



基本的な Inter-VSAN Routing 設定

この章では、Inter-VSAN Routing (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 上でリソースを共有するための基本的な手順を紹介します。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 設定」を参照してください。

この章で説明する基本的な IVR 設定に関する内容は次のとおりです。

- 「IVR について」 (P.1-1)
- 「基本的な IVR 設定」 (P.1-6)
- 「IVR 仮想ドメイン」 (P.1-13)
- 「IVR ゾーンと IVR ゾーンセット」 (P.1-14)
- 「IVR ロギング」 (P.1-23)
- 「データベース マージに関するガイドライン」 (P.1-24)
- 「デフォルト設定」 (P.1-27)

IVR について

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。

ここで説明する内容は、次のとおりです。

- 「IVR の機能」 (P.1-2)
- 「IVR の用語」 (P.1-3)
- 「IVR の設定制限」 (P.1-4)
- 「ファイバチャネルヘッダーの変更」 (P.1-4)
- 「IVR ネットワークアドレス変換」 (P.1-5)
- 「IVR VSAN トポロジ」 (P.1-5)
- 「IVR の相互運用性」 (P.1-5)

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ぐ 1 つ以上の VSAN を横断する、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障害回復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。

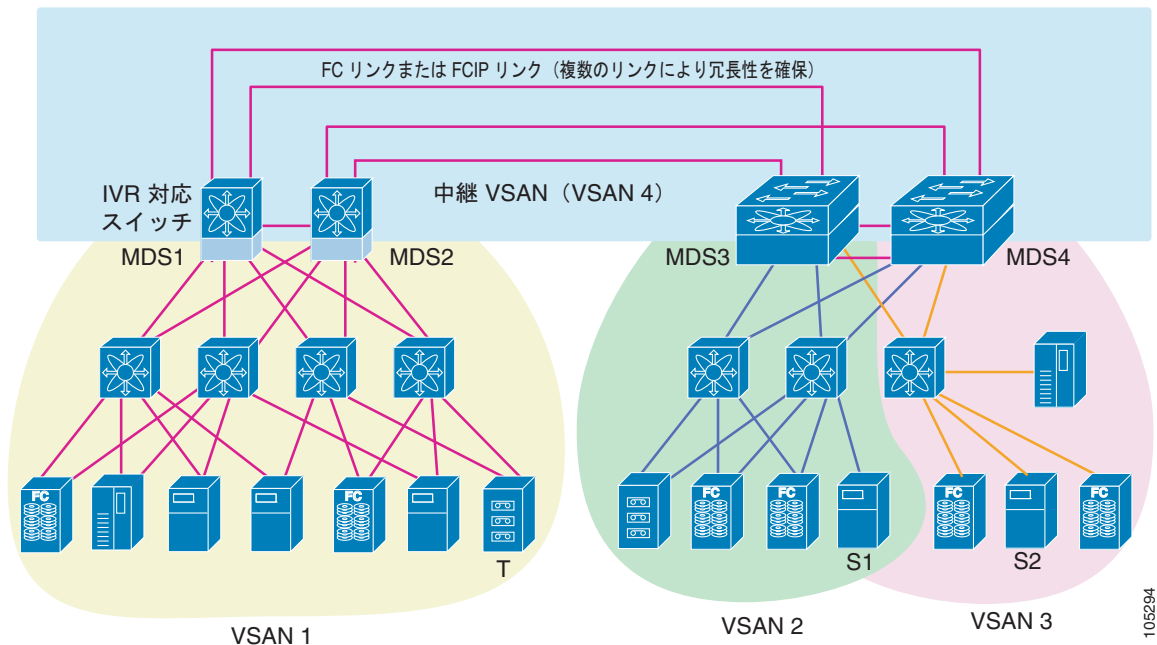


(注)

IVR は、Cisco MDS 9124 Fabric Switch、Cisco MDS 9134 Fabric Switch、Cisco Fabric Switch for HP c-Class BladeSystem、および Cisco Fabric Switch for IBM BladeCenter では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



105294

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オンしている 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 ファミリー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 | 上限 |
|---------------|---|
| 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.2-9) 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 ファミリー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 モードについて](#)」(P.1-10) を参照してください。

IVR VSAN 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 の相互運用性

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 モードのいずれかがイネーブルの場合は、中継 VSAN またはエッジ VSAN 上に非 MDS スイッチを存在させることもできます。

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。

基本的な IVR 設定タスク リスト

IVR を設定するには、次の手順を実行します。

| タスク | 参照 |
|--------|--|
| 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 モードについて」 (P.1-10) 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 モードについて」 (P.1-10) 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.1-16) 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。 |

基本的な IVR 設定

ここでは、IVR の設定方法について説明します。内容は次のとおりです。

- [「IVR Zone Wizard を使用した IVR と IVR ゾーンの設定」 \(P.1-6\)](#)
- [「IVR のイネーブル化」 \(P.1-8\)](#)
- [「CFS を使用した IVR 設定の配信」 \(P.1-8\)](#)
- [「IVR NAT と IVR 自動トポロジ モードについて」 \(P.1-10\)](#)
- [「IVR NAT の要件とガイドライン」 \(P.1-10\)](#)
- [「IVR NAT と IVR 自動トポロジ モードのイネーブル化」 \(P.1-12\)](#)

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

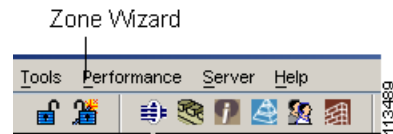
IVR Zone Wizard を使用すれば、ファブリック内の IVR ゾーンの設定プロセスが容易になります。IVR Zone Wizard は次の条件を調べて、関連する問題を特定します。

- 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。

Fabric Manager の 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 (図 1-2 を参照)。

図 1-2 [IVR Zone Wizard] アイコン

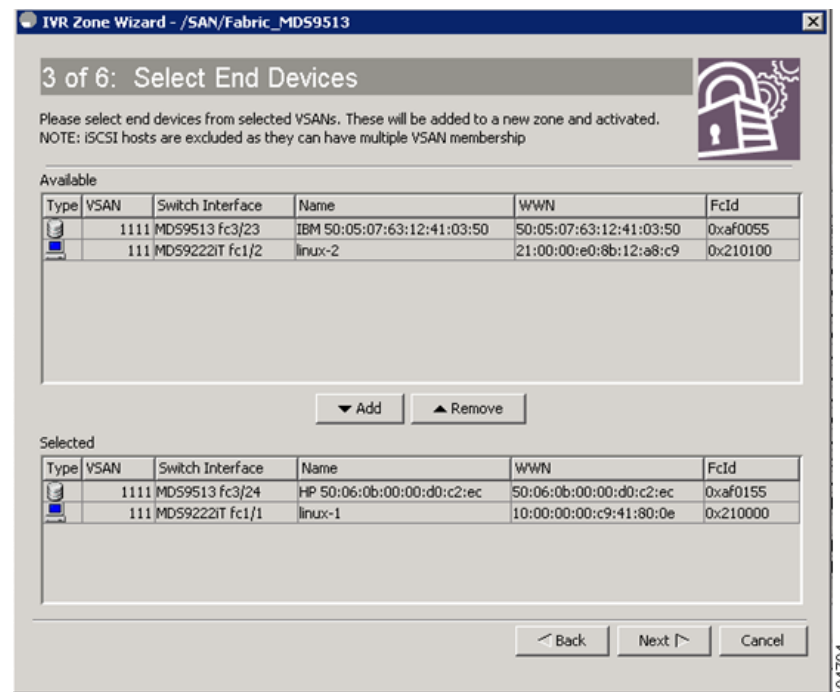


IVR NAT モードに移行するには [Yes] をクリックします。それ以外の場合は [No] をクリックします。[IVR Zone Wizard] ダイアログボックスが表示されます。

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。

図 1-3 は、[Select End Devices] ダイアログボックスを示しています。

図 1-3 [Select End Devices] ダイアログボックス



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的なドメイン ID が設定されていない場合は、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 モードで Fabric Manager がイネーブルになることをスイッチで確認します。

- 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、Fabric Manager 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 Fabric Manager 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 IVR 設定](#)」(P.1-6) 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.1-8) を参照してください。



(注) 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すると、関連するすべての設定が自動的に廃棄されます。

CFS を使用した IVR 設定の配信

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



(注)

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。

ここで説明する内容は、次のとおりです。

- 「データベースの実装」(P.1-9)
- 「ファブリックのロック」(P.1-9)
- 「変更のコミット」(P.1-9)
- 「変更の破棄」(P.1-9)
- 「ロック済みセッションのクリア」(P.1-9)

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。ファブリックは、この期間中、ロック状態を保持します。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

データベースの変更を開始すると、保留データベースが作成され、VSAN 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。

- 他のユーザは、この機能の設定を変更できなくなります。
- 設定データベースのコピーは、最初のアクティブな変更によって、保留データベースになります。

変更のコミット

アクティブ データベースに対して行った変更をコミットすると、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。コミットが正常に実行されると、ファブリック全体に設定の変更が適用され、ロックが解除されます。

変更の破棄

保留データベースへの変更を破棄 (abort) すると、設定データベースは影響されずに保持され、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。管理者がこの作業を行うと、保留データベースに対する変更は廃棄され、ファブリックのロックは解除されます。



ヒント

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 モードについて

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。



(注)

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。



ヒント

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。



(注)

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。

IVR NAT の要件とガイドライン

IVR NAT を使用する場合は要件とガイドラインを以下に示します。

- 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 Fabric Manager Server 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 Fabric Manager 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 1-2 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 1-2 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 |
| 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 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 モードの自動検出をイネーブルにする方法に関する手順について説明します。



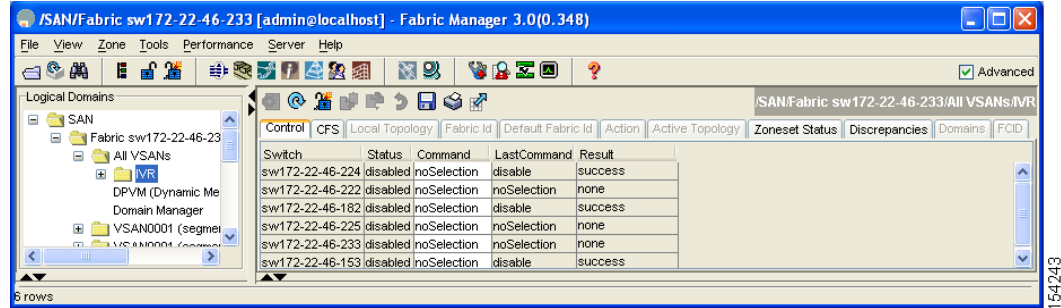
(注)

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ておく必要があります (「CFS を使用した IVR 設定の配信」(P.1-8) 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。

Fabric Manager を使用して 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] を展開してから、[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 (図 1-4 を参照)。

図 1-4 IVR ルーティング設定の [Control] タブ



- 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、ファブリック内のすべてのスイッチにこの変更を配信します。
- 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て、スイッチ上で IVR をイネーブルにします。

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 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。



(注)

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。



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 fcdomain データベースの消去

Fabric Manager を使用して 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] を展開してから、[IVR] を選択します。
[Information] ペインに IVR 設定が表示されます。

図 1-5 [Domains] タブ

| Action | RDI VSANs | Active Topology | Zoneset Status | Discrepancies | Domains | FCI |
|--------|--|-----------------|----------------|---------------|-----------|-----|
| Master | Current Fabric, VSAN Ids & Native Fabric, VSAN Ids | | | | Domain Id | 5 |

- 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（図 1-5 を参照）。
- 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 ゾーンと IVR ゾーンセット

ここでは、IVR ゾーンと IVR ゾーンセットの設定方法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」 (P.1-14)
- 「IVR ゾーンの制限とイメージダウングレードに関する注意事項」 (P.1-15)
- 「IVR ゾーンの自動作成」 (P.1-15)
- 「IVR ゾーンと IVR ゾーンセットの設定」 (P.1-16)
- 「ゾーンセットのアクティベーションと force オプションの使用方法について」 (P.1-19)
- 「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 フルゾーンデータベースの回復」 (P.1-22)
- 「IVR トポロジの回復」 (P.1-23)

IVR ゾーンについて

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 1-3 は、IVR ゾーンとゾーンの主な違いをまとめたものです。

表 1-3 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 ゾーンの制限とイメージダウングレードに関する注意事項

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 マージに関するガイドライン」(P.1-24) を参照してください。



注意

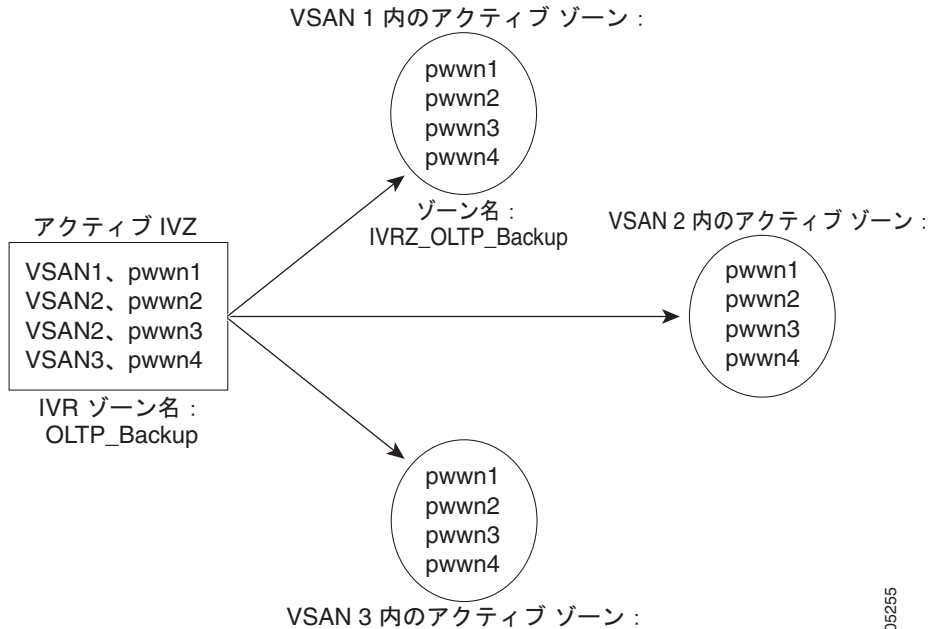
Cisco SAN-OS Release 3.0(3) よりも前のリリースにダウングレードする場合は、IVR ゾーン数を 2,000 以下に、IVR ゾーンメンバーを 10,000 以下にする必要があります。

IVR ゾーンの自動作成

図 1-6 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 1-6 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 マージに関するガイドライン](#)」(P.1-24) を参照してください。

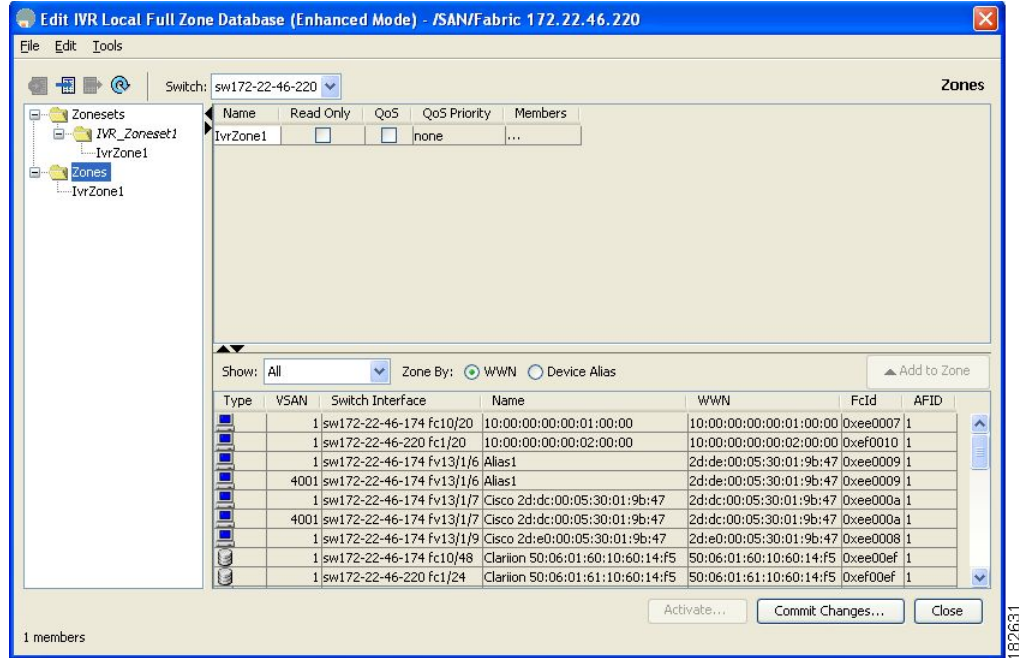
IVR ゾーンと IVR ゾーンセットの設定

Fabric Manager を使用して 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 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(図 1-7 を参照)。

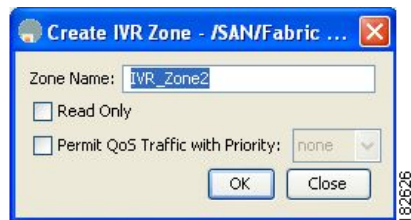
図 1-7 [Edit IVR Local Full Zone Database] ダイアログボックス



ゾーンメンバ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。

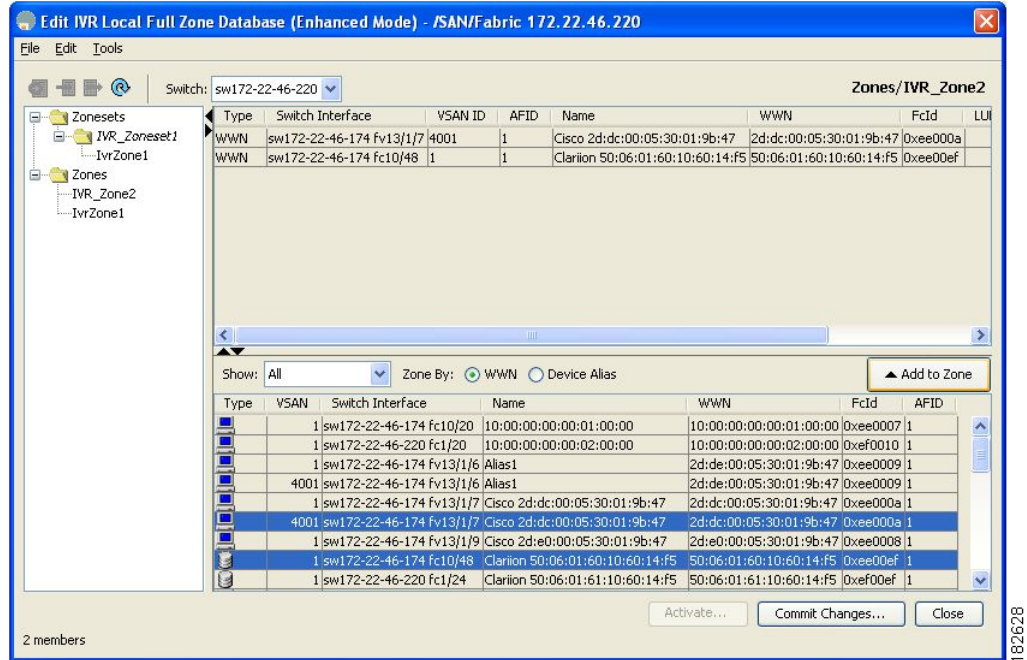
- ステップ 2** 左側のペインで [Zones] をクリックし、[Insert] アイコンをクリックしてゾーンを作成します。[Create IVR] ダイアログボックスが表示されます（図 1-8 を参照）。

図 1-8 [Create IVR Zone] ダイアログボックス



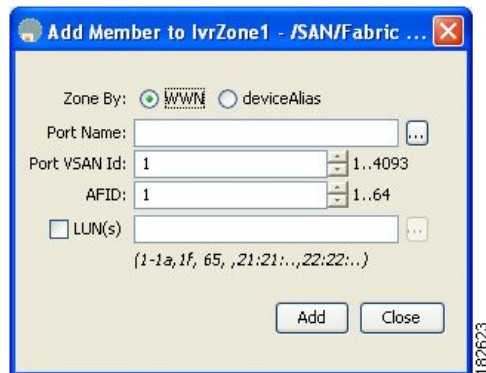
- ステップ 3** IVR ゾーン名を入力します。
- ステップ 4** 次のチェックボックスのうち 1 つをオンにします。
- [Read Only] : このゾーンでは読み込みが許可され、書き込みが拒否されます。
 - [Permit QoS traffic with Priority] : ドロップダウンメニューでプライオリティを設定します。
- ステップ 5** [OK] をクリックして IVR ゾーンを作成します。
- ステップ 6** このゾーンにメンバーを追加するには、[Fabric] ペインから追加するメンバーを選択して（図 1-9 を参照）、[Add to Zone] をクリックします。

図 1-9 [Edit IVR Local Full Zone Database] ダイアログボックス



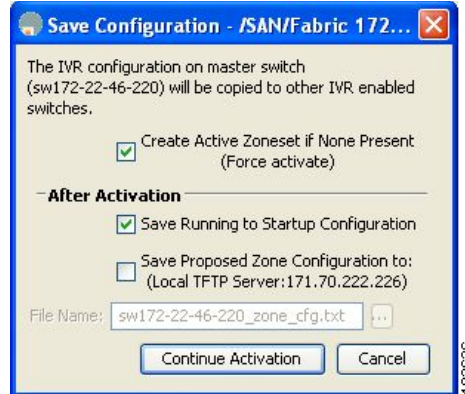
ステップ 7 または、メンバーを追加するゾーンをクリックして、[Insert] アイコンをクリックします。
[Add Member to Zone] ダイアログボックスが表示されます (図 1-10 を参照)。

図 1-10 [Add Member to IVR Zone] ダイアログボックス



ステップ 8 ゾーンセットを追加したら、その新しいゾーンセットを選択して、[Activate] をクリックします。
[FICON Port Configuration] ダイアログボックスが表示されます (図 1-11 を参照)。

図 1-11 [Save Configuration] ダイアログボックス



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、プレフィックスの IVRZ で始まるゾーン名と [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。プレフィックスが 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、自動的にプレフィックスの 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 ゾーンを表示/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 Fabric Manager Fundamentals Configuration Guide*』を参照してください。



(注) プレフィックスが IVRZ のゾーンまたは [nozoneset] 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。

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。

ゾーンセットのアクティベーションと force オプションの使用方法について

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。

force activate 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もできます。表 1-5 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 1-5 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 | いいえ | エラー | いいえ | いいえ |
| 2 | | | はい | 成功 | はい | いいえ |
| 3 ¹ | Deny | アクティブゾーンセットが存在する | いいえ/ はい | 成功 | はい | いいえ |
| 4 | Permit | アクティブゾーンセットが存在しない | いいえ | エラー | いいえ | いいえ |
| 5 | | | はい | 成功 | はい | はい |
| | | または アクティブゾーンセットが存在する | | | | |

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。ゾーンは IVR ゾーンに対応するエッジ VSAN 上に作成されるため、デフォルトゾーンポリシーが permit のエッジ 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



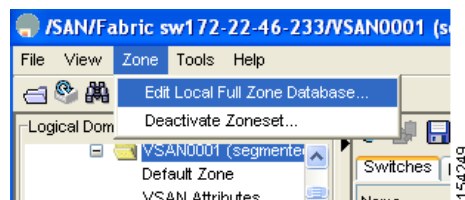
(注)

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。

Fabric Manager を使用して既存の 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。

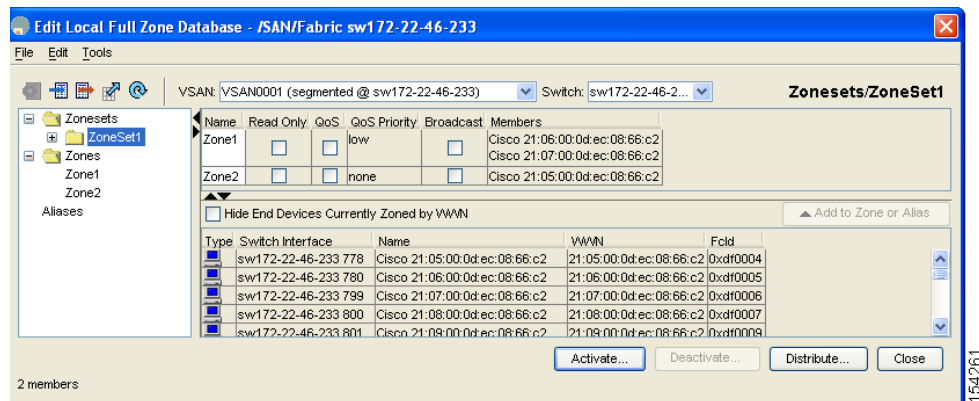
ステップ 1 [Zone] をクリックして、[Edit Local Full Zone Database] を選択します (図 1-12 を参照)。

図 1-12 [Zone] メニュー



[Edit Local Full Zone Database] ダイアログボックスが表示されます (図 1-13 を参照)。

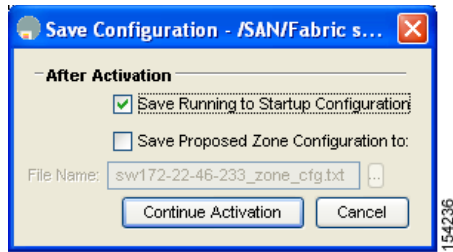
図 1-13 [Edit Local Full Zone Database] ダイアログボックス



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 (図 1-13 を参照)、[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。

[FICON Port Configuration] ダイアログボックスが表示されます (図 1-14 を参照)。

図 1-14 新しいゾーンセット用の設定保存オプション



- ステップ 3** オプションで、[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 (図 1-14 を参照)。
- 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 (図 1-14 を参照)。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。

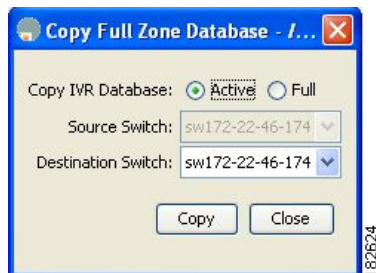
IVR フル ゾーン データベースの回復

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。

Fabric Manager を使用して 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 (図 1-15 を参照)。

図 1-15 [Copy Full Zone Database] ダイアログボックス



- 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

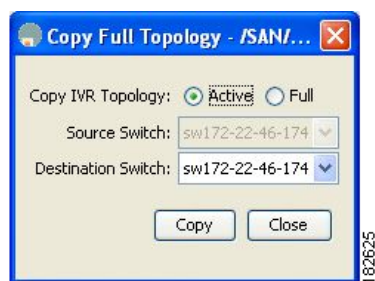
トポロジを回復するには、アクティブ ゾーン データベースまたはフル ゾーン データベースをコピーします。

Fabric Manager を使用してゾーン 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 (図 1-16 を参照)。

図 1-16 [Copy Full Topology] ダイアログボックス



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。

IVR ロギング

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。

- 「IVR ロギング重大度の設定」(P.1-23)

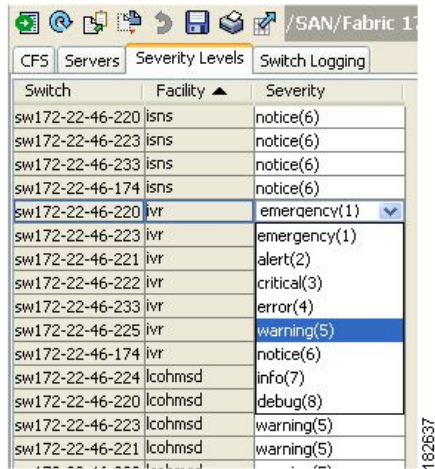
IVR ロギング重大度の設定

Fabric Manager を使用して IVR 機能によるロギング 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。

■ データベース マージに関するガイドライン

- ステップ 1** [Switches] > [Events] を展開して、[Physical Attributes] ペインで [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て、ファシリティ名で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 (図 1-17 を参照)。

図 1-17 [Syslog Severity] ドロップダウン メニュー



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 Fabric Manager 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。

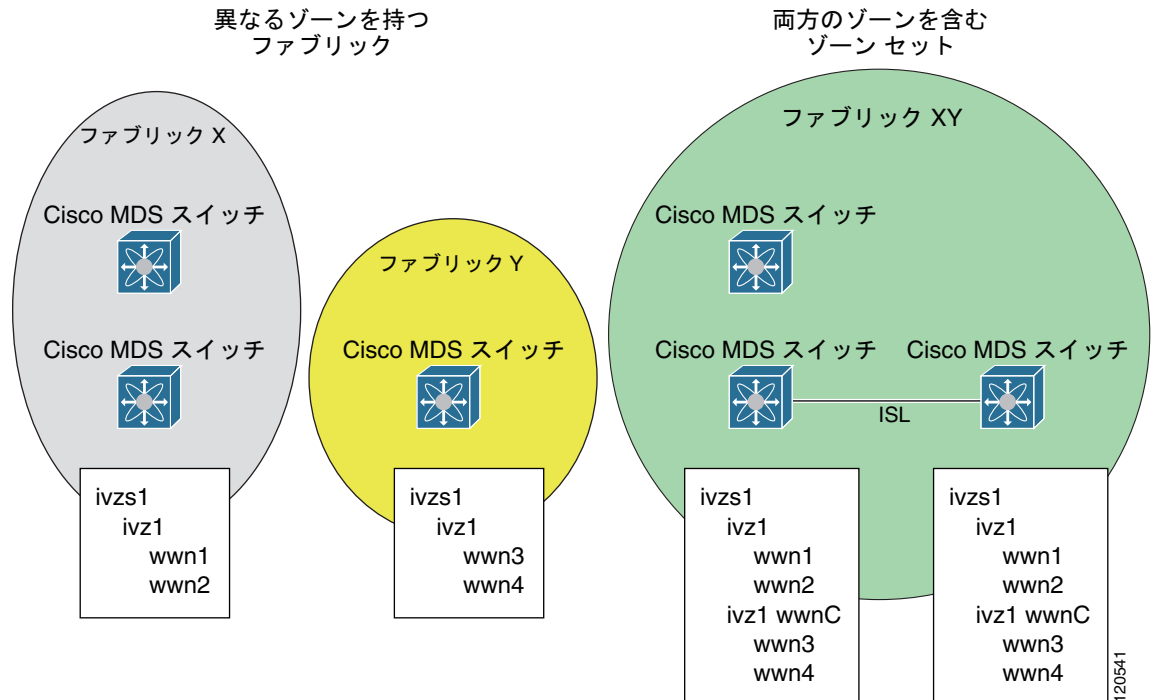
データベース マージに関するガイドライン

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『Cisco Fabric Manager System Management Configuration Guide』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、次の内容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前で配信ゾーン セットにコピーされます (図 1-18 を参照)。

図 1-18 ファブリック マージの結果



- Cisco MDS スイッチごとに IVR 設定を変更することができます。
- 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もゾーン 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 1-6 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 1-6 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。次の配信で、データベースとファブリック内のアクティベーション状態が強制的に同期化されます。

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.1-8) と「[Autonomous Fabric ID](#)」(P.2-4) 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.1-8) と「[Autonomous Fabric ID](#)」(P.2-4) 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。

デフォルト設定

表 1-7 に、IVR パラメータのデフォルト設定を示します。

表 1-7 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 |

