを割り当てて管理することができます。
- デバイス専用の仮想 FC ID を割り当てて管理することができます。

IVR の永続的 FC ID のメリットを以下に示します。

- ホスト デバイスは、常に、同じ FC ID でターゲットを識別できます。
- IVR が使用する仮想ドメインを割り当てることで、SAN レイアウトをより適切に計画できます。
- SAN モニタリングと管理が容易になります。一貫して同じドメインまたは FC ID が割り当てられていれば、それが参照するネイティブ VSAN やデバイスを容易に識別できます。

高度な IVR ゾーンと IVR ゾーン セット

ここでは、IVR ゾーンと IVR ゾーン セットに関する高度な設定について説明します。IVR ゾーンとゾーン セットの設定に関する基本的な情報については、「IVR ゾーンと IVR ゾーン セットの設定」（P.1-18）を参照してください。

IVR 設定の一部として、1 つ以上の IVR ゾーンを設定して、VSAN 間通信をイネーブルにする必要があります。そのためには、各 IVR ゾーンを（pWWN、VSAN）エントリの集合として指定する必要があります。IVR ゾーンは 1 つ以上の IVR ゾーン セットのメンバーにすることができるため、複数の IVR ゾーン セットに同じ IVR ゾーンを含めることができます。

（注）　同じ IVR ゾーン セットは、すべての IVR 対応スイッチ上でアクティブにする必要があります。

注意　Cisco SAN-OS Release 3.0(3) よりも前のリリースでは、ネットワーク内のスイッチ上に合計で最大 10,000 のゾーン メンバーしか設定できません。Cisco SAN-OS Release 3.0(3) 以降のリリースでは、ネットワーク内のスイッチ上に合計で最大 20,000 のゾーン メンバーを設定できます。1 つのゾーン メンバーが 2 つのゾーンに存在する場合は、2 回カウントされます。「データベース マージに関する注意事項」（P.1-11）を参照してください。

IVR CFS リージョン

IVR は、異なる VSAN のデバイスが相互に通信するために使用されます。ファブリック サイズの増大に合わせて、IVR アイランドを作成する必要があります。IVR データ通信は、アイランド内に制限されます。さまざまな IVR CFS リージョンを作成して、データ通信をリージョン内に制限することができます。

現在、DCNM-SAN は単一の IVR CFS リージョンのみをサポートします。

Release 5.2 から、DCNM-SAN は複数の IVR リージョンをサポートし、次の機能が搭載されます。

- 複数の IVR 適用ゾーン セットと、IVR マスター スイッチのサポート（リージョン単位）。
- DCNM-SAN テーブルのすべてのスイッチに対するアクティブでローカルなトポロジの表示。各リージョンのトポロジを変更するには、マスター スイッチを選択する必要があります。
- CFS IVR リージョンが設定されていない場合、スイッチはデフォルト リージョンに属します。
- DCNM-SAN は、各スイッチのリージョン、リージョン ID、および IVR CFS ステートによって、複数の適用 IVR ゾーンを検出します。
- クライアント イベントまたはサーバ イベントは、（各リージョンの）IVR CFS ステート、リージョン ID、および適用 IVR ゾーンの変更を考慮して修正されます。
- DCNM-SAN クライアントのログ ウィンドウには、IVR のすべてのリージョン情報が反映されます。

現在、DCNM-SAN クライアントは、CFS リージョンのゾーン分割をサポートしています。

IVR フローにおける高度なファブリック サービス

高度なファブリック サービス（SME や IOA など）は、ファブリック全体の FC リダイレクト インフラストラクチャを使用して、トラフィック フローをリダイレクトします。これらのサービスは、内部機能の Abstract ACL Manager（AAM）を使用して IVR フロー上でイネーブルにできるようになりました。

注意事項と制限

ここでは、次の内容について説明します。

- 「サービス グループに関するガイドライン」（P.2-4）
- 「Autonomous Fabric ID に関するガイドライン」（P.2-4）
- 「IVR NAT または IVR 自動トポロジを使用しない IVR に関するガイドライン」（P.2-5）
- 「手動での IVR トポロジ設定に関するガイドライン」（P.2-6）
- 「FC ID に関するガイドライン」（P.2-7）

- 「IVR ゾーン設定に関するガイドライン」（P.2-8）
- 「高度なファブリック サービスに関する注意事項および制約事項」（P.2-8）

サービス グループに関するガイドライン

IVR サービス グループを設定する場合は、次のガイドラインについて考慮してください。

- IVR 自動トポロジ モードと一緒にサービス グループを使用する場合は、IVR をイネーブルにしてサービス グループを設定し、それらを CFS を使用して配信してから、IVR 自動トポロジ モードを設定します。
- IVR VSAN トポロジが IVR 自動トポロジ モードの場合にのみ、CFS 配信がサービス グループ内に制限されます。「IVR VSAN のトポロジ」（P.1-6）を参照してください。
- ネットワーク上には、最大 16 個のサービス グループを設定できます。
- 新しい IVR 対応スイッチをネットワークに追加した場合は、新しい VSAN を含むようにサービス グループを更新する必要があります。
- 同じ VSAN と AFID の組み合わせを複数のサービス グループのメンバーにはできません。そうした場合は、CFS マージが失敗します。
- すべてのサービス グループ内の AFID と VSAN の組み合わせの総数は 128 以下にする必要があります。1 つのサービス グループ内の AFID と VSAN の組み合わせの最大数は 128 です。
- IVR サービス グループ設定は、すべての IVR 対応スイッチに配信されます。同じサービス グループに属している 2 つのエンド デバイス間の IVR データ トラフィックは、そのサービス グループ以外には配信されません。たとえば、2 つのメンバー（pWWN 1 と pWWN 2 など）が同じ IVR ゾーンに属しているが、サービス グループが異なる場合は、通信することができません。
- CFS マージでは、他のサービス グループと競合しない限り、同じ名前のサービス グループがマージされます。
- CFS マージ中にサービス グループの総数が 16 を超えた場合は、CFS マージが失敗します。
- CFS から到達可能なすべての SAN にサービス グループの設定情報が配信されます。CFS 配信をイネーブルにしない場合は、すべての VSAN 内のすべての IVR 対応スイッチ上でサービス グループ設定が同じであることを保証する必要があります。
- ある IVR サービス グループに属している IVR エンド デバイスは、他のサービス グループに属している AFID または VSAN にエクスポートされません。
- 1 つ以上のサービス グループが定義されており、ある IVR ゾーン メンバーがどのサービス グループにも属していない場合、その IVR ゾーン メンバーは他のどのデバイスとも通信できません。
- デフォルト サービス グループ ID はゼロ（0）です。

Autonomous Fabric ID に関するガイドライン

各 VSAN に AFID を個別に設定するか、またはすべての VSAN に対応したデフォルト AFID を特定のスイッチに設定できます。デフォルトの AFID を持つスイッチ上の VSAN のサブセットに対して個別の AFID を設定した場合は、そのサブセットでは設定した AFID が使用されますが、そのスイッチ上の他の VSAN ではデフォルトの AFID が使用されます。

VSAN トポロジが IVR 自動トポロジ モードの場合は、1 つの AFID 設定しか使用できません。IVR 手動トポロジ モードでは、VSAN トポロジ設定自体で AFID が指定されるため、個別に AFID を設定する必要がありません。

（注）　VSAN 番号は同じだが、AFID が異なる 2 つの VSAN は、ファブリック内で許可された全部で 128 個の VSAN 以外の 2 つの VSAN としてカウントされます。

複数のスイッチに接続されたデバイスが 1 つの VSAN に属している場合は、AFID が異なるため、標準ゾーン セットを設定しても相互通信はできません。ファブリックごとに AFID を変えることを検討することができます。つまり、3 つのスイッチは 3 つの異なるファブリックを意味します。

IVR NAT または IVR 自動トポロジを使用しない IVR に関するガイドライン

NAT モード、または IVR 自動トポロジ モードの IVR を使用しない IVR SAN ファブリックを設定する前に、次の一般的なガイドラインを考慮してください。

- 必須の Enterprise License Package または SAN-EXTENSION ライセンス パッケージとこの機能に使用可能な IPS カードを調達します。
- FSPF リンク コストを変更した場合は、すべての IVR パスの FSPF パス距離（パスのリンク コストの合計）が 30,000 未満であるか確認します。
- interop モードがイネーブルでもディセーブルでも、IVR 対応 VSAN を設定できます。

ここでは次の項目についても説明します。

- 「ドメイン ID に関するガイドライン」（P.2-5）
- 「中継 VSAN に関するガイドライン」（P.2-6）
- 「境界スイッチに関するガイドライン」（P.2-6）

ドメイン ID に関するガイドライン

ドメイン ID を設定する前に、次のガイドラインを考慮してください。

- IVR NAT を使用しない場合は、IVR 動作に関与するすべての VSAN とスイッチを通して一意のドメイン ID を設定します。次のスイッチが IVR 動作に関与します。
  - エッジ VSAN 内のすべてのエッジ スイッチ（送信元と送信先）
  - 中継 VSAN 内のすべてのスイッチ
- ドメイン ID 割り当てが必要なスイッチ数を最小にします。これによって、トラフィック中断が最小限に抑えられます。
- SAN を初めて設定する場合と新しいスイッチを追加する場合に、相互接続された VSAN 間の調整を最小にします。

ドメイン ID を設定するには、次の 2 つのオプションのどちらかを使用します。

- 関与するすべてのスイッチと VSAN 上で、異なる VSAN 内のドメインが重複しないように、許可ドメイン リストを設定します。
- 関与するスイッチと VSAN ごとに、重複していない静的なドメインを設定します。

（注）　NAT を使用しない IVR に関する設定で、IVR トポロジ内の 1 つの VSAN が静的なドメイン ID で設定されている場合は、そのトポロジ内の他の VSAN（エッジまたは中継）を静的なドメイン ID で設定する必要があります。

中継 VSAN に関するガイドライン

中継 VSAN を設定する前に、次のガイドラインを考慮してください。

- IVR ゾーン メンバーシップを定義するほかに、一連の中継 VSAN を指定して、2 つのエッジ VSAN を接続することもできます。
  - IVR ゾーン内の 2 つのエッジ VSAN が重複している場合は、中継 VSAN がなくても接続できます（ただし、禁止されるわけではありません）。
  - IVR ゾーン内の 2 つのエッジ VSAN が重複していない場合は、1 つ以上の中継 VSAN がなければ接続できません。送信元と送信先の両方のエッジ VSAN に属しているスイッチ上で IVR がイネーブルになっていない場合は、IVR ゾーン内の 2 つのエッジ VSAN が重複することはありません。
- エッジ VSAN 間のトラフィックは、必ず最短の IVR パスを経由します。
- 中継 VSAN 情報は、すべての IVR ゾーン セットで共通です。場合によっては、中継 VSAN が別の IVR ゾーン内のエッジ VSAN として機能することもできます。

境界スイッチに関するガイドライン

境界スイッチを設定する前に、次のガイドラインを考慮してください。

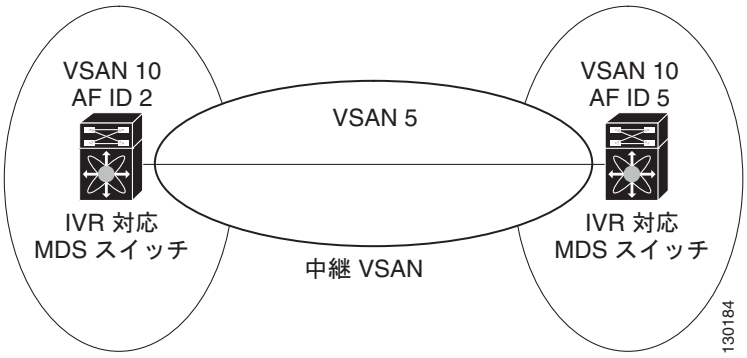
- 関連する境界スイッチ以外で IVR を設定しないようにします。
- 境界スイッチには Cisco MDS SAN-OS Release 1.3(1) 以降が必要です。
- 境界スイッチは複数の VSAN のメンバーにする必要があります。
- IVR 通信を実行する境界スイッチは IVR に対応している必要があります。
- 追加の境界スイッチ上で IVR をイネーブルにして、アクティブな IVR ゾーン メンバー間に冗長パスを提供することもできます。
- 境界スイッチを追加または削除する前に、VSAN トポロジ設定を更新する必要があります。

手動での IVR トポロジ設定に関するガイドライン

IVR 自動トポロジ モードをイネーブルにしなかった場合は、ファブリック内のすべての IVR 対応スイッチ上で IVR トポロジを作成する必要があります。IVR 手動トポロジ モードを使用する場合は、次のガイドラインを考慮してください。

- 1 つの IVR トポロジ内に設定できるのは、最大 128 台の IVR 対応スイッチと 128 個の異なる VSAN です（「データベース マージに関する注意事項」（P.1-11）を参照）。
- 次の情報を使用して、IVR トポロジを指定する必要があります。
  - IVR 対応スイッチのスイッチ WWN
  - IVR 対応スイッチが属する 2 つ以上の VSAN
  - 論理的にも物理的にも分離されているが、VSAN 番号が同じ 2 つの VSAN を区別する AFID。最大 64 個の AFID を指定できます。図 2-1 を参照してください。

図 2-1　AFID を使用し、一意ではない VSAN ID を持つ IVR トポロジの例



- 1 つの IVR トポロジ内の 2 つの VSAN が VSAN ID は同じだが AFID が異なる場合、それらは IVR の 128 VSAN 制限に対して、2 つの VSAN としてカウントされます。
- 単一の AFID を使用している場合は、VSAN 間ルーティング トポロジ内で VSAN を分割できません。

FC ID に関するガイドライン

永続的 FC ID を設定する前に、次のガイドラインを考慮してください。

- 永続的 IVR FC ID に対して、次の 2 種類のデータベース エントリを設定できます。
  - 仮想ドメイン エントリ - 特定の VSAN（現在の VSAN）内のネイティブ VSAN を表すために使用すべき仮想ドメインが格納されます。仮想ドメイン エントリには、次の情報が格納されます。

    ネイティブ AFID

    ネイティブ VSAN

    現在の AFID

    現在の VSAN

    現在の AFID および VSAN 内のネイティブ AFID および VSAN で使用する仮想ドメイン

  - 仮想 FC ID エントリ - 特定の VSAN（現在の VSAN）内のデバイスを表すために使用すべき仮想 FC ID が格納されます。仮想 FC ID エントリには、次の情報が格納されます。

    ポート WWN

    現在の AFID

    現在の VSAN

    現在の AFID および VSAN 内で特定の pWWN のデバイスを表すために使用する仮想 FC ID
- IVR の永続的 FC ID を使用する場合は、IVR ゾーン セット内のすべてのデバイスに対して永続的 FC ID を使用することをお勧めします。一部の IVR デバイスに対して永続的 FC ID を使用し、その他のデバイスに対して自動割り当てを使用することはお勧めできません。
- IVR 永続的 FC ID を使用するには、IVR NAT をイネーブルに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。

IVR ゾーン設定に関するガイドライン

interop モードがイネーブルになっている場合は、次の IVR 設定に関するガイドラインを考慮してください。

- メンバーのネイティブ VSAN が interop モードの場合（interop モードが 2、3、または 4 の場合）は、ReadOnly、QoS 属性、および LUN ゾーン分割が許可されません。
- メンバーの VSAN がすでに interop モードになっている状態で、ReadOnly、QoS 属性、または LUN ゾーン分割を設定しようとすると、その設定が許可されていないことを示す警告メッセージが表示されます。
- ReadOnly、QoS 属性、または LUN ゾーン分割を設定してから、メンバーの VSAN interop モードを変更した場合は、その設定が許可されていないことを示す警告メッセージが表示されます。その後で設定を変更するように促されます。

高度なファブリック サービスに関する注意事項および制約事項

IVR に対して AAM をイネーブルにする前に、次の注意事項および制約事項について考慮する必要があります。

- IVR に対して CFS 配信をイネーブルにする必要がある。
- AAM は IVR-NAT モードだけでサポートされている。
- ファブリック サービス（SME や IOA など）がイネーブルになっているスイッチは、NX-OS Release 5.0(1) 以降でサポートされている AAM を実行する必要がある。
- FC リダイレクトは、バージョン 1 またはバージョン 2 のモードで実行できる。
- FCR に対する IVR サポートをイネーブルにする前に、IVR に対する AAM サポートをイネーブルにしておく必要がある。
- FCR に対して IVR サポートがイネーブルになっている場合、第 1 世代のモジュールはサポートされない。特に、ISL は第 1 世代のモジュールには設定できません。また、FCR に対して IVR をサポートしているデバイスは、第 1 世代のモジュールに接続できません。
- IVR に対して AAM がイネーブルになっている場合、LUN ゾーン分割はサポートされない。
- IVR マージは、両方のファブリックで AMM がイネーブルになっているか、または両方のファブリックで AAM がディセーブルになっている場合のみサポートされる。一方のファブリックで AAM がイネーブルになっていて、もう一方のファブリックでは AAM がディセーブルになっている場合、IVR マージは失敗します。
- IVR に対する AMM サポートをディセーブルにする前に、IVR デバイスに対する高度なファブリック サービス（SME や IOA）の設定をすべて削除し、その後で FCR に対する IVR サポートをディセーブルにする必要がある。
- MDS NX-OS Release 5.0(1) 以前のリリースにダウングレードする場合、その前に、IVR デバイスに対する高度なファブリック サービス（SME や IOA）の設定をすべて削除し、FCR に対する IVR のサポートをディセーブルにしたうえで、IVR に対する AAM サポートをディセーブルにする必要がある。

高度な Inter-VSAN Routing の設定

ここでは、次の内容について説明します。

- 「高度な Inter-VSAN Routing の設定のタスク フロー」（P.2-9）

- 「IVR サービス グループの設定」（P.2-10）
- 「デフォルト AFID の設定」（P.2-10）
- 「個別の AFID の設定」（P.2-11）
- 「NAT を使用しない IVR の設定」（P.2-11）
- 「IVR トポロジの手動設定」（P.2-11）
- 「手動で設定された IVR トポロジのアクティベーション」（P.2-12）
- 「手動で設定された IVR トポロジ データベースの削除」（P.2-13）
- 「IVR 自動トポロジ モードから IVR 手動トポロジ モードへの移行」（P.2-13）
- 「IVR の永続的 FC ID の設定」（P.2-13）
- 「IVR ゾーン分割における LUN の設定」（P.2-14）
- 「IVR ゾーンの QoS の設定」（P.2-14）
- 「IVR ゾーンと IVR ゾーン セットの名前の変更」（P.2-15）
- 「読み取り専用ゾーン分割を使用した IVR の設定」（P.2-15）

高度な Inter-VSAN Routing の設定のタスク フロー

SAN ファブリック内で高度な IVR トポロジを設定するには、次の手順を実行します。

	設定作業	リソース
ステップ 1	IVR Network Address Translation（NAT; ネットワーク アドレス変換）を使用すべきかどうかを判断します。	「IVR ネットワーク アドレス変換」（P.1-6）および「IVR NAT の要件とガイドライン」（P.1-9）を参照してください。
ステップ 2	IVR NAT を使用しない場合は、IVR に関与するすべてのスイッチと VSAN に一意のドメイン ID が設定されていることを確認します。	「ドメイン ID に関するガイドライン」（P.2-5）を参照してください。
ステップ 3	境界スイッチで IVR をイネーブルにします。	「IVR Zone Wizard を使用した IVR と IVR ゾーンの設定」（P.1-15）を参照してください。
ステップ 4	必要に応じて、サービス グループを設定します。	「IVR サービス グループ」（P.2-1）を参照してください。
ステップ 5	必要に応じて、IVR 配信を設定します。	
ステップ 6	手動または自動で IVR トポロジを設定します。	「IVR トポロジの手動設定」（P.2-11）と「基本的な Inter-VSAN Routing の設定」（P.1-14）を参照してください。
ステップ 7	手動で、またはファブリック配信を使用して、すべての IVR 対応境界スイッチで IVR ゾーン セットを作成してアクティブにします。	「高度な IVR ゾーンと IVR ゾーン セット」（P.2-2）を参照してください。

IVR サービス グループの設定

手順の詳細

IVR サービス グループを設定するには、次の手順を実行します。

ステップ 1　[Logical Domains] ペインで、[All VSANs] を開き、[IVR] を選択します。

[Information] ペインに IVR 設定が表示されます。

ステップ 2　[Service Group] タブをクリックして、既存のサービス グループを表示します。

ステップ 3　[Create Row] アイコンをクリックして、新しいサービス グループを作成します。

サービス グループのダイアログ ボックスが表示されます。

ステップ 4　IVR に関与するスイッチに対応するチェックボックスをオンにします。

ステップ 5　サービス グループの [Name] フィールドにデータを入力し、対応する [Fabric ID] フィールドにデータを入力します。

ステップ 6　[VSAN List] テキスト ボックスに、VSAN ID のカンマ区切りのリストを入力します。

ステップ 7　この入力を作成する場合は [Create] をクリックし、すべての変更を破棄する場合は [Cancel] をクリックします。

ステップ 8　IVR トポロジに関連するすべてのスイッチと AFID に対してステップ 1 からステップ 7 までを繰り返します。

デフォルト AFID の設定

手順の詳細

デフォルト AFID を設定するには、次の手順を実行します。

ステップ 1　[Logical Domains] ペインで、[All VSANs] を開き、[IVR] を選択します。

[Information] ペインに IVR 設定が表示されます。

ステップ 2　[Default Fabric ID] タブをクリックして、既存のデフォルト AFID を表示します。

ステップ 3　[Create Row] アイコンをクリックして、デフォルト AFID を作成します。

ステップ 4　このデフォルト AFID を使用する IVR に関与するスイッチの横のチェック ボックスをオンにします。

ステップ 5　各スイッチ WWN の名前を入力して、デフォルト ファブリック ID を設定します。

ステップ 6　[Create] をクリックして、このエントリを作成します。

ステップ 7　IVR トポロジ内に設定するすべてのデフォルト AFID に対してステップ 1 ～ステップ 6 を繰り返します。

個別の AFID の設定

手順の詳細

個別の AFID を設定するには、次の手順を実行します。

ステップ 1　[Logical Domains] ペインで、[All VSANs] を開き、[IVR] を選択します。
[Information] ペインに IVR 設定が表示されます。

ステップ 2　[Fabric ID] タブをクリックして、既存の AFID を表示します。

ステップ 3　[Create Row] アイコンをクリックして、AFID を作成します。

ステップ 4　このデフォルトの AFID を使用する IVR に関与するスイッチの横のチェック ボックスをオンにします。

ステップ 5　各スイッチ WWN の名前を入力して、ファブリック ID を設定します。

ステップ 6　[VSAN List] テキスト ボックスに、VSAN ID のカンマ区切りのリストを入力します。

ステップ 7　[Create] をクリックして、このエントリを作成します。

ステップ 8　IVR トポロジ内に設定するすべてのスイッチと AFID に対してステップ 1 ～ステップ 6 を繰り返します。

NAT を使用しない IVR の設定

手順の詳細

NAT を使用しない IVR をイネーブルにするには、次の手順を実行します。

ステップ 1　[Logical Domains] ペインで、[All VSANs] を開き、[IVR] を選択します。
[Information] ペインに IVR 設定が表示されます。

ステップ 2　[Action] タブをクリックします。

ステップ 3　[Enable IVR NAT] チェックボックスをオフにします。

ステップ 4　[Apply Changes] アイコンをクリックして、この変更をファブリック内のすべてのスイッチに配信します。

IVR トポロジの手動設定

制約事項

- 中継 VSAN はユーザ設定に基づいて決定されます。IVR には中継 VSAN の明示的な設定機能がありません。
- CFS を使用している機能の [Information] ペインのほとんどのタブは、[CFS] タブをクリックするまで薄く表示されます。[CFS] タブには、CFS がイネーブルになっているスイッチと、この機能のマスター スイッチが表示されます。[CFS] タブをクリックすると、[Information] ペインのその他のタブがアクティブになります。

- DCNM-SAN の [Information] ペインの IVR テーブルを使用して IVR を設定できます。このテーブルは、IVR の概念を完全に理解した上で使用してください。IVR の設定には、IVR Wizard の使用をお勧めします。「IVR Zone Wizard を使用した IVR と IVR ゾーンの設定」（P.1-15）を参照してください。

手順の詳細

IVR トポロジを手動で設定するには、次の手順を実行します。

ステップ 1　[Logical Domains] ペインで、[All VSANs] を開き、[IVR] を選択します。
[Information] ペインに IVR 設定が表示されます。

ステップ 2　[Local Topology] タブをクリックして、既存の IVR トポロジを表示します。

ステップ 3　[Create Row] アイコンをクリックして、IVR トポロジに行を作成します。

ステップ 4　このトポロジのスイッチ、スイッチ WWN、および VSAN ID のカンマ区切りリストを選択します。

ステップ 5　[Create] をクリックして新しい行を作成します。

ステップ 6　[Apply Changes] アイコンをクリックして IVR トポロジを作成します。

すべての IVR 対応スイッチ上でこの設定を繰り返すか、CFS を使用して IVR 設定を配信します。

手動で設定された IVR トポロジのアクティベーション

IVR トポロジは手動で設定した後にアクティブにする必要があります。

制約事項

- アクティブな IVR トポロジは非アクティブにできません。IVR 自動トポロジ モードに切り替えることはできます。

手順の詳細

手動で設定された IVR トポロジをアクティブにするには、次の手順を実行します。

ステップ 1　[Logical Domains] ペインで、[All VSANs] を開き、[IVR] を選択します。
[Information] ペインに IVR 設定が表示されます。

ステップ 2　[Action] タブをクリックして、既存の IVR トポロジを表示します。

ステップ 3　[Activate Local Topology] チェックボックスをオンにします。

ステップ 4　[Apply Changes] アイコンをクリックして IVR トポロジをアクティブ化します。

手動で設定された IVR トポロジ データベースの削除

手順の詳細

手動で作成された IVR トポロジ データベースを削除するには、次の手順を実行します。

ステップ 1　[Logical Domains] ペインで、[All VSANs] を開き、[IVR] を選択します。

ステップ 2　[Control] タブが表示されていない場合は、クリックします。

ステップ 3　IVR トポロジから削除する行を強調表示します。

ステップ 4　[Delete Row] アイコンをクリックして、IVR トポロジからこの行を削除します。

ステップ 5　[Apply Changes] アイコンをクリックして IVR トポロジを削除します。

IVR 自動トポロジ モードから IVR 手動トポロジ モードへの移行

前提条件

- IVR 自動トポロジ モードから IVR 手動トポロジ モードに移行する場合は、アクティブな IVR VSAN トポロジ データベースをユーザ設定 IVR VSAN トポロジ データベースにコピーしてから、モードを切り替えます。

手順の詳細

IVR 自動トポロジ モードから IVR 手動トポロジ モードへ移行するには、次の手順を実行します。

ステップ 1　[Logical Domains] ペインで、[All VSANs] を開き、[IVR] を選択します。
[Information] ペインに IVR 設定が表示されます。

ステップ 2　[Action] タブをクリックします。

ステップ 3　IVR 自動トポロジ モードをディセーブルにするスイッチを強調表示します。

ステップ 4　[Auto Discover Topology] チェックボックスをオフにします。

ステップ 5　[Apply Changes] アイコンをクリックします。

IVR の永続的 FC ID の設定

手順の詳細

IVR の永続的 FC ID を設定するには、次の手順を実行します。

ステップ 1　[Logical Domains] ペインで、[All VSANs] を開き、[IVR] を選択します。
[Information] ペインに IVR 設定が表示されます。

ステップ 2　[FCID] タブをクリックします。

ステップ 3　[Create Row] アイコンをクリックして、FC ID を作成します。

ステップ 4　特定の VSAN（現在の VSAN）内のデバイスを表すための仮想 FC ID を設定しているスイッチを選択します。

ステップ 5　fcdomain データベースの [Current Fabric ID] フィールドに現在のファブリックを入力します。

ステップ 6　fcdomain データベースの [Current VSAN ID] フィールドに現在の VSAN を入力します。

ステップ 7　[pWWN] を入力します。

ステップ 8　ドロップダウン メニューをクリックして FC ID を選択し、選択した pWWN にマップします。

ステップ 9　[Create] をクリックして新しい行を作成します。

IVR ゾーン分割における LUN の設定

LUN ゾーン分割は、アクティブな IVR のメンバー間で使用できます。サービスを設定するには、ゾーン分割インターフェイスを使用して、関連するすべてのエッジ VSAN において必要な IVR ゾーン メンバー間で LUN ゾーンを作成してアクティブにするか、または IVR によって直接サポートされている LUN ゾーン分割を使用します。LUN ゾーン分割の利点の詳細については、『*Cisco MDS 9000 Family NX-OS Fabric Configuration Guide*』または『*Fabric Configuration Guide, Cisco DCNM for SAN*』を参照してください。

（注）　LUN のゾーン分割は、IVR ゾーン セットのセットアップで設定できます。

IVR ゾーンの QoS の設定

（注）　デフォルトの QoS 属性の設定値は low です。

手順の詳細

IVR ゾーンの QoS を設定するには、次の手順を実行します。

ステップ 1　[Zone] > [Edit Local Full Zone Database] を選択します。

選択した VSAN に関する [Edit Local Full Zone Database] ダイアログボックスが表示されます。

ステップ 2　[Zones] またはゾーン セットを選択します。

ステップ 3　[QoS] チェックボックスをオンにして、QoS プライオリティを設定します。

ステップ 4　[Activate] をクリックして変更を行います。

IVR ゾーンと IVR ゾーン セットの名前の変更

手順の詳細

IVR ゾーンと IVR ゾーン セットの名前を変更するには、次の手順を実行します。

ステップ 1　[Zone] > [Edit Local Full Zone Database] を選択します。

選択した VSAN に関する [Edit Local Full Zone Database] ダイアログボックスが表示されます。

ステップ 2　左側のペインでゾーンまたはゾーン セットをクリックします。

ステップ 3　[Edit] > [Rename] を選択します。

ゾーンまたはゾーン セット名の周囲にエディット ボックスが表示されます。

ステップ 4　新しい名前を入力します。

ステップ 5　[Activate] または [Commit Changes] をクリックします。

IVR CFS リージョン ID の設定

IVR CFS リージョンを設定するには、次の手順を実行します。

ステップ 1　[Logical Domains] ペインで、[All VSANs] を開き、[IVR] を選択します。

[Information] ペインに IVR 設定が表示されます。

ステップ 2　[Control] タブをクリックして、スイッチでこの機能をイネーブルにします。

選択したリージョンのスイッチだけが表示されます。IVR リージョンが設定されていないスイッチはすべて、デフォルト リージョンの一部になります。

ステップ 3　[Physical Attributes] ペインで、[Switches] を展開し、[CFS] を選択します。

機能が正常にイネーブルになっていれば、[CFS] タブにスイッチが表示されます。

ステップ 4　[All Regions] を選択して、[Create Row] をクリックします。

ステップ 5　[Region ID] にスイッチのリージョン ID を入力します。

ステップ 6　[Activate] または [Commit Changes] をクリックします。

読み取り専用ゾーン分割を使用した IVR の設定

読み取り専用ゾーン分割（LUN を使用する場合としない場合がある）は、アクティブな IVR ゾーンのメンバー間で使用できます。このサービスを設定するには、ゾーン分割インターフェイスを使用して、関連するすべてのエッジ VSAN 上で必要な IVR ゾーン メンバー間の読み取り専用ゾーンを作成してアクティブにする必要があります。

（注）　読み取り専用ゾーン分割は、IVR ゾーン セットのセットアップ時には設定できません。

INDEX

A

AFID
- ガイドライン 2-4
- 個別の設定 2-11
- 説明 1-4, 2-2, 2-6
- デフォルトの設定 2-10

「AFID」を参照

autonomous fabric ID
- 「AFID」を参照

autonomous fabric 識別番号。 1-4

F

Fabric Manager 1-15

FC ID
- ガイドライン 2-7
- 機能とメリット 2-2
- 設定 2-13

I

Inter-VSAN Routing ゾーン。 1-3

Inter-VSAN Routing ゾーン セット。 1-3

IVR
- AF ID 2-6
- CFS を使用した配信のイネーブル化 1-16
- IVR NAT を使用しない設定
  - ガイドライン 2-5
- VSAN トポロジ 1-6
- Zone Wizard 1-15
- イネーブル化 1-16
- 永続的 FC ID 2-13

エッジ VSAN 1-3

エッジ スイッチ 1-4

仮想ドメイン 1-6

機能 1-2

基本的な設定 1-1

基本的な設定タスク リスト 1-14

境界スイッチ 1-4

境界スイッチ、ガイドライン 2-6

境界スイッチの設定に関するガイドライン 2-6

現在の VSAN 1-3

サービス グループ 2-1

設定 2-12
- 基本 1-14
- 高度 2-8

設定タスク リスト 1-14, 2-9

設定の制限 1-4

相互運用性 1-8

ゾーン 1-3, 1-7

ゾーン セット 1-3

ゾーン通信 1-7

ゾーンの設定に関するガイドライン 2-8

中継 VSAN 1-4

中継 VSAN の設定に関するガイドライン 2-6

データベース 1-5

データベースのマージに関するガイドライン 1-11

デフォルト設定 1-13

デフォルトのゾーン ポリシー 1-7

トポロジのアクティブ化 2-12

ドメイン ID に関するガイドライン 2-5

ドメイン ID の設定に関するガイドライン 2-5

ネイティブ VSAN 1-3

パス 1-3

ファイバ チャネル ヘッダーの変更 1-5

用語 1-3
読み取り専用ゾーン分割 2-15
ロギング 1-22
ロギング レベルの設定 1-22
IVR CFS
リージョン ID 2-15
IVR NAT
境界スイッチ、ガイドライン 1-10
自動検出のイネーブル化 1-17
説明 1-9
中継 VSAN、ガイドライン 1-10
変更 1-17
要件 1-9
ロード バランシング 1-9
「IVR NAT」を参照
IVR、NAT を使用しない
設定 2-11
IVR Zone Wizard 1-15
IVR 永続的 FC ID
永続的 2-13
設定 2-13
IVR 仮想ドメイン
削除 1-23
説明 1-6
IVR サービス グループ
IVR の設定に関するガイドライン 2-4
アクティブ化 2-2
設定 2-10
説明 1-4
デフォルト 2-1
特性 2-1
IVR ゾーン
force オプションを使用したアクティブ化 1-20
IVR CFS リージョン 1-19
IVR Zone Wizard を使用した設定 1-15
LUN の設定 2-14
QoS 属性の設定 2-14
高度な
説明 2-2
自動作成 1-7
設定 1-18 ～ 1-19
説明 1-3, 1-7
ゾーンとの相違点（表） 1-7
ゾーンの最大数 1-4
データベース全体の回復 1-23
名前の変更 2-15
メンバーの最大数 1-4
IVR ゾーン セット
アクティブ化 1-21
高度な設定
説明 2-2
最大数 1-4
設定 1-18 ～ 1-22
説明 1-3
名前の変更 2-15
非アクティブ化 1-21
「IVR ゾーン セット」を参照
「IVR ゾーン」を参照
IVR データベース
アクティブな 1-5
設定された 1-5
保留 1-5
マージに関するガイドライン 1-11
IVR トポロジ
IVR 自動トポロジ モードから IVR 手動トポロジ モードへの移行 2-13
回復 1-23
自動検出のイネーブル化 1-17
手動で設定したトポロジのアクティベーション 2-12
手動入力の削除 2-13
手動による設定 2-11
IVR の手動設定
ガイドライン 2-6
IVR ロギング
レベルの設定 1-22

N

NAT。 1-6

V

VSAN
中継 2-11

え

永続的 FC ID
設定 2-13
エッジ VSAN
説明 1-3
エッジ スイッチ
説明 1-4

き

基本
IVR 設定 1-1
基本的な設定
タスク リスト 1-14
境界スイッチ
IVR の設定に関するガイドライン 2-6
説明 1-4

け

現在の VSAN
説明 1-3

こ

高度な
IVR ゾーンとゾーン セット 2-2
IVR の設定 2-1

し

自動トポロジ モード
イネーブル化 1-17

せ

設定の制限 1-4

そ

ゾーン
IVR ゾーンとの相違点 1-7
IVR 通信 1-7
IVR 用の読み取り専用 2-15
設定に関するガイドライン 2-8

ち

中継 VSAN
IVR の設定に関するガイドライン 2-6
設定に関するガイドライン 1-10
説明 1-4, 2-11

と

ドメイン ID
IVR の設定に関するガイドライン 2-5
一意ではない、IVR NAT 1-9
一意の 2-5

ね

ネイティブ VSAN
説明 1-3

ふ

ファイバ チャネル ヘッダーの変更 1-5