Cisco MDS 9000 シリーズ VSAN 間ルーティング構成ガイド、リリース 9.x

最終更新：2025 年 7 月 30 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、関連マニュアルの入手方法についても説明します。次のセクションを含んでいます：

対象読者

このマニュアルは、Cisco MDS 9000 シリーズ スイッチの設置、構成、および維持に携わるネットワーク管理者を対象としています。

表記法

コマンドの説明では、次の表記法を使用しています。

表記法	説明
bold	太字の文字は、表示どおりにユーザが入力するコマンドおよびキーワードです。
italic	イタリック体の文字は、ユーザが値を入力する引数です。
[x]	省略可能な要素（キーワードまたは引数）は、角かっこで囲んで示しています。
[x | y]	いずれか1つを選択できる省略可能なキーワードや引数は、角カッコで囲み、縦棒で区切って示しています。

表記法	説明
{x | y}	必ずいずれか1つを選択しなければならない必須キーワードや引数は、波かっこで囲み、縦棒で区切って示しています。
[x {y | z}]	角かっこまたは波かっこが入れ子になっている箇所は、任意または必須の要素内の任意または必須の選択肢であることを表します。角かっこ内の波かっこと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。
`variable`	ユーザが値を入力する変数であることを表します。イタリック体が使用できない場合に使用されます。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。

例では、次の表記法を使用しています。

表記法	説明
`screen フォント`	スイッチが表示する端末セッションおよび情報は、スクリーン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、太字のスクリーン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 安全上の重要事項

「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。装置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、一般的な事故防止策に留意してください。各警告の最後に記載されているステートメント番号を基に、装置に付属の安全についての警告を参照してください。

これらの注意事項を保管しておいてください。

マニュアルに関するフィードバック

このマニュアルに関する技術的なフィードバック、または誤りや記載もれなどお気づきの点がございましたら、mds-docfeedback@cisco.comよりご連絡ください。ご協力をよろしくお願いいたします。

関連資料

Cisco MDS 9000 シリーズ スイッチ全体のマニュアル セットは、次の URL にあります:

https://www.cisco.com/c/en/us/support/storage-networking/mds-9000-nx-os-san-os-software/series.html

ドキュメント ロードマップ

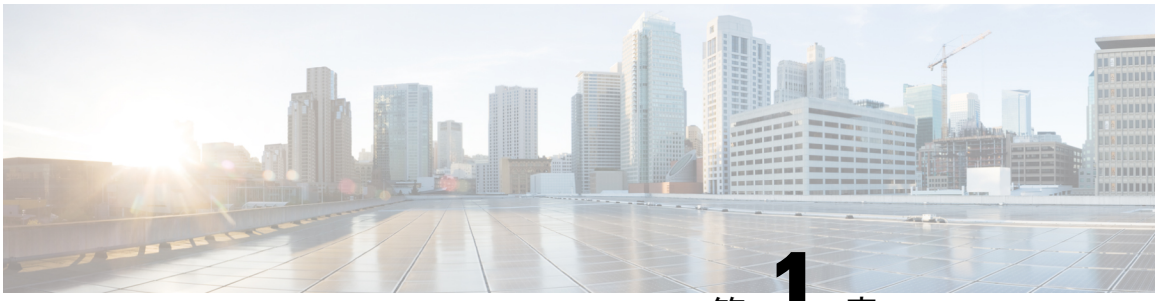
https://www.cisco.com/c/en/us/td/docs/storage/san_switches/mds9000/roadmaps/rel90.html

通信、サービス、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、Cisco Profile Manager でサインアップしてください。
- 重要な技術によって求めるビジネス成果を得るには、Cisco Services [英語] にアクセスしてください。
- サービスリクエストを送信するには、Cisco Support [英語] にアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、Cisco DevNet [英語] にアクセスしてください。
- 一般的なネットワーク、トレーニング、認定関連の出版物を入手するには、Cisco Press [英語] にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、Cisco Warranty Finder にアクセスしてください。

シスコバグ検索ツール

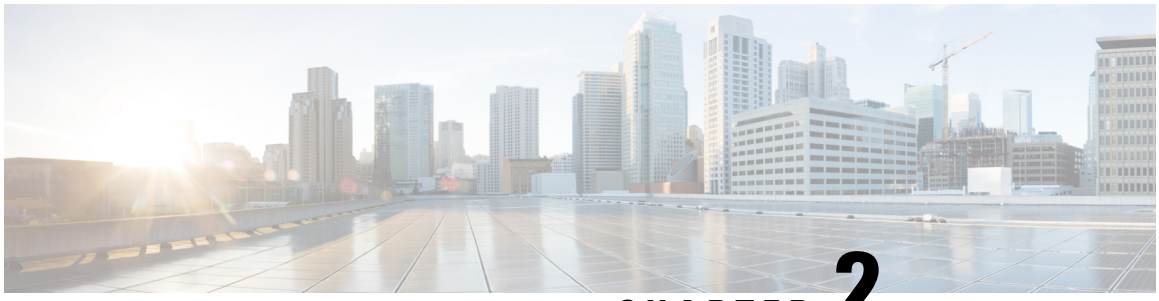
シスコバグ検索ツール（BST）は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理するシスコバグ追跡システムへのゲートウェイとして機能する、Webベースのツールです。BST は、製品とソフトウェアに関する詳細な障害情報を提供します。



第 1 章

新機能および変更された機能に関する情報

Cisco MDS NX-OS リリース 8.x 向けの、Cisco MDS 9000 シリーズ VSAN 間ルーティング構成ガイドには、新機能はありません。



CHAPTER 2

基本 VSAN間のルーティング構成

この章では、VSAN 間ルーティング（IVR）機能について説明し、IVR 管理インターフェイスを使用して VSAN 間で技術情報を共有するための基本的な手順を示します。基本的な IVR 構成を設定した後、高度な IVR 構成を設定する必要がある場合は、高度 VSAN間のルーティング構成, on page 35 を参照してください。

VSAN 間ルーティングについて

仮想 SAN（VSAN）は、複数のファイバ チャネル SAN がスイッチと ISL の共通の物理インフラストラクチャを共有できるようにすることで、ストレージ エリア ネットワーク（SAN）の拡張性、可用性、およびセキュリティを向上させます。これらの利点は、各VSANでのファイバチャネルサービスの分離と、VSAN間のトラフィックの分離から得られます。また、VSAN 間のデータ トラフィックの分離により、VSAN に接続されているリソース（ロボット テープ ライブラリなど）の共有も本質的に防止されます。IVRを使用すると、他のVSANの利点を損なうことなく、VSAN 全体のリソースにアクセスできます。

IVR 機能

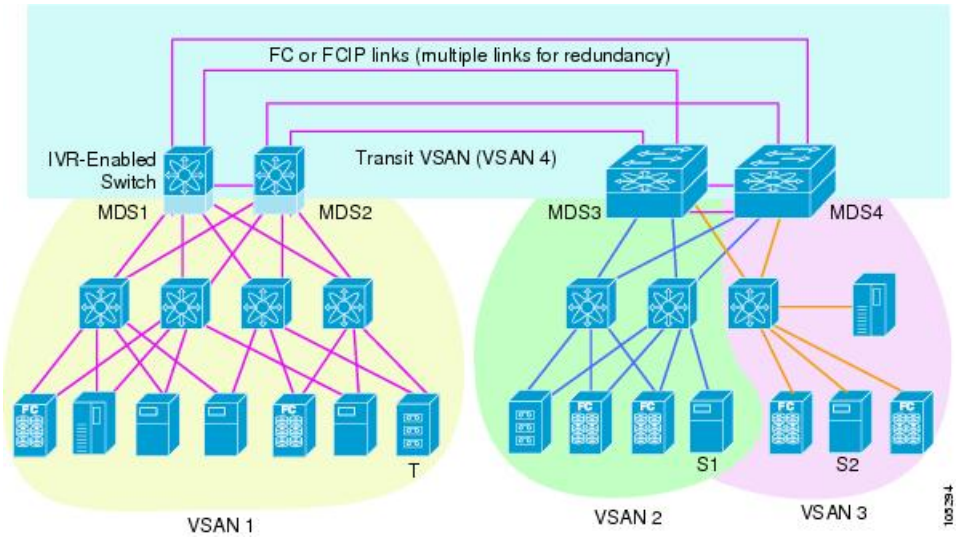
IVR は次の機能をサポートしています：

- 他の VSAN の利点を損なうことなく、VSAN 全体の技術情報にアクセスします。

- VSANを単一の論理ファブリックにマージすることなく、異なるVSAN上の特定のイニシエータとターゲットの間でデータ トラフィックを転送します。
- 複数のスイッチ間で 1 つ以上の VSAN を移動する適切な相互接続ルートを確立します。IVR は、共通のスイッチ上に存在する VSAN に限定されません。
- 貴重な技術情報（テープライブラリなど）を VSAN 間で妥協することなく共有します。ファイバ チャネル トラフィックは VSAN 間を流れることはなく、発信側は指定された VSAN 以外の VSAN 間でリソースにアクセスすることもできません。
- FCIP と組み合わせて使用すると、効率的なビジネス継続性またはディザスタ リカバリ ソリューションを提供します。図 「IVR および FCIP を使用したトラフィックの継続性」を参照してください。
- 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が組み込まれていますが、IVR 対応 VSAN はいずれかの相互運用モードで構成する必要がある場合があります。

Note 次の図に示すサンプルシナリオを構成するには、「IVR 自動トポロジモードの構成例」の手順に従います。

***Figure 1: IVR* および *FCIP* を使用したトラフィックの継続性**



IVR 用語

次の IVR 関連用語は、IVR ドキュメントで使用されています。

- ネイティブ VSAN：エンド デバイスがログ オンする VSAN は、そのエンド デバイスのネイティブ VSAN です。
- [現在のVSAN（Current VSAN）]：現在 IVR 用に構成されている VSAN。
- VSAN 間ルーティング ゾーン（IVR ゾーン）：相互接続された SAN ファブリック内の VSAN 間で通信できるエンド デバイスのセット。この定義は、ポートのワールド ワイド

名（pWWN）とネイティブ VSAN の関連付けに基づいています。Cisco SAN-OS リリース 3.0（3）より前は、ネットワーク内のスイッチで最大 2000 の IVR ゾーンと 10,000 の IVR ゾーンメンバーを構成できました。Cisco SAN-OS リリース 3.0（3）では、ネットワーク内のスイッチに最大 8000 の IVR ゾーンと 20,000 の IVR ゾーンメンバーを構成できます。

- VSAN 間ルーティング ゾーン セット（IVR ゾーン セット）：1 つ以上の IVR ゾーンが IVR ゾーン セットを構成します。Cisco MDS 9000 シリーズのスイッチには、最大 32 の IVR ゾーン セットを構成できます。アクティブにできる IVR ゾーン セットは常に 1 つだけです。
- IVR パス：IVR パスは、ある VSAN 内のエンド デバイスからのフレームが別の VSAN 内の別のエンドデバイスに到達できるようにするためのスイッチとスイッチ間リンク（ISL）のセットです。このような 2 つのエンド デバイス間には、複数のパスが存在できます。
- IVR 対応スイッチ：IVR 機能が有効になっているスイッチ。
- エッジ VSAN：IVR パスを開始（送信元エッジ VSAN）または終了（宛先エッジ VSAN）する VSAN。エッジ VSAN は、相互に隣接している場合もあれば、1 つ以上の中継 VSAN によって接続されている場合もあります。VSAN 1、2、および 3（Figure 1: IVR および FCIP を使用したトラフィックの継続性, on page 4を参照）は、エッジ VSAN です。

Note 1 つの 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：そのパスの送信元エッジ VSAN からそのパスの宛先エッジ VSAN への IVR パスに沿って存在する VSAN。VSAN 4 は中継 VSANです（Figure 1: IVR および FCIP を使用したトラフィックの継続性, on page 4を参照）。

Note 送信元エッジVSANと宛先エッジVSANが相互に隣接している場合、それらの間に中継VSANは必要ありません。

- ボーダー スイッチ：2 つ以上の VSAN のメンバーである IVR 対応スイッチ。VSAN 1 と VSAN 4 間の IVR 対応スイッチ（Figure 1: IVR および FCIP を使用したトラフィックの継続性, on page 4を参照）などのボーダースイッチは、色分けされた 2 つ以上の VSAN にまたがります。
- 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、ボーダー スイッチの IVR 構成を認識しません。エッジスイッチは IVR 対応である必要はありません。
- 自律ファブリック識別子（AFID）：同じ VSAN ID を使用してネットワーク内に複数の VSAN を構成でき、同じ ID を持つ VSAN を含むファブリック間で IVR を構成する際のダウンタイムを回避できます。
- サービス グループ：IVR 対応 VSAN へのトラフィックを制限する 1 つ以上のサービス グループを構成することで、IVR 非対応 VSAN への IVR トラフィックの量を減らすことができます。

IVR 構成の制限

IVR 構成の制限の詳細については、Cisco MDS NX-OS の構成の制限、リリース 8.x を参照してください。

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 が構成されている場合、IVR ボーダー スイッチは、エンド デバイス間のすべての通信のファイバ チャネル ヘッダーを変更します。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
- 宛先 FCID

フレームがイニシエータからターゲットに移動すると、ファイバ チャネル フレーム ヘッダーが変更され、イニシエータ VSAN 番号がターゲット VSAN 番号に変更されます。IVR ネットワーク アドレス変換（NAT）がイネーブルの場合、送信元および宛先の FCID もエッジ ボーダー スイッチで変換されます。IVR NAT が有効になっていない場合は、IVR パスに関連するすべてのスイッチに一意のドメイン ID を構成する必要があります。

IVR ネットワーク アドレス変換

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 IVR NAT を有効にする必要があります。CFS を使用した IVR 構成の配布については、「CFS を使用した IVR 構成の配布, on page 9」を参照してください。デフォルトでは、IVR NAT および IVR 構成の配信は、Cisco MDS 9000 ファミリのすべてのスイッチで無効になっています。

IVR の要件とガイドライン、および構成情報については、IVR NAT および IVR 自動トポロジ モードについて, on page 11 を参照してください。

IVR VSAN トポロジ

IVR は、構成された IVR VSAN トポロジを使用して、ファブリックを介したイニシエータとターゲット間のトラフィックのルーティング方法を決定します。

IVR 自動トポロジモードは、ファブリックの再構成が発生したときに、IVR VSAN トポロジを自動的に構築し、トポロジデータベースを維持します。また、IVR 自動トポロジモードでは、CFS を使用して IVR VSAN トポロジを IVR 対応スイッチに配信します。

IVR 自動トポロジ モードを使用すると、ファブリックで再構成が発生したときに IVR VSAN トポロジを手動で更新する必要がなくなります。IVR 手動トポロジデータベースが存在する場合、IVR 自動トポロジ モードは最初にそのトポロジ情報を使用します。自動更新では、ユーザー指定のトポロジ データベースから自動的に学習されたトポロジ データベースに徐々に移

行することで、ネットワークの中断が軽減されます。ネットワークの一部ではないユーザーの構成したのトポロジエントリは、約3分で期限切れになります。ユーザが構成したデータベースの一部ではない新しいエントリは、ネットワークで検出されると追加されます。

IVR 自動トポロジ モードを有効にすると、以前にアクティブだった IVR 手動トポロジが存在する場合はそのトポロジで開始され、ディスカバリ プロセスが開始されます。新しいパス、代替パス、またはより適切なパスを検出できます。トラフィックが代替パスまたはより適切なパスに切り替えられると、通常はスイッチングパスに関連する一時的なトラフィックの中断が発生する可能性があります。

Note IVR 自動トポロジ モードの IVR トポロジには、Cisco MDS SAN-OS リリース 2.1（1a）以降が必要であり、ファブリック内のすべてのスイッチで IVR に対して CFS を有効にする必要があります。

IVR 相互運用性

IVR機能を使用する場合、ファブリック内のすべての境界スイッチはCisco MDS スイッチである必要があります。ただし、ファブリック内の他のスイッチは非 MDS スイッチである場合があります。たとえば、アクティブ IVR ゾーン セットのメンバーであるエンド デバイスは、非 MDS スイッチに接続できます。相互運用モードの 1 つが有効になっている場合は、非 MDS スイッチがトランジット VSAN またはエッジ VSAN に存在することもあります。

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。

基本 IVR 構成タスク リスト

IVR 構成するには、次の手順に従います：

Procedure

ステップ 1 「IVR NAT を有効にします, on page 14」を参照してください。

IVR NAT を有効にします。

ステップ 2 「IVR を有効化 , on page 8」を参照してください。

すべての境界スイッチで IVR を有効にします。

ステップ 3 「CFS を使用した IVR 構成の配布, on page 9」を参照してください。

IVR 配信を有効にします。

ステップ 4 IVR NAT および IVR 自動トポロジ モードについて, on page 11を参照してください。

IVR 自動トポロジ モードを有効にします。

ステップ 5 IVR 仮想ドメインを構成します。

ステップ 6 「IVR ゾーンと IVR ゾーン セットの構成, on page 20」を参照してください。

ゾーン セットを構成し、アクティブにします。

ステップ 7 「変更のコミット, on page 10」を参照してください。

IVR 構成をコミットします。

ステップ 8 「IVR ゾーンと IVR ゾーン設定構成の確認, on page 23」を参照してください。

IVR 構成を確認します。

基本 IVR 構成

ここでは、IVR の構成方法について説明します。このセクションの内容は次のとおりです：

IVR を有効化

IVR機能は、IVRに参加するファブリック内のすべてのボーダースイッチで有効にする必要があります。デフォルトでは、この機能は全てのCisco MDS 9000シリーズスイッチで無効になっています。ファブリック内の必要なすべてのスイッチでIVRを手動で有効にするか、IVR設定のファブリック全体への配信を構成できます。「CFS を使用した IVR 構成の配布, on page 9」を参照してください。

Note IVR機能の構成および確認コマンドを使用できるのは、スイッチ上でIVRが有効にされている場合だけです。この構成を無効にした場合、関連するすべての構成は自動的に廃棄されます。

参加させるスイッチの IVR を有効にするには、次のステップを実行します：

Procedure

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 スイッチで IVR NAT を有効にします。

switch(config)# **ivr nat**

ステップ 3 スイッチで IVR を有効にします。

switch(config)# **feature ivr**

ステップ 4 スイッチ上の IVR を無効にします（デフォルト）。

switch(config)# **no feature ivr**

CFS を使用した IVR 構成の配布

IVR 機能は、Cisco Fabric Services（CFS）インフラストラクチャを利用して効率的な構成管理を可能にし、VSAN内のファブリック全体に対するシングルポイントでの構成を提供します。CFSの詳細については、『*Cisco MDS 9000* ファミリ *NX-OS* システム管理構成ガイド』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アクティブ トポロジおよびゾーンセット（1つのスイッチでこれらの機能をアクティブにすると、ファブリック内の他のすべてのディストリビューション対応スイッチに構成が伝播されます）
- AFID データベース

Note IVR構成の配信は、デフォルトでは無効になっています。この機能を正しく機能させるには、ネットワーク内のすべての IVR 対応スイッチでこの機能を有効にする必要があります。

データベースを導入

IVR 機能は、これらのデータベースを使用して、構成を受け入れ、実装します。

- 構成済みデータベース：データベースはユーザが手動で設定します。
- アクティブ データベース：データベースは、ファブリックが現在実行されています。
- 保留中データベース：構成を修正した場合は、構成済みのデータベースの変更内容を保留中データベースにコミットするかまたは廃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。保留中のデータベースへの変更は、CFSに変更をコミットするまで現用系データベースに反映されません。

構成流通の有効化

IVR 構成の配信を有効にするには、次の手順を実行します：

Procedure

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 IVR 配信をイネーブルにします。

switch(config)# **ivr distribute**

ステップ 3 IVR の配布をディセーブル（デフォルト）にします。

switch(config)# **no ivr distribute**

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。

- 他のユーザー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。

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構成がコミットされます。コミットが正常に行われると、構成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。

IVR 構成変更をコミットするには、次のステップに従います：

Procedure

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 IVR の変更をコミットします。

switch(config)# **ivr commit**

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（終了）する場合、構成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。

IVR 構成の変更を廃棄するには、次の手順を実行します：

Procedure

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 IVR の変更を廃棄し、保留中の構成データベースをクリアします。

switch(config)# **ivr abort**

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、ユーザー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。

Tip 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。

管理者の特権を使用して、ロックされた DPVM セッションを解除するには、EXEC モードで **clear ivr session** コマンドを使用します。

```
switch# clear ivr session
```

IVR NAT および IVR 自動トポロジ モードについて

IVR NAT および IVR 自動トポロジ モードを使用するように IVR SAN ファブリックを構成する前に、次の点を考慮してください：

- 関連するスイッチでのみ IVR を構成します。
- ファブリック内のすべてのスイッチで IVR の CFS を有効にします。
- ファブリック内の全てのスイッチは、Cisco MDS SAN-OS リリース 2.2（1a）以降が稼働していることを確認します。
- Cisco MDS SAN-OS リリース 2.1（1a）以降とこの機能用のアクティブな IPS カードがある場合は、必須のエンタープライズ ライセンス パッケージまたは 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* シリーズ *NX-OS* ライセンス ガイド』を参照してください。

Note FCIP 上の IVR 機能は Cisco MDS 9216i スイッチにバンドルされており、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 パッケージは必要ありません。

Tip FSPF リンク コストを変更する場合は、IVR パスの FSPF パス ディスタンス（つまり、パス上のリンク コストの合計）が 30,000 未満になるようにしてください。

Note IVR 対応 VSAN は、interop モードが有効（任意の相互運用モード）または無効（非相互運用モード）の場合に設定できます。

IVR NAT の要件とガイドライン

IVR NAT を使用するための要件とガイドラインを次に示します：

- ホストから受信した IVR NAT ポート ログイン（PLOGI）要求は、FC ID アドレスの書き換えを実行するために数秒遅延します。ホストの PLOGI タイムアウト値が 5 秒未満の値に設定されている場合、PLOGI が不必要に終了し、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 アダプタのタイムアウトを 10 秒以上に構成することを推奨します（ほとんどの HBA のデフォルト値は 10 または 20 秒です）。
- IVR NAT には、ファブリック内のすべての IVR スイッチで Cisco MDS SAN-OS リリース 2.1（1a）以降が必要です。
- Cisco NX-OS リリース 5.2（x）以降から IVR 非 NAT モードがサポートされません。IVR 非 NAT モードが構成されている場合は、IVR NAT モードへ移行するための手順については、「NX-OS リリース 5.2（8c）固有のアップグレード ガイドライン」セクションを参照します。
- IVR NAT を使用すると、IVR パス内のすべてのスイッチで一意のドメイン ID を必要とせずに、ファブリック内に IVR を設定できます。IVR NAT は、ファイバ チャネル ヘッダーの宛先 ID にローカル VSAN を使用して、他の VSAN 内のスイッチを仮想化します。一部の拡張リンク サービス メッセージ タイプでは、宛先 ID がパケット データに含まれています。このような場合、IVR NAT は実際の宛先 ID を仮想化された宛先 ID に置き換えます。IVR NAT は、次の表に示す拡張リンクサービスメッセージの宛先 ID の置換をサポートします。

***Table 1: IVR NAT* でサポートされる拡張リンク サービス メッセージ**

拡張リンク サービス メッセージ	リンク サービス コマンド（**LS_COMMAND**）	**Mnemonic**
Abort Exchange	0x06 00 00 00	ABTX

拡張リンク サービス メッセージ	リンク サービス コマンド（LS_COMMAND）	Mnemonic
Discover Address	0x52 00 00 00	ADISC
Discover Address Accept	0x02 00 00 00	ADISC ACC
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 によって認識されないメッセージがあり、パケット データに宛先 ID が含まれている場合、トポロジ内の NAT で IVR を使用することはできません。

Note IVR トポロジに FICON VSAN が含まれている場合は、IVR NAT を有効にしないでください。IVR NAT が FICON VSAN とともにイネーブルの場合、スイッチは **fcid-nat cannot be enabled if FICON enabled VSANs and topology VSANs overlap** エラーをスローします。

中継 VSAN ガイドライン

トランジット VSAN については、次のガイドラインを考慮してください：

- IVR ゾーン メンバーシップの定義に加えて、トランジット VSAN のセットを指定して、2 つのエッジ VSAN 間の接続を提供することもできます。

- IVR ゾーン内で二つのエッジ VSAN で重なった場合、トランジット VSAN は接続を提供する必要はありません。
- IVR ゾーン内で二つのエッジ VSAN で重ならない場合、接続を提供するために1 つ以上の中継 VSAN が必要な場合があります。送信元と接続先エッジ VSAN 両方のメンバーのスイッチ上で IVR が有効ではない場合、IVR ゾーン内の二つのエッジ VSAN は重なりません。

- エッジ VSAN の間のトラフィックは、最短 IVR パスのみ通過します。
- 中継 VSAN 情報は、全ての IVR ゾーン セットで共通です。時には中継 VSAN は、別の IVR ゾーンでエッジ VSAN として機能することができます。

ボーダー スイッチ ガイドライン

ボーダー スイッチを構成する前に、次のガイドラインを考慮してください：

- ボーダー スイッチには、Cisco MDS SAN-OS リリース 2.1（1a）以降が必要です。
- ボーダー スイッチは、2 つ以上の VSAN のメンバーである必要があります。
- IVR 通信を容易にする境界スイッチは、IVR 対応である必要があります。
- IVR は、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ために、追加のボーダー スイッチで（オプションで）有効にすることができます。
- VSAN トポロジ構成は、境界スイッチが追加または削除されると自動的に更新されます。

IVR NAT を有効にします

ここでは、IVR NAT を有効にする方法と、IVR 自動トポロジモードを有効にする方法について説明します。

IVR NAT を有効にするには、次の手順を実行します：

Procedure

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 スイッチで IVR NAT を有効にします。

switch(config)# **ivr nat**

ステップ 3 スイッチ上の IVR NAT を無効にします（デフォルト）。

switch(config)# **no ivr nat**

IVR 自動トポロジ モードの有効化

Note IVR 自動トポロジモードを構成する前に、IVR 構成の配信を有効にする必要があります（CFS を使用した IVR 構成の配布, on page 9 を参照）。IVR 自動トポロジ モードを有効にすると、IVR 構成の配信を無効にすることはできません。

IVR 自動トポロジ モードを有効にするには、次の手順を実行します：

Procedure

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 IVR 自動トポロジ モードを有効にします。

switch(config)# **ivr vsan-topology auto**

What to do next

自動的に検出された IVR トポロジを表示するには、 **show ivr vsan-topology** コマンドを使用します。

```
switch# show ivr vsan-topology

AFID  SWITCH WWN                 Active   Cfg. VSANS
------------------------------------------------------------
   1  20:00:54:7f:ee:1b:0b:d0     yes      no  11,1109
   1  20:00:54:7f:ee:1c:0e:00 *   yes      no  2,11-12,28,1110


Total:   2 entries in active and configured IVR VSAN-Topology
```

Note アスタリスク（*）はローカル スイッチを示します。

IVR 仮想ドメイン

リモート VSAN では、IVR アプリケーションは、割り当て済みドメイン リストに仮想ドメインを自動的に追加しません。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 ドメインが表示されるまで、リモート ネーム サーバーにクエリを実行しません。このような場合は、特定の VSAN 内の IVR 仮想ドメインを、その VSAN 内の割り当て済みドメイン リストに追加します。IVR ドメインを追加すると、

ファブリックに現在存在するすべての IVR 仮想ドメイン（および今後作成される仮想ドメイン）が、その VSAN の割り当て済みドメイン リストに表示されます。

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

IVR 仮想ドメインを有効にすると、仮想ドメイン ID の重複が原因でリンクがアップに失敗することがあります。この場合は、重複する仮想ドメインをその VSAN から一時的に取り消します。

Note IVR VSAN から重複する仮想ドメインを取り消すと、そのドメインとの間の IVR トラフィックが中断されます。

EXEC モードで **ivr withdraw domain** コマンドを使用すると、影響を受ける VSAN から重複する仮想ドメイン インターフェイスを一時的に取り消すことができます。

Tip 中継 VSAN ではなく、エッジ VSAN にのみ IVR ドメインを追加します。

IVR 仮想ドメインの手動構成

指定した VSAN で IVR 仮想ドメインを手動で構成するには、次の手順を実行します：

Procedure

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 VSAN 1 に IVR 仮想ドメインを追加します。すべての IVR スイッチでこの手順を実行します。

switch(config)# **ivr virtual-fcdomain-add vsan-ranges 1-4093**

ステップ 3 IVR 仮想ドメインを追加しない工場出荷時のデフォルトに戻し、その VSAN の現在アクティブな仮想ドメインを fcdomain マネージャ リストから削除します。

switch(config)# no **ivr virtual-fcdomain-add vsan-ranges 1-4093**

ファブリック全体の IVR 仮想ドメインの手動構成

Note Cisco SAN-OS リリース 3.1（2）の時点で、Cisco ファブリック構成サービス（FCS）は仮想デバイスの検出をサポートしています。FCS 構成 サブモードで **fcs virtual-device-add vsan-ranges** コマンドを実行すると、特定の VSAN またはすべての VSAN で仮想デバイスを検出できます。このコマンドを使用して IVRのためにゾーンされたデバイスを検出する場合、デバイスはリクエスト domain_ID（RDI）を有効にする必要があります。FCS の使用の詳細については、『Cisco MDS 9000 ファミリ NX-OS システム管理構成ガイド』を参照してください。

指定した VSAN にファブリック全体の IVR 仮想ドメインを構成するには、次の手順を実行します：

Procedure

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 VSAN 1 に IVR 仮想ドメインを追加します。すべての IVR スイッチでこの手順を実行します。

switch(config)# **ivr virtual-fcdomain-add 2 vsan-ranges 1-4093**

ステップ 3 ファブリック全体の構成をコミットします。

switch(config)# **ivr commit**

ステップ 4 IVR 仮想ドメインを追加しない工場出荷時のデフォルトに戻し、その VSAN の現在アクティブな仮想ドメインを fcdomain マネージャ リストから削除します。

switch(config)# no **ivr virtual-fcdomain-add2 vsan-ranges 1-4093**

仮想ドメイン構成を確認

IVR 仮想ドメイン構成のステータスを表示するには、 **show ivr virtual-fcdomain-add-status** コマンドを使用します。

```
switch# show ivr virtual-fcdomain-add-status
IVR virtual domains are added to fcdomain list in VSANS: 1
(As well as to VSANs in interoperability mode 2 or 3)
```

IVR fcdomain データベースのクリア

IVR fcdomain データベースをクリアするには、次のコマンドを使用します：

```
switch# clear ivr fcdomain database
```

IVR ゾーンと IVR ゾーン セット

ここでは、IVR ゾーンおよび IVR ゾーン セットの構成について説明します。内容は次のとおりです：

IVR ゾーンについて

IVR 構成の一部として、1 つ以上の IVR ゾーンを構成して、VSAN 間通信を有効にする必要があります。この結果を得るには、各IVRゾーンを（pWWN、VSAN）エントリのセット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 セットを 1 つの IVR ゾーンに属するように 構成できます。複数の IVR ゾーン セットを定義し、定義した IVR ゾーン セットの 1 つだけをアクティブにすることができます。

Note すべての IVR 対応スイッチで同じ IVR ゾーン セットをアクティブにする必要があります。

次の表は、IVR ゾーンとゾーンの主な違いを識別します。

***Table 2: IVR* ゾーンとゾーンの主な違い**

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されます。	ゾーン メンバーシップは、pWWN、ファブリック WWN、sWWN、または AFID を使用して指定されます。
デフォルトのゾーン ポリシーは常に拒否（構成不可）です。	デフォルトのゾーン ポリシーは deny（構成可能）です。

IVR ゾーンの制限とイメージのダウングレードに関する考慮事項

次の表に、物理ファブリックごとの IVR ゾーン制限を示します。

***Table 3: IVR* ゾーン制限**

Cisco リリース	IVR ゾーン制限	IVR ゾーン メンバー制限	IVR ゾーン設定制限
SAN-OS リリース 3.0（3 以降）	8000	20,000	32
SAN-OS リリース 3.0（2b）以前	2000	10,000	32

Note 2 つのゾーンに存在する場合、ゾーン メンバーは、2 回数えられます。「データベース マージの注意事項, on page 27」を参照してください。

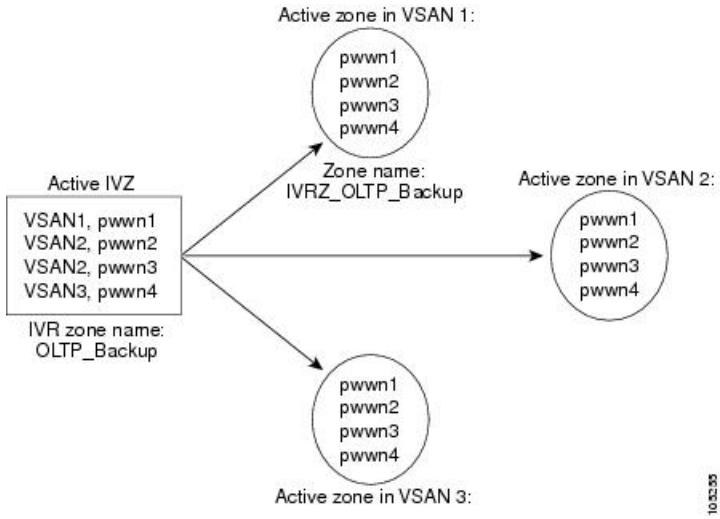
Caution Cisco SAN-OS リリース 3.0（3）より前のリリースにダウングレードする場合、IVR ゾーンの数は 2000 を超えることはできず、IVR ゾーン メンバーの数は 10,000 を超えることはできません。

自動 IVR ゾーン作成

次の図は、4 つのメンバーで構成される IVR ゾーンを示しています。pWWn1 が pWWn2 と通信できるようにするには、それらが VSAN 1 と VSAN 2 の同じゾーンに存在する必要があります。それらが同じゾーンにない場合、ハードゾーン分割 ACL エントリは、pWWn1 が pWWn2 と通信することを禁止します。

各アクティブ IVR ゾーンに対応するゾーンは、アクティブ IVR ゾーンで指定された各エッジ VSAN に自動的に作成されます。IVR ゾーン内のすべての pWWN は、各 VSAN 内のこれらのゾーンのメンバーです。

***Figure 2: IVR* ゾーンのアクティブ化時のゾーンの作成**



ゾーンは、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作成されます。これらはフル ゾーン セット データベースには保存されず、スイッチがリブートしたとき、または新しいゾーンセットがアクティブになったときに失われます。IVR機能は、これらのイベントをモニターし、新しいゾーンセットがアクティブになると、アクティブな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 セットも中断なしでアクティブ化されます。

Note pWWn1 と pWWn2 が現在の IVR ゾーン セットと新しい IVR ゾーン セットの IVR ゾーンにある場合、新しい IVR ゾーン セットをアクティブにしても、それらの間のトラフィックは中断されません。

IVR ゾーンおよび IVR ゾーン セット名は、64 文字の英数字に制限されています。

Caution Cisco SAN-OS リリース 3.0（3）より前では、ネットワーク内のスイッチには合計 2000 の IVR ゾーンと 32 の IVR ゾーン セットしか構成できません。Cisco SAN-OS リリース 3.0（3）では、ネットワーク内のスイッチに合計 8000 の IVR ゾーンと 32 の IVR ゾーン セットのみを構成できます。データベース マージの注意事項, on page 27を参照してください。

IVR ゾーンと IVR ゾーン セットの構成

IVR ゾーンおよび IVR ゾーン セットを作成するには、次の手順を実行します：

Procedure

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 sample_vsan2-3 という名前の IVR ゾーンを作成します。

switch(config)# **ivr zone name sample_vsan2-3**

ステップ 3 VSAN 3 の指定された pWWN を IVR ゾーン メンバーとして追加します。

switch(config-ivr-zone)# **member pwwn 21:00:00:e0:8b:02:ca:4a vsan 3**

ステップ 4 VSAN 2 の指定された pWWN を IVR ゾーン メンバーとして追加します。

switch(config-ivr-zone)# **member pwwn 21:00:00:20:37:c8:5c:6b vsan 2**

ステップ 5 コンフィギュレーション モードに戻ります。

switch(config-ivr-zone)# **exit**

ステップ 6 sample_vsan4-5 という名前の IVR ゾーンを作成します。

switch(config)# **ivr zone name sample_vsan4-5**

ステップ 7 VSAN 4 の指定された pWWN を IVR ゾーン メンバーとして追加します。

switch(config-ivr-zone)# **member pwwn 21:00:00:e0:8b:06:d9:1d vsan 4**

ステップ 8 VSAN 4 の指定された pWWN を IVR ゾーン メンバーとして追加します。

switch(config-ivr-zone)# **member pwwn 21:01:00:e0:8b:2e:80:93 vsan 4**

ステップ 9 VSAN 5 の指定された pWWN を IVR ゾーン メンバーとして追加します。

switch(config-ivr-zone)# **member pwwn 10:00:00:00:c9:2d:5a:dd vsan 5**

ステップ 10 コンフィギュレーション モードに戻ります。

switch(config-ivr-zone)# **exit**

ステップ 11 Ivr_zoneset1 という名前の IVR ゾーン セットを作成します。

switch(config)# **ivr zoneset name Ivr_zoneset1**

ステップ 12 sample_vsan2-3 IVR ゾーンを IVR ゾーン セット メンバーとして追加します。

switch(config-ivr-zoneset)# **member sample_vsan2-3**

ステップ 13 sample_vsan4-5 IVR ゾーンを IVR ゾーン セット メンバーとして追加します。

switch(config-ivr-zoneset)# **member sample_vsan4-5**

ステップ 14 コンフィギュレーション モードに戻ります。

switch(config-ivr-zoneset)# **exit**

ステップ 15 新しく作成された IVR ゾーン セットをアクティブにします。

switch(config)# **ivr zoneset activate name IVR_ZoneSet1**

ステップ 16 指定した IVR ゾーン セットを強制的にアクティブにします。

switch(config)# **ivr zoneset activate name IVR_ZoneSet1 force**

ステップ 17 指定された IVR ゾーン セットを非アクティブにします。

switch(config)# **no ivr zoneset activate name IVR_ZoneSet1**

ステップ 18 EXEC モードに戻ります。

switch(config)# **end**

ゾーン セットのアクティブ化と force オプションの使用について

ゾーンセットを作成して設定したら、ゾーンセットを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、IVR は各エッジ VSAN の通常のアクティブ ゾーン セットに IVR ゾーンを自動的に追加します。VSAN にアクティブ ゾーン セットがない場合、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。これにより、IVR は「nozoneset」と呼ばれるアクティブ ゾーン セットを作成し、そのアクティブ ゾーン セットに IVR ゾーンを追加します。

Caution VSAN で通常のアクティブ 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、通常のアクティブ ゾーン セットの IVR ゾーンと、スイッチとの間で送受信されるすべての IVR トラフィックが停止するために発生します。IVR ゾーンセットを再アクティブ化するには、通常のゾーン セットを再アクティブ化する必要があります。

Note

- 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。ゾーン分割関連の設定またはアクティブ化の操作（通常のゾーン、IVR ゾーン、または iSLB ゾーンに対して）は、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。
- セグメント化された VSAN が IVR トポロジに存在する場合、IVR ゾーン セットはアクティブになりません。

force コマンド を使用して、IVR ゾーン セットをアクティブにすることもできます。次の表に、**force command** オプションを使用する場合と使用しない場合のさまざまなシナリオを示します。

***Table 4: force* コマンドを使用する場合と使用しない場合の *IVR* シナリオ**

大文字/小文字	デフォルト ゾーン ポリシー	IVR ゾーンのアクティブ化前のアクティブゾーンセット	force command 使用されるオプション	IVR ゾーン セットのアクティブ化ステータス	アクティブな IVR ゾーンが作成されましたか?	起こりうる中断トラフィック
1	拒否	アクティブ ゾーン セットなし	非対応	エラー	×	×
2			はい	成功（Success）	○	×
3[1]	拒否	アクティブ ゾーン セットが存在します	×/○	成功（Success）	○	×
4	許可	アクティブ ゾーン セットがないか、アクティブ ゾーン セットが存在しません	非対応	エラー	×	×
5			はい	成功（Success）	○	○

[1] ケース 3 のシナリオを使用することをお勧めします。

Caution IVR ゾーン セット アクティベーションの **force** コマンド を使用すると、IVR に関与していないデバイスであっても、トラフィックの中断が発生する可能性があります。たとえば、設定にアクティブなゾーン セットがなく、デフォルトのゾーン ポリシーが permit の場合、IVR ゾーン セットのアクティブ化は失敗します。ただし、 **force** コマンド を使用すると、IVR ゾーン セットのアクティブ化は成功します。ゾーンは各 IVR ゾーンに対応するエッジ VSAN で作成されるため、デフォルトのゾーン ポリシーが許可であるエッジ VSAN で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

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。

Procedure

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 新しく作成された IVR ゾーン セットをアクティブにします。

switch(config)# **ivr zoneset activate name IVR_ZoneSet1**

ステップ 3 指定した IVR ゾーン セットを強制的にアクティブにします。

switch(config)# **ivr zoneset activate name IVR_ZoneSet1 force**

ステップ 4 指定された IVR ゾーン セットを非アクティブにします。

switch(config)# **no ivr zoneset activate name IVR_ZoneSet1**

What to do next

Note 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 セットに置き換えるには、現在のアクティブな IVR ゾーン セットを非アクティブ化せずに、新しい IVR ゾーン セットをアクティブ化します。

IVR ゾーンと IVR ゾーン設定構成の確認

show ivr zone および **show ivr zoneset** コマンドを使用して、IVR ゾーンおよび IVR ゾーン セットの構成を確認します。

IVR ゾーン構成の表示

```
switch# show ivr zone
zone name sample_vsan2-3
    pwwn 21:00:00:e0:8b:02:ca:4a vsan 3
    pwwn 21:00:00:20:37:c8:5c:6b vsan 2
zone name ivr_qa_z_all
    pwwn 21:00:00:e0:8b:06:d9:1d vsan 1
    pwwn 21:01:00:e0:8b:2e:80:93 vsan 4
    pwwn 10:00:00:00:c9:2d:5a:dd vsan 1
    pwwn 10:00:00:00:c9:2d:5a:de vsan 2
    pwwn 21:00:00:20:37:5b:ce:af vsan 6
    pwwn 21:00:00:20:37:39:6b:dd vsan 6
    pwwn 22:00:00:20:37:39:6b:dd vsan 3
    pwwn 22:00:00:20:37:5b:ce:af vsan 3
    pwwn 50:06:04:82:bc:01:c3:84 vsan 5
```

指定した IVR ゾーンの情報の表示

```
switch# show ivr zone name sample_vsan2-3
zone name sample_vsan2-3
    pwwn 21:00:00:e0:8b:02:ca:4a vsan 3
    pwwn 21:00:00:20:37:c8:5c:6b vsan 2
```

アクティブ IVR ゾーン内の指定されたゾーンの表示

```
switch# show ivr zone name sample_vsan2-3 active
zone name sample_vsan2-3
    pwwn 21:00:00:e0:8b:02:ca:4a vsan 3
    pwwn 21:00:00:20:37:c8:5c:6b vsan 2
```

IVR ゾーン セット構成の表示

```
switch# show ivr zoneset
zoneset name ivr_qa_zs_all
  zone name ivr_qa_z_all
    pwwn 21:00:00:e0:8b:06:d9:1d vsan 1
    pwwn 21:01:00:e0:8b:2e:80:93 vsan 4
    pwwn 10:00:00:00:c9:2d:5a:dd vsan 1
    pwwn 10:00:00:00:c9:2d:5a:de vsan 2
    pwwn 21:00:00:20:37:5b:ce:af vsan 6
    pwwn 21:00:00:20:37:39:6b:dd vsan 6
    pwwn 22:00:00:20:37:39:6b:dd vsan 3
    pwwn 22:00:00:20:37:5b:ce:af vsan 3
    pwwn 50:06:04:82:bc:01:c3:84 vsan 5
zoneset name IVR_ZoneSet1
  zone name sample_vsan2-3
    pwwn 21:00:00:e0:8b:02:ca:4a vsan 3
    pwwn 21:00:00:20:37:c8:5c:6b vsan 2
```

アクティブな IVR ゾーン セット構成の表示

```
switch# show ivr zoneset active
zoneset name IVR_ZoneSet1
  zone name sample_vsan2-3
```

```
    pwwn 21:00:00:e0:8b:02:ca:4a vsan 3
    pwwn 21:00:00:20:37:c8:5c:6b vsan 2
```

指定された IVR ゾーン セット構成の表示

```
switch# show ivr zoneset name IVR_ZoneSet1
zoneset name IVR_ZoneSet1
  zone name sample_vsan2-3
    pwwn 21:00:00:e0:8b:02:ca:4a vsan 3
    pwwn 21:00:00:20:37:c8:5c:6b vsan 2
```

すべての IVR ゾーン セットの簡易情報の表示

```
switch# show ivr zoneset brief Active
zoneset name IVR_ZoneSet1
  zone name sample_vsan2-3
```

アクティブな IVR ゾーン セットの簡単な情報の表示

```
switch# show ivr zoneset brief Active
zoneset name IVR_ZoneSet1
  zone name sample_vsan2-3
```

IVR ゾーン セットのステータス情報の表示

```
switch# show ivr zoneset status
Zoneset Status
_______________
    name               : IVR_ZoneSet1
    state              : activation success
    last activate time : Sat Mar 22 21:38:46 1980
    force option       : off
status per vsan:
_________________
     vsan     status
     ____     ______
       1      active
       2      active
```

Tip IVR 構成に参加しているすべてのボーダー スイッチで、この構成を繰り返します。

Note Cisco ファブリック マネージャを使用して、相互接続された VSAN ネットワーク内のすべての IVR 対応スイッチに IVR ゾーン構成を配信できます。*Cisco* ファブリック マネージャ *VSAN* 間 ルーティング 構成ガイドを参照します。

IVR ゾーン データベースのクリア

ゾーンセットをクリアすると、構成済みゾーンデータベースのみが消去され、アクティブ ゾーン データベースは消去されません。

IVR ゾーン データベースをクリアするには、 **clear ivr zone database** コマンドを使用します。

```
switch# clear ivr zone database
```

このコマンドは、構成されているすべての IVR ゾーン情報をクリアします。

Note **clear ivr zone database**コマンドを実行した後に、明示的に**copy running-config startup-config** コマンドを実行して、スイッチの次の起動時に確実に実行構成が使用されるようにする必要があります。

IVR ロギング

IVR 機能の Telnet または SSH ロギングを構成できます。たとえば、IVR ロギング レベルをレベル 4（警告）に構成すると、重大度が 4 以上のメッセージが表示されます。このセクションの手順を使用して、ロギングレベルを構成および確認します：

IVR ロギング シビラティ レベルの構成

IVR 機能からのロギング メッセージのシビラティ レベルの構成をするには、次の手順を実行します：

Procedure

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 レベル 4（Warning（注意））で、IVR 機能に関する Telnet または SSH ロギングを構成します。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。

switch(config)# **logging level ivr 4**

ロギング レベル構成の確認

show logging level コマンドを使用して、IVR 機能に構成されているロギング レベルを表示します。

```
switch# show logging level
Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
...
ivr                     5                       4
...
0(emergencies)          1(alerts)       2(critical)
3(errors)               4(warnings)     5(notifications)
6(information)          7(debugging)
```

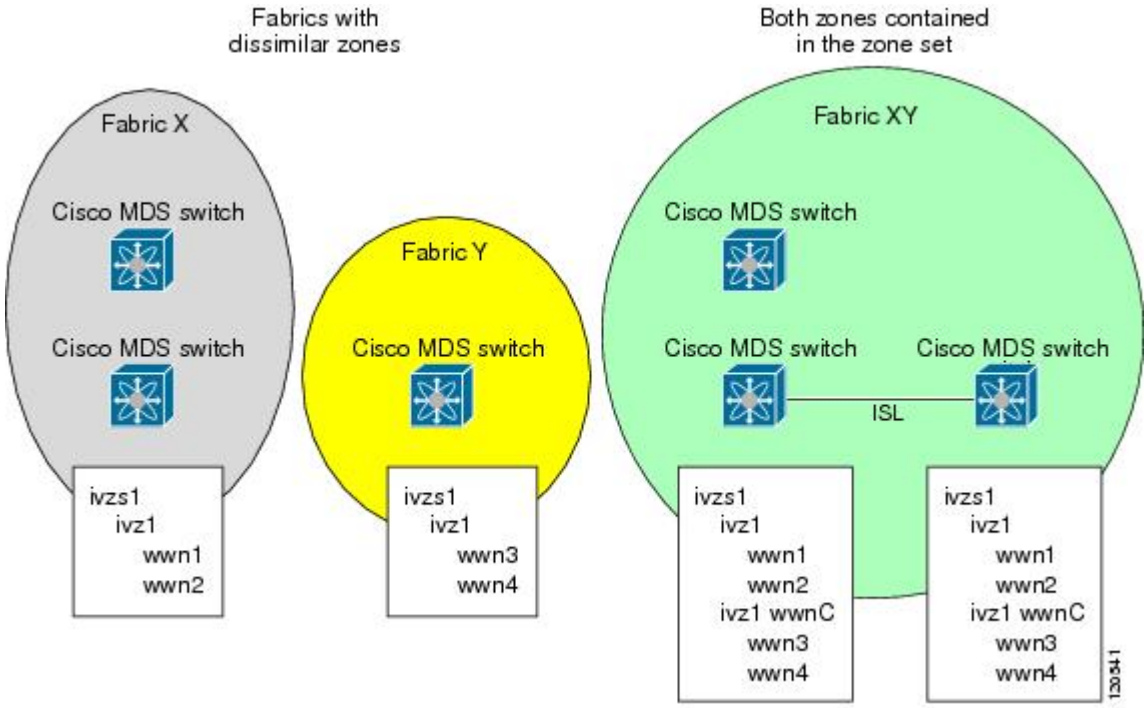
データベース マージの注意事項

データベースのマージとは、構成データベースとアクティブ データベース内のスタティック（学習されていない）エントリの統合を指します。CFS マージ サポートの詳細については、「*Cisco MDS 9000* シリーズ システム 管理構成ガイド」 または、 「*Cisco* ファブリックマネージャ管理構成ガイド」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、次の点を考慮してください。

- 2 つのファブリックに異なる構成が含まれている場合でも、IVR 構成はマージされます。
- 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、各ファブリックのゾーンは、適切な名前で分散ゾーン セットに複製されます。

Figure 3: ファブリック マージの結果



- Cisco MDS スイッチごとに異なる IVR 構成を構成できます。

- トラフィックの中断を回避するために、データベースのマージが完了した後の構成は、マージに関連する 2 つのスイッチに存在していた構成の組み合わせになります。
  - 両方のファブリックの構成が異なる場合でも、構成はマージされます。
  - ゾーンとゾーン セットの組み合わせを使用して、マージされたゾーンとゾーン セットを取得します。2 つのファブリックに異なるゾーンが存在する場合、異なるゾーンが適切な名前のゾーン セットに複製されるため、両方のゾーンが存在します。
  - 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の組み合わせが含まれます。
  - マージされたデータベースに許容される最大数よりも多くのトポロジエントリが含まれている場合、マージは失敗します。
  - 2 つのファブリックの VSAN の合計数が 128 を超えることはできません。

Note VSAN ID が同じで AFID が異なる VSAN は、2 つの個別の VSAN としてカウントされます。

- - 2 つのファブリックの IVR 対応スイッチの合計数が 128 を超えることはできません。
  - 2 つのファブリックのゾーンメンバーの合計数が 10,000 を超えることはできません。Cisco SAN-OS リリース 3.0（3）では、2 つのファブリックのゾーン メンバーの合計数が 20,000 を超えることはできません。ゾーン メンバーは、2 つのゾーンに存在する場合、2 回カウントされます。

Note 1 つ以上のファブリック スイッチが Cisco SAN-OS リリース 3.0（3）以降を実行しており、ゾーン メンバーの数が 10,000 を超えている場合は、ファブリックのゾーン メンバーの数を減らすか、両方のファブリックのすべてのスイッチをアップグレードする必要があります。 Cisco SAN-OS リリース 3.0（3）以降。

- - 2 つのファブリックの合計ゾーン数が 2000 を超えることはできません。Cisco SAN-OS リリース 3.0（3）では、2 つのファブリックの合計ゾーン数が 8000 を超えることはできません。

Note ファブリック内の一部のスイッチのみが Cisco SAN-OS リリース 3.0（3）以降を実行しており、ゾーンの数が 2000 を超えている場合は、ファブリック内のゾーンの数を減らすか、両方のファブリックのすべてのスイッチをアップグレードする必要があります。 Cisco SAN-OS リリース 3.0（3）以降。

- - 2 つのファブリックの合計数またはゾーン セットが 32 を超えることはできません。

次の表に、さまざまな条件下での 2 つの IVR 対応ファブリックの CFS マージの結果を示します。

Table 5: 2 つの *IVR* 対応ファブリックのマージの結果

IVR ファブリック 1	IVR ファブリック 2	マージ後
NAT 有効	NAT 無効	マージが成功し、NAT が有効になります
自動モードが有効	自動モードが無効	マージが成功し、IVR 自動トポロジ モードが有効になります
競合する AFID データベース	マージに失敗する	
競合する IVR ゾーンセットデータベース	競合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	
組み合わせた構成が制限（ゾーンまたは VSAN の最大数など）を超えている	マージに失敗する	
サービス グループ 1	サービス グループ 2	マージはサービス グループを組み合わせて成功します
ユーザ設定の VSAN トポロジ構成と競合	マージに失敗する	
競合のないユーザー構成の VSAN トポロジ構成	マージに成功しました	

Caution この条件に従わない場合は、マージに失敗します。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。

データベース マージ失敗の解決

マージに失敗した場合は、次の CLI コマンドを使用してエラー状態を表示できます。

- **show ivr merge status**
- **show cfs merge status name ivr**
- **show logging last** *lines*（および MERGE の失敗を探します）

マージの失敗を解決するには、 **show** コマンドの出力に示されている失敗情報を確認し、このリストで失敗に関連するシナリオを見つけ、トラブル シューティングの手順に従います：

Note CFS コミットが成功すると、マージが成功します。

IVR 自動トポロジ モードの構成例

ここでは、IVR 自動トポロジ モードを有効にするための構成手順の例を示します。

Procedure

ステップ 1 ファブリック内のすべての境界スイッチで IVR を有効にします。

Example:

```
switch# config t
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# feature ivr
switch(config)# exit
switch#
```

ステップ 2 すべての IVR 対応スイッチで IVR が有効になっていることを確認します。

Example:

```
switch# show ivr
Inter-VSAN Routing is enabled
Inter-VSAN enabled switches
---------------------------
No IVR-enabled VSAN is active. Check VSAN-Topology configuration.
Inter-VSAN topology status
--------------------------
Current Status: Inter-VSAN topology is INACTIVE
Inter-VSAN zoneset status
-------------------------
    name               :
    state              : idle
    last activate time :
Fabric distribution status
----------------------
fabric distribution disabled
Last Action                : None
Last Action Result         : None
Last Action Failure Reason : None
Inter-VSAN NAT mode status
--------------------------
FCID-NAT is disabled
License status
-----------------
IVR is running based on the following license(s)
ENTERPRISE_PKG
```

ステップ 3 ファブリック内のすべての IVR 対応スイッチで CFS 配信をイネーブルにします。

Example:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ivr distribution
```

ステップ 4 IVR 自動トポロジ モードを有効にします。

Example:

```
switch(config)# ivr vsan-topology auto
fabric is locked for configuration. Please commit after configuration is done.
```

ステップ 5 変更をファブリックにコミットします。

Example:

```
switch(config)# ivr commit
switch(config)# exit
switch#
```

ステップ 6 コミット要求のステータスを確認します。

Example:

```
switch# show ivr session status
Last Action                : Commit
Last Action Result         : Success
Last Action Failure Reason : None
```

ステップ 7 アクティブな IVR 自動トポロジを確認します。

Example:

```
switch# show ivr vsan-topology active
AFID  SWITCH WWN                 Active   Cfg. VSANS
--------------------------------------------------------------
   1  20:00:00:0d:ec:08:6e:40 *  yes      no   1,336-338
   1  20:00:00:0d:ec:0c:99:40    yes      no   336,339
```

ステップ 8 IVR ゾーン セットとゾーンを構成します。次の 2 つのゾーンが必要です。

- 1 つのゾーンにはテープ T（pWWn 10:02:50:45:32:20:7a:52）とサーバー S1（pWWn 10:02:66:45:00:20:89:04）があります。
- 別のゾーンにはテープ T とサーバー S2（pWWn 10:00:ad:51:78:33:f9:86）があります。

Tip
2 つの IVR ゾーンを作成する代わりに、テープと両方のサーバーで 1 つの IVR ゾーンを作成することもできます。

Example:

```
mds(config)# ivr zoneset name tape_server1_server2
mds(config-ivr-zoneset)# zone name tape_server1
mds(config-ivr-zoneset-zone)# member pwwn 10:02:50:45:32:20:7a:52 vsan 1
mds(config-ivr-zoneset-zone)# member pwwn 10:02:66:45:00:20:89:04 vsan 2
mds(config-ivr-zoneset-zone)# exit
mds(config-ivr-zoneset)# zone name tape_server2
mds(config-ivr-zoneset-zone)# member pwwn 10:02:50:45:32:20:7a:52 vsan 1
```

```
mds(config-ivr-zoneset-zone)# member pwwn 10:00:ad:51:78:33:f9:86 vsan 3
mds(config-ivr-zoneset-zone)# exit
```

ステップ 9 IVR ゾーン構成を表示して、IVR ゾーン セットと IVR ゾーンが正しく構成されていることを確認します。

Example:

```
mds(config)# do show ivr zoneset
zoneset name tape_server1_server2
  zone name tape_server1
      pwwn 10:02:50:45:32:20:7a:52 vsan 1
      pwwn 10:02:66:45:00:20:89:04 vsan 2
  zone name tape_server2
      pwwn 10:02:50:45:32:20:7a:52 vsan 1
      pwwn 10:00:ad:51:78:33:f9:86 vsan 3
```

ステップ 10 IVR ゾーン セットをアクティブ化する前にゾーン セットを表示します。IVR ゾーン セットをアクティブにする前に、アクティブ ゾーン セットを表示します。VSAN 2 および 3 に対してこの手順を繰り返します。

Example:

```
mds(config)# do show zoneset active vsan 1
zoneset name finance_dept vsan 1
  zone name accounts_database vsan 1
    pwwn 10:00:23:11:ed:f6:23:12
    pwwn 10:00:56:43:11:56:fe:ee

  zone name $default_zone$ vsan 1
```

ステップ 11 設定された IVR ゾーン セットをアクティブにします。

Example:

```
mds(config)# ivr zoneset activate name tape_server1_server2
zoneset activation initiated. check inter-VSAN zoneset status
mds(config)# exit
mds#
```

ステップ 12 IVR ゾーン セットのアクティブ化を確認します。

Example:

```
mds# show ivr zoneset active
zoneset name tape_server1_server2
  zone name tape_server1
      pwwn 10:02:50:45:32:20:7a:52 vsan 1
      pwwn 10:02:66:45:00:20:89:04 vsan 2
  zone name tape_server2
      pwwn 10:02:50:45:32:20:7a:52 vsan 1
      pwwn 10:00:ad:51:78:33:f9:86 vsan 3
```

ステップ 13 ゾーン セットの更新を確認します。IVR ゾーン セットのアクティブ化が成功したら、適切なゾーンがアクティブ ゾーン セットに追加されていることを確認します。VSAN 2 および 3 に対してこの手順を繰り返します。

Example:

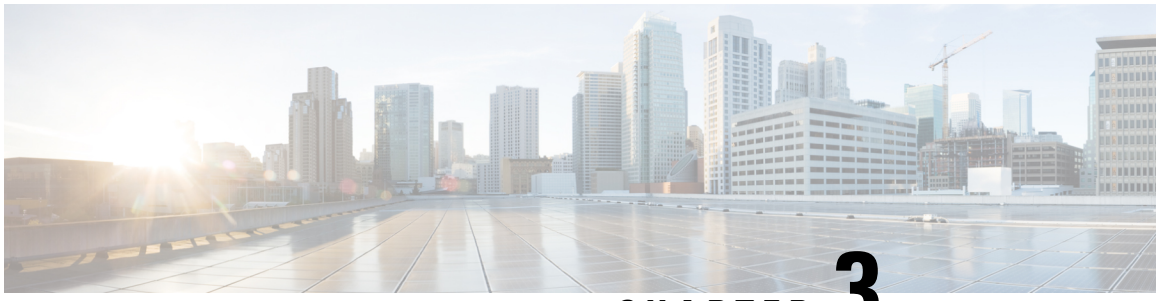
```
mds# show zoneset active vsan 1
zoneset name finance_dept vsan 1
  zone name accounts_database vsan 1
    pwwn 10:00:23:11:ed:f6:23:12
    pwwn 10:00:56:43:11:56:fe:ee

  zone name IVRZ_tape_server1 vsan 1
    pwwn 10:02:66:45:00:20:89:04
    pwwn 10:02:50:45:32:20:7a:52

  zone name IVRZ_tape_server2 vsan 1
    pwwn 10:02:50:45:32:20:7a:52
    pwwn 10:00:ad:51:78:33:f9:86

  zone name $default_zone$ vsan 1
mds# show ivr zoneset status
Zoneset Status
_____________
    name               : tape_server1_server2
    state              : activation success
    last activate time : Tue May 20 23:23:01 1980
    force option       : on
status per vsan:
__________________
     vsan     status
     ____     ______
     1        active
```

デフォルト設定

次の表に、IVR パラメータのデフォルト設定を示します。

Table 6: デフォルトの ***IVR*** パラメータ

パラメータ	デフォルト
IVR 機能	無効（Disabled）
IVR VSAN	仮想ドメインに追加されていません
IVR NAT	無効（Disabled）
IVR ゾーンの QoS	低
構成の配布	ディセーブル



CHAPTER 3

高度 VSAN間のルーティング構成

この章では、高度な構成情報と手順について説明します。高度なIVR構成をセットアップする前に、基本的な構成手順と、IVRの機能、制限事項、および用語の説明が記載されている 基本VSAN間のルーティング構成, on page 3 を参照してください。

詳細 IVR 構成 タスク リスト

SAN ファブリックで Advanced IVR トポロジを構成するには、次の手順を実行します：

Procedure

ステップ 1 IVR ネットワーク アドレス変換, on page 6 およびIVR NAT の要件とガイドライン, on page 12 を参照してください。

IVR ネットワーク アドレス変換（NAT）を使用するかどうかを決定します。

ステップ 2 「ドメイン ID ガイドライン, on page 42」を参照してください。

IVR NAT を使用しない場合は、IVR に参加しているすべてのスイッチおよび VSAN で一意のドメイン ID が構成されていることを確認します。

ステップ 3 「IVR を有効化 , on page 8」を参照してください。

境界スイッチで IVR を有効にします。

ステップ 4 「IVR サービス グループ, on page 36」を参照してください。

必要に応じてサービスグループを構成します。

ステップ 5 「CFS を使用した IVR 構成の配布, on page 9」を参照してください。

必要に応じて IVR 配信を構成します。

ステップ 6 IVR トポロジを手動または自動で構成します。

IVR トポロジの手動構成およびアクティブ化, on page 43および詳細 IVR 構成, on page 36を参照してください。

ステップ 7 「高度な IVR ゾーンと IVR ゾーン セット, on page 53」を参照してください。

手動で、またはファブリック分散を使用して、 すべての IVR 対応ボーダー スイッチで IVR ゾーン セットを作成し、アクティブにします。

ステップ 8 「IVR トポロジの確認, on page 48」を参照してください。

IVR 構成を確認します。

詳細 IVR 構成

このセクションでは、詳細IVR構成の手順について説明します。説明する項目は次のとおりです：

IVR サービス グループ

複雑なネットワーク トポロジでは、IVR対応のVSANが少数しかない場合があります。非IVR対応 VSAN へのトラフィック量を減らすために、IVR 対応 VSAN へのトラフィックを制限するサービス グループを構成できます。1 つのネットワークで最大 16 の IVR サービス グループを使用できます。新しいIVR対応スイッチがネットワークに追加された場合は、新しいVSANを含めるようにサービス グループを更新する必要があります。

サービス グループ ガイドライン

IVR サービス グループを構成する場合は、次の注意事項を考慮してください：

- IVR 自動トポロジ モードでサービス グループを使用する場合は、まず IVR を有効にしてサービス グループを構成し、次に CFS でそれらを配布してから、IVR 自動トポロジ モードを構成する必要があります。
- CFS 配信は、IVR VSAN トポロジが IVR 自動トポロジ モードの場合にのみ、サービス グループ内で制限されます。IVR VSAN トポロジ, on page 6を参照してください。
- ネットワークには最大 16 のサービス グループを構成できます。
- 新しい IVR 対応スイッチがネットワークに追加された場合は、新しい VSAN を含めるようにサービス 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することはできません。メンバーになると、CFS マージは失敗します。
- すべてのサービスグループを合わせた AFID と VSAN の組み合わせの合計数が 128 を超えることはできません。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 グループの構成は、すべての IVR 対応スイッチに配信されます。サービス グループに属する 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 グループ内に留まります。たとえば、2 つのメンバー（たとえば、pWWN 1 と pWWN 2）は、同じ IVR ゾーンに属し、異なるサービス グループに属している場合、通信できません。
- CFS マージ中に、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 を超えると、CFS マージは失敗します。
- CFS は、サービス グループの構成情報を到達可能なすべての SAN に配信します。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 対応スイッチでサービス グループ構成が同じであることを確認する必要があります。
- IVR サービス グループに属する IVR エンド デバイスは、そのサービス グループ外の AFID または VSAN にエクスポートされません。
- 少なくとも 1 つのサービスグループが定義されていて、IVR ゾーンメンバーがサービスグループに属していない場合、その IVR ゾーンメンバーは他のデバイスと通信できません。
- デフォルトのサービス グループ ID はゼロ（0）です。

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、ユーザー定義のサービス グループの一部ではないすべての AFID と VSAN の組み合わせは、デフォルト サービス グループのメンバーです。デフォルトのサービス グループの ID は 0 です。

デフォルトでは、デフォルト サービス グループのメンバー間で 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 グループの構成, on page 37」を参照してください。デフォルト ポリシーは、ASCII の構成の一部ではありません。

サービス グループのアクティブ化

設定されたサービス グループをアクティブにする必要があります。ゾーン セットのアクティブ化や VSAN トポロジのアクティブ化と同様に、設定済みのサービス グループをアクティブ化すると、現在アクティブなサービス グループ（存在する場合）が設定済みのサービス グループに置き換えられます。設定されているサービス 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 つだけです。これらの各データベースには、最大 16 のサービス グループを含めることができます。

IVR サービス グループの構成

IVR サービス グループを構成するには、次の手順に従います：

Procedure

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 IVR-SG1 と呼ばれる IVR サービス グループを構成し、IVR サーバー グループ構成モードを開始します。

switch(config)# **ivr service-group name IVR-SG1**

ステップ 3 IVR サービス グループを削除します。

switch(config)# **no ivr service-group name IVR-SG1**

ステップ 4 VSAN 1、2、および 6 ～ 10 の AFID 10 を構成します。

switch(config-ivr-sg)# **autonomous-fabric-id 10 vsan-ranges 1,2,6-10**

ステップ 5 VSAN 1 の AFID 11 を構成します。

switch(config-ivr-sg)# **autonomous-fabric-id 11 vsan-ranges 1**

ステップ 6 VSAN 3 ～ 5 の AFID 12 を構成します。

switch(config-ivr-sg)# **autonomous-fabric-id 12 vsan-ranges 3-5**

ステップ 7 AFID 12 と VSAN 3 ～ 5 の間の関連付けを削除します。

switch(config-ivr-sg)# **no autonomous-fabric-id 12 vsan-ranges 3-5**

ステップ 8 構成モードに戻ります。

switch(config-ivr-sg)# **exit**

ステップ 9 IVR-SG2 と呼ばれる IVR サービス グループを構成し、IVR サーバー グループ構成 モードを開始します。

switch(config)# **ivr service-group name IVR-SG2**

ステップ 10 VSAN 3 ～ 5 の AFID 20 を構成します。

switch(config-ivr-sg)# **autonomous-fabric-id 20 vsan-ranges 3-5**

ステップ 11 構成モードに戻ります。

switch(config-ivr-sg)# **exit**

ステップ 12 サービス グループ構成をアクティブにし、デフォルトのサービス グループ内のスイッチ間の通信ポリシーを allow（デフォルト）に構成します。

switch(config)# **ivr service-group activate**

ステップ 13 サービス グループ構成をアクティブにし、デフォルト サービス グループ内のスイッチ間の通信ポリシーを deny に設定します。

switch(config)# **ivr service-group activate default-sg-deny**

Note

通信ポリシーを許可に戻すには、 **ivr service-group activate** コマンドを再度発行する必要があります。

ステップ 14 サービス グループ構成を非アクティブにします（デフォルト）。

switch(config)# **no ivr service-group activate**

ステップ 15 VSAN トポロジをアクティブにします

switch(config)# **ivr vsan-topology activate**

ステップ 16 IVR 構成の CFS 配信をイネーブルにします。

switch(config)# **ivr distribute**

ステップ 17 IVR 構成をファブリックにコミットします。

switch(config)# **ivr commit**

アクティブ IVR サービス グループ データベースのコピー

設定済みの IVR サービス グループ データベースを変更できます。ただし、アクティブな IVR サービス グループ データベースは変更できません。アクティブ IVR サービス グループ データベースを手動で構成したサービス グループ データベースにコピーするには、EXEC モードで次のコマンドを使用します：

```
switch# ivr copy active-service-group user-configured-service-group
```

IVR サービス グループ データベースのクリア

IVR サービス グループ データベースのすべてのエントリをクリアするには、EXEC モードで **clear ivr service-group databas**e コマンドを使用します。このコマンドは、アクティブなデータベースではなく、構成されたデータベースのみをクリアします。

```
switch# clear ivr service-group database
```

IVR サービス グループ構成の確認

show ivr service-group active コマンドを使用して、アクティブな IVR サービス グループ データベースを表示します。

```
switch# show ivr service-group active
IVR ACTIVE Service Group
====================================
SG-ID  SG-NAME    AFID  VSANS
--------------------------------------------------------------------------------
 1     IVR-SG1      10  1-2,6-10
 1     IVR-SG1      11  1
 2     IVR-SG2      20  3-5
Total:   3 entries in active service group table
```

show ivr service-group configured コマンドを使用して、 構成された IVR サービス グループ データベースを表示します。

```
switch# show ivr service-group configured
IVR CONFIGURED Service Group
====================================
SG-ID  SG-NAME    AFID  VSANS
--------------------------------------------------------------------------------
 1     IVR-SG1      10  1-2,6-10
 1     IVR-SG1      11  1
 2     IVR-SG2      20  3-5
Total:   3 entries in configured service group table
```

自律ファブリック ID

自律ファブリック ID（AFID）は、セグメント化された VSAN を識別します（例えば、二つの VSAN が論理的および物理的に分かれているが同じ VSAN 番号を持つ）。Cisco MDS NX-OS リリース 4.2（1）は、AFID 1 ～ 64 をサポートします。AFID は、IVR 自動トポロジ モードと組み合わせて使用され、IVR VSAN トポロジ データベースでセグメント化された VSAN を許可します。

自律ファブリック ID ガイドライン

VSAN に対して個別に AFID を構成することも、スイッチ上のすべての VSAN に対してデフォルトの AFID を構成することもできます。デフォルトの AFID を持つスイッチ上の VSAN のサブセットに個別の AFID を構成すると、そのサブセットは構成された AFID を使用し、そのスイッチ上の他のすべての VSAN はデフォルトの AFID を使用します。

VSAN トポロジが IVR 自動トポロジ モードの場合にのみ、AFID 構成を使用できます。IVR 手動トポロジ モードでは、AFID は VSAN トポロジ構成自体で指定され、個別の AFID 構成は必要ありません。

Note VSAN 番号が同じで AFID が異なる 2 つの VSAN は、ファブリックで許可される合計 128 個の VSAN のうちの 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ているデバイスが 1 つの VSAN に属している場合、AFID が異なるため、通常のゾーンセットを構成して相互に通信することはできません。異なる AFID は異なるファブリックであると見なすことができます。したがって、3 つのスイッチは 3 つの異なるファブリックを表します。

次の例に示すように IVR VSAN トポロジを指定すると、同じ VSAN であっても、IVR はスイッチ間でデバイス間の接続を設定します。

同じ VSAN を使用した IVR VSAN トポロジ

```
switch# show ivr vsan-topology
AFID  SWITCH WWN                 Active   Cfg.    VSANS
-------------------------------------------------------
   1  20:00:00:0d:ec:27:6b:c0     yes     yes       1
   2  20:00:00:0d:ec:27:6c:00     yes     yes       1
```

```
   3  20:00:00:0d:ec:27:6c:40     yes     yes       1
Total:   3 entries in active and configured IVR VSAN-Topology
```

デフォルト AFID の構成

デフォルト AFID を構成するには、次のステップを実行します：

Procedure

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 terminal**

ステップ 2 AFID データベース構成サブモードを開始します。

switch(config)# **autonomous-fabric-id** database

ステップ 3 AFID に明示的に関連付けられていないすべての VSAN のデフォルト AFID を構成します。デフォルトの AFID の有効な範囲は 1 ～ 64 です。

switch(config-afid-db)# **switch-wwn 20:00:00:0c:91:90:3e:80 default-autonomous-fabric-id 5**

ステップ 4 デフォルトの AFID をデフォルト値（1）に戻します。

switch(config-afid-db)# **no switch-wwn 20:00:00:0c:91:90:3e:80 default-autonomous-fabric-id 5**

個々の AFID の構成

個々の AFID を構成するには、次の手順を実行します：

Procedure

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 AFID データベース構成サブモードを開始します。

switch(config)# **autonomous-fabric-id** database

ステップ 3 スイッチの AFID および VSAN 範囲を構成します。AFID の有効な範囲は 1 ～ 64 です。

switch(config-afid-db)# **switch-wwn 20:00:00:0c:91:90:3e:80 autonomous-fabric-id 10 vsan-ranges 1,2,5-8**

ステップ 4 AFID 10 から VSAN 2 を削除します。

switch(config-afid-db)# **no switch-wwn 20:00:00:0c:91:90:3e:80 autonomous-fabric-id 10 vsan-ranges 2**

AFID データベース構成の確認

AFID データベースの格納ファイルを表示するために、**show autonomous-fabric-id database** コマンドを使用します。

```
switch# show autonomous-fabric-id database
SWITCH WWN                    Default-AFID
------------------------------------------------------------
20:00:00:0c:91:90:3e:80          5
Total:   1 entry in default AFID table
SWITCH WWN                    AFID      VSANS
------------------------------------------------------------
20:00:00:0c:91:90:3e:80          10    1,2,5-8
Total:   1 entry in AFID table
```

IVR 自動トポロジのガイドライン

NAT モードまたは IVR 自動トポロジ モードで IVR を使用せずに IVR SAN ファブリックを構成する前に、次の一般的なガイドラインを考慮してください：

- この機能には、必須のエンタープライズ ライセンス パッケージまたは SAN-EXTENSION ライセンス パッケージと 1 つのアクティブな IPS カードを取得します。
- FSPF リンク コストを変更する場合は、任意の IVR パスの FSPF パス ディスタンス（パス上のリンク コストの合計）が 30,000 未満になるようにしてください。
- IVR 対応 VSAN は、interop モードが有効または無効のときに構成できます。

ドメイン ID ガイドライン

ドメイン ID を構成する前に、次のガイドラインを考慮してください：

- IVR NAT を使用していない場合は、IVR 動作に参加しているすべての VSAN およびスイッチで一意のドメイン ID を構成します。次のスイッチが IVR 動作に参加します：
  - エッジ VSAN 内のすべてのエッジ スイッチ（送信元および宛先）
  - 中継 VSAN 内のすべてのスイッチ
- ドメイン ID の割り当てが必要なスイッチの数を最小限に抑えます。これにより、トラフィックの中断が最小限に抑えられます。
- SAN を初めて構成するとき、および新しいスイッチをそれぞれ追加するときは、相互接続された VSAN 間の調整を最小限に抑えます。

次の 2 つのオプションのいずれかを使用してドメイン ID を構成できます：

- 異なる VSAN のドメインが参加しているすべてのスイッチおよび VSAN で重複しないように、許可ドメイン リストを構成します。
- 参加しているスイッチおよび VSAN ごとに、重複しない静的ドメインを構成します。

Note NAT の含まない IVR を伴う構成では、IVR トポロジ内の 1 つの VSAN でスタティック ドメイン ID が構成されている場合、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 を構成する必要があります。

中継 VSAN ガイドライン

中継 VSAN を構成する前に、次の注意事項を考慮してください：

- IVR ゾーン メンバーシップの定義に加えて、トランジット VSAN のセットを指定して、2 つのエッジ VSAN 間の接続を提供することもできます：
  - IVR ゾーン内で二つのエッジ VSAN で重なった場合、トランジット VSAN は接続を提供する必要はありません。
  - IVR ゾーン内で二つのエッジ VSAN で重ならない場合、接続を提供するために1 つ以上の中継 VSAN が必要な場合があります。送信元と接続先エッジ VSAN 両方のメンバーのスイッチ上で IVR が有効ではない場合、IVR ゾーン内の二つのエッジ VSAN は重なりません。
- エッジ VSAN の間のトラフィックは、最短 IVR パスのみ通過します。
- 中継 VSAN 情報は、全ての IVR ゾーン セットで共通です。時には中継 VSAN は、別の IVR ゾーンでエッジ VSAN として機能することができます。

ボーダー スイッチ ガイドライン

ボーダー スイッチを構成する前に、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でのみ IVR を構成します。
- ボーダー スイッチには、Cisco MDS SAN-OS リリース 1.3（1）以降が必要です。
- ボーダー スイッチは、2 つ以上の VSAN のメンバーである必要があります。
- IVR 通信を容易にする境界スイッチは、IVR 対応である必要があります。
- 追加の境界スイッチで IVR を有効にして、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 トポロジ構成を更新する必要があります。

IVR トポロジの手動構成およびアクティブ化

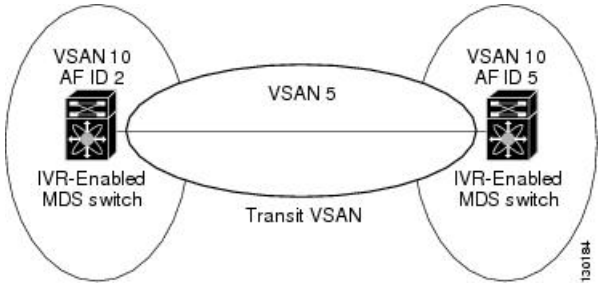
IVR 自動トポロジ モードをイネーブルにしていない場合は、ファブリック内のすべての IVR 対応スイッチで IVR トポロジを作成する必要があります。IVR 手動トポロジ モードを使用するには、このセクションの手順に従います。

手動構成のガイドライン

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：

- IVR トポロジでは、最大 128 の IVR 対応スイッチと 128 の異なる VSAN を構成できます（Figure 4: 例：AFID を使用した一意でない VSAN ID を持つ IVR トポロジ, on page 44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。
  - AFID は、論理的および物理的に分離された 2 つの VSAN が区別されますが、これらの VSAN 番号は同じです。最大 64 個の AFID を指定できます。

Figure 4: 例：***AFID*** を使用した一意でない ***VSAN ID*** を持つ ***IVR*** トポロジ



- IVR トポロジ内の 2 つの VSAN の VSAN ID が同じで AFID が異なる場合、IVR の 128 VSAN 制限では、2 つの VSAN としてカウントされます。
- 単一の AFID を使用する場合、VSAN 間ルーティング トポロジでセグメント化された VSAN は使用できません。

IVR トポロジの手動構成

Note IVR 対応スイッチのスイッチ WWN を取得するには、**show wwn switch** コマンドを使用します。

Cisco NX-OS を使用して IVR トポロジを手動で構成するには、次の手順を実行します：

Procedure

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 IVR 機能の VSAN トポロジ データベース構成モードを開始します。

switch(config)# **ivr vsan-topology database**。

ステップ 3 このスイッチの IVR に参加するように VSAN 1、2、および 6 を構成します。

switch(config-ivr-topology-db)# **autonomous-fabric-id 1 switch 20:00:00:05:30:01:1b:b8 vsan-ranges 1-2,6**。

ステップ 4 このスイッチの IVR に参加するように VSAN 1、2、および 3 を構成します。

switch(config-ivr-topology-db)# **autonomous-fabric-id 1 switch 20:00:00:05:30:01:1b:c2 vsan-ranges 1-3**。

ステップ 5 このスイッチの IVR から VSAN 1 および 2 を削除します。

switch(config-ivr-topology-db)# **no autonomous-fabric-id 1 switch 20:00:00:05:30:01:1b:c2 vsan-ranges 1-2**。

ステップ 6 EXEC モードに戻ります。

switch(config-ivr-topology-db)# **end**

What to do next

show ivr vsan-topology コマンドを使用して、IVR トポロジを表示します。次の出力例では、VSAN 2 は VSAN 1、5、および 6 の間の中継 VSAN です。

```
switch# show ivr vsan-topology
AFID  SWITCH WWN                 Active   Cfg. VSANS
--------------------------------------------------------------
   1  20:00:00:05:30:01:1b:c2 *   no      yes  1-2
   1  20:02:00:44:22:00:4a:05     no      yes  1-2,6
   1  20:02:00:44:22:00:4a:07     no      yes  2-5
Total:   3 entries in active and configured IVR VSAN-Topology

Current Status: Inter-VSAN topology is INACTIVE
```

すべての IVR 対応スイッチでこの構成を繰り返すか、CFS を使用して IVR 構成を配布します。「CFS を使用した IVR 構成の配布, on page 9」を参照してください。

Tip トランジット VSAN は、構成に基づいて推定されます。IVR 機能には、明示的な中継 VSAN 構成はありません。

手動で構成した IVR トポロジのアクティブ化

IVR トポロジを手動で構成した後、アクティブにする必要があります。

Caution アクティブな IVR トポロジは非アクティブ化できません。IVR 自動トポロジ モードにのみ切り替えることができます。

IVR トポロジを手動で Activate するには、次のステップに従います：

Procedure

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 terminal**

ステップ 2 手動で構成した IVR トポロジをアクティブにします。

switch(config)# **ivr vsan-topology activate**

アクティブな IVR トポロジの表示

show ivr vsan-topology コマンドを使用して、アクティブな IVR トポロジを表示します。

```
switch# show ivr vsan-topology
AFID  SWITCH WWN                 Active   Cfg. VSANS
------------------------------------------------------------
   1  20:00:00:05:30:01:1b:c2 *   yes     yes  1-2
   1  20:02:00:44:22:00:4a:05     yes     yes  1-2,6
   1  20:02:00:44:22:00:4a:07     yes     yes  2-5
Total:   3 entries in active and configured IVR VSAN-Topology
Current Status: Inter-VSAN topology is ACTIVE
Last activation time: Mon Mar 24 07:19:53 2009
```

Note アスタリスク（*）はローカル スイッチを示します。

既存の IVR トポロジの使用

ここでは、既存の IVR トポロジの高度な IVR 構成について説明します：

既存の IVR トポロジへの IVR 対応スイッチの追加

IVR対応スイッチを既存のファブリックに追加する前に、新しいスイッチのIVRトポロジにエントリを追加し、新しい IVR トポロジをアクティブにする必要があります。

IVR 対応スイッチを既存の IVR トポロジに追加するには、次の手順を実行します：

Procedure

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 terminal**

ステップ 2 VSAN データベース構成サブモードを開始します。

mds(config)# ivr vsan-topology database

ステップ 3 新しい IVR 対応スイッチをトポロジに追加します。

mds(config-ivr-topology-db)# **autonomous-fabric-id 1 switch-wwn 20:00:00:05:40:01:1b:c2 vsan-ranges 1,4**

ステップ 4 構成モードに戻ります。

switch(config-ivr-topology-db)# **exit**

ステップ 5 IVR VSAN トポロジをアクティブにします。

switch(config)# ivr vsan-topology activate

ステップ 6 IVR 構成の変更をファブリックにコミットします。

switch(config)# **ivr commit**

ステップ 7 EXEC モードに戻ります。

switch(config)# **exit**

ステップ 8 実行コンフィギュレーションを保存します。

switch# **copy running-config startup-config**

What to do next

IVR トポロジにスイッチを追加した後、新しいスイッチで IVR と CFS を有効にします（IVR を有効化 , on page 8 および CFS を使用した IVR 構成の配布, on page 9を参照）。

既存の IVR トポロジへの VSAN の追加

既存の IVR トポロジに VSAN を追加するには、コマンド構文ですべての VSAN を指定する必要があります。VSAN 1101 ～ 1102 および 2101 ～ 2102 を使用した最初の IVR 構成, on page 47 に、VSAN 1101 ～ 1102 および VSAN 2101 ～ 2102 の IVR 構成を示します。IVR 構成への VSAN 1103 および 2103 の追加, on page 48 に、IVR トポロジへの VSAN 1103 および 2103 の追加を示します。

VSAN 1101 ～ 1102 および 2101 ～ 2102 を使用した最初の IVR 構成

```
switch(config)# ivr enable
switch(config)# ivr distribute
switch(config)# ivr vsan-topology database
switch(config-ivr-topology-db)# autonomous-fabric-id    1 switch-wwn
20:00:00:0d:ec:4a:5e:00 vsan-ranges 1101-1102,1199,3100,3150
switch(config-ivr-topology-db)# autonomous-fabric-id    1 switch-wwn
20:00:00:0d:ec:4a:5f:00 vsan-ranges 2101-2102,2199,3100,3150
switch(config)# ivr vsan-topology activate
```

IVR 構成への VSAN 1103 および 2103 の追加

```
switch(config)# ivr enable
switch(config)# ivr distribute
switch(config)# ivr vsan-topology database
switch(config-ivr-topology-db)# autonomous-fabric-id    1 switch-wwn
20:00:00:0d:ec:4a:5e:00 vsan-ranges 1101-1103,1199,3100,3150
switch(config-ivr-topology-db)# autonomous-fabric-id    1 switch-wwn
20:00:00:0d:ec:4a:5f:00 vsan-ranges 2101-2103,2199,3100,3150
switch(config)# ivr vsan-topology activate
```

アクティブな IVR トポロジをコピー

手動で構成した IVR トポロジを編集できます。ただし、アクティブな IVR トポロジは編集できません。アクティブな IVR トポロジ データベースを手動構成トポロジにコピーするには、EXEC モードで **ivr copy active-topology user-configured-topology** コマンドを発行します。

```
switch# ivr copy active-topology user-configured-topology
```

手動で構成した IVR トポロジ データベースのクリア

手動で構成された IVR トポロジ データベースをクリアするには、次の手順を実行します：

Procedure

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 terminal**

ステップ 2 以前に作成した IVR トポロジをクリアします。

switch(config)# no **ivr vsan-topology database**

IVR トポロジの確認

IVR トポロジを確認するには、 **show ivr vsan-topology** コマンドを発行します。

構成された IVR VSAN トポロジの表示

```
switch# show ivr vsan-topology
AFID    SWITCH WWN                Active   Cfg. VSANS
-----------------------------------------------------------
   1    20:00:00:05:30:01:1b:c2 *   yes     yes  1-2
   1    20:02:00:44:22:00:4a:05     yes     yes  1-2,6
   1    20:02:00:44:22:00:4a:07     yes     yes  2-5
Total:   5 entries in active and configured IVR VSAN-Topology
```

```
Current Status: Inter-VSAN topology is ACTIVE
Last activation time: Sat Mar 22 21:46:15 1980
```

Note アスタリスク（*）はローカル スイッチを示します。

アクティブな IVR VSAN トポロジの表示

```
switch# show ivr vsan-topology active
AFID   SWITCH WWN                 Active   Cfg. VSANS
-----------------------------------------------------------
    1  20:00:00:05:30:01:1b:c2 *   yes     yes  1-2
    1  20:02:00:44:22:00:4a:05     yes     yes  1-2,6
    1  20:02:00:44:22:00:4a:07     yes     yes  2-5
Total:   5 entries in active IVR VSAN-Topology
Current Status: Inter-VSAN topology is ACTIVE
Last activation time: Sat Mar 22 21:46:15
```

構成された IVR VSAN トポロジの表示

```
switch# show ivr vsan-topology configured
AFID  SWITCH WWN                Active   Cfg. VSANS
-----------------------------------------------------------
    1  20:00:00:05:30:01:1b:c2 *   yes     yes  1-2
    1  20:02:00:44:22:00:4a:05     yes     yes  1-2,6
    1  20:02:00:44:22:00:4a:07     yes     yes  2-5
Total:   5 entries in configured IVR VSAN-Topology
```

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

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、モードを切り替える前に、アクティブな IVR VSAN トポロジ データベースをユーザー構成の IVR VSAN トポロジ データベースにコピーします。

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

Procedure

ステップ 1 自動 IVR トポロジ データベースをユーザー構成の IVR トポロジにコピーします。

switch# **ivr copy auto-topology user-configured-topology**

ステップ 2 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 3 IVR トポロジ データベースの IVR 自動トポロジ モードを無効にし、IVR 手動トポロジ モードを有効にします。

switch(config)# **ivr vsan-topology activate**

IVR の永続的 FC ID

ここでは次の内容について説明します。

FC ID の機能と利点

FC ID の永続性は、次の機能を提供することで IVR 管理を改善します。

- ネイティブ VSAN で使用する特定の仮想ドメインを制御および割り当てることができます。
- デバイスの特定の仮想 FC ID を制御および割り当てることができます。

IVR の永続的 FC ID の利点は次のとおりです：

- ホストデバイスは、ターゲットに対して常に同じ FC ID を認識します。
- FC ID は、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するのに役立ちます。
- FC ID を使用すると、SAN のモニタリングと管理が容易になります。同じドメインまたは FC ID が一貫して割り当てられている場合は、参照先のネイティブ VSAN またはデバイスを簡単に特定できます。

FC ID のガイドライン

永続的 FC ID を構成する前に、次の点を考慮してください：

- 永続 IVR FC ID には、次の 2 種類のデータベース エントリを構成できます：
  - 仮想ドメインエントリ：特定の VSAN（現在の VSAN）でネイティブ VSAN を表すために使用する必要がある仮想ドメインが含まれています。仮想ドメインエントリには、次の情報が含まれています：

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 でネイティブ AFID および VSAN に使用される仮想ドメイン

- • 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る必要がある仮想 FC ID が含まれています。仮想 FC ID エントリには、次の情報が含まれています：

ポートWWN

現在の AFID

現在の VSAN

現在の AFID および VSAN 内の特定の pWWN のデバイスを表すために使用される仮想 FC ID

- IVR に永続的な 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それらを使用することを推奨します。他のデバイスに自動割り当てを使用しながら、一部の IVR デバイスに永続的な FC ID を使用することは推奨されません。
- IVR 永続的 FC ID を使用するには、IVR NAT を有効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 の永続的 FC ID の構成

永続的 FC ID を構成するには、次の手順を実行します：

Procedure

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 現在の AFID 21 および VSAN 22 の IVR fcdomain データベース構成サブモードを開始します。

switch(config)# **ivr fcdomain database autonomous-fabric-num 21 vsan 22**。

ステップ 3 現在の AFID 21 および VSAN 22 のすべてのデータベース エントリ（対応するすべての永続的 FC ID エントリを含む）を削除します。

switch(config)# **no ivr fcdomain database autonomous-fabric-num 21 vsan 22**。

ステップ 4 ネイティブ AFID 20、ネイティブ VSAN 11、およびドメイン 12 のデータベース エントリを追加または置換し、IVR fcdomain FC ID 構成サブモードを開始します。対応するすべての永続的 FC ID エントリのドメインも 12 に変更されます。

switch(config-fcdomain)# **native-autonomous-fabric-num 20 native-vsan 11 domain 12**

ステップ 5 仮想ドメイン エントリのネイティブ AFID 20 とネイティブ VSAN 11、および対応するすべての FC ID エントリを削除します。

switch(config-fcdomain)# **no native-autonomous-fabric-num 20 native-vsan 11**。

ステップ 6 pWWN を FC ID にマッピングするためのデータベース エントリを追加または置換します。

switch(config-fcdomain-fcid)# **pwwn 11:22:33:44:55:66:77:88 fcid 0x114466**

ステップ 7 pWWN のデータベース エントリを削除します。

switch(config-fcdomain-fcid)# **no pwwn 11:22:33:44:55:66:77:88**。

ステップ 8 デバイス エイリアスを FC ID にマッピングするためのデータベース エントリを追加します。

switch(config-fcdomain-fcid)# **device-alias SampleName fcid 0x123456**

ステップ 9 デバイス エイリアスのデータベース エントリを削除します。

switch(config-fcdomain-fcid)# **no device-alias SampleName**

固定的 FC ID 構成を確認

show ivr fcdomain database コマンドを使用して、永続的な FC ID の構成を確認します。

すべての IVR fcdomain データベース エントリの表示

```
switch# show ivr fcdomain database
-------------------------------------------------
  AFID  Vsan  Native-AFID  Native-Vsan  Virtual-domain
-------------------------------------------------
    1     2        10          11         0xc(12)
   21    22        20          11         0xc(12)
Number of Virtual-domain entries: 2
-------------------------------------------------
  AFID  Vsan          Pwwn           Virtual-fcid
-------------------------------------------------
   21    22  11:22:33:44:55:66:77:88  0x114466
   21    22  21:22:33:44:55:66:77:88  0x0c4466
   21    22  21:22:33:44:55:66:78:88  0x0c4466
Number of Virtual-fcid entries: 3
```

特定の AFID および VSAN の IVR fcdomain データベース エントリの表示

```
switch# show ivr fcdomain database autonomous-fabric-num 21 vsan 22
-------------------------------------------------
  AFID  Vsan  Native-AFID  Native-Vsan  Virtual-domain
-------------------------------------------------
   21    22        20          11         0xc(12)
Number of Virtual-domain entries: 1
-------------------------------------------------
  AFID  Vsan          Pwwn           Virtual-fcid
-------------------------------------------------
   21    22  11:22:33:44:55:66:77:88  0x114466
   21    22  21:22:33:44:55:66:77:88  0x0c4466
   21    22  21:22:33:44:55:66:78:88  0x0c4466
Number of Virtual-fcid entries: 3
```

高度な IVR ゾーンと IVR ゾーン セット

ここでは、IVR ゾーンおよび IVR ゾーン セットの詳細構成について説明します。IVR ゾーンとゾーン セットの構成の基本情報については、「IVR ゾーンと IVR ゾーン セット, on page 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 間通信を有効にする必要があります。これを実現するには、各IVRゾーンを（pWWN、VSAN）エントリのセット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なることができるため、異なる 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。

Note すべての IVR 対応スイッチで同じ IVR ゾーン セットをアクティブにする必要があります。

Caution Cisco SAN-OS リリース 3.0（3）より前は、ネットワーク内のすべてのスイッチで合計 10,000 のゾーン メンバーのみを構成できます。Cisco SAN-OS リリース 3.0（3）では、ネットワーク内のすべてのスイッチで合計 20,000 のゾーンメンバーのみを構成できます。2 つのゾーンに存在する場合、ゾーン メンバーは、2 回数えられます。データベース マージの注意事項, on page 27を参照してください。

IVR ゾーン構成ガイドライン

相互運用モードが有効になっている場合は、次の IVR 構成時の注意事項を考慮してください：

- メンバーのネイティブ VSAN が相互運用モードの場合（たとえば、相互運用モードが 2、3、または 4 の場合）、ReadOnly、QoS 属性、および LUN ゾーン分割は許可されません。
- メンバーの VSAN がすでに相互運用モードであり、ReadOnly、QoS 属性、または LUN ゾーン分割を構成しようとすると、構成が許可されないことを示す警告メッセージが表示されます。
- 最初に読み取り専用、QoS 属性、または LUN ゾーン分割を構成してから、メンバーの VSAN 相互運用モードを変更すると、構成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。構成を変更するように求められます。

次に、ReadOnly、QoS 属性、および LUN ゾーン分割に影響する構成変更が行われたときに表示される警告メッセージの例を示します。

IVR ゾーン構成の警告メッセージ

```
switch(config)# vsan database
switch(config-vsan-db)# vsan 2
switch(config-vsan-db)# vsan 2 interop 2
switch(config-vsan-db)# exit
switch(config)# ivr zoneset name ivr_zs1 switch(config-ivr-zoneset)# zone name ivr_z1
```

```
 switch(config-ivr-zoneset-zone)# member pwwn 21:00:00:14:c3:3d:45:22 lun 0x32 vsan 2
VSAN is in interop mode, and LUN zoning cannot be set.
switch(config)# ivr zoneset name ivr_zs1 switch(config-ivr-zoneset)# zone name ivr_z1
 switch(config-ivr-zoneset-zone)# member pwwn 21:00:00:14:c3:3d:45:22 vsan 2
 switch(config-ivr-zoneset-zone)# attribute read-only VSAN is in interop mode and zone
member has been configured, zone cannot be set to READ-ONLY.
switch(config-ivr-zoneset-zone)# attribute qos priority medium VSAN is in interop mode
and zone member has been configured, QoS cannot be assigned to zone.
```

IVR ゾーン分割での LUN の構成

LUN ゾーン分割は、アクティブな IVR ゾーンのメンバー間で使用できます。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 で目的の IVR ゾーン メンバー間で LUN ゾーンを作成およびアクティブ化することで、サービスを構成できます。または、IVR で直接サポートされている LUN ゾーン分割を使用できます。LUN ゾーン分割の利点の詳細については、『Cisco MDS 9000 シリーズ *NX-OS* ファブリック構成ガイド』 または『 *Cisco* ファブリック マネージャ ファブリック構成ガイド』 を参照してください。

IVR ゾーン分割に LUN を構成するには、次の手順に従います：

Procedure

ステップ 1 設定モードを開始します。

switch# **config t**

ステップ 2 IvrLunZone と呼ばれる IVR ゾーンを構成します。

switch(config)# **ivr zone name IvrLunZone**

ステップ 3 指定された pWWN と LUN 値に基づいて IVR ゾーン メンバーを構成します。

switch(config-ivr-zone)# **member pwwn 10:00:00:23:45:67:89:ab lun 0x64 vsan 10**

Note
CLI は、**0x** プレフィックスが含まれているかどうかに関係なく、LUN ID の値を 16 進値として解釈します。

ステップ 4 指定された pWWN、LUN 値と AFID に基づいて IVR ゾーン メンバーを構成します。

switch(config-ivr-zone)# **member pwwn 10:00:00:23:45:67:89:ab lun 0x64 vsan 10 autonomous-fabric-id 20**

ステップ 5 IVR ゾーン メンバーを削除します。

switch(config-ivr-zone)# **no member pwwn 20:81:00:0c:85:90:3e:80 lun 0x32 vsan 13 autonomous-fabric-id 10**

What to do next

Note IVR ゾーン セット セットアップで LUN ゾーン分割を構成できます。

QoS 属性の構成

IVR ゾーンの QoS 属性を設定するには、次の手順を実行します：

SUMMARY STEPS

1. コンフィギュレーション モードに入ります。
2. IvrZone と呼ばれる IVR ゾーンを構成します。
3. IVR ゾーン トラフィックの QoS を中程度に構成します。
4. デフォルトの QoS 設定に戻します。デフォルトは [低（Low）] です。

DETAILED STEPS

Procedure

	Command or Action	Purpose
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	IvrZone と呼ばれる IVR ゾーンを構成します。	switch(config)# **ivr zone name IvrZone**
ステップ 3	IVR ゾーン トラフィックの QoS を中程度に構成します。	switch(config-ivr-zone)# **attribute qos priority medium**。
ステップ 4	デフォルトの QoS 設定に戻します。デフォルトは [低（Low）] です。	switch(config-ivr-zone)# **no attribute qos priority medium**

What to do next

Note 他の QoS 属性が構成されている場合は、最も高い設定が優先されます。

IVR ゾーンの QoS 属性の確認

show ivr zone コマンドを使用して、IVR ゾーンの QoS 属性を確認します。

```
switch(config)# show ivr zone
zone name IvrZone
    attribute qos priority medium
```

IVR ゾーンと IVR ゾーン セットの名前変更

IVR ゾーンの名前を変更するには、EXEC モードで **ivr zone rename** コマンドを使用します。

```
switch# ivr zone rename ivrzone1 ivrzone2
```

IVR ゾーン セットの名前を変更するには、EXEC モードで **ivr zoneset rename** コマンドを使用します。

```
switch# ivr zoneset rename ivrzone1 ivrzone2
```

構成された IVR ゾーン データベースのクリア

ゾーン セットをクリアすると、構成済みゾーン データベースが消去され、アクティブ ゾーン データベースは消去されません。

構成された IVR ゾーン データベースをクリアするには、 **clear ivr zone database** コマンドを使用します。

Procedure

ステップ 1 設定されているすべての IVR ゾーン情報をクリアします。

switch# **clear ivr zone database**

ステップ 2 スイッチの再起動時に実行構成が使用されるようにします。

switch# **copy running-config startup-config**

読み取り専用ゾーン分割を使用する IVR の構成

読み取り専用ゾーン分割（LUNの有無にかかわらず）は、アクティブなIVRゾーンのメンバー間で使用できます。このサービスを構成するには、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 内の目的の IVR ゾーン メンバー間で読み取り専用ゾーンを作成し、アクティブにする必要があります。

Note 読み取り専用ゾーン分割は、IVR ゾーン セット セットアップでは構成できません。

IVR フローでの Advanced Fabric Services の有効化

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、内部機能である抽象 ACL マネージャ（AAM）を使用して IVR フローで有効にできるようになりました。

ガイドラインおよび制約事項の構成

IVR の AAM を有効にする前に、次の前提条件を考慮する必要があります：

- CFS 配信は、IVR に対して有効にする必要があります。
- AAM は、IVR-NAT モードでのみサポートされます。
- ファブリック サービス（SME や IOA など）が有効になっているスイッチは、AAM がサポートする NX-OS リリース 5.0（1）以降を実行している必要があります。
- FC リダイレクトは、バージョン 1 またはバージョン 2 モードで実行できます。
- FCR の IVR サポートを有効にする前に、IVR の AAM サポートを有効にする必要があります。
- AAM が IVR に対して有効になっている場合、LUN ゾーン分割はサポートされません。
- IVR マージは、両方のファブリックで AAM が有効になっている場合、または両方のファブリックで AAM が無効になっている場合にのみサポートされます。ファブリックの 1 つで AAM が有効になっており、もう一方のファブリックで AAM が無効になっている場合、IVR マージは失敗します。
- IVR デバイスのすべての高度なファブリック サービス（SME および IOA）設定を削除し、FCR の IVR サポートを無効にしてから、IVR の AAM サポートを無効にする必要があります。
- MDS NX-OS リリース 5.0（1）に以前のリリースにダウングレードする前に、IVR デバイスのすべての高度なファブリック サービス（SME および IOA）構成を削除し、FCR の IVR サポートを無効にしてから、IVR の AAM サポートを無効にする必要があります。

IVR の AAM サポートの有効化

IVR の AAM を有効にするには、次の手順を実行します：

Procedure

ステップ 1 コンフィギュレーション モードを開始します。

switch# **config t**

ステップ 2 IVRを有効にします。

switch(config)# **feature ivr**

ステップ 3 IVR の CFS 配信を有効にします。

switch(config)# **ivr distribute**

ステップ 4 IVR の NAT モードを有効にします。

switch(config)# **ivr nat**

ステップ 5 IVR 構成変更をコミットします。

switch(config)# **ivr commit**

ステップ 6 IVR の AAM を有効にします。

switch(config)# **ivr aam register**

ステップ 7 IVR 構成変更をコミットします。

switch(config)# **ivr commit**

What to do next

show ivr aam コマンドを使用して、AAM サポートが IVR に対して有効になっているかどうかを確認できます。

```
switch(config)# show ivr aam
AAM mode status
--------------------------
AAM is enabled
```

FCR の IVR サポートの有効化

FCR の IVR サポートを有効にするには、次の手順に従います：

Procedure

ステップ 1 コンフィギュレーション モードを開始します。

switch# **config t**

ステップ 2 FCR の IVR サポートを有効にします。

switch(config)# **fc-redirect ivr-support enable**

What to do next

show fc-redirect config コマンドを使用して、AAM サポートが FCR に対して有効になっているかどうかを確認できます。

```
switch(config)# show fc-redirect config
switch(config)#
switch(config)#
switch(config)#
```

IVR の AAM サポートの無効化

IVR の AAM サポートを無効にするには、次の手順を実行します：

Procedure

ステップ 1 コンフィギュレーション モードを開始します。

switch# **config t**

ステップ 2 IVR デバイスの高度なファブリック サービス構成が存在するかどうかを確認します。

switch(config)# **ivr aam pre-deregister-check**

ステップ 3 IVR デバイスの高度なファブリック サービス構成のステータスを表示します。

switch(config)# **show ivr aam pre-deregister-check**

ステップ 4 IVR デバイスのすべての高度なファブリックサービス（SME および IOA）構成を削除します。

『Cisco MDS 9000 シリーズ SME と IOA構成ガイド』を参照してください。

ステップ 5 FCR の IVR サポートを無効にします。

switch(config)# **no fc-redirect ivr-support enable**

ステップ 6 IVR の AAM サポートを無効にします。

switch(config)# **no ivr aam register**

ステップ 7 IVR 構成変更をコミットします。

switch(config)# **ivr commit**

What to do next

IVR の AAM サポートを無効にする前に、 **ivr aam pre-deregister-check** コマンドを使用して、IVR デバイスの SME または IOA 構成があるかどうかを確認する必要があります。

```
switch(config)# show ivr aam pre-deregister-check
AAM pre-deregister check status
--------------------------
Run the "ivr aam pre-deregister-check" command first to check whether an ivr aam deregister
 can be done.
switch(config)# ivr aam pre-deregister-check
switch(config)# show ivr aam pre-deregister-check
AAM pre-deregister check status
```

```
-------------------------
FAILURE
There are merged entries or AAM has not been enabled with the following switches:
  switch swwn 20:00:00:05:30:00:15:de
User has two options:
 1. User can go ahead to issue ivr commit, but the above switches in the fabric may fail
 to deregister.
 2. User may also run "ivr abort", then resolve above switches and re-issue the ivr aam
 deregister.
Warning: IVR AAM pre-deregister-check status may not be up-to-date. Please issue the
command "ivr aam pre-deregister-check" to get updated status.
switch(config)# ivr aam pre-deregister-check
switch(config)# show ivr aam pre-deregister-check
AAM pre-deregister check status
-------------------------
SUCCESS
Warning: IVR AAM pre-deregister-check status may not be up-to-date. Please issue the
command "ivr aam pre-deregister-check" to get updated status.
```

翻訳について
このドキュメントは、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。