CHAPTER 4

# iSCSI の設定

Cisco MDS 9000 ファミリの IP Storage（IPS; IP ストレージ）サービスは、オープン規格の IP ベース テクノロジーを使用して、ファイバ チャネル Storage Area Network（SAN; ストレージ エリア ネットワーク）の到達距離を延長します。このスイッチを使用すると、iSCSI プロトコルを使用して IP ホストからファイバ チャネル ストレージにアクセスできます。

（注） iSCSI 機能は、IPS モジュールに特有の機能であり、Cisco MDS 9200 スイッチまたは Cisco MDS 9500 ディレクタで使用できます。

Cisco MDS 9216i スイッチと 14/2 Multiprotocol Services（MPS-14/2）モジュールを使用すると、ファイバ チャネル、FCIP、および iSCSI の機能も利用できます。MPS-14/2 モジュールは、Cisco MDS 9200 シリーズまたは Cisco MDS 9500 シリーズのどのスイッチでも使用できます。

（注） ギガビット イーサネット インターフェイスの設定については、「IPv4 の基本的なギガビット イーサネットの設定」（P.7-2）を参照してください。

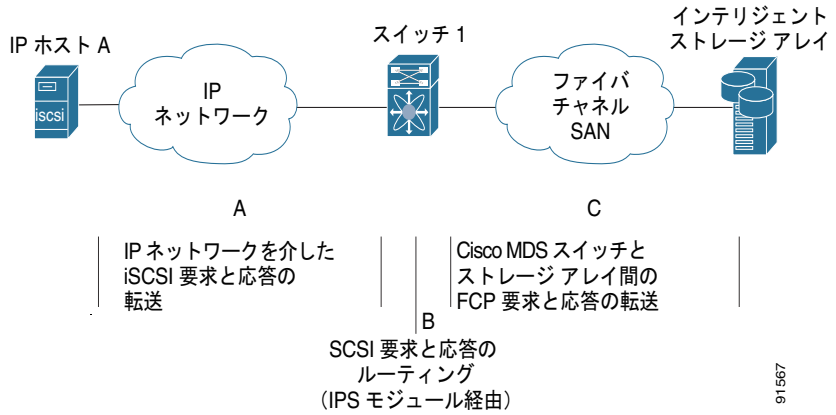
この章の内容は、次のとおりです。

# iSCSI の概要

（注）　iSCSI 機能は、Cisco Fabric Switch for HP c-Class Bladesystem 上および Cisco Fabric Switch for IBM BladeCenter 上ではサポートされていません。

iSCSI 機能は、IP ネットワークでの iSCSI ホスト間の iSCSI 要求と応答のルーティングと、Cisco MDS 9000 ファミリのスイッチのファイバ チャネル インターフェイスからアクセス可能なファイバ チャネル SAN 内のファイバ チャネル ストレージ デバイスで構成されます（図 4-1 を参照）。

**図 4-1　透過的な iSCSI ルーティングのための iSCSI 要求と応答の転送**

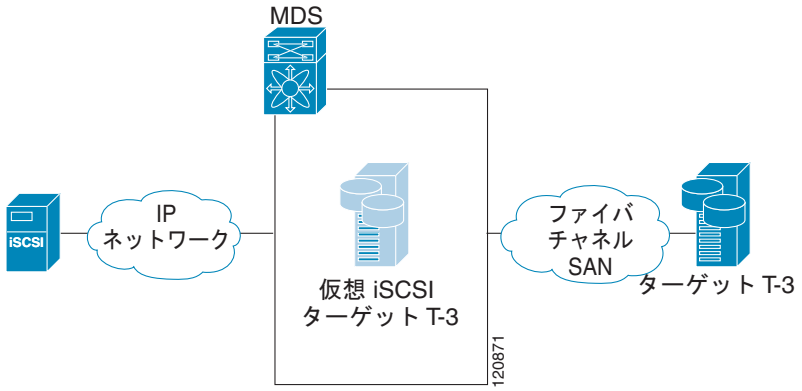



IPS モジュールまたは MPS-14/2 モジュールを介してストレージにアクセスする必要のある iSCSI ホストそれぞれに、互換性のある iSCSI ドライバがインストールされている必要があります（Cisco.com Web サイトの http://www.cisco.com/cgi-bin/tablebuild.pl/sn5420-scsi では、互換ドライバの一覧を確認できます）。iSCSI プロトコルを使用して、iSCSI ドライバは、iSCSI ホストからの SCSI の要求と応答を IP ネットワークを介して 転送できます。ホストのオペレーティング システムの観点から、iSCSI ドライバは、ホスト内にファイバ チャネル ドライバに似た SCSI 転送ドライバであるように見えます。

IPS モジュールまたは MPS-14/2 モジュールにより、透過的な SCSI ルーティングが提供されます。iSCSI プロトコルを使用する IP ホストは、ファイバ チャネル ネットワーク上のターゲットに透過的にアクセスできます。図 4-1 に、IP ネットワークを介して IPS モジュールまたは MPS-14/2 モジュールに接続した iSCSI ホストがファイバ チャネル SAN 上のファイバ チャネル ストレージにアクセスする場合の一般的な設定例を示します。

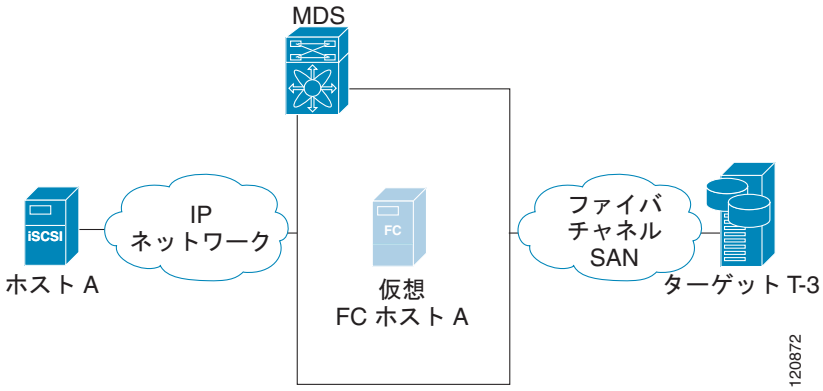
IPS モジュールまたは MPS-14/2 モジュールは、iSCSI SAN ビューとファイバ チャネル SAN ビューを別々に作成します。iSCSI SAN ビューの場合、IPS モジュールまたは MPS-14/2 モジュールは、iSCSI 仮想ターゲットを作成してから、それをファイバ チャネル SAN で使用可能な物理ファイバ チャネル ターゲットにマッピングします。物理 iSCSI ターゲットが IP ネットワークに接続されているかのように、IP ホストに対してファイバ チャネル ターゲットを示します（図 4-2 を参照）。

**図 4-2　iSCSI SAN ビュー：iSCSI 仮想ターゲット**



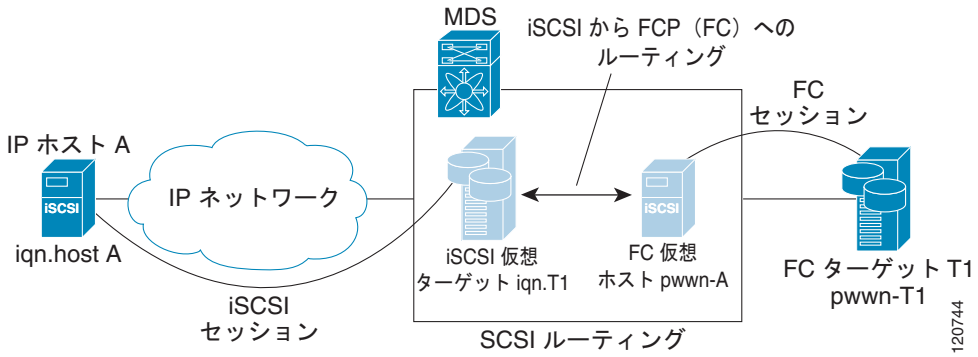

ファイバ チャネル SAN ビューの場合、IPS モジュールまたは MPS-14/2 モジュールは、iSCSI ホストを仮想ファイバ チャネル ホストとして示します。ストレージ デバイスは、実際のファイバ チャネル ホストと行う通信と同じように、仮想ファイバ チャネル ホストと通信します（図 4-3 を参照）。

**図 4-3　ファイバ チャネル SAN ビュー：HBA としての iSCSI ホスト**




IPS モジュールまたは MPS-14/2 モジュールは、iSCSI 仮想ターゲットと仮想ファイバ チャネル ホスト間のコマンドを透過的に対応付けます（図 4-4 を参照）。

**図 4-4　iSCSI から FCP（ファイバ チャネル）へのルーティング**



IP ホストからファイバ チャネル ストレージ デバイスへの SCSI のルーティングは、次の主要な処理で構成されます。

- iSCSI の要求と応答は、ホストと IPS モジュールまたは MPS-14/2 モジュールの間を IP ネットワークを介して転送されます。
- SCSI の要求と応答が、IP ネットワーク上のホストとファイバ チャネル ストレージ デバイスの間でルーティングされます（iSCSI から FCP に変換されます。この逆も同様です）。IPS モジュールまたは MPS-14/2 モジュールは、このような変換とルーティングを実行します。
- FCP の要求または応答は、IPS モジュールまたは MPS-14/2 モジュールとファイバ チャネル ストレージ デバイスの間で転送されます。

（注）　FCP（ファイバ チャネルから見た場合 iSCSI に相当する）は、ファイバ チャネル SAN を介して SCSI コマンドを渡します。
iSCSI プロトコルの詳細については、http://www.ietf.org で IP ストレージの IETF 標準を参照してください。

# iSCSI 設定制限の概要

iSCSI 設定には次の制限があります。

- 1 つのファブリック内でサポートされる iSCSI イニシエータおよび iSLB イニシエータの最大数は 2000 です。
- サポートされる iSCSI イニシエータおよび iSLB イニシエータの最大数は、ポートあたり 200 です。
- トランスペアレント イニシエータ モードまたはプロキシ イニシエータ モードの IPS ポートでサポートされる iSCSI セッションおよび iSLB セッションの最大数は 500 です。
- スイッチでサポートされる iSCSI セッションおよび iSLB セッションの最大数は 5000 です。
- 1 つのファブリック内でサポートされる iSCSI ターゲットおよび iSLB ターゲットの最大数は 6000 です。

# iSCSI の設定

ここでは、Cisco MDS 9000 ファミリのスイッチで iSCSI を設定する方法について説明します。

ここで説明する内容は、次のとおりです。

# iSCSI のイネーブル化

iSCSI の機能を使用するには、ファブリック内の必要なスイッチで iSCSI を明示的にイネーブルにする必要があります。別の方法として Fabric Manager または Device Manager を使用しても、必要なモジュールで直接 iSCSI の機能をイネーブルまたはディセーブルにできます。デフォルトでは、Cisco MDS 9000 ファミリの全スイッチでこの機能がディセーブルに設定されています。

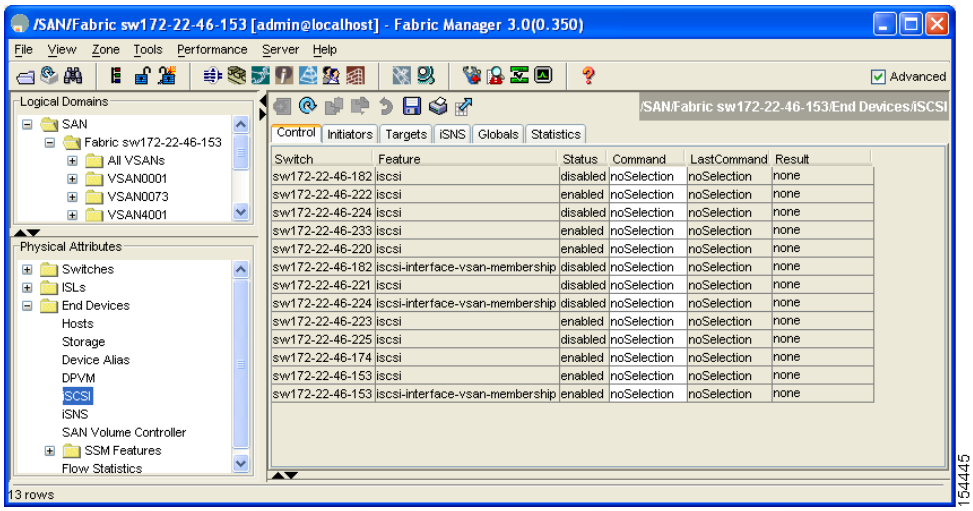
**注意**　この機能をディセーブルにすると、関連するすべての設定が自動的に廃棄されます。

Fabric Manager を使用して任意のスイッチで iSCSI をイネーブルにする手順は、次のとおりです。

**ステップ 1**　[Physical Attributes] ペインで [End Devices] > [iSCSI] を選択します。

[Information] ペインに iSCSI テーブルが表示されます（図 4-5 を参照）。

**図 4-5　Fabric Manager の iSCSI テーブル**




[Control] タブがデフォルトのタブです。ファブリック内の IPS ポートを持つすべてのスイッチについて、iSCSI のイネーブルの状態が表示されます。

**ステップ 2**　iSCSI をイネーブルにする各スイッチの [Command] 列で [enable] を選択します。

**ステップ 3**　[Apply Changes] アイコンをクリックして、これらの変更を保存します。

Fabric Manager を使用してモジュールで iSCSI をイネーブルにする手順は、次のとおりです。

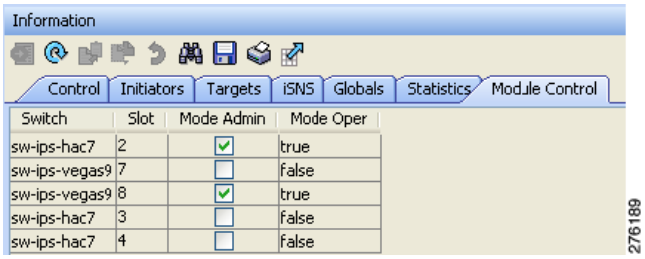
**ステップ 1**　[Physical Attributes] ペインで [End Devices] > [iSCSI] を選択します。

[Information] ペインに iSCSI テーブルが表示されます。

**ステップ 2**　[Module Control] タブをクリックします。

[Information] ペインに [Module Control] ダイアログボックスが表示されます（図 4-6 を参照）。

図 4-6　[Module Control] ダイアログボックス




**ステップ 3**　[Mode Admin] チェックボックスをオンにすると、選択したモジュールの特定のポートに対して iSCSI がイネーブルになります。

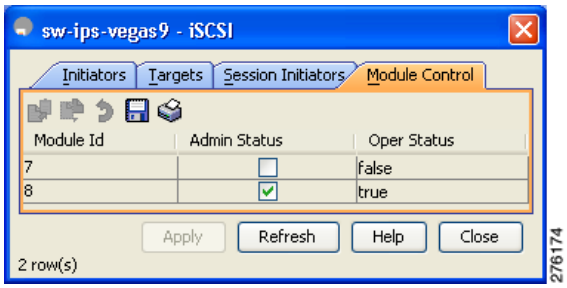
**ステップ 4**　[Apply Changes] アイコンをクリックして、これらの変更を保存します。

Device Manager を使用してモジュールで iSCSI をイネーブルにする手順は、次のとおりです。

**ステップ 1**　[IP] > [iSCSI] を選択します。

iSCSI テーブルが表示されます（図 4-7 を参照）。

図 4-7　iSCSI テーブル




**ステップ 2**　[Admin Status] チェックボックスをオンにすると、選択したモジュールの指定ポートに対して iSCSI がイネーブルになります。

**ステップ 3**　[Apply] をクリックして、これらの変更を保存します。

# iSCSI インターフェイスの作成

IPS モジュールまたは MPS-14/2 モジュールの各物理ギガビット イーサネット インターフェイスを使用して、iSCSI 要求を変換してファイバ チャネル ターゲットにルーティングし、これと反対の方向に応答を返します。この機能をイネーブルにするには、対応する iSCSI インターフェイスがイネーブルの状態になっている必要があります。

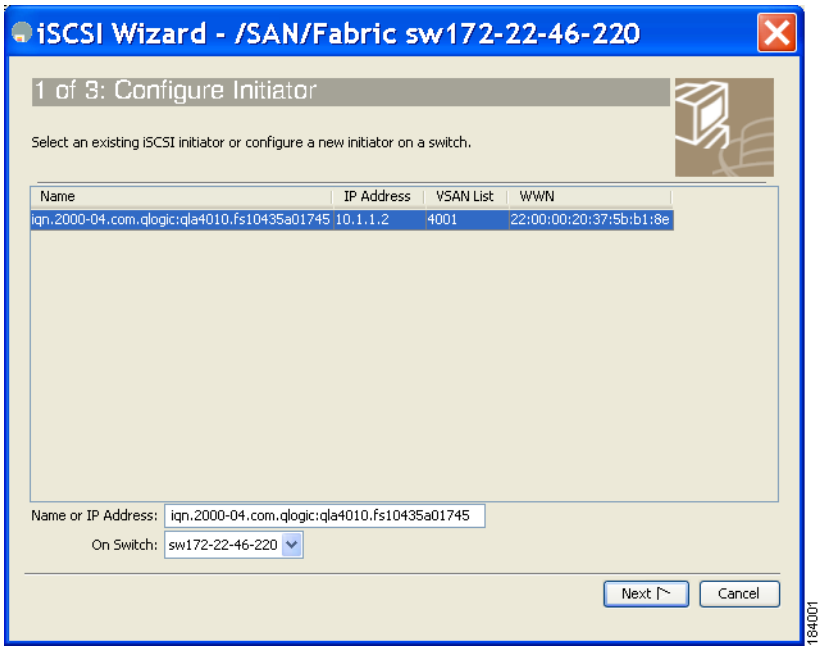
# iSCSI ウィザードの使用

Fabric Manager の iSCSI ウィザードを使用する手順は、次のとおりです。

**ステップ 1**　[iSCSI Setup Wizard] アイコンをクリックします。

iSCSI ウィザードの [Configure Initiator] ダイアログボックスが表示されます（図 4-8 を参照）。

**図 4-8　iSCSI ウィザードの [Configure Initiator] ダイアログボックス**

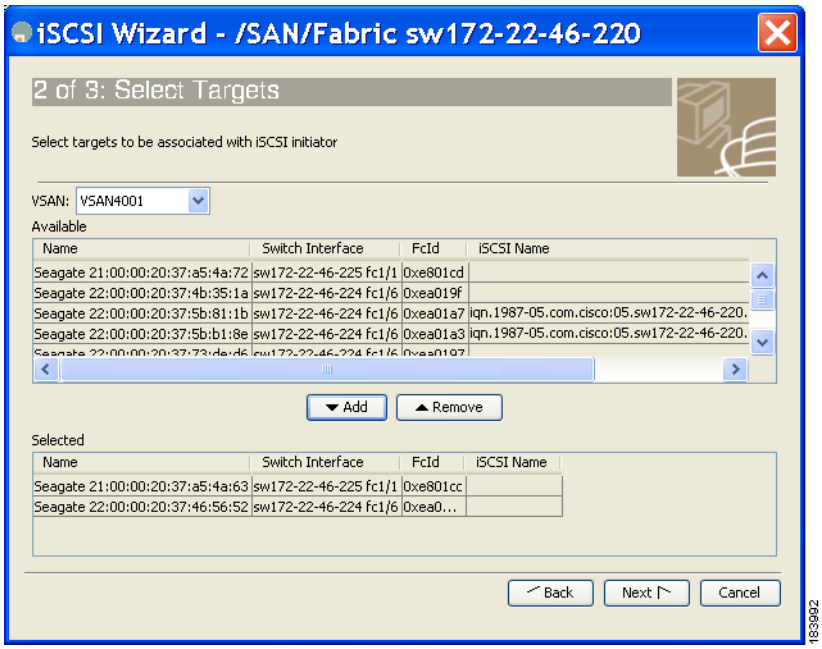



**ステップ 2**　既存の iSCSI イニシエータを選択するか、新規 iSCSI イニシエータの iSCSI ノード名または IP アドレスを追加します。

**ステップ 3**　新規 iSCSI イニシエータを追加する場合は、この iSCSI イニシエータに使用するスイッチを選択して、[Next] をクリックします。

iSCSI ウィザードの [Select Targets] ダイアログボックスが表示されます（図 4-9 を参照）。

図 4-9　iSCSI ウィザードの [Select Targets] ダイアログボックス

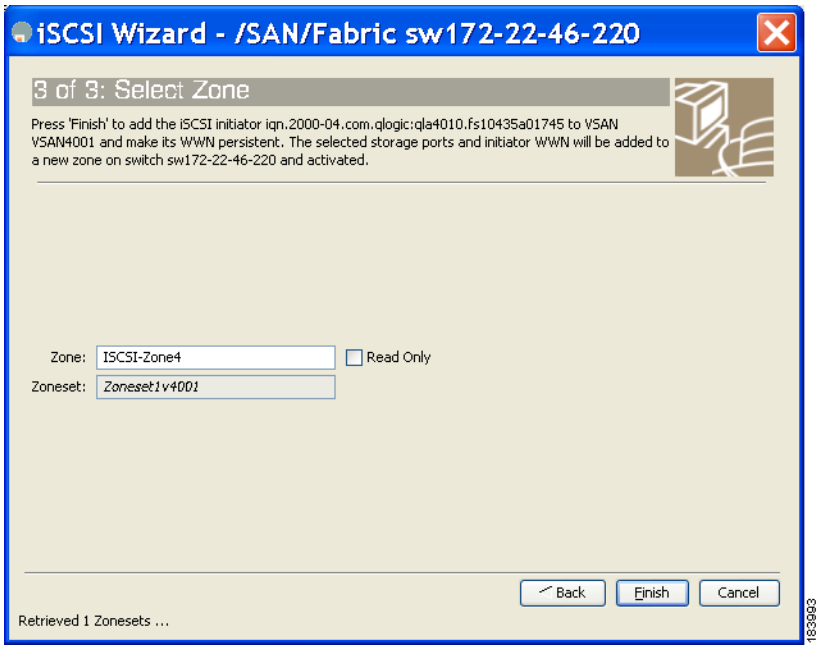



**ステップ 4**　この iSCSI イニシエータに関連付ける VSAN およびターゲットを選択して、[Next] をクリックします。

**（注）**　iSCSI ウィザードにより、FC ターゲットを動的にインポートする機能が有効になります。

iSCSI ウィザードの [Select Zone] ダイアログボックスが表示されます（図 4-10 を参照）。

図 4-10　iSCSI ウィザードの [Select Zone] ダイアログボックス




**ステップ 5**　この新しい iSCSI ゾーンにゾーン名を設定し、必要に応じて [Read Only] チェックボックスをオンにします。

**ステップ 6**　[Finish] をクリックして、この iSCSI イニシエータを作成します。

作成されると、ターゲット VSAN が iSCSI ホストの VSAN リストに追加されます。

**（注）**　iSCSI ウィザードにより、FC ターゲットを動的にインポートする機能が自動的に有効になります。

# iSCSI ターゲットとしてのファイバ チャネル ターゲットの提示

IPS モジュールまたは MPS-14/2 モジュールが物理ファイバ チャネル ターゲットを iSCSI 仮想ターゲットとして示すことで、iSCSI ホストはそれにアクセスできるようになります。このモジュールは、これらのターゲットを次の 2 つのうちいずれかの方法で示します。

- ダイナミック マッピング：すべてのファイバ チャネル ターゲット デバイス/ポートを iSCSI デバイスとして自動的にマッピングします。このマッピングを使用すると、自動的に iSCSI ターゲット名を作成します。
- スタティック マッピング：iSCSI ターゲット デバイスを手動で作成し、それをファイバ チャネル ターゲット ポート全体、またはファイバ チャネルの Logical Unit Number（LUN）のサブセットにマッピングします。このマッピングを使用する場合は、固有の iSCSI ターゲット名を指定する必要があります。

iSCSI ホストをファイバ チャネル ターゲットの LU のサブセットに制限すべき場合、iSCSI アクセス コントロールを必要とする場合（「iSCSI アクセス コントロール」（P.4-26）を参照）、またはどちらの条件もあてはまる場合は、スタティック マッピングを使用する必要があります。また、スタティック マッピングを使用すると、冗長ファイバ チャネル ポートがファイバ チャネル ターゲットの LU に到達可能な場合、透過的なフェールオーバーを設定できます（「透過的なターゲット フェールオーバー」（P.4-54）を参照）。

（注）　IPS モジュールまたは MPS-14/2 モジュールは、デフォルトではファイバ チャネル ターゲットを iSCSI にインポートしません。IPS モジュールまたは MPS-14/2 モジュールで iSCSI イニシエータが使用可能なファイバ チャネル ターゲットを作成する前に、ダイナミック マッピングまたはスタティック マッピングのいずれかを設定する必要があります。

## ダイナミック マッピング

ダイナミック マッピングを設定する場合、IPS モジュールまたは MPS-14/2 モジュールは、すべてのファイバ チャネル ターゲットを iSCSI ドメインにインポートして、物理ファイバ チャネル ターゲット ポートをそれぞれ 1 つの iSCSI ターゲットとしてマッピングします。つまり、物理ストレージ ターゲット ポートを使用してアクセス可能なすべての LU を、物理ファイバ チャネル ターゲット ポート内と同じ LU Number（LUN）を用いて iSCSI LU として使用できます。

iSCSI ターゲット ノード名は、iSCSI Qualified Name（IQN; iSCSI 修飾名）フォーマットを使用して自動的に作成されます。iSCSI 修飾名には、名前の長さを最大 223 文字、最小 16 文字の英数字とする制約があります。

SAN 内では固有の名前になる必要があるため、IPS モジュールまたは MPS-14/2 モジュールは、次の表記法を使用して IQN フォーマットに基づいた iSCSI ターゲット ノード名を作成します。

- Virtual Router Redundancy Protocol（VRRP; 仮想ルータ冗長プロトコル）グループまたは PortChannel に属していない IPS ギガビット イーサネット ポートは、次のフォーマットを使用します。

  `iqn.1987-05.com.cisco:05.<mgmt-ip-address>.<slot#>-<port#>-<sub-intf#>.<Target-pWWN>`

- VRRP グループに属している IPS ポートは、次のフォーマットを使用します。

  `iqn.1987-05.com.cisco:05.vrrp-<vrrp-ID#>-<vrrp-IP-addr>.<Target-pWWN>`

- PortChannel に属しているポートは、次のフォーマットを使用します。

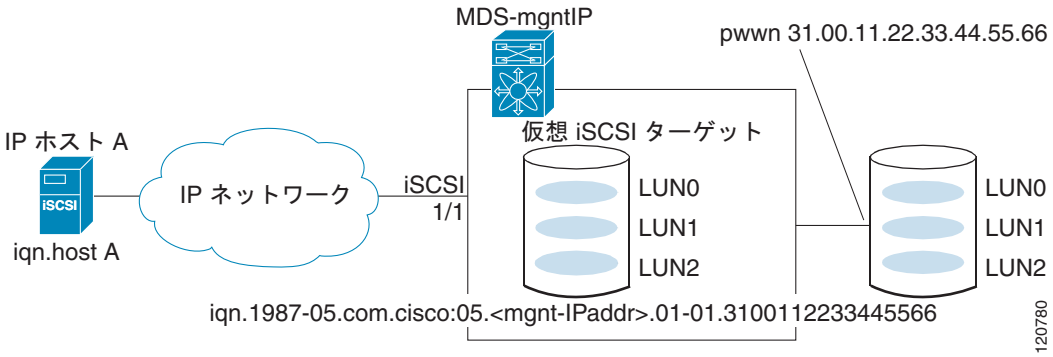
  `iqn.1987-02.com.cisco:02.<mgmt-ip-address>.pc-<port-ch-sub-intf#>.<Target-pWWN>`

（注）　スイッチ名を設定している場合は、管理 IP アドレスの代わりにスイッチ名を使用します。スイッチ名を設定していない場合は、管理 IP アドレスを使用します。

この表記法を使用して、Cisco MDS 9000 ファミリのスイッチの IPS ポートはそれぞれ、SAN 内で同一のファイバ チャネル ターゲット ポートに対する固有の iSCSI ターゲット ノード名を作成します。

たとえば、pWWN 31:00:11:22:33:44:55:66 のファイバ チャネル ターゲット ポートに対して iSCSI ターゲットを作成した場合で、その pWWN に LUN 0、LUN 1、および LUN 2 が含まれるとき、IP ホストは iSCSI ターゲット ノード名 iqn.1987-05.com.cisco:05.*MDS_switch_management_IP_address*.01-01.3100112233445566 を使用して、これらの LUN を使用できるようになります（図 4-11 を参照）。

図 4-11　ダイナミック ターゲット マッピング



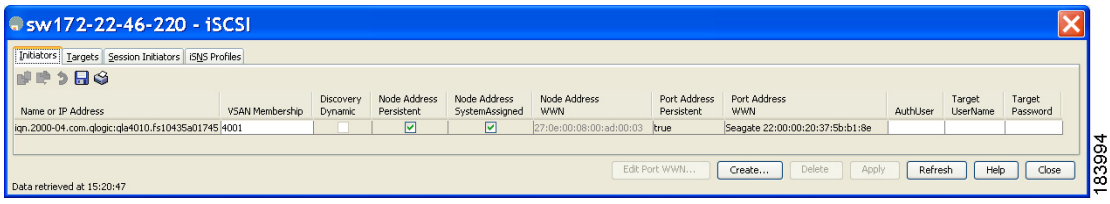

（注）　設定されているアクセス コントロールのメカニズムによっては、各 iSCSI イニシエータがアクセスできるターゲットがすべてのターゲットではない場合もあります（「iSCSI アクセス コントロール」（P.4-26）を参照）。

Device Manager を使用してファイバ チャネル ターゲットの iSCSI へのダイナミック マッピングをイネーブルにする手順は、次のとおりです。

**ステップ 1**　[IP] > [iSCSI] を選択します。

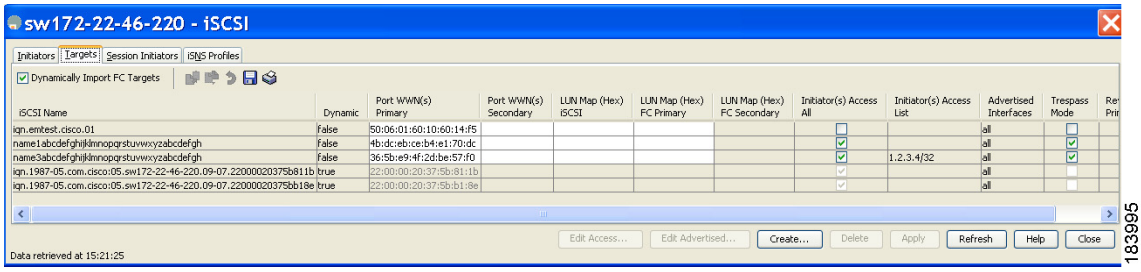
iSCSI 設定が表示されます（図 4-12 を参照）。

図 4-12　Device Manager での iSCSI 設定




**ステップ 2**　[Targets] タブをクリックして、既存の iSCSI ターゲットのリストを表示します（図 4-13 を参照）。

図 4-13　iSCSI の [Targets] タブ



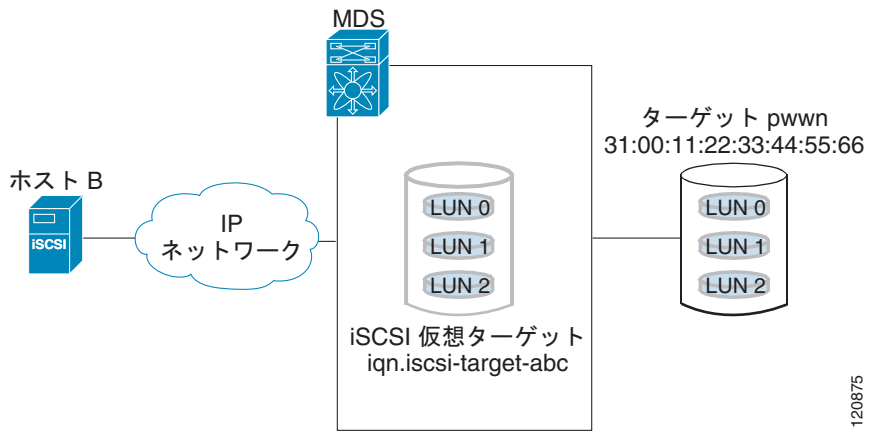
**ステップ 3**　[Dynamically Import FC Targets] チェックボックスをオンにします。

**ステップ 4**　[Apply] をクリックして、この変更を保存します。

## スタティック マッピング

ユーザ定義の固有の iSCSI ノード名を割り当てることで iSCSI ターゲットを手動で（静的に）作成できます。iSCSI 修飾名の長さには、最小 16 文字、最大 223 文字の制約があります。スタティック マッピングされた iSCSI ターゲットは、ファイバ チャネル ターゲット ポート全体（iSCSI ターゲットにマッピングされたターゲット ポートのすべての LUN）をマッピングすることも、ファイバ チャネル ターゲット ポートから 1 つ以上の LU を含めることもできます（図 4-14 を参照）。

**図 4-14　スタティック マッピングされた iSCSI ターゲット**




Device Manager を使用してファイバ チャネル ターゲット ポート全体に対してスタティック iSCSI 仮想ターゲットを作成する手順は、次のとおりです。

**ステップ 1**　[IP] > [iSCSI] をクリックします。

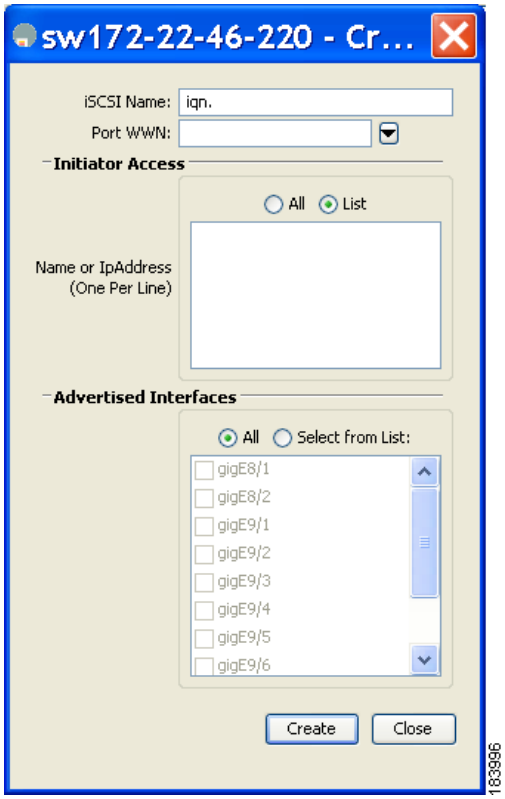
iSCSI 設定が表示されます（図 4-12 を参照）。

**ステップ 2**　[Targets] タブをクリックして、既存の iSCSI ターゲットのリストを表示します（図 4-13 を参照）。

**ステップ 3**　[Create] をクリックして iSCSI ターゲットを作成します。

[Create iSCSI Targets] ダイアログボックスが表示されます（図 4-15 を参照）。

図 4-15　[Create iSCSI Targets] ダイアログボックス




**ステップ 4**　[iSCSI Name] フィールドに iSCSI ターゲット ノード名を IQN フォーマットで設定します。

**ステップ 5**　[Port WWN] フィールドにマッピングするファイバ チャネル ターゲット ポートを設定します。

**ステップ 6**　[Select from List] オプション ボタンをクリックして、この仮想 iSCSI ターゲットをアクセスさせる iSCSI イニシエータ ノード名または IP アドレスを設定するか、または、[All] オプション ボタンをクリックして、この仮想 iSCSI ターゲットをすべての iSCSI イニシエータにアクセスさせるようにします。「iSCSI アクセス コントロール」（P.4-26）も参照してください。

**ステップ 7**　[Select from List] オプション ボタンをクリックして、iSCSI ターゲットをアドバタイズするインターフェイスをそれぞれ選択するか、[All] オプション ボタンをクリックして、すべてのインターフェイスをアドバタイズします。

**ステップ 8**　[Apply] をクリックして、この変更を保存します。

**ヒント**　iSCSI ターゲットに複数のファイバ チャネル ターゲット ポートを含めることはできません。すでにファイバ チャネル ターゲット ポート全体をマッピングしている場合は、LUN マッピング オプションを使用できません。

**（注）**　スタティック マッピングされたターゲットへのアクセスの制御については、「iSCSI ベースのアクセス コントロール」（P.4-28）を参照してください。

### スタティック iSCSI ターゲットのアドバタイジング

スタティック iSCSI ターゲットをアドバタイズするギガビット イーサネット インターフェイスを制限できます。iSCSI ターゲットは、デフォルトで、すべてのギガビット イーサネット インターフェイス、サブインターフェイス、PortChannel インターフェイス、および PortChannel サブインターフェイスでアドバタイズされます。

Device Manager を使用して iSCSI 仮想ターゲットをアドバタイズする必要のある特定のインターフェイスを設定する手順は、次のとおりです。

**ステップ 1**　[IP] > [iSCSI] を選択します。

iSCSI 設定が表示されます（図 4-12 を参照）。

**ステップ 2**　[Targets] タブをクリックして、既存の iSCSI ターゲットのリストを表示します（図 4-13 を参照）。

**ステップ 3**　修正する iSCSI ターゲットを右クリックして [Edit Advertised] をクリックします。

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

**ステップ 4**　（任意）削除するインターフェイスを右クリックして [Delete] をクリックします。

**ステップ 5**　（任意）アドバタイズするインターフェイスをさらに作成する場合は、[Create] をクリックします。

[Create Advertised Interfaces] ダイアログボックスが表示されます。

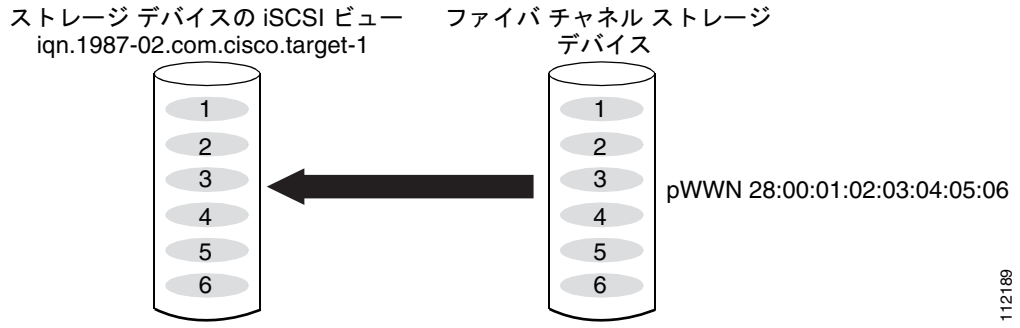
## iSCSI 仮想ターゲットの設定例

ここでは、iSCSI 仮想ターゲットの設定例を 3 つ説明します。

### 例 1

この例では、ファイバ チャネル ターゲット全体を iSCSI 仮想ターゲットとして割り当てます。ファイバ チャネル ターゲットに属しているすべての LUN は、iSCSI ターゲットに属しているものとして使用できます（図 4-16 を参照）。

**図 4-16　iSCSI ノード名の割り当て**

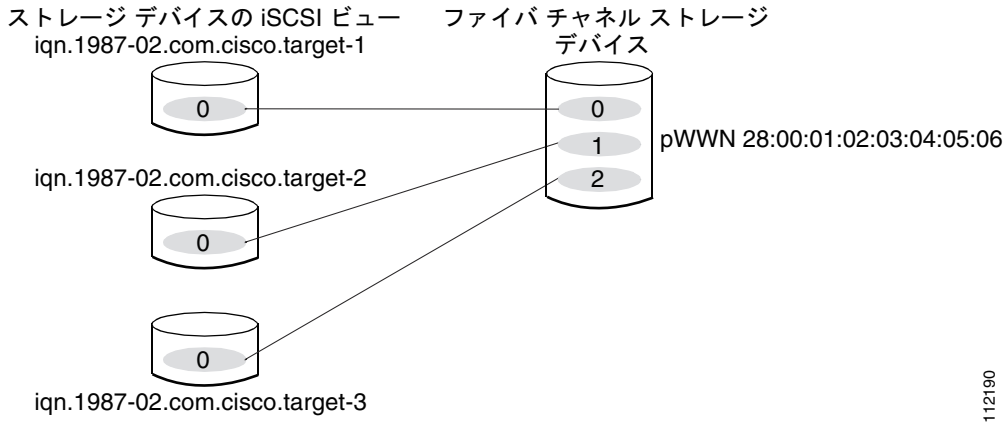



```
iscsi virtual-target name iqn.1987-02.com.cisco.target-1
    pWWN 28:00:01:02:03:04:05:06
```

### 例 2

この例では、ファイバ チャネル ターゲットの LUN のサブネットを 3 つの iSCSI 仮想ターゲットにマッピングします。各 iSCSI ターゲットは LUN を 1 つずつ持ちます（図 4-17 を参照）。

**図 4-17　LUN の iSCSI ノード名へのマッピング**

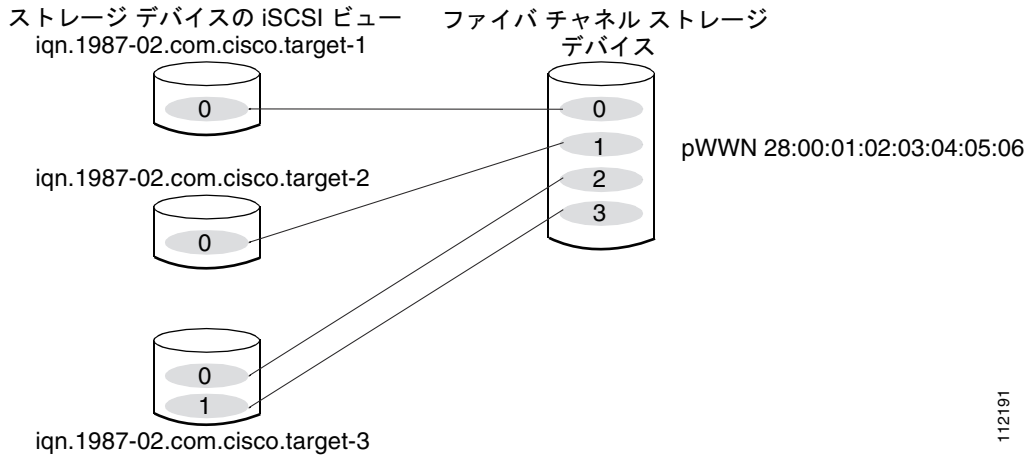



```
iscsi virtual-target name iqn.1987-02.com.cisco.target-1
    pWWN 28:00:01:02:03:04:05:06 fc-lun 0 iscsi-lun 0
iscsi virtual-target name iqn.1987-02.com.cisco.target-2
    pWWN 28:00:01:02:03:04:05:06 fc-lun 1 iscsi-lun 0
iscsi virtual-target name iqn.1987-02.com.cisco.target-3
    pWWN 28:00:01:02:03:04:05:06 fc-lun 2 iscsi-lun 0
```

### 例 3

この例では、ファイバ チャネル LUN ターゲットの 3 つのサブネットを 3 つの iSCSI 仮想ターゲットにマッピングします。2 つの iSCSI ターゲットはそれぞれ LUN を 1 つずつ持ち、3 つめの iSCSI ターゲットは 2 つの LUN を持ちます（図 4-18 を参照）。

**図 4-18　LUN の複数の iSCSI ノード名へのマッピング**



```
iscsi virtual-target name iqn.1987-02.com.cisco.target-1
    pWWN 28:00:01:02:03:04:05:06 fc-lun 0 iscsi-lun 0
iscsi virtual-target name iqn.1987-02.com.cisco.target-2
    pWWN 28:00:01:02:03:04:05:06 fc-lun 1 iscsi-lun 0
iscsi virtual-target name iqn.1987-02.com.cisco.target-3
    pWWN 28:00:01:02:03:04:05:06 fc-lun 2 iscsi-lun 0
    pWWN 28:00:01:02:03:04:05:06 fc-lun 3 iscsi-lun 1
```

# iSCSI ホストの仮想ファイバ チャネル ホストとしての提示

IPS モジュールまたは MPS-14/2 モジュールは、iSCSI ホストの代わりにファイバ チャネル ストレージ デバイスに接続し、コマンドを送信してストレージ デバイスを出入りするデータを転送します。これらのモジュールは、仮想ファイバ チャネル N ポートを使用して、iSCSI ホストの代わりにファイバ チャネル ストレージ デバイスにアクセスします。iSCSI ホストは、iSCSI 修飾名（IQN）または IP アドレスのいずれかで識別されます。

## イニシエータの識別

IPS モジュールまたは MPS-14/2 モジュールでは、次の情報を使用して iSCSI ホストを識別できます。

- iSCSI 修飾名（IQN）

  iSCSI イニシエータは、iSCSI ログインの際に提供する iSCSI ノード名に基づいて識別されます。iSCSI ホストに複数の IP アドレスがある場合で、そのホストで使用する IP アドレスに依存せずに、同一サービスを提供する場合にはこのモードが便利です。複数の IP アドレス（複数の Network Interface Card [NIC; ネットワーク インターフェイス カード]）を持つイニシエータは、ログインする IPS ポートそれぞれに 1 つずつ仮想 N ポートを持ちます。

- IP アドレス

  iSCSI イニシエータは、iSCSI ホストの IP アドレスに基づいて識別されます。iSCSI ホストに複数の IP アドレスがある場合で、そのホストで使用する IP アドレスに基づいて異なるサービスを提供する場合にはこのモードが便利です。また、iSCSI ノード名の取得に比べ、ホストの IP アドレスを取得する方が簡単です。仮想 N ポートは、iSCSI ターゲットへのログインに使用する IP アドレスごとに作成されます。ホストが 1 つの IP アドレスを使用して複数の IPS ポートにログインする場合、各 IPS ポートがその IP アドレスに対して仮想 N ポートを 1 つずつ作成します。

各 IPS ポートで iSCSI イニシエータの識別モードを設定し、その設定に従って、IPS ポートで終端するすべての iSCSI ホストを識別できます。デフォルト モードは、名前によるイニシエータの識別です。

Fabric Manager を使用してイニシエータの識別モードを指定する手順は、次のとおりです。

**ステップ 1**　[Physical Attributes] ペインで [Interfaces] > [FC Logical] を選択します。

[Information] ペインにインターフェイス設定が表示されます。

**ステップ 2**　[iSCSI] タブをクリックします。

iSCSI インターフェイス設定が表示されます。

**ステップ 3**　修正する iSCSI インターフェイスの [Initiator ID Mode] フィールドを右クリックして、ドロップダウン メニューから [name] または [ipaddress] を選択します。

**ステップ 4**　[Apply Changes] をクリックして、この変更を保存します。

# イニシエータ プレゼンテーション モード

ファイバ チャネル ファブリック内で iSCSI ホストを示すために、トランスペアレント イニシエータ モードおよびプロキシ イニシエータ モードの 2 つのモードを使用できます。

- トランスペアレント イニシエータ モードでは、iSCSI ホストがそれぞれ 1 つの仮想ファイバ チャネル ホストとして示されます。トランスペアレント モードの利点は、（「実際の」ファイバ チャネル ホストを管理するのと同じように）より詳細にファイバ チャネル アクセス コントロールを設定できることです。iSCSI からファイバ チャネルへのマッピングは 1 対 1 であるため、ホストごとに異なるゾーン分割が設定されるか、ファイバ チャネル ストレージ デバイスでの LUN アクセス コントロールが設定されます。
- プロキシ イニシエータ モードでは、1 つの IPS ポート単位に仮想ファイバ チャネル ホストが 1 つだけあり、すべての iSCSI ホストがそれを使用してファイバ チャネル ターゲットにアクセスします。ファイバ チャネル ストレージ デバイスですべてのホストに対して明示的な LUN アクセス コントロールを必要とする状況では、iSCSI イニシエータごとに固定した設定を避けられない場合もあります。この場合は、プロキシ イニシエータ モードを使用すると、設定を簡易化できます。

**注意**　iSLB VRRP グループに属している iSCSI インターフェイスのプロキシ イニシエータ モードをイネーブルにすると、そのインターフェイスのロード バランシングに影響します。「iSCSI インターフェイス パラメータの変更とロード バランシングに対するその影響」（P.4-48）を参照してください。

Cisco MDS スイッチには、次の iSCSI セッション制限があります。

- スイッチでの iSCSI セッションの最大数は 5000 です。
- トランスペアレント イニシエータ モードの IPS ポートあたりの iSCSI セッションの最大数は 500 です。
- プロキシ イニシエータ モードの IPS ポートあたりの iSCSI セッションの最大数は 500 です。
- IPS ポートが同時に作成できるセッションの最大数は 5 です（ただし、サポートできるセッションの合計は 500 です）。

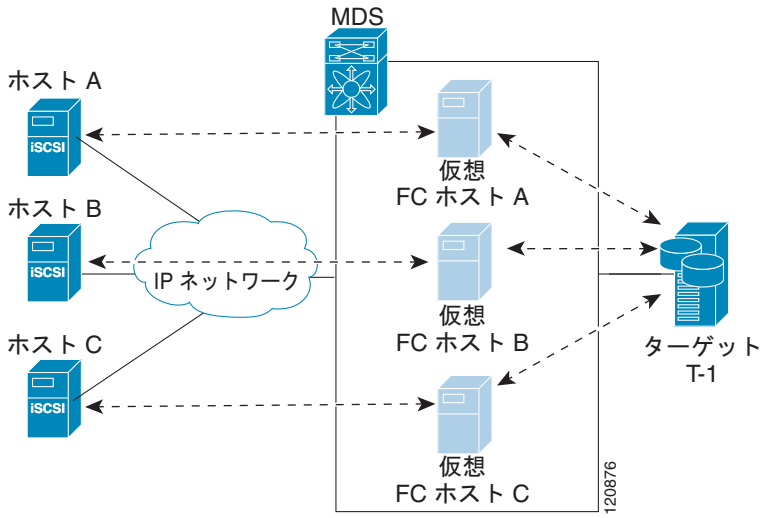
**（注）**　5 個を超えて iSCSI セッションが 1 つのポート上に同時に発生しそうになると、イニシエータが一時的なエラーを受信して、セッションの作成を後で再試行します。

## トランスペアレント イニシエータ モード

iSCSI ホストはそれぞれ、1 つの仮想ファイバ チャネル ホスト（つまり、1 つのファイバ チャネル N ポート）として示されます。トランスペアレント モードの利点は、より詳細にファイバ チャネル アクセス コントロールを設定できることです。iSCSI からファイバ チャネルへのマッピングは 1 対 1 であるため、ホストごとに異なるゾーン分割が設定されるか、ファイバ チャネル ストレージ デバイスでの LUN アクセス コントロールが設定されます。

iSCSI ホストが IPS モジュールまたは MPS-14/2 モジュールに接続するときに、そのホストに対する仮想ホスト N ポート（Host Bus Adapter [HBA] ポート）が作成されます（図 4-19 を参照）。どのファイバ チャネル N ポートにも固有のノード WWN とポート WWN が必要です。

図 4-19　仮想ホストの HBA ポート




仮想 N ポートを WWN で作成した後、IPS ポートの仮想 iSCSI インターフェイスを介して Fabric Login（FLOGI; ファブリック ログイン）が実行されます。FLOGI が完了すると、仮想 N ポートがファイバ チャネル SAN でオンラインになり、ファイバ チャネル ネーム サーバに仮想 N ポートが登録されます。IPS モジュールまたは MPS-14/2 モジュールは、ファイバ チャネル ネーム サーバに次のエントリを登録します。

- ネーム サーバの IP-address フィールドに iSCSI ホストの IP アドレス
- ネーム サーバの symbolic-node-name フィールドに iSCSI ホストの IQN
- ネーム サーバの FC-4 type フィールドに SCSI_FCP
- ネーム サーバの FC-4 機能のイニシエータ フラグ
- FC-4 type フィールドにベンダー固有の iSCSI GW フラグ（ネーム サーバで N ポート デバイスを iSCSI ゲートウェイ デバイスとして識別するため）

iSCSI ホストからの iSCSI セッションがすべて終了すると、IPS モジュールまたは MPS-14/2 モジュールは、明示的な Fabric Logout（FLOGO; ファブリック ログアウト）を実行して、仮想 N ポート デバイスをファイバ チャネル SAN から削除します（これにより、間接的にファイバ チャネル ネーム サーバからデバイスが登録解除されます）。

ホストから iSCSI 仮想ターゲットへのどの iSCSI セッションにも、実際のファイバ チャネル ターゲットへの対応するファイバ チャネル セッションが 1 つずつ存在します。図 4-19 では、3 つの iSCSI ホストが存在し、その 3 つすべてが同じファイバ チャネル ターゲットに接続しています。3 つの仮想ファイバ チャネル ホストごとにターゲットへのファイバ チャネル セッションが 1 つずつあります。

## iSCSI イニシエータのアイドル タイムアウト

iSCSI イニシエータのアイドル タイムアウトは、イニシエータが自身の最後の iSCSI セッションをログアウトしてから、仮想ファイバ チャネル N ポートがアイドル状態を続ける時間を指定します。このタイマーのデフォルト値は 300 秒です。これは、IP ネットワークで一時的な障害が発生したときに、N ポートがファイバ チャネル SAN に対してログインおよびログアウトを行わないようにするのに役立ちます。これにより、ファイバ チャネル SAN で不必要に生成される Registered State Change Notification（RSCN）が削減されます。

Fabric Manager を使用してイニシエータのアイドル タイムアウトを設定する手順は、次のとおりです。

**ステップ 1**　[Physical Attributes] ペインで [End Devices] > [iSCSI] を選択します。

[Information] ペインに iSCSI テーブルが表示されます（図 4-5 を参照）。

**ステップ 2**　[Globals] タブをクリックします。

iSCSI グローバル設定が表示されます。

**ステップ 3**　修正する [InitiatorIdle Timeout] フィールドを右クリックして、新しいタイムアウト値を入力します。

**ステップ 4**　[Apply Changes] アイコンをクリックして、これらの変更を保存します。

## iSCSI イニシエータの WWN の割り当て

iSCSI ホストは、次のメカニズムのいずれかを使用して N ポートの WWN にマッピングされます。

- ダイナミック マッピング（デフォルト）
- スタティック マッピング

### ダイナミック マッピング

ダイナミック マッピングの場合、iSCSI ホストは、動的に生成された port WWN（pWWN; ポート WWN）および node WWN（nWWN; ノード WWN）にマッピングされます。iSCSI ホストが接続するたびに、異なる WWN にマッピングされる可能性があります。ファイバ チャネル ターゲット デバイスでアクセス コントロールを必要としない場合は、このオプションを使用します（ターゲット デバイスのアクセス コントロールは、通常ホスト WWN を使用して設定されるためです）。

WWN は、MDS スイッチの WWN プールから割り当てられます。iSCSI に対する WWN マッピングは、iSCSI ホストから IPS ポートへの iSCSI セッションが 1 つ以上存在する限り維持されます。ホストからの iSCSI セッションがすべて終了し、IPS モジュールまたは MPS-14/2 モジュールがホストの仮想 N ポートに対して FLOGO を実行すると、WWN は解放されてスイッチのファイバ チャネル WWN プールに戻されます。これで、ファイバ チャネル ファブリックへのアクセスを要求している他の iSCSI ホストの割り当てに、これらのアドレスを使用できるようになります。

サポートされるダイナミック イニシエータ モードは次の 3 つです。

- iSCSI：ダイナミック イニシエータは、iSCSI イニシエータとして扱われ、ダイナミック仮想ターゲットおよび設定された iSCSI 仮想ターゲットにアクセスできます。
- iSLB：ダイナミック イニシエータは、iSLB イニシエータとして扱われます。
- Deny：ダイナミック イニシエータは、MDS スイッチにログインできません。

iSCSI ダイナミック マッピングがデフォルトで動作するモードです。この設定は、CFS を使用して配信されます。

**（注）**　ダイナミック イニシエータ モードは、Device Manager または Fabric Manager ではなく、CLI による設定だけがサポートされます。

### スタティック マッピング

スタティック マッピングの場合、iSCSI ホストは特定の pWWN および nWWN にマッピングされます。このマッピングは永続的なストレージに保持され、iSCSI ホストが接続するたびに同じ WWN マッピングが使用されます。ターゲット デバイスでアクセス コントロールを使用する場合は、このモードを使用する必要があります。

スタティック マッピングは次の 2 つのうちいずれかの方法で実装できます。

- ユーザ割り当て：設定処理中に WWN を指定することで、独自に固有の WWN を指定できます。

- システム割り当て：スイッチが自身のファイバ チャネル WWN プールから WWN を提供し、スイッチの設定にマッピングを保持するように要求できます。

**ヒント** **システム割り当て**のオプションを使用することをお勧めします。手動で WWN を割り当てる場合は、それが固有の割り当てになるようにする必要があります（詳細については、『*Cisco Fabric Manager Fabric Configuration Guide*』を参照してください）。すでに割り当てられている WWN は使用しないでください。

Device Manager を使用して iSCSI イニシエータのスタティック マッピングを設定する手順は、次のとおりです。

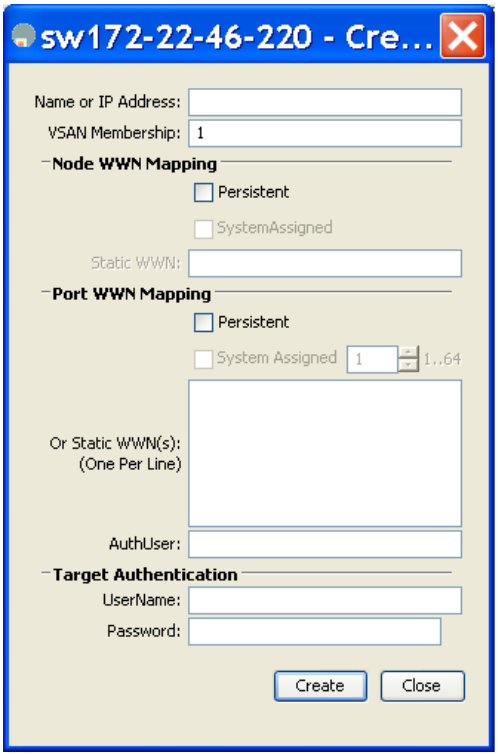
**ステップ 1**　[IP] > [iSCSI] を選択します。

iSCSI 設定が表示されます（図 4-12 を参照）。[Initiators] タブがデフォルトです。

**ステップ 2**　[Create] をクリックして iSCSI イニシエータを作成します。

[Create iSCSI Initiators] ダイアログボックスが表示されます（図 4-20 を参照）。

**図 4-20　[Create iSCSI Initiators] ダイアログボックス**




**ステップ 3**　iSCSI ノード名または IP アドレス、および VSAN メンバシップを設定します。

**ステップ 4**　[Node WWN Mapping] セクションの [Persistent] チェックボックスをオンにします。

**ステップ 5**　スイッチで nWWN を割り当てるようにする場合は [System Assigned] チェックボックスをオンにし、それ以外の場合は、このチェックボックスをオフのままにして [Static WWN] フィールドを設定します。

**ステップ 6**　pWWN を iSCSI イニシエータにスタティック マッピングする場合は、[Port WWN Mapping] セクションの [Persistent] チェックボックスをオンにします。

**ステップ 7**　[Persistent] をオンにした場合、スイッチで pWWN を割り当てるようにするときは、[System Assigned] チェックボックスをオンにして、この iSCSI イニシエータ用に予約する pWWN の数を設定します。または、このチェックボックスをオフのままにして、この iSCSI イニシエータ用に 1 つ以上の pWWN を設定することもできます。

**ステップ 8**　（任意）認証をイネーブルにする場合は [AuthUser] フィールドを設定します。「iSCSI セッション認証」（P.4-30）も参照してください。

**ステップ 9**　[Create] をクリックして、この iSCSI イニシエータを作成します。

**（注）**　システム割り当てのオプションを使用して iSCSI イニシエータに WWN を設定する場合、その設定を ASCII ファイルに保存すると、システム割り当てされた WWN も保存されます。以降、write erase を実行した場合は、ASCII ファイルから WWN 設定を手動で削除する必要があります。これを行わないと、ASCII 設定ファイルがスイッチ上で再適用されたときに、WWN 割り当てが重複する可能性があります。

### ダイナミック iSCSI イニシエータの WWN マッピングをスタティックにする

ダイナミック iSCSI イニシエータがログインした後、このイニシエータで次回のログイン時に同じマッピングを使用できるように、自動的に割り当てられた nWWN/pWWN マッピングを永続的に保持するかどうかを判断できます。

ダイナミック iSCSI イニシエータをスタティック iSCSI イニシエータに変換して、その WWN を永続的に使用することができます（「ダイナミック マッピング」（P.4-19）を参照）。

**（注）**　ダイナミック iSCSI イニシエータをスタティック iSLB イニシエータに変換したり、ダイナミック iSLB イニシエータをスタティック iSCSI イニシエータに変換したりすることはできません。

**（注）**　イニシエータ作成後にダイナミック pWWN をスタティックにする方法は、Device Manager または Fabric Manager ではなく、CLI による設定だけがサポートされます。Fabric Manager または Device Manager では、このイニシエータを削除してから再作成し、pWWN をスタティックに設定する必要があります。

### WWN の競合の確認

システムによってスタティック iSCSI イニシエータに割り当てられた WWN は、アップグレードに失敗したり、システム ソフトウェアをダウングレードしたりすると、予期せずシステムに戻される場合があります。このような場合、その後システムがその WWN を他の（ダイナミックまたはスタティックの）iSCSI イニシエータに割り当てる可能性があるため、競合が発生する場合があります。

このような状況が発生した場合はすぐに、システムに属している WWN を確認し、設定済みの WWN があれば削除することで、この問題に対処できます。

Fabric Manager を使用して自動的に割り当てられた nWWN マッピングを永続的に保持する手順は、次のとおりです。

**ステップ 1**　[Physical Attributes] ペインで [End Devices] > [iSCSI] を選択します。

[Information] ペインに iSCSI テーブルが表示されます（図 4-5 を参照）。

**ステップ 2**　[Initiators] タブをクリックします。

設定されている iSCSI イニシエータが表示されます。

**ステップ 3**　スタティックにする iSCSI イニシエータの [Persistent Node WWN] チェックボックスをオンにします。

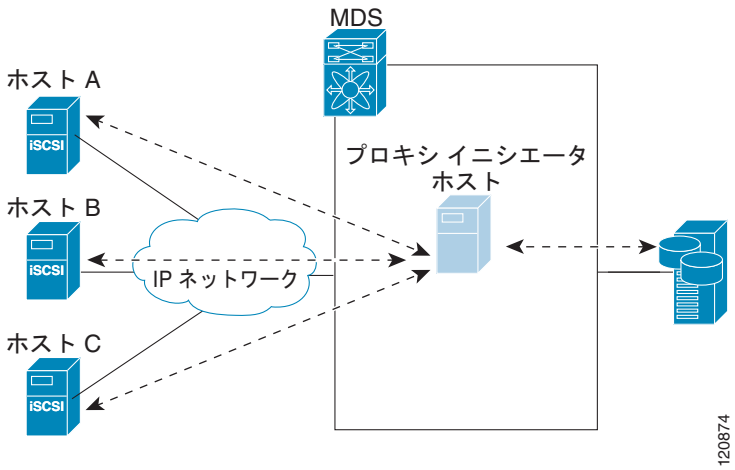
**ステップ 4**　[Apply Changes] アイコンをクリックして、これらの変更を保存します。

## プロキシ イニシエータ モード

ファイバ チャネル ストレージ デバイスですべてのホストに対して明示的な LUN アクセス コントロールを必要とする場合に、トランスペアレント イニシエータ モード（1 つの iSCSI ホストを 1 つのファイバ チャネル ホストとして示すモード）を使用することは、すべての iSCSI ホストをスタティックに設定しなければならないことを意味します。つまり、iSCSI ホストごとにいくつかの設定作業が発生することになります。この場合は、プロキシ イニシエータ モードを使用すると、設定を簡易化できます。

このモードでは、IPS ポート単位に仮想ホスト N ポート（HBA ポート）が 1 つだけ作成されます。この IPS ポートに接続しているすべての iSCSI ホストは、同一の仮想ホスト N ポートを使用して多重化されます（図 4-21 を参照）。このモードは、WWN を静的にバインディングする作業を簡易化します。この IPS ポートを介して接続する各 iSCSI イニシエータが使用するすべての LUN に対して、プロキシ仮想 N ポートの pWWN からアクセスできるように、ファイバ チャネル ストレージ アレイでの LUN マッピングおよび割り当てを設定する必要があります。その後、LUN マッピングおよび iSCSI アクセス コントロール（「iSCSI アクセス コントロール」（P.4-26）を参照）を設定した iSCSI 仮想ターゲット（「スタティック マッピング」（P.4-12）を参照）を設定することで、LUN が各 iSCSI イニシエータに割り当てられます。

**図 4-21　IPS ポートの多重化**




プロキシ イニシエータ モードは IPS ポート単位に設定できます。この場合、これを設定した IPS ポートで終端する iSCSI イニシエータだけがこのモードになります。

プロキシ イニシエータ モードで IPS ポートを作成すると、その IPS ポートの仮想 iSCSI インターフェイスを介してファブリック ログイン（FLOGI）が実行されます。FLOGI の完了後、プロキシ イニシエータの仮想 N ポートがファイバ チャネル ファブリックでオンラインになり、ファイバ チャネル ネーム サーバに仮想 N ポートが登録されます。IPS モジュールまたは MPS-14/2 モジュールは、ファイバ チャネル ネーム サーバに次のエントリを登録します。

- 「iSCSI インターフェイス名 iSCSI スロット / ポート」がネーム サーバの symbolic-node-name フィールドに登録されます。

- ネーム サーバの FC-4 type フィールドに SCSI_FCP
- ネーム サーバの FC-4 機能のイニシエータ フラグ
- FC-4 type フィールドにベンダー固有のフラグ（iscsi-gw）、（ネーム サーバで N ポート デバイスを iSCSI ゲートウェイ デバイスとして識別するため）

トランスペアレント イニシエータ モードと同様に、ユーザが pWWN および nWWN を指定したり、プロキシ イニシエータ N ポートに対してシステム割り当てされた WWN を要求したりすることもできます。

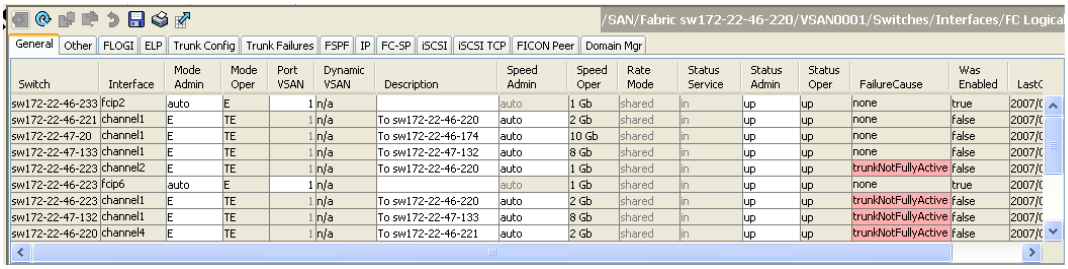
**注意**　iSLB VRRP グループに属している iSCSI インターフェイスのプロキシ イニシエータ モードをイネーブルにすると、そのインターフェイスのロード バランシングに影響します。「iSCSI インターフェイス パラメータの変更とロード バランシングに対するその影響」（P.4-48）を参照してください。

Fabric Manager を使用してプロキシ イニシエータを設定する手順は、次のとおりです。

**ステップ 1**　[Switches] を展開し、[Interfaces] を展開して [Physical Attributes] ペインの [FC Logical] を選択します。

[Information] ペインにインターフェイス テーブルが表示されます（図 4-22 を参照）。

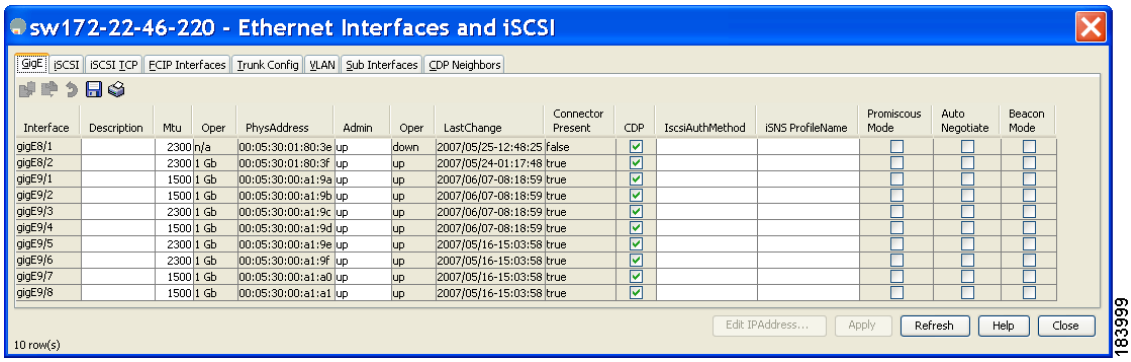
**図 4-22　FC 論理インターフェイス テーブル**




**ステップ 2**　Device Manager で [Interface] > [Ethernet and iSCSI] を選択します。

[Ethernet Interfaces and iSCSI] ダイアログボックスが表示されます（図 4-23 を参照）。

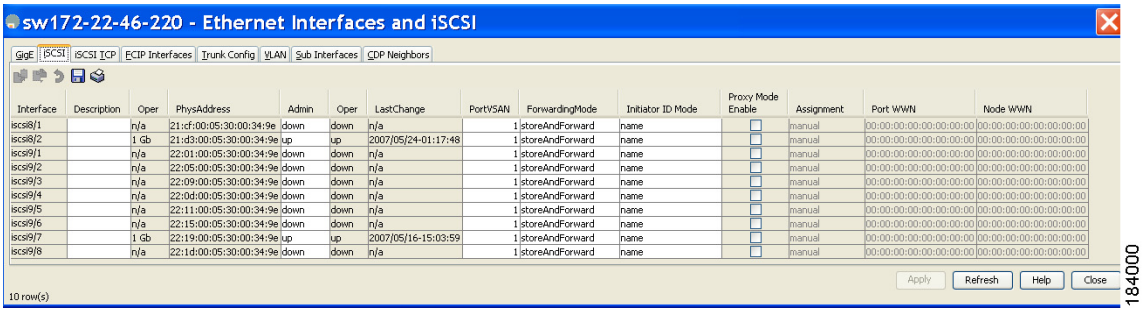
**図 4-23　[Ethernet Interfaces and iSCSI] ダイアログボックス**



**ステップ 3**　FM または DM で [iSCSI] タブをクリックします。

iSCSI インターフェイス設定テーブルが表示されます（図 4-24 を参照）。

**図 4-24　Device Manager の [iSCSI] タブ**




**ステップ 4**　[Proxy Mode Enable] チェックボックスをオンにします。

**ステップ 5**　Fabric Manager の [Apply Changes] アイコンをクリックするか、Device Manager の [Apply] をクリックして、これらの変更を保存します。

**（注）**　インターフェイスがプロキシ イニシエータ モードの場合、iSCSI インターフェイスのプロキシ N ポート属性である、WWN ペアまたは FC ID に基づいて、ファイバ チャネル アクセス コントロール（ゾーン分割）だけを設定できます。IP アドレスや iSCSI イニシエータの IQN などの iSCSI 属性を使用してゾーン分割を設定することはできません。イニシエータ ベースのアクセス コントロールを実行するには、iSCSI ベースのアクセス コントロールを使用します（「iSCSI アクセス コントロール」（P.4-26）を参照）。

## iSCSI の VSAN メンバシップ

ファイバ チャネル デバイスと同様に、iSCSI デバイスには、VSAN メンバシップを定義できる 2 つのメカニズムがあります。

- iSCSI ホスト：iSCSI ホストに対する VSAN メンバシップ（この方法は、iSCSI インターフェイスより優先して実行されます）。
- iSCSI インターフェイス：iSCSI インターフェイスに対する VSAN メンバシップ（ホストが iSCSI ホストによる方法でどの VSAN にも設定されていない場合、この iSCSI インターフェイスに接続するすべての iSCSI ホストがインターフェイス VSAN メンバシップを継承します）。

### iSCSI ホストの VSAN メンバシップ

個々の iSCSI ホストを特定の VSAN に属すように設定できます。指定された VSAN は、iSCSI インターフェイスの VSAN メンバシップを上書きします。

Fabric Manager を使用して iSCSI ホストの VSAN メンバシップを割り当てる手順は、次のとおりです。

**ステップ 1**　[Physical Attributes] ペインで [End Devices] > [iSCSI] を選択します。

[Information] ペインに iSCSI テーブルが表示されます（図 4-5 を参照）。

**ステップ 2**　[Initiators] タブをクリックします。

設定されている iSCSI イニシエータが表示されます。

**ステップ 3**　[VSAN Membership] フィールドを入力して、VSAN を iSCSI ホストに割り当てます。

**ステップ 4**　[Apply Changes] アイコンをクリックして、これらの変更を保存します。

**（注）**　他の VSAN（VSAN 1 以外）、たとえば VSAN 2 にイニシエータを設定すると、そのイニシエータは VSAN 1 から自動的に削除されます。このイニシエータを VSAN 1 にも存在させる場合は、VSAN 1 でイニシエータを明示的に設定する必要があります。

### iSCSI インターフェイスの VSAN メンバシップ

*ポート VSAN* と呼ばれる iSCSI インターフェイスに VSAN メンバシップを設定できます。このインターフェイスに接続するすべての iSCSI デバイスは、VSAN で明示的に設定されていない場合、自動的にこの VSAN のメンバーになります。つまり、iSCSI インターフェイスのポート VSAN は、すべてのダイナミック iSCSI イニシエータのデフォルト VSAN となります。iSCSI インターフェイスのデフォルト ポート VSAN は VSAN 1 です。

**注意**　iSLB VRRP グループに属している iSCSI インターフェイスの VSAN メンバシップを変更すると、インターフェイスのロード バランシングに影響します。「iSCSI インターフェイス パラメータの変更とロード バランシングに対するその影響」（P.4-48）を参照してください。

Device Manager を使用して iSCSI インターフェイスのデフォルト ポート VSAN を変更する手順は、次のとおりです。

**ステップ 1**　[Interface] > [Ethernet and iSCSI] を選択します。

[Ethernet Interfaces and iSCSI] ダイアログボックスが表示されます（図 4-23 を参照）。

**ステップ 2**　[iSCSI] タブをクリックします。

iSCSI インターフェイス設定テーブルが表示されます（図 4-24 を参照）。

**ステップ 3**　[PortVSAN] 列をダブルクリックして、デフォルトのポート VSAN を修正します。

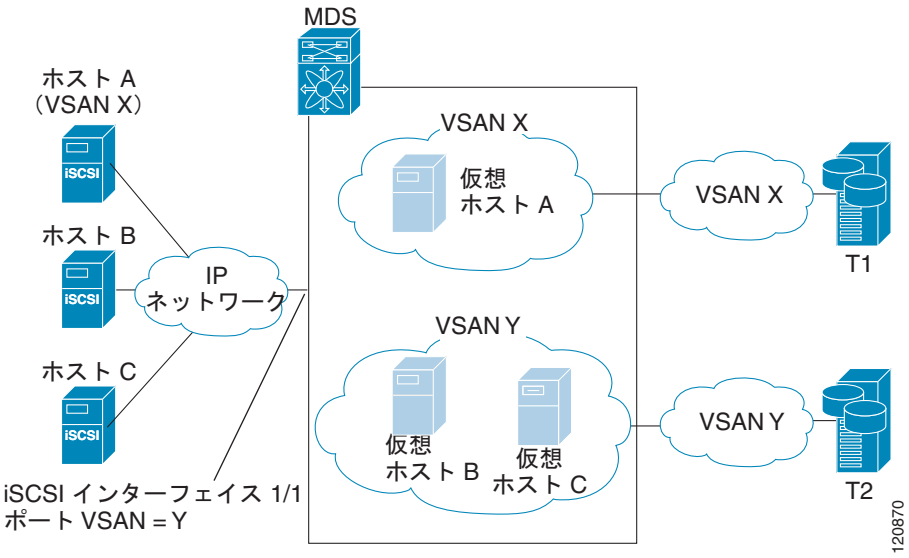
**ステップ 4**　[Apply] をクリックして、これらの変更を保存します。

## iSCSI デバイスの VSAN メンバシップの例

図 4-25 に、次の iSCSI デバイスの VSAN メンバシップの例を示します。

- iSCSI インターフェイス 1/1 は、VSAN Y のメンバーです。
- iSCSI イニシエータのホスト A は、VSAN X に対する明示的な VSAN メンバシップを持ちます。
- 3 つの iSCSI イニシエータ（ホスト A、ホスト B、およびホスト C）は、iSCSI インターフェイス 1/1 に接続します。

図 4-25　iSCSI インターフェイスの VSAN メンバシップ




ホスト A の仮想ファイバ チャネル N ポートは、イニシエータの明示的なメンバシップを持つため、VSAN X に追加されます。仮想ホスト B と C の N ポートは、明示的なメンバシップ設定を持たないため、iSCSI インターフェイスの VSAN メンバシップを継承して、VSAN Y に所属します。

## iSCSI ホストの詳細な VSAN メンバシップ

iSCSI ホストは、複数の VSAN のメンバーになることができます。この場合、iSCSI ホストがメンバーになっている VSAN ごとに 1 つずつ仮想ファイバ チャネル ホストが複数作成されます。この設定は、ファイバ チャネル テープ デバイスなど、特定のリソースを異なる VSAN 間で共有する必要がある場合に便利です。

# iSCSI アクセス コントロール

iSCSI デバイスに使用できるアクセス コントロールには、次の 2 つのメカニズムがあります。

- ファイバ チャネル ゾーン分割ベースのアクセス コントロール
- iSCSI ACL ベースのアクセス コントロール

ファイバ チャネル ファブリック内で iSCSI ホストを示すために使用されるイニシエータ モードに応じて、いずれかのアクセス コントロール メカニズムを使用することも、両方のメカニズムを使用することも使用できます。

ここで説明する内容は、次のとおりです。

- 「ファイバ チャネル ゾーン分割ベースのアクセス コントロール」（P.4-27）
- 「iSCSI ベースのアクセス コントロール」（P.4-28）
- 「アクセス コントロールの実行」（P.4-29）

## ファイバ チャネル ゾーン分割ベースのアクセス コントロール

Cisco SAN-OS リリース 3.x と NX-OS リリース 4.1(1b) の VSAN およびゾーン分割の概念は、ファイバ チャネル デバイスと iSCSI デバイスの両方を対象とするように拡張されました。ゾーン分割は、ファイバ チャネル デバイスの標準的なアクセス コントロール メカニズムであり、VSAN のコンテキスト内で適用されます。ファイバ チャネルのゾーン分割は、iSCSI デバイスをサポートするように拡張され、この拡張には、SAN 全体で一貫した柔軟なアクセス コントロール メカニズムを得られるというメリットがあります。

ファイバ チャネル ゾーンのメンバーを識別する共通のメカニズムは、次のとおりです（ファイバ チャネルのゾーン分割については、『*Cisco Fabric Manager Fabric Configuration Guide*』を参照してください）。

- ファイバ チャネル デバイスの pWWN。
- インターフェイスおよびスイッチの WWN。このインターフェイスを介して接続するデバイスはゾーン内に存在します。

iSCSI の場合、複数の iSCSI デバイスが iSCSI インターフェイスの背後に接続される可能性があります。インターフェイス ベースのゾーン分割は、インターフェイスの背後に接続されるすべての iSCSI デバイスが自動的に同じゾーン内に存在することになるため、実用的ではない場合があります。

トランスペアレント イニシエータ モードでは（「トランスペアレント イニシエータ モード」（P.4-17）で説明したように、ファイバ チャネル仮想 N ポートが iSCSI ごとに 1 つずつ作成される場合）、iSCSI ホストにスタティック WWN マッピングが設定されていれば、標準のファイバ チャネル デバイスの pWWN ベースのゾーン分割メンバシップ メカニズムを使用できます。

ゾーン分割メンバシップ メカニズムは、次の情報に基づいて iSCSI デバイスをゾーンに追加するように拡張されました。

- IPv4 アドレス/サブネット マスク
- IPv6 アドレス/プレフィクス長
- iSCSI 修飾名（IQN）
- Symbolic-node-name（IQN）

スタティック WWN マッピングが設定されていない iSCSI ホストの場合、この機能により、IP アドレスまたは iSCSI ノード名をゾーン メンバーとして指定できます。スタティック WWN マッピングが設定された iSCSI ホストがこれらの機能も使用できることに留意してください。IP アドレス ベースのゾーン メンバシップは、サブネット マスクを指定して 1 つのコマンドで複数のデバイスを指定できます。

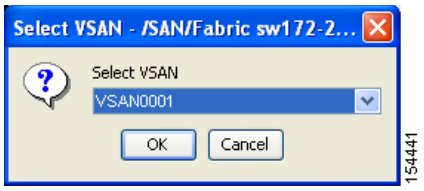
**（注）** プロキシ イニシエータ モードでは、IPS ポートに接続するすべての iSCSI デバイスは、単一の仮想ファイバ チャネル N ポートを介してファイバ チャネル ファブリックにアクセスできます。iSCSI ノード名または IP アドレスに基づくゾーン分割を設定しても効果はありません。pWWN に基づくゾーン分割を使用する場合、この IPS ポートに接続するすべての iSCSI デバイスは、同じゾーンに配置されます。プロキシ イニシエータ モードで個別のイニシエータのアクセス コントロールを実装するには、仮想ターゲット上で iSCSI ACL を設定します（「iSCSI ベースのアクセス コントロール」（P.4-28）を参照）。

Fabric Manager を使用して iSCSI イニシエータをゾーン データベースに追加する手順は、次のとおりです。

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

[Edit Local Zone Database] ダイアログボックスが表示されます（図 4-26 を参照）。

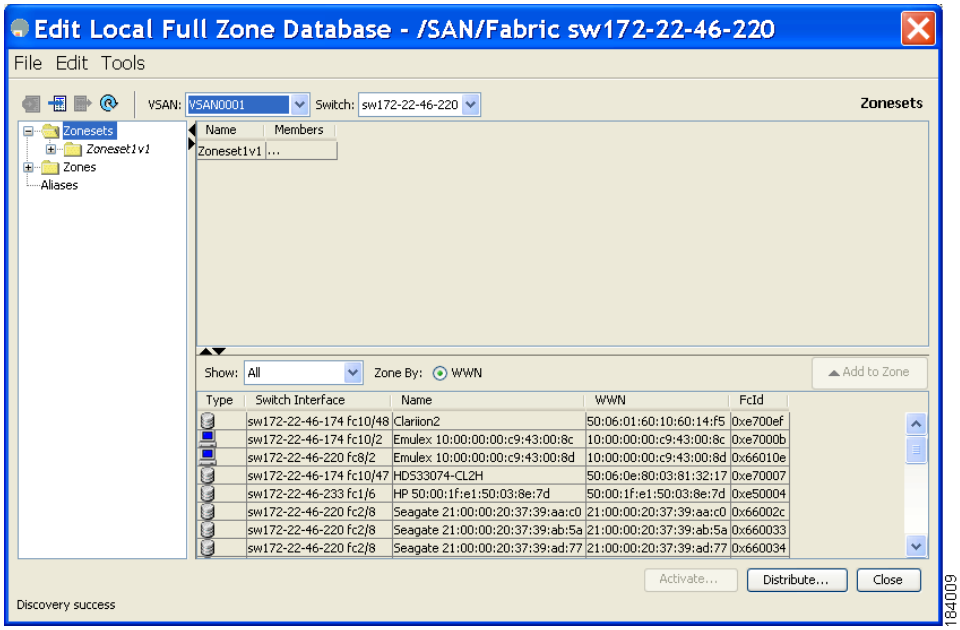
図 4-26　Fabric Manager の [Edit Local Zone Database] ダイアログボックス




**ステップ 2**　iSCSI ホスト イニシエータを追加する VSAN を選択して [OK] をクリックします。

この VSAN に使用可能なゾーンおよびゾーン セットが表示されます（図 4-27 を参照）。

図 4-27　使用可能なゾーンおよびゾーン セット




**ステップ 3**　iSCSI ホスト イニシエータで使用可能なデバイスのリストから、ゾーンに追加するイニシエータをドラッグします。

**ステップ 4**　[Distribute] をクリックして変更を配信します。

## iSCSI ベースのアクセス コントロール

iSCSI ベースのアクセス コントロールは、スタティック iSCSI 仮想ターゲットを作成する場合にだけ適用できます（「スタティック マッピング」（P.4-12）を参照）。スタティック iSCSI ターゲットの場合、そのターゲットにアクセスできる iSCSI イニシエータのリストを設定できます。

デフォルトでは、スタティック iSCSI 仮想ターゲットはどの iSCSI ホストにもアクセスできるわけではありません。すべてのホストが iSCSI 仮想ターゲットにアクセスできるようにアクセシビリティを明示的に設定する必要があります。イニシエータ アクセス リストには、1 つ以上のイニシエータを含めることができます。次のいずれかのメカニズムを使用して、iSCSI イニシエータを識別できます。

- iSCSI ノード名

- IPv4 アドレスおよびサブネット
- IPv6 アドレス

（注）　トランスペアレント モードの iSCSI イニシエータで、ファイバ チャネル ゾーン分割と iSCSI ACL の両方を使用する場合は、その iSCSI ホストにアクセス可能なすべてのスタティック iSCSI ターゲットに対するイニシエータの仮想 N ポートがファイバ チャネル ターゲットと同じファイバ チャネル ゾーンに存在する必要があります。

**ステップ 1**　[IP] > [iSCSI] を選択します。

iSCSI 設定が表示されます（図 4-12 を参照）。

**ステップ 2**　[Targets] タブをクリックします。

iSCSI 仮想ターゲットが表示されます。

**ステップ 3**　[Initiators Access All] チェックボックスがオンになっている場合はオフにします。

**ステップ 4**　[Edit Access] をクリックします。

[Initiators Access] ダイアログボックスが表示されます。

**ステップ 5**　[Create] をクリックして、イニシエータ アクセス リストにさらにイニシエータを追加します。

[Create Initiators Access] ダイアログボックスが表示されます。

**ステップ 6**　この仮想ターゲットに許可するイニシエータの名前または IP アドレスを追加します。

**ステップ 7**　[Create] をクリックして、イニシエータ アクセス リストにこのイニシエータを追加します。

## アクセス コントロールの実行

IPS モジュールおよび MPS-14/2 モジュールは、iSCSI ベースとファイバ チャネル ゾーン分割ベースの両方のアクセス コントロール リストを使用して、アクセス コントロールを実行します。アクセス コントロールは、iSCSI 検出フェーズと iSCSI セッション作成フェーズの両方で実行されます。IPS モジュールも MPS-14/2 モジュールも iSCSI トラフィックのファイバ チャネルへのルーティングに関与していないため、I/O フェーズではアクセス コントロールを実行する必要はありません。

- iSCSI 検出フェーズ：iSCSI ホストが iSCSI 検出セッションを作成し、すべての iSCSI ターゲットを問い合せると、IPS モジュールまたは MPS-14/2 モジュールは、前述したアクセス コントロール ポリシーに基づいてこの iSCSI ホストがアクセスできる iSCSI ターゲットのリストだけを返します。IPS モジュールまたは MPS-14/2 モジュールは、すべての VSAN でイニシエータと同じゾーンにあるすべてのデバイスについて、ファイバ チャネル ネーム サーバに問い合せすることで、これを実行します。次に、FCNS エントリの FC4-feature フィールドを検索して、イニシエータになっているデバイスをフィルタします（デバイスが FC4-feature フィールドにイニシエータとしてもターゲットとしても登録していない場合、IPS モジュールまたは MPS-14/2 モジュールはそれをアドバタイズします）。その後に iSCSI ホストにターゲットのリストを返します。それぞれのターゲットには、ユーザが設定するスタティック iSCSI ターゲット名、あるいは IPS モジュールまたは MPS-14/2 モジュールがそのターゲット用に作成するダイナミック iSCSI ターゲット名のいずれかが付けられています（「ダイナミック マッピング」（P.4-10）を参照）。

- iSCSI セッション作成：IP ホストが iSCSI セッションを開始すると、IPS モジュールまたは MPS-14/2 モジュールは、（セッション ログイン要求で）指定された iSCSI ターゲットが、「iSCSI ベースのアクセス コントロール」（P.4-28）で説明したアクセス コントロールの両方のメカニズムで許可されているかどうかを確認します。

  iSCSI ターゲットがスタティック マッピングされたターゲットである場合、IPS モジュールまたは MPS-14/2 モジュールは、iSCSI ホストが iSCSI ターゲットのアクセス リスト内で許可されているかどうかを確認します。IP ホストがアクセスできない場合、そのログインは拒否されます。iSCSI ホストが許可されている場合、iSCSI ホストで使用する仮想ファイバ チャネル N ポート、およびスタティック iSCSI 仮想ターゲットにマッピングされているファイバ チャネル ターゲットが同じファイバ チャネル ゾーンに存在するかどうかを確認します。

  iSCSI ターゲットが自動生成された iSCSI ターゲットである場合、IPS モジュールまたは MPS-14/2 モジュールは、ファイバ チャネル ターゲットの WWN を iSCSI ターゲット名から抽出し、イニシエータとファイバ チャネル ターゲットが同じファイバ チャネル ゾーンに存在するかどうかを確認します。同じゾーンに存在している場合、アクセスが許可されます。

IPS モジュールまたは MPS-14/2 モジュールは、iSCSI ホストのファイバ チャネル仮想 N ポートを使用して、ネーム サーバにゾーンを制限したファイバ チャネル ターゲットの WWN を問い合せます。ネーム サーバから FC ID が返されると、iSCSI セッションが受け入れられます。そうでない場合は、ログイン要求が拒否されます。

# iSCSI セッション認証

IPS モジュールまたは MPS-14/2 モジュールは、ストレージ デバイスへのアクセスを要求する iSCSI ホストを認証するための iSCSI 認証メカニズムをサポートします。デフォルトでは、IPS モジュールまたは MPS-14/2 モジュールは、iSCSI イニシエータの CHAP 認証または None 認証を許可します。認証を常に使用する場合は、CHAP 認証だけを許可するようにスイッチを設定する必要があります。

CHAP ユーザ名または CHAP シークレットの検証には、Cisco MDS AAA インフラストラクチャでサポートされ許可されている方法であれば任意に使用できます（詳細については、『*Cisco Fabric Manager Security Configuration Guide*』を参照してください）。AAA 認証は、RADIUS、TACACS+、またはローカル認証デバイスをサポートします。

Fabric Manager を使用して iSCSI ユーザの AAA 認証を設定する手順は、次のとおりです。

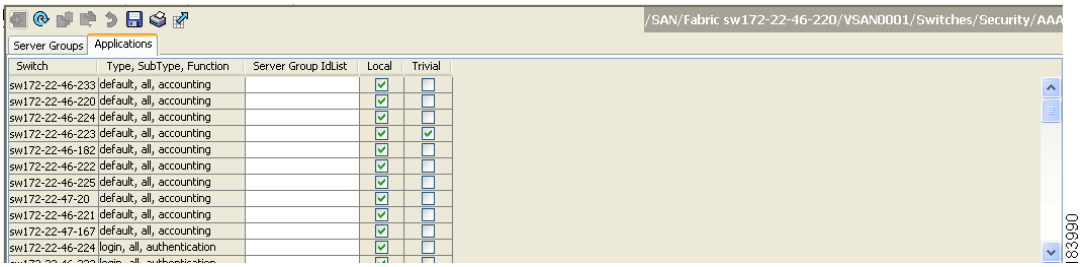
**ステップ 1**　[Physical Attributes] ペインで [Switches] > [Security] > [AAA] を選択します。

[Information] ペインに AAA 設定が表示されます。

**ステップ 2**　[Applications] タブをクリックします。

アプリケーションごとに AAA 設定が表示されます（図 4-28 を参照）。

**図 4-28　アプリケーション設定ごとの AAA**



**ステップ 3**　iSCSI アプリケーションの [Server Group IdList] フィールドを右クリックして、iSCSI に使用するサーバ グループを入力します。

**（注）**　既存のサーバ グループを使用するか、新規サーバ グループを作成してから、そのグループを iSCSI セッション認証用に設定する必要があります。

**ステップ 4**　[Apply Changes] アイコンをクリックして、これらの変更を保存します。

ここで説明する内容は、次のとおりです。



## 認証メカニズムの設定

iSCSI の CHAP 認証または None 認証を、グローバル レベルでも各インターフェイス レベルでも設定することができます。

ギガビット イーサネットのインターフェイスまたはサブインターフェイスの認証は、グローバル レベルで設定された認証方法を上書きします。

Fabric Manager を使用して iSCSI ユーザの AAA 認証を設定する手順は、次のとおりです。

**ステップ 1**　[Physical Attributes] ペインで [End Devices] > [iSCSI] を選択します。

[Information] ペインに iSCSI テーブルが表示されます（図 4-5 を参照）。

**ステップ 2**　[Globals] タブをクリックします。

iSCSI 認証設定テーブルが表示されます。

**ステップ 3**　[authMethod] 列から [chap] または [none] を選択します。

**ステップ 4**　Fabric Manager の [Apply Changes] アイコンをクリックして、これらの変更を保存します。

Fabric Manager を使用して、特定のインターフェイスへの iSCSI セッションに認証メカニズムを設定する手順は、次のとおりです。

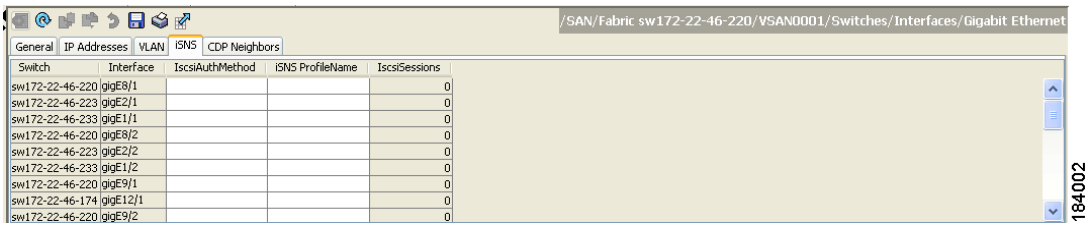
**ステップ 1**　[Physical Attributes] ペインで [Switches] > [Interfaces] > [Gigabit Ethernet] を選択します。

[Information] ペインにギガビット イーサネットの設定が表示されます。

**ステップ 2**　[iSNS] タブをクリックします。

iSCSI および iSNS の設定が表示されます（図 4-29 を参照）。

図 4-29　インターフェイス上での iSCSI 認証の設定




**ステップ 3**　[IscsiAuthMethod] フィールドを右クリックして、[none] または [chap] を選択します。

**ステップ 4**　[Apply Changes] アイコンをクリックして、これらの変更を保存します。

## ローカル認証の設定

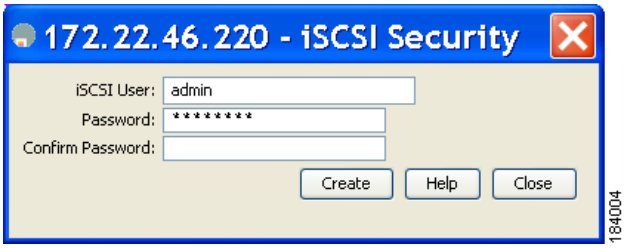
『*Cisco Fabric Manager Security Configuration Guide*』を参照して、ローカル パスワード データベースを作成します。iSCSI イニシエータのローカル パスワード データベースにユーザを作成するには、iSCSI キーワードが必須です。

Device Manager を使用してローカル認証の iSCSI ユーザを設定する手順は、次のとおりです。

**ステップ 1**　[Security] > [iSCSI] を選択します。

[iSCSI Security] ダイアログボックスが表示されます（図 4-30 を参照）。

図 4-30　[iSCSI Security] ダイアログボックス




**ステップ 2**　[iSCSI User]、[Password]、および [Password Confirmation] の各フィールドを入力します。

**ステップ 3**　[Create] をクリックして、この新しいユーザを保存します。

## iSCSI イニシエータ認証の制約

デフォルトでは、iSCSI イニシエータは、IPS モジュールまたは MPS-14/2 モジュールに対して自身を認証する際に、RADIUS サーバまたはローカル データベースの任意のユーザ名を使用できます（CHAP ユーザ名は、iSCSI イニシエータ名とは関係ありません）。IPS モジュールまたは MPS-14/2 モジュールは、スイッチから送信される CHAP 認証確認に正しい応答を返している間は、イニシエータのログインを許可します。これは、CHAP ユーザ名およびパスワードが 1 つでも侵害されると問題に発展する可能性があります。

Fabric Manager を使用してイニシエータが CHAP 認証に特定のユーザ名を使用するように制限する手順は、次のとおりです。

**ステップ 1**　[Physical Attributes] ペインで [End Devices] > [iSCSI] を選択します。

[Information] ペインに iSCSI テーブルが表示されます（図 4-5 を参照）。

**ステップ 2**　[AuthUser] フィールドを右クリックして、iSCSI イニシエータに限定するユーザ名を入力します。

**ステップ 3**　[Apply Changes] アイコンをクリックして、これらの変更を保存します。

## 相互 CHAP 認証の設定

iSCSI イニシエータの IPS モジュールまたは MPS-14/2 モジュールの認証の他にも、IPS モジュールまたは MPS-14/2 モジュールは、iSCSI のログイン フェーズで Cisco MDS スイッチの iSCSI ターゲットを iSCSI イニシエータが認証するメカニズムをサポートします。この認証では、iSCSI イニシエータに対して示すスイッチのユーザ名とパスワードをユーザが設定する必要があります。指定されたパスワードを使用して、イニシエータが IPS ポートに送信する CHAP 認証確認に対する CHAP 応答を計算します。

Fabric Manager を使用して、イニシエータに対するスイッチの認証のために、そのスイッチで使用するグローバル iSCSI ターゲットのユーザ名とパスワードを設定する手順は、次のとおりです。

**ステップ 1**　[Physical Attributes] ペインで [End Devices] > [iSCSI] を選択します。

[Information] ペインに iSCSI テーブルが表示されます（図 4-5 を参照）。

**ステップ 2**　[Globals] タブを選択します。

グローバル iSCSI 設定が表示されます。

**ステップ 3**　[Target UserName] フィールドと [Target Password] フィールドに入力します。

**ステップ 4**　[Apply Changes] アイコンをクリックして、これらの変更を保存します。

Device Manager を使用して、イニシエータに対するスイッチの認証のために、そのスイッチで使用するイニシエータごとの iSCSI ターゲットのユーザ名とパスワードを設定する手順は、次のとおりです。

**ステップ 1**　[IP] > [iSCSI] を選択します。

iSCSI 設定が表示されます（図 4-12 を参照）。

**ステップ 2**　設定するイニシエータの [Target UserName] フィールドと [Target Password] フィールドを入力します。

**ステップ 3**　[Create] をクリックして、イニシエータ アクセス リストにこのイニシエータを追加します。

## iSCSI RADIUS サーバの設定

iSCSI RADIUS サーバを設定する手順は、次のとおりです。

**ステップ 1**　Cisco MDS スイッチの管理イーサネット IP アドレスからのアクセスを許可するように RADIUS サーバを設定します。

**ステップ 2**　Cisco MDS スイッチを認証する RADIUS サーバの共有秘密を設定します。

**ステップ 3**　RADIUS サーバで iSCSI ユーザとパスワードを設定します。

# iSCSI の即時データ機能と非請求データ機能

Cisco MDS スイッチは、ログイン ネゴシエーション フェーズにイニシエータによって要求された場合、iSCSI の即時データ機能と非請求データ機能をサポートします。即時データは、書き込みコマンドと書き込みデータを 1 つの Protocol Data Unit（PDU; プロトコル データ ユニット）にまとめるなど、iSCSI コマンドの PDU のデータ部分に含まれる iSCSI 書き込みデータのことです。非請求データは、イニシエータがターゲットからの明示的な Ready to Transfer（R2T）PDU の受信を必要とせず、MDS スイッチなどの iSCSI ターゲットに iSCSI データ出力 PDU で送信する iSCSI 書き込みデータのことです。

これら 2 つの機能により、R2T PDU のイニシエータとターゲット間の 1 往復がなくなるため、小さい書き込みコマンドの I/O 時間を短縮できるようになります。iSCSI ターゲットの場合、MDS スイッチは、コマンドあたり最大 64 KB の非請求データを許可します。これは、iSCSI ログイン ネゴシエーション フェーズで FirstBurstLength パラメータによって制御されます。

iSCSI イニシエータが即時データ機能と非請求データ機能をサポートする場合、これらの機能は、MDS スイッチ上で設定の必要なく自動的にイネーブルになります。

# iSCSI インターフェイスの詳細機能

IPS ポートごとに iSCSI インターフェイスの詳細設定オプションを使用できます。これらの設定については、詳細な FCIP 設定と同様で、この該当セクションですでに説明されています。

Cisco MDS スイッチは、iSCSI インターフェイスの次の詳細機能をサポートします。

- 「iSCSI リスナー ポート」（P.4-34）
- 「TCP 調整パラメータ」（P.4-34）
- 「QoS 値の設定」（P.4-35）
- 「iSCSI ルーティング モード」（P.4-35）

## iSCSI リスナー ポート

新規 TCP 接続をリッスンする iSCSI インターフェイスの TCP ポート番号を設定できます。デフォルト ポート番号は 3260 です。TCP ポート番号を変更するとすぐに、iSCSI ポートは、新しく設定されたポート上の TCP 接続だけを受け入れます。

## TCP 調整パラメータ

設定できる TCP パラメータは次のとおりです。

- 最小再送信タイムアウト（詳細については、「最小再送信タイムアウト」（P.2-18）を参照してください）。
- キープアライブ タイムアウト（詳細については、「キープアライブ タイムアウト」（P.2-18）を参照してください）。
- 最大再送信回数（詳細については、「最大再送信数」（P.2-19）を参照してください）。
- Path MTU（詳細については、「Path MTU」（P.2-19）を参照してください）。
- SACK（SACK は、iSCSI TCP 設定でデフォルトでイネーブルです）。
- ウィンドウ管理（iSCSI のデフォルトは、最大帯域幅 1 Gbps、最小使用可能帯域幅 70 Mbps、往復時間 1 ミリ秒です）、（詳細については、「ウィンドウ 管理」（P.2-19）を参照してください）。

- バッファ サイズ（iSCSI のデフォルト送信バッファ サイズは 4096 KB です）、（詳細については、「バッファ サイズ」（P.2-20）を参照してください）。
- ウィンドウ輻輳監視（デフォルトでイネーブルで、デフォルト バースト サイズは 50 KB）、（詳細については、「輻輳の監視」（P.2-19）を参照してください）。
- 最大遅延ジッタ（デフォルトでイネーブルで、デフォルト時間は 500 マイクロ秒です）。

## QoS 値の設定

Fabric Manager を使用して QoS 値を設定する手順は、次のとおりです。

**ステップ 1**　[Switches] を展開し、[Interfaces] を展開して [Physical Attributes] ペインの [FC Logical] を選択します。

[Information] ペインにインターフェイス テーブルが表示されます（図 4-22 を参照）。

**ステップ 2**　Device Manager で [Interface] > [Ethernet and iSCSI] を選択します。

[Ethernet Interfaces and iSCSI] ダイアログボックスが表示されます（図 4-23 を参照）。

**ステップ 3**　Fabric Manager または Device Manager のいずれかで、[iSCSI TCP] タブをクリックします。

iSCSI TCP 設定テーブルが表示されます。

**ステップ 4**　[QoS] フィールドを 1 ～ 6 の範囲で設定します。

**ステップ 5**　Fabric Manager の [Apply Changes] アイコンをクリックするか、Device Manager の [Apply] をクリックして、これらの変更を保存します。

## iSCSI ルーティング モード

Cisco MDS 9000 ファミリのスイッチは、複数の iSCSI ルーティング モードをサポートします。各モードは、さまざまな運用パラメータが調整され、異なるメリットとデメリットを持ちながら、さまざまな使用状況に合わせることができます。

- パススルー モード

  パススルー モードでは、IPS モジュールまたは MPS 14/2 モジュール上のポートがファイバ チャネル ターゲットからの読み取りデータ フレームを変換して、iSCSI ホストにバッファリングせずにフレーム単位で転送します。これは、データ入力フレームを 1 回受信するとすぐに、iSCSI データ入力 PDU として 1 回送信することを指します。

  これと反対の方向では、IPS モジュールまたは MPS 14/2 モジュール上のポートは、iSCSI ホストが送信できる iSCSI 書き込みデータ出力 PDU の最大サイズを、ファイバ チャネル ターゲットで受信可能なサイズとして規定された最大データ サイズに制限します。この結果、iSCSI データ出力 PDU を 1 回受信すると、ファイバ チャネル ターゲットにファイバ チャネル データ フレームが 1 回送信されることになります。

  両方向でのバッファリングを行わないため、転送遅延を小さくするメリットにつながります。ただし、最大データ セグメント長が小さいと、通常は、ホスト システムで処理オーバーヘッドが増加するため、ホストからのデータ転送パフォーマンスが低下します。このモードの別の利点は、iSCSI データ ダイジェストをイネーブルにできることです。これにより、PDU で運ばれる iSCSI データの完全性の保護は、TCP チェックサムで提供される以上に優れたものになります。

- ストア アンド フォワード モード（デフォルト）

  ストア アンド フォワード モードでは、IPS モジュールまたは MPS 14/2 モジュール上のポートが交換のためのすべてのファイバ チャネル データ フレームをアセンブルして、1 つの大きい iSCSI データ入力 PDU に組み立ててから iSCSI クライアントに転送します。

  これと反対の方向では、IPS モジュールまたは MPS 14/2 モジュール上のポートが小さいデータ セグメント サイズをホストに強制しないため、iSCSI ホストは任意のサイズ（最大 256 KB）の iSCSI データ出力 PDU を送信できます。次に、ポートは、PDU を変換または分割してファイバ チャネル フレームをファイバ チャネル ターゲットに転送する前に、iSCSI データ出力 PDU を受信するまで待機します。

  このモードのメリットは、ホストからのデータ転送パフォーマンスが高くなることです。デメリットは、転送遅延が大きくなり、iSCSI データ ダイジェスト（CRC）を使用できないことです。

（注）　ストア アンド フォワード モードは、デフォルトのフォワーディング モードです。

- カットスルー モード

  カットスルー モードは、ストア アンド フォワード モードよりも読み取り動作のパフォーマンスが向上します。IPS モジュールまたは MPS 14/2 モジュール上のポートは、交換が全部完了するのを待たずに受信している間も各ファイバ チャネル データ入力フレームを iSCSI ホストに転送することで、これを実現します。書き込みデータ出力動作に、ストア アンド フォワード モードとの違いはありません。

図 4-31 では、iSCSI ルーティング モードで交換されるメッセージを比較しています。

**図 4-31　iSCSI ルーティング モード**

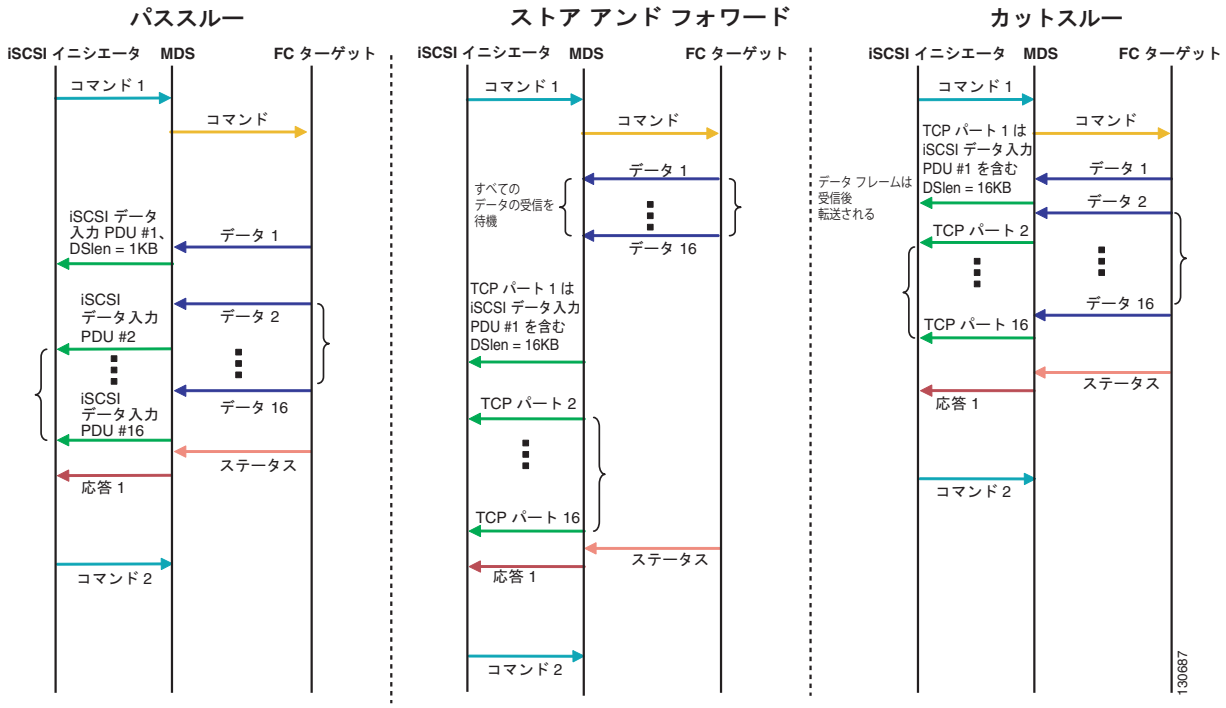


表 4-1 では、iSCSI ルーティング モードの違いによるメリットとデメリットを比較しています。

**表 4-1　iSCSI ルーティング モードの比較**

| モード | メリット | デメリット |
|---|---|---|
| パススルー | 遅延が小さい<br>データ ダイジェストを使用できる | データ転送パフォーマンスが下がる |
| ストア アンド フォワード | データ転送パフォーマンスが上がる | データ ダイジェストを使用できない |
| カットスルー | ストア アンド フォワードよりも読み取りパフォーマンスが向上する | ファイバ チャネル ターゲットが異なるコマンドで相互に置き換えて使用できるように読み取りデータを送信した場合、最初のコマンドのデータは、カットスルー モードで転送されますが、それ以降のコマンドのデータはバッファリングされ、ストア アンド フォワード モードと同じ動作になります。<br>データ ダイジェストを使用できない |

**注意**　iSLB VRRP グループに属している iSCSI インターフェイスのフォワーディング モードを変更すると、インターフェイスのロード バランシングに影響します。「iSCSI インターフェイス パラメータの変更とロード バランシングに対するその影響」（P.4-48）を参照してください。

# iSLB の設定

iSCSI サーバのロード バランシング（iSLB）機能は、数百あるいは数千にも上る数のイニシエータを含む大規模な iSCSI の導入を簡単に設定する手段を提供します。iSLB を使用しない場合、iSCSI の設定には次の作業が必要になります。

- 次の手順を含め、MDS スイッチで複数の設定手順を実行する必要があります。
  - スタティック pWWN および VSAN を使用するイニシエータの設定
  - イニシエータおよびターゲットのゾーン分割設定
  - 任意で、仮想ターゲットの作成およびイニシエータへのアクセス権付与
  - MDS スイッチ上のイニシエータ用に作成されたスタティック pWWN に基づいた、イニシエータに対する、ストレージ システム上でのターゲット LUN のマッピングおよびマスキングの設定
- 複数の MDS スイッチ上で手動で設定を複製する必要があります。
- IPS ポートに対するロード バランシングはありません。例：
  - 仮想ルータ冗長プロトコル（VRRP）がサポートするのはアクティブおよびバックアップだけであり、ロード バランシングはサポートされません。
  - 複数の VRRP グループを使用して、区別されたグループでホストを設定する必要があります。

iSLB には次の機能があります。

- iSLB イニシエータ設定は、イニシエータ ターゲットおよび自動ゾーンのサポートによって簡易化されます。

- Cisco Fabric Service（CFS）により、ファブリック内のすべての MDS スイッチ間で iSLB イニシエータ設定を配信する手動による設定の必要性がなくなります。

（注）　スタティック マッピングされた iSLB イニシエータ設定だけが、CFS を使用するファブリック全体で配信されます。ダイナミック マッピングおよびスタティック マッピングされた iSCSI イニシエータ設定は配信されません。

- iSLB イニシエータのダイナミック ロード バランシングは、iSCSI ログイン リダイレクトおよび VRRP を使用して利用できます。

ここでは、次の内容について説明します。



（注）　iSLB を設定する前に、iSCSI をイネーブルにする必要があります（「iSCSI のイネーブル化」（P.4-5）を参照）。

（注）　iSLB の場合、ファブリック内のすべてのスイッチで Cisco MDS SAN-OS リリース 2.1(1a) 以降を実行する必要があります。

# iSLB 設定制限の概要

iSLB 設定には次の制限があります。

- 1 つのファブリック内でサポートされる iSLB イニシエータおよび iSCSI イニシエータの最大数は 2000 です。
- トランスペアレント イニシエータ モードまたはプロキシ イニシエータ モードの IPS ポートでサポートされる iSLB セッションおよび iSCSI セッションの最大数は 500 です。
- 1 つのファブリック内でサポートされる iSLB イニシエータの最大数は、2000 です。
- トランスペアレント イニシエータ モードまたはプロキシ イニシエータ モードの IPS ポートあたりの iSLB セッションの最大数は、500 です。
- CFS 配信がイネーブルに設定された iSLB を備えることができるファブリック内のスイッチの最大数は 4 です。
- 200 を超える新規 iSLB イニシエータを保留設定に追加できません。それ以上のイニシエータを追加する前に、設定を確定する必要があります。

- 実行コンフィギュレーションに 200 を超える iSLB イニシエータを含む場合は、iSCSI をディセーブルにできません。iSLB イニシエータの数を 200 よりも少なくしてから iSCSI をディセーブルにします。
- CFS 配信を設定しなくても iSLB を使用できますが、iSLB 自動ゾーン機能を使用する場合は、いずれかのゾーンセットがアクティブになるとトラフィックが中断されます。
- Inter-VSAN Routing（IVR）および iSLB の機能が同じファブリック内でイネーブルになっている場合、ファブリック内にこれらの機能がどちらもイネーブルになっているスイッチが少なくとも 1 つ必要です。ゾーン分割関連の設定とアクティベーション（通常ゾーン用、IVR ゾーン用、または iSLB ゾーン用）をこのスイッチ上で実行する必要があります。このようにしないと、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。

# iSLB 設定の前提条件

iSLB を設定する前に次の前提条件の処理を実行します。

- iSCSI のイネーブル化（詳細については、「iSCSI のイネーブル化」（P.4-5）を参照してください）。
- ギガビット イーサネット インターフェイスの設定（「IPv4 の基本的なギガビット イーサネットの設定」（P.7-2）を参照）。
- VRRP グループの設定（「VRRP を使用するロード バランシングの設定」（P.4-49）を参照）。
- ゾーン セットの設定とアクティブ化（詳細については、『*Cisco Fabric Manager Fabric Configuration Guide*』を参照してください）。
- iSLB の CFS 配信のイネーブル化（「iSLB 設定配信のイネーブル化」（P.4-51）を参照）。

# iSLB イニシエータの概要

iSLB イニシエータには、iSCSI イニシエータでサポートされる機能の他に次の機能があります。

- iSLB イニシエータは、iSLB 仮想ターゲットもサポートします。これらのターゲットは、iSCSI 仮想ターゲットと非常に類似しています。アドバタイズ インターフェイス オプションがない例外はありますが、結果的には CFS を使用して配信できます。
- イニシエータ ターゲット：これらのターゲットを特定のイニシエータに設定します。
- iSCSI ログイン リダイレクトおよび VRRP を使用するロード バランシング：ロード バランシングがイネーブルの場合、IPS Manager は、インターフェイスごとに計算した負荷に基づく最適なインターフェイスへ着信セッションをリダイレクトします。
- CFS を使用した他のスイッチへの配信の設定

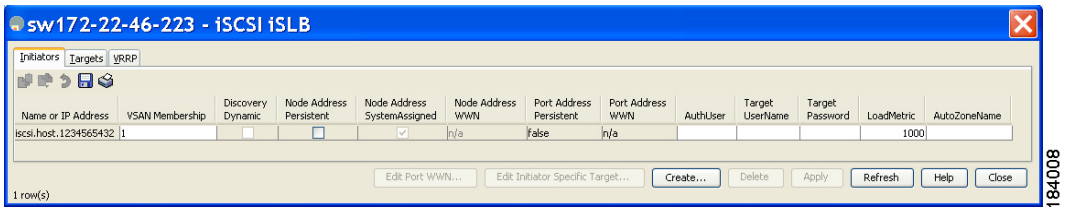
# Device Manager を使用した iSLB の設定

Device Manager を使用して iSLB を設定する手順は、次のとおりです。

**ステップ 1**　[IP] > [iSCSI iSLB] を選択します。

[iSCSI iSLB] ダイアログボックスが表示されます（図 4-32 を参照）。

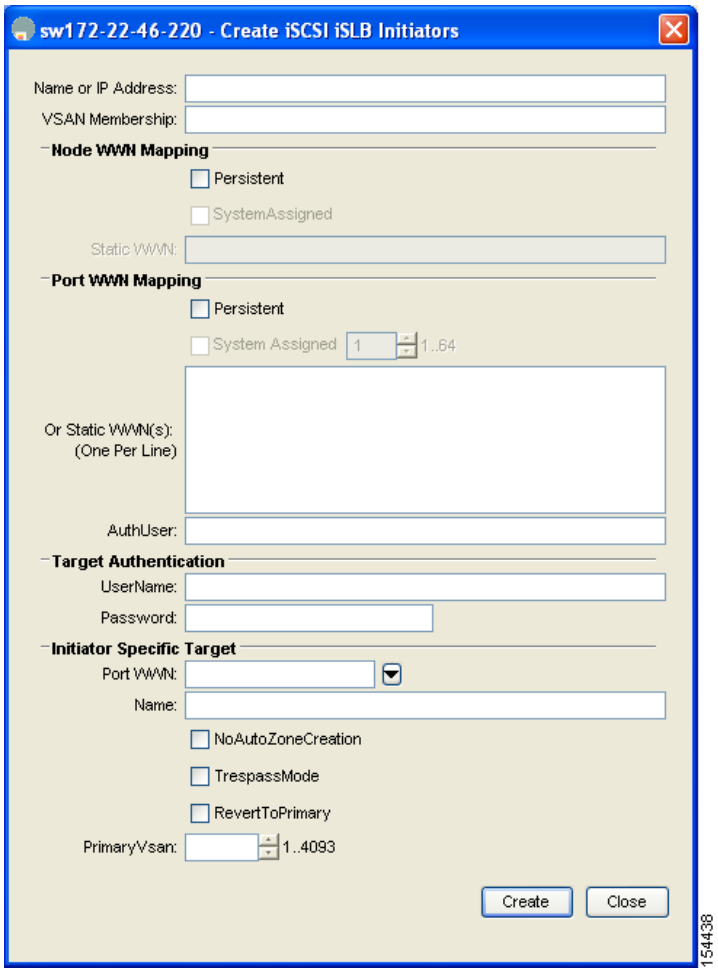
図 4-32　[iSCSI iSLB] ダイアログボックス




ステップ 2　[Create] をクリックして新しい iSCSI iSLB イニシエータを作成します。

[Create iSCSI iSLB Initiators] ダイアログボックスが表示されます（図 4-33 を参照）。

図 4-33　[Create iSCSI iSLB Initiators] ダイアログボックス




ステップ 3　[Name or IP Address] フィールドに iSLB 名または IP アドレスを設定します。

ステップ 4　[VSAN Membership] フィールドに iSLB イニシエータを参加させる VSAN を設定します。

「iSLB イニシエータの VSAN メンバシップの割り当て」（P.4-43）も参照してください。

**ステップ 5**　iSLB イニシエータのダイナミック nWWN をスタティックに変換する場合は、[Persistent] チェックボックスをオンにします。

「ダイナミック iSLB イニシエータの WWN マッピングをスタティックにする」（P.4-42）も参照してください。

**ステップ 6**　（任意）スイッチで nWWN を割り当てるようにする場合は、[SystemAssigned] チェックボックスをオンにします。

**ステップ 7**　（任意）手動でスタティック nWWN を割り当てる場合は [Static WWN] フィールドを設定します。この nWWN に対して固有の割り当てになるようにする必要があります。

**ステップ 8**　（任意）iSLB イニシエータのダイナミック pWWN をスタティックに変換する場合は、[Port WWN Mapping] の [Persistent] チェックボックスをオンにします。

「ダイナミック iSLB イニシエータの WWN マッピングをスタティックにする」（P.4-42）を参照してください。

**ステップ 9**　（任意）[SystemAssigned] チェックボックスをオンにして、スイッチで割り当てるようにする pWWN の数を設定します。

**ステップ 10**　（任意）手動でスタティック pWWN を割り当てる場合は、[Static WWN(s)] フィールドを設定します。

これらの pWWN に対して固有の割り当てになるようにする必要があります。

**ステップ 11**　（任意）iSLB 認証用に iSLB イニシエータに限定するユーザ名を設定する場合は、[AuthUser] フィールドを設定します。

「iSLB イニシエータ認証の制約」（P.4-46）も参照してください。

**ステップ 12**　iSLB イニシエータ ターゲットの CHAP 認証を設定する場合は、[Username] フィールドと [Password] フィールドを入力します。

「iSLB セッション認証の設定」（P.4-45）も参照してください。

**ステップ 13**　[Initiator Specific Target] セクションでは、iSLB イニシエータ ターゲットを設定する pWWN を設定します。

**ステップ 14**　（任意）[Name] フィールドにグローバルな固有識別情報（IQN）を設定します。

**ステップ 15**　（任意）自動ゾーン分割をディセーブルにする場合は、[NoAutoZoneCreation] チェックボックスをオンにします。

「iSLB のイニシエータおよびイニシエータ ターゲットのゾーンの設定とアクティブ化」（P.4-45）も参照してください。

**ステップ 16**　（任意）[TresspassMode] チェックボックスをオンにします。

「ストレージ ポート フェールオーバーの LUN trespass」（P.4-56）も参照してください。

**ステップ 17**　（任意）HA フェールオーバーの後、プライマリ ポートが再びアップになったときにプライマリ ポートに戻す場合は、[RevertToPrimary] チェックボックスをオンにします。

**ステップ 18**　[PrimaryVsan] を iSLB イニシエータ ターゲットの VSAN に設定します。

**ステップ 19**　[Create] をクリックして、この iSLB イニシエータを作成します。

**ステップ 20**　CFS がイネーブルの場合、[CFS] ドロップダウン メニューから [commit] を選択します。

# iSLB イニシエータの設定

ここで説明する内容は、次のとおりです。



## WWN の iSLB イニシエータへの割り当て

iSLB ホストは、次のメカニズムのいずれかを使用して N ポートの WWN にマッピングされます。

- ダイナミック マッピング（デフォルト）
- スタティック マッピング

**（注）** iSLB イニシエータの WWN を割り当てる方法は、iSCSI イニシエータの場合と同様です。ダイナミック マッピングおよびスタティック マッピングの詳細については、「iSCSI イニシエータの WWN の割り当て」（P.4-19）を参照してください。

**ヒント** [SystemAssign] オプションを使用することを推奨します。手動で WWN を割り当てる場合は、それが固有の割り当てになるようにする必要があります（詳細については、『*Cisco Fabric Manager Fabric Configuration* Guide』を参照してください）。すでに割り当てられている WWN は使用しないでください。

「Device Manager を使用した iSLB の設定」の手順（P.4-39）を参照してください。

## ダイナミック iSLB イニシエータの WWN マッピングをスタティックにする

ダイナミック iSLB イニシエータがログインした後、このイニシエータで次回のログイン時に同じマッピングを使用できるように、自動的に割り当てられた nWWN/pWWN マッピングを永続的に保持するかどうかを判断できます（「ダイナミック マッピング」（P.4-10）を参照）。

ダイナミック iSLB イニシエータをスタティック iSLB イニシエータに変換して、その WWN を永続的に使用することができます。

**（注）** iSLB イニシエータのダイナミック マッピングをスタティックにする方法は、iSCSI の場合と同様です。「ダイナミック iSLB イニシエータの WWN マッピングをスタティックにする」（P.4-42）を参照してください。

（注）　スタティック マッピングされた iSLB イニシエータ設定だけが、CFS を使用するファブリック全体で配信されます。動的および静的に設定された iSCSI イニシエータ設定は配信されません。

「Device Manager を使用した iSLB の設定」の手順（P.4-39）を参照してください。

## iSLB イニシエータの VSAN メンバシップの割り当て

特定の VSAN に参加するように個々の iSLB ホストを設定できます（ファイバ チャネルの Dynamic Port VSAN Membership [DPVM] 機能と同様です。詳細については、『Cisco Fabric Manager Fabric Configuration Guide』を参照してください）。指定された VSAN は、iSCSI インターフェイスの VSAN メンバシップを上書きします。

（注）　iSLB イニシエータの VSAN を指定する方法は、iSCSI イニシエータの場合と同様です。「iSCSI の VSAN メンバシップ」（P.4-24）を参照してください。

（注）　他の VSAN（デフォルト VSAN である VSAN 1 以外）、たとえば VSAN 2 に iSLB イニシエータを設定すると、そのイニシエータは VSAN 1 から自動的に削除されます。このイニシエータを VSAN 1 にも存在させる場合は、VSAN 1 でイニシエータを明示的に設定する必要があります。

「Device Manager を使用した iSLB の設定」の手順（P.4-39）を参照してください。

## ロード バランシングのメトリックの設定

ロード バランシングの重み付けのために、イニシエータごとに負荷メトリックを割り当てることができます。計算された負荷は、特定の iSCSI インターフェイス上にあるイニシエータの数に基づいています。この機能には、さまざまな帯域幅の要求を持つイニシエータに対応します。たとえば、Web サーバよりもデータベース サーバに大きい負荷メトリックを割り当てることができます。重み付けされたロード バランシングもまた、さまざまなリンク速度のイニシエータに対応します。

ロード バランシングの詳細については、「VRRP を使用するロード バランシングの概要」（P.4-46）を参照してください。

Device Manager で [IP] > [iSCSI iSLB] を選択し、[LoadMetric] フィールドを設定して iSLB イニシエータのロード バランシング メトリックを変更します。

「Device Manager を使用した iSLB の設定」の手順（P.4-39）を参照してください。

## iSLB イニシエータ ターゲットの設定

デバイス エイリアスまたは pWWN を使用して、イニシエータ ターゲットを設定できます。必要に応じて、次のオプション パラメータを 1 つ以上指定することもできます。

- セカンダリ pWWN
- セカンダリ デバイス エイリアス
- LUN マッピング
- IQN
- VSAN ID

（注）　ターゲットがオンラインの場合、VSAN ID は省略可能です。ターゲットがオンラインではない場合、VSAN ID は必須です。

さらに、自動ゾーン分割をディセーブルにすることができます。

イニシエータ ターゲットの IQN を設定した場合、その名前を使用してイニシエータ ターゲットを識別します。設定していない場合は、イニシエータ ターゲットに固有の IQN が生成されます。

Device Manager を使用して追加の iSLB イニシエータ ターゲットを設定する手順は、次のとおりです。

**ステップ 1**　[IP] > [iSCSI iSLB] を選択します。

[iSCSI iSLB] ダイアログボックスが表示されます（図 4-32 を参照）。

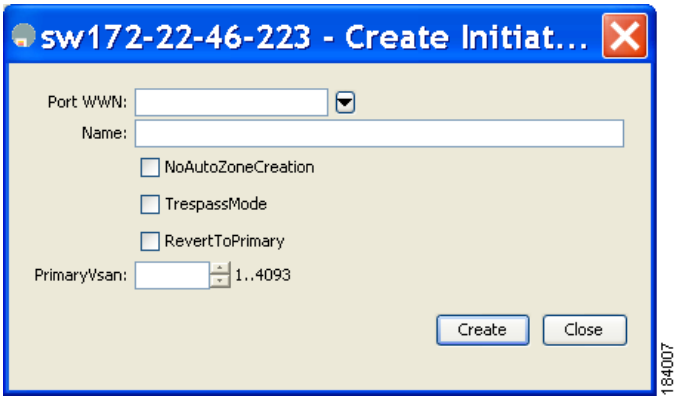
**ステップ 2**　ターゲットを追加するイニシエータをクリックして、[Edit Initiator Specific Targets] をクリックします。

[Initiator Specific Target] ダイアログボックスが表示されます。

**ステップ 3**　[Create] をクリックして新規イニシエータ ターゲットを作成します。

[Create Initiator Specific Target] ダイアログボックスが表示されます（図 4-34 を参照）。

**図 4-34　[Create Initiator Specific Target] ダイアログボックス**




**ステップ 4**　[Port WWN] フィールドにイニシエータ ターゲットの pWWN を入力します。

**ステップ 5**　（任意）[Name] フィールドにグローバルな固有識別情報（IQN）を設定します。

**ステップ 6**　（任意）自動ゾーン分割をディセーブルにする場合は、[NoAutoZoneCreation] チェックボックスをオンにします（図 4-33 を参照）。「iSLB のイニシエータおよびイニシエータ ターゲットのゾーンの設定とアクティブ化」（P.4-45）を参照してください。

**ステップ 7**　（任意）[TresspassMode] チェックボックスをオンにします。「ストレージ ポート フェールオーバーの LUN trespass」（P.4-56）を参照してください。

**ステップ 8**　（任意）HA フェールオーバーの後、プライマリ ポートが再びアップになったときにプライマリ ポートに戻す場合は、[RevertToPrimary] チェックボックスをオンにします。

**ステップ 9**　[PrimaryVsan] を iSLB イニシエータ ターゲットの VSAN に設定します。

**ステップ 10**　[Create] をクリックして、この iSLB イニシエータ ターゲットを作成します。

**ステップ 11**　CFS がイネーブルの場合、[CFS] ドロップダウン メニューから [commit] を選択します。

## iSLB のイニシエータおよびイニシエータ ターゲットのゾーンの設定とアクティブ化

iSLB のイニシエータおよびイニシエータ ターゲットの追加時にゾーン名を設定できます。ゾーン名を指定しない場合、IPS Manager によって動的にゾーン名が作成されます。iSLB ゾーン セットには次の考慮事項があります。

- イニシエータ ターゲットが設定されているイニシエータの自動ゾーン分割は、デフォルトでイネーブルです。
- VSAN 内に自動ゾーンを作成する場合は、ゾーン セットがその VSAN 内でアクティブである必要があります。
- 別のゾーン セットのアクティブ化の処理中の場合、またはゾーン分割データベースがロックされている場合は、iSLB ゾーン セットのアクティブ化に失敗する場合があります。失敗した場合は、iSLB ゾーン セットのアクティブ化を再試行してください。この問題を回避するには、一度に実行するゾーン分割に関する操作（通常ゾーン、IVR ゾーンまたは iSLB ゾーン）はいずれか 1 つだけにします。
- ゾーン セットがアクティブ化されたときに、そのゾーン セット内に 1 つ以上の変更がある場合、自動ゾーンが作成されます。自動ゾーンだけが変更された場合、アクティブ化は無効です。

**注意**　IVR および iSLB が同じファブリック内でイネーブルになっている場合、ファブリック内で少なくとも 1 つのスイッチで両方の機能がイネーブルになっている必要があります。ゾーン分割関連の設定とアクティベーション操作（通常ゾーン用、IVR ゾーン用、または iSLB ゾーン用）をこのスイッチ上で実行する必要があります。このようにしないと、ファブリック内でトラフィックが中断される可能性があります。

Device Manager で [IP] > [iSCSI iSLB] を選択し、[autoZoneName] フィールドを設定して iSLB イニシエータの自動ゾーン名を変更します。

「Device Manager を使用した iSLB の設定」の手順（P.4-39）を参照してください。

## iSLB セッション認証の設定

IPS モジュールまたは MPS-14/2 モジュールは、ストレージへのアクセスを要求する iSLB ホストを認証するための iSLB 認証メカニズムをサポートします。デフォルトでは、IPS モジュールおよび MPS-14/2 モジュールは、iSCSI イニシエータの CHAP 認証または None 認証を許可します。認証を常に使用する場合は、CHAP 認証だけを許可するようにスイッチを設定する必要があります。

CHAP ユーザ名または CHAP シークレットの検証には、Cisco MDS AAA インフラストラクチャでサポートされ許可されている方法であれば任意に使用できます（詳細については、『*Cisco Fabric Manager Security Configuration Guide*』を参照してください）。AAA 認証は、RADIUS、TACACS+、またはローカル認証デバイスをサポートします。

**（注）**　iSLB セッション認証を指定する方法は、iSCSI の場合と同様です。「iSCSI セッション認証」（P.4-30）を参照してください。

### iSLB イニシエータ認証の制約

デフォルトでは、iSLB イニシエータは、IPS モジュールまたは MPS-14/2 モジュールに対して自身を認証する際に、RADIUS またはローカル AAA データベースの任意のユーザ名を使用できます（CHAP ユーザ名は、iSLB イニシエータ名とは関係ありません）。IPS モジュールまたは MPS-14/2 モジュールは、スイッチから送信される CHAP 認証確認に正しい応答を返している間は、イニシエータのログインを許可します。これは、CHAP ユーザ名およびパスワードが 1 つでも侵害されると問題に発展する可能性があります。

Device Manager で [IP] > [iSCSI iSLB] を選択し、[AuthName] フィールドを設定してイニシエータが CHAP 認証に特定のユーザ名を使用するように制限します。

「Device Manager を使用した iSLB の設定」の手順（P.4-39）を参照してください。

### 相互 CHAP 認証

iSLB イニシエータの IPS モジュールまたは MPS-14/2 モジュールの認証の他にも、IPS モジュールまたは MPS-14/2 モジュールは、iSCSI のログイン フェーズで Cisco MDS スイッチのイニシエータ ターゲットを iSLB イニシエータが認証するメカニズムをサポートします。この認証では、iSLB イニシエータに対して示すスイッチのユーザ名とパスワードをユーザが設定する必要があります。指定されたパスワードを使用して、イニシエータが IPS ポートに送信する CHAP 認証確認に対する CHAP 応答を計算します。

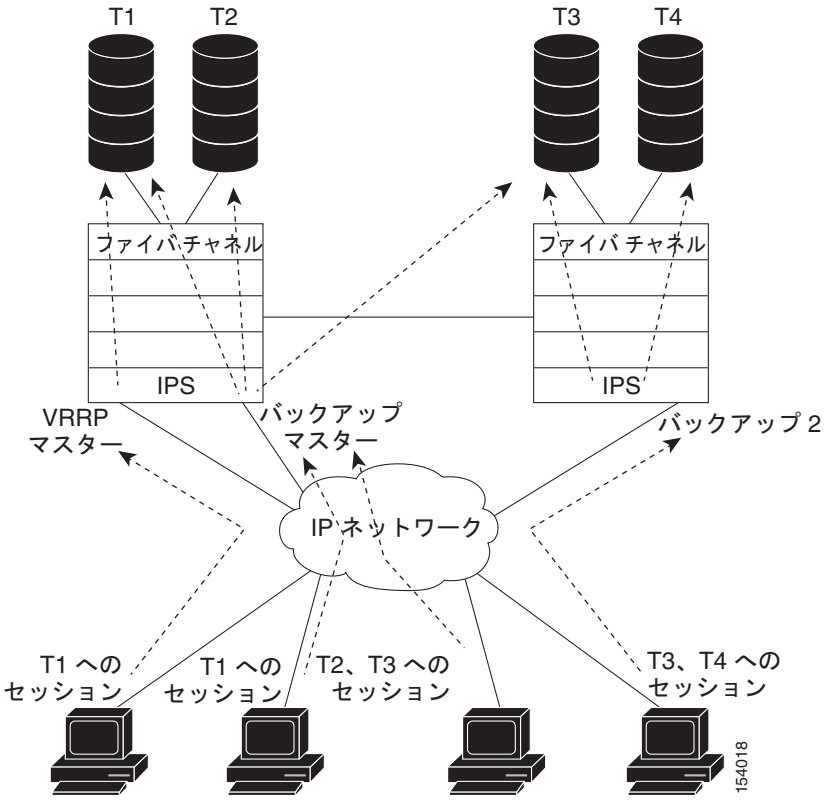
Device Manager で [IP] > [iSCSI iSLB] を選択し、[Target Username] フィールドと [Target Password] フィールドを設定して、イニシエータに対するスイッチの認証のために、そのスイッチで使用するイニシエータごとのユーザ名とパスワードを設定します。

「Device Manager を使用した iSLB の設定」の手順（P.4-39）を参照してください。

## VRRP を使用するロード バランシングの概要

仮想ルータ冗長プロトコル（VRRP）ロード バランシングを iSLB に設定できます。図 4-35 に、iSLB を使用するロード バランシングの例を示します。

図 4-35　iSLB イニシエータのロード バランシングの例




ポータル アドレスとして VRRP アドレスを指定してホストが設定されています。VRRP マスター ポートがイニシエータから最初の iSCSI セッションを受信すると、その特定ホストを提供するバックアップ ポートを割り当てます。マスター ポートに障害が発生した際に復旧が必要な場合、CFS を使用してこの情報がすべてのスイッチに同期されます。イニシエータは、一時的にリダイレクトされた iSCSI ログイン応答を受け取ります。次に、ホストがその物理 IP アドレスでバックアップ ポートにログインします。バックアップ ポートがダウンすると、ホストはマスター ポートに戻ります。マスター ポートは CFS により、バックアップ ポートがダウンしていることを認識し、ホストを別のバックアップ ポートにリダイレクトします。

（注）　イーサネット PortChannel が IPS モジュールとイーサネット スイッチ間に設定されている場合、VRRP を設定したロード バランシングを正常に動作させるためには、イーサネット スイッチ上のロード バランシング ポリシーは、ポート番号ではなく、送信元および宛先 IP アドレスだけに基づいている必要があります。

（注）　イニシエータをマスター インターフェイスの物理 IP アドレスにリダイレクトすることもできます。

**ヒント**　iSLB VRRP ロード バランシングは、セッション数ではなく、iSLB イニシエータの数に基づいています。他の iSLB イニシエータよりも設定されているターゲットの数が多い（結果としてセッション数の多い）iSLB イニシエータは、より大きい負荷メトリックを指定して設定する必要があります。たとえば、ターゲットの多い iSLB イニシエータの負荷メトリックを、デフォルト値の 1000 から 3000 に増やすことができます。

**注意**　リダイレクトされたセッションが VRRP IP アドレスや VRRP グループに関する情報を運ばないため、iSLB に設定されたギガビット イーサネット インターフェイスが所属できる VRRP グループは 1 つだけです。この制約により、スレーブ ポートが属する VRRP グループを一意に識別できます。

## iSCSI インターフェイス パラメータの変更とロード バランシングに対するその影響

ロード バランシングがイネーブルにされている VRRP グループのすべての iSCSI インターフェイスは、インターフェイスの VSAN、認証、プロキシ イニシエータ モード、およびフォワーディング モードがすべて同じである必要があります。VRRP グループの iSCSI インターフェイスのこれらのパラメータのうちいずれでも変更が必要な場合は、一度に変更するインターフェイスは 1 つにする必要があります。VRRP グループ内でパラメータを変更したインターフェイスと変更していないインターフェイスが混在する移行期間、マスター ポートは新しいイニシエータをリダイレクトしない代わりにローカルで処理します。

**注意**　VRRP グループ内の iSCSI インターフェイスの VSAN、プロキシ イニシエータ、認証、および フォワーディング モードを変更すると、セッションが何度もダウン状態になる可能性があります。

## ギガビット イーサネット インターフェイス選択のための VRRP ロード バランシング アルゴリズム

VRRP マスターが iSCSI セッション要求をイニシエータから受信すると、最初にその VRRP グループ内の 1 つのインターフェイスに対して既存のマッピングをチェックします。そのマッピングが存在する場合、VRRP マスターはイニシエータをそのインターフェイスにリダイレクトします。そのマッピングが存在しない場合、VRRP マスターは、最も負荷の小さいインターフェイスを選択し、選択したインターフェイスの負荷をイニシエータの iSLB メトリック（重み）で更新します。

**（注）**　VRRP マスター インターフェイスは特別に扱い、他のインターフェイスに比べて小さい負荷で済むようにする必要があります。これは、すべてのセッションに対してマスター インターフェイスが実行するリダイレクト処理のためです。新規イニシエータは、次の式が他のすべてのインターフェイスで真となる場合にだけ、マスター インターフェイスに割り当てられます。

VRRP バックアップ インターフェイスの負荷 > [2 * VRRP マスター インターフェイスの負荷 + 1]

# VRRP を使用するロード バランシングの設定

最初に IP ネットワークに接続するスイッチ上のギガビット イーサネット インターフェイスで VRRP を設定してから、iSLB の VRRP を設定する必要があります。ギガビット イーサネット インターフェイス上での VRRP の設定方法については、「仮想ルータ冗長プロトコル」（P.5-11）を参照してください。

Device Manager を使用して VRRP ロード バランシングを設定する手順は、次のとおりです。

**ステップ 1**　[IP] > [iSCSI iSLB] を選択します。

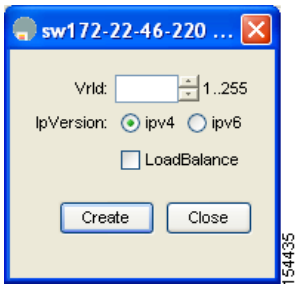
[iSCSI iSLB] ダイアログボックスが表示されます（図 4-32 を参照）。

**ステップ 2**　[VRRP] タブをクリックします。

**ステップ 3**　[Create] をクリックして iSLB イニシエータの VRRP ロード バランシングを設定します。

[Create iSCSI iSLB VRRP] ダイアログボックスが表示されます（図 4-36 を参照）。

**図 4-36　[Create iSCSI iSLB VRRP] ダイアログボックス**




**ステップ 4**　[Vrld] に VRRP グループ番号を設定します。

**ステップ 5**　[ipv4] または [ipv6] を選択して [LoadBalance] チェックボックスをオンにします。

**ステップ 6**　[Create] をクリックしてロード バランシングをイネーブルにします。

**ステップ 7**　CFS がイネーブルの場合、[CFS] ドロップダウン メニューから [commit] を選択します。

# CFS を使用した iSLB 設定配信の概要

MDS スイッチ上の iSLB のイニシエータおよびイニシエータ ターゲットの設定は、Cisco Fabric Service（CFS）を使用して配信できます。この機能により、1 つの MDS スイッチのコンソールからファブリック内で iSLB 設定を同期できます。iSCSI イニシエータのアイドル タイムアウト、iSCSI ダイナミック イニシエータ モード、およびグローバル認証のパラメータも配信されます。CFS 配信はデフォルトでディセーブルです（詳細については、『*Cisco Fabric Manager System Management Configuration Guide*』を参照してください）。

配信をイネーブルにした後、最初の設定を行ったときに暗黙的なセッションが開始されます。それ以降入力されたすべてのサーバ設定変更は、一時データベースに保管され、そのデータベースが明示的に確定されると、ファブリック内の（発信元スイッチを含む）すべてのスイッチに適用されます。

iSLB で CFS をイネーブルにすると、最初の iSLB 設定操作を行ったときに、CFS セッションが開始され、ファブリック内の iSLB 設定がロックされます。設定変更は、保留中の設定データベースに適用されます。ファブリックに対して変更を行うと、保留中の設定がファブリック内のすべてのスイッチに配信されます。そして、各スイッチが設定を確認します。この確認では次の内容が保証されます。

- iSLB イニシエータに割り当てられた VSAN がすべてのスイッチ上で設定されていること。
- iSLB イニシエータに設定されたスタティック WWN が固有であり、すべてのスイッチで使用できること。
- iSLB イニシエータ ノード名がすべてのスイッチ上の iSCSI イニシエータと競合しないこと。

確認が正常に完了すると、すべてのスイッチが保留中の設定を実行コンフィギュレーションに確定します。確認ができないものがある場合は、すべての確定に失敗します。

**（注）** iSLB は、CFS がイネーブルの場合にだけサポートされます。CFS モードをイネーブルにせずに iSLB 自動ゾーン分割を使用すると、いずれかのゾーン セットがアクティブになったときにトラフィックが中断する可能性があります。

**（注）** CFS は、非 iSLB イニシエータの設定を配信することも、ファイバ チャネル ターゲットの設定をインポートすることもありません。

非 iSLB 仮想ターゲットは、アドバタイズ対象インターフェイス オプションを引き続きサポートします。

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

# CFS を使用した iSLB 設定の配信

ここで説明する内容は、次のとおりです。

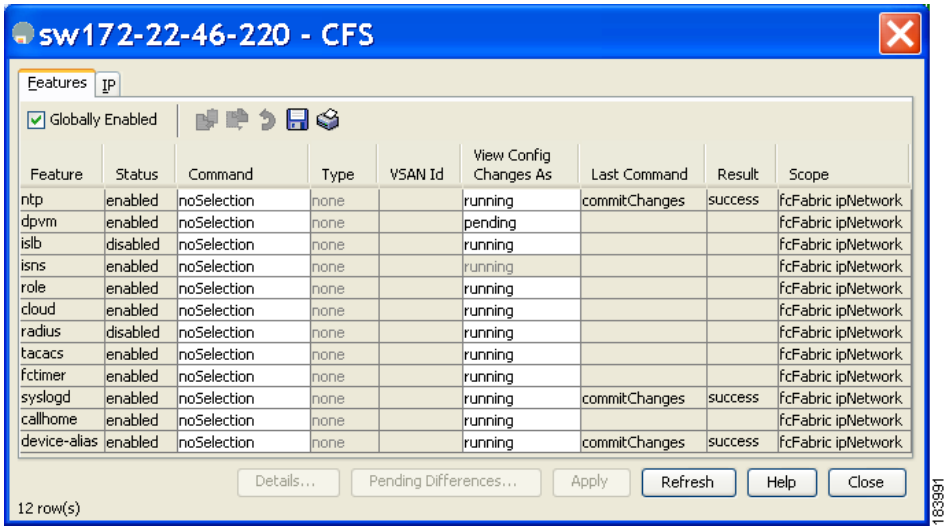
## iSLB 設定配信のイネーブル化

Device Manager を使用して iSLB 設定の CFS 配信をイネーブルにする手順は、次のとおりです。

**ステップ 1**　[Admin] > [CFS] を選択します。

[CFS] ダイアログボックスが表示されます（図 4-37 を参照）。

**図 4-37　Device Manager の CFS のイネーブル化**




**ステップ 2**　iSLB 機能の [Command] フィールドを [enable] に設定します。

**ステップ 3**　[Apply] をクリックして、この変更を保存します。

## ファブリックのロック

既存の設定を変更する最初の処理により、保留設定が作成されてファブリックの機能がロックされます。ファブリックがロックされると、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。
- アクティブな設定をコピーすると、保留設定が作成されます。これ以後の変更は保留設定に対して行われ、アクティブな設定（およびファブリック内の他のスイッチ）に変更をコミットするか、または変更を廃棄するまで、保留設定にとどまります。

**（注）**　iSLB CFS セッションがアクティブの場合、iSCSI 設定を変更することはできません。

## ファブリックに対する変更の確定

保留中の iSLB 設定の変更をアクティブな設定およびファブリック内の他の MDS スイッチに適用するには、変更を確定する必要があります。保留中の設定変更が配信され、正常に確定された時点で、設定変更がファブリック全体の MDS スイッチのアクティブな設定に適用され、自動ゾーンのアクティブ化とファブリックのロック解除が実行されます。

ファブリック内の他の MDS スイッチに iSLB の設定変更を確定するために、Device Manager を使用して、iSLB 自動ゾーンをアクティブにしてファブリックのロックを解除する手順は、次のとおりです。

**ステップ 1**　[Admin] > [CFS] を選択します。

[CFS Configuration] ダイアログボックスが表示されます（図 4-37 を参照）。

**ステップ 2**　iSLB 機能の [Command] フィールドを [commit] に設定します。

**ステップ 3**　[Apply] をクリックして、この変更を保存します。

## 保留中の変更の廃棄

iSLB 設定に対する保留中の変更をいつでも廃棄し、ファブリックのロックを解除できます。この処理は、ファブリック内のスイッチのアクティブな設定に対しては何の作用もありません。

Device Manager を使用して保留中の iSLB 設定変更を廃棄し、ファブリックのロックを解除する手順は次のとおりです。

**ステップ 1**　[Admin] > [CFS] を選択します。

[CFS Configuration] ダイアログボックスが表示されます（図 4-37 を参照）。

**ステップ 2**　iSLB 機能の [Command] フィールドを [abort] に設定します。

**ステップ 3**　[Apply] をクリックして、この変更を保存します。

## ファブリックのロックの解除

iSLB 設定タスクを実行し、変更の確定か廃棄を行ってロックを解除していない場合、管理者はファブリック内のスイッチからロックを解除できます。管理者がこのタスクを実行すると、保留中の変更は廃棄され、ファブリックのロックは解除されます。

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

Device Manager を使用してファブリックのロックを解除する手順は、次のとおりです。

**ステップ 1**　[Admin] > [CFS] を選択します。

[CFS Configuration] ダイアログボックスが表示されます（図 4-37 を参照）。

**ステップ 2**　iSLB 機能の [Command] フィールドを [clear] に設定します。

**ステップ 3**　[Apply] をクリックして、この変更を保存します。

## CFS マージ プロセス

2 つのファブリックがマージされると、CFS は両方のファブリックの iSLB 設定のマージを試行します。一方のファブリック内の指定スイッチ（*上位スイッチ*と呼ぶ）がその iSLB 設定を、もう一方のファブリック内の指定スイッチ（*下位スイッチ*と呼ぶ）に送信します。下位スイッチは、受信した設定と自身の実行コンフィギュレーションを比較して、矛盾がないか確認します。矛盾が検出されなかった場合は、2 つの設定をマージして、それを両方のファブリック内のすべてのスイッチに送信します。そして、各スイッチが設定を確認します。この確認では次の内容が保証されます。

- iSLB イニシエータに割り当てられた VSAN がすべてのスイッチ上で設定されていること。
- iSLB イニシエータに設定されたスタティック WWN が固有であり、すべてのスイッチで使用できること。
- iSLB イニシエータ ノード名にすべてのスイッチ上の iSCSI イニシエータとの競合がないこと。

この確認が正常に完了すると、下位スイッチはすべてのスイッチに、マージされた設定を実行コンフィギュレーションに確定するように指示します。確認ができないものがある場合は、マージに失敗します。

## iSLB CFS マージ ステータスの矛盾

マージで矛盾が発生する場合があります。マージで次の矛盾が発生した場合はユーザの介入が必要です。

- iSCSI グローバル認証または iSCSI イニシエータのアイドル タイムアウトのパラメータは、2 つのファブリックで同じ値には設定されていません。
- 同一の iSLB イニシエータは、2 つのファブリックで別々に設定されています。
- 一方のファブリックの iSLB イニシエータは、もう一方のファブリックの iSCSI イニシエータと同じ名前を持ちます。
- 2 つのファブリックには重複する pWWN/nWWN 設定が見つかります。たとえば、一方のファブリックの iSLB イニシエータに設定された pWWN/nWWN は、もう一方のファブリックの iSCSI イニシエータまたは別の iSLB イニシエータに設定されています。
- 一方のファブリックの iSLB イニシエータに設定された VSAN は、もう一方のファブリックには存在しません。

**ヒント**　マージの矛盾に関する詳細は syslog を確認してください。

同一 iSLB イニシエータが矛盾していない別のセットのイニシエータ ターゲットを持つ場合は、ユーザの介入は必要ありません。マージされた設定は、すべてのイニシエータ ターゲットの和集合になります。

# iSCSI ハイ アベイラビリティ

iSCSI 設定には、次のハイ アベイラビリティ機能を使用できます。

- 「透過的なターゲット フェールオーバー」（P.4-54）
- 「同一 IP ネットワークに接続された複数の IPS ポート」（P.4-57）
- 「VRRP ベースのハイ アベイラビリティ」（P.4-59）
- 「イーサネット PortChannel ベースのハイ アベイラビリティ」（P.4-60）

# 透過的なターゲット フェールオーバー

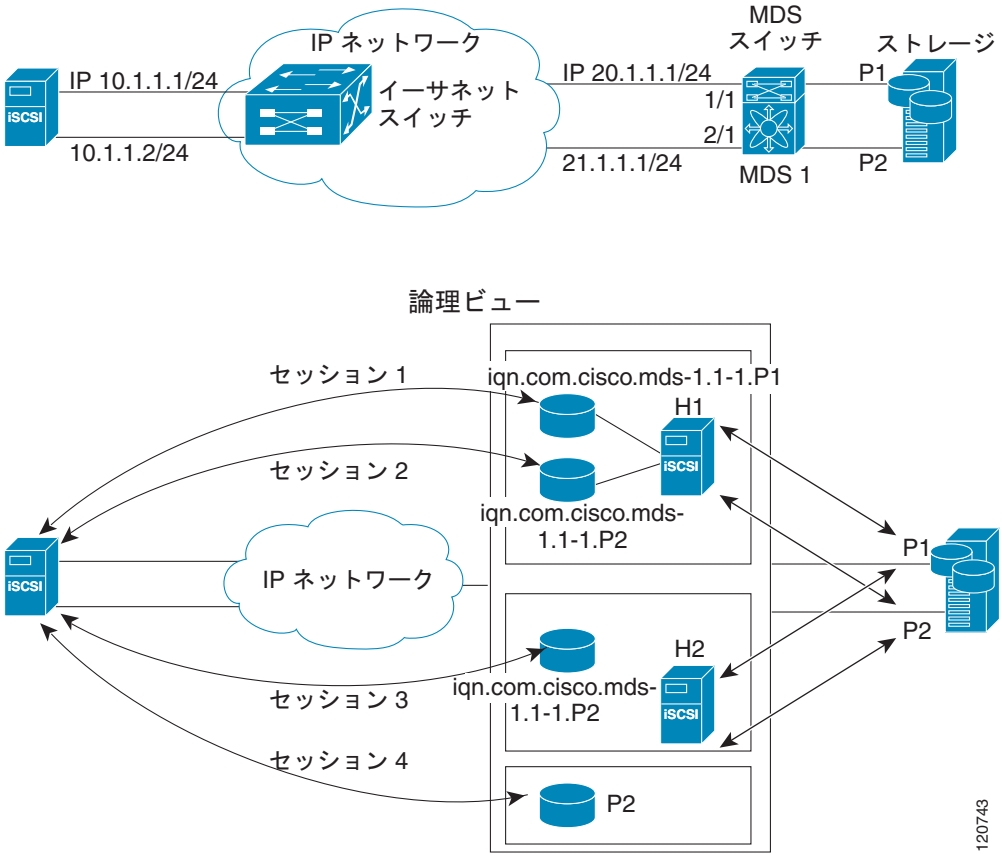
次のハイ アベイラビリティ設定を使用できます。

- マルチパス ソフトウェアを実行しているホストでの iSCSI ハイ アベイラビリティ
- マルチパス ソフトウェアを実行していないホストでの iSCSI ハイ アベイラビリティ

## マルチパス ソフトウェアを実行しているホストでの iSCSI ハイ アベイラビリティ

図 4-38 に、複数のマルチパス ソフトウェアを実行しているホストに対する iSCSI HA ソリューションの物理トポロジと論理トポロジを示します。このシナリオでは、ホストに 4 つの iSCSI セッションがあります。各ホストの NIC から 2 つの IPS ポートへ向かう iSCSI セッションが 2 つあります。

**図 4-38　マルチパス ソフトウェアを実行しているホスト**




各 IPS ポートは、ストレージの同じファイバ チャネル ターゲット ポートを 2 つエクスポートしますが、ダイナミック iSCSI ターゲットを使用している場合は異なる iSCSI ターゲット名としてエクスポートします。このため、2 つの IPS ポートは、合計 4 つの iSCSI ターゲット デバイスをエクスポートします。これら 4 つの iSCSI ターゲットは、ファイバ チャネル ターゲットの同じ 2 つのポートをマッピングします。

iSCSI ホストは、NIC-1 を使用して IPS ポート 1 に接続し、NIC-2 を使用して IPS ポート 2 に接続します。IPS ポートがそれぞれ 2 つの iSCSI ターゲットをエクスポートするため、iSCSI ホストは 4 つの iSCSI セッションを作成します。

iSCSI ホストの NIC-1 に障害が発生すると（物理構成図については、図 4-38 を参照してください）、セッション 1 とセッション 2 は失敗しても、セッション 3 とセッション 4 はそのまま維持されます。

IPS ポート 1 に障害が発生すると、iSCSI ホストは IPS ポートに接続できず、セッション 1、およびセッション 2 は失敗します。それでも、セッション 3 とセッション 4 はそのまま維持されます。

ストレージのポート 1 に障害が発生すると、IPS ポートはセッション 1 とセッション 3 を終了します（iSCSI 仮想ターゲットの iqn.com.cisco.mds-5.1-2.p1 および iqn-com.cisco.mds-5.1-1.p1 をオフラインの状態にします）。それでも、セッション 2 とセッション 4 はそのまま維持されます。

このトポロジでは、どの構成要素の障害からでも復旧できることになります。ホストのマルチパス ソフトウェアは、ストレージにアクセスするためのさまざまなパス全体のロード バランシングまたはフェールオーバーに対処します。

## マルチパス ソフトウェアを使用していないホストでの iSCSI HA

ホストがマルチパス ソフトウェアを使用していない場合、ホストに同一ストレージへの複数のセッションが発生するため、上記トポロジは機能しません。マルチパス ソフトウェアを使用しない場合、ホストは同一ストレージへの複数のパスを把握できません。

IP ストレージには、この状況での HA ソリューションを提供する、2 つの追加機能があります。

- IPS ポートは、VRRP 機能をサポートし（「ギガビット イーサネット インターフェイスに対する VRRP の設定」（P.6-9）を参照）、IPS ポートのフェールオーバーを提供します。
- IPS は、iSCSI スタティック仮想ターゲットに対する透過的なファイバ チャネル ターゲット フェールオーバーを備えています。

スタティックにインポートされた iSCSI ターゲットには、ファイバ チャネル ターゲットのセカンダリ pWWN を提供する別のオプションもあります。冗長ポート間で LU を可視化するように物理ファイバ チャネル ターゲットを設定する際にはこれを使用できます。アクティブ ポートに障害が発生した場合、セカンダリ ポートがアクティブになり、iSCSI セッションは新しいアクティブ ポートを使用するように切り替わります（図 4-39 を参照）。

**図 4-39　　2 つのファイバ チャネル ポートを介してインポートするスタティック ターゲット**

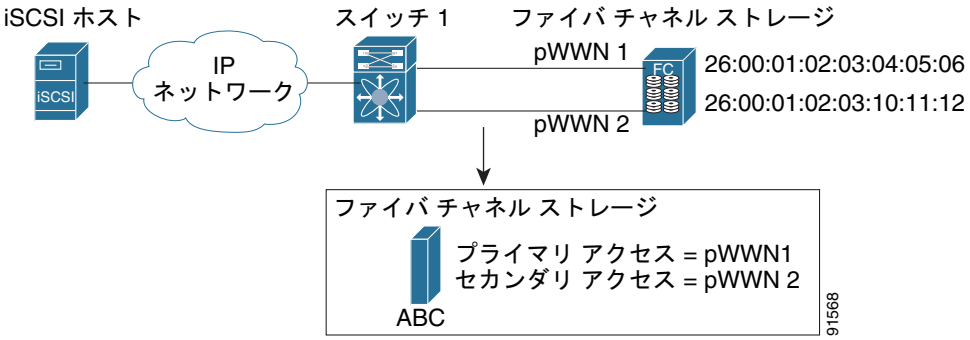



図 4-39 では、pWWN1 と pWWN2 の両方にマッピングされた iSCSI 仮想ターゲットを作成して、ファイバ チャネル ターゲットへの冗長アクセスを提供します。

IPS ポートによって、セカンダリ ポートへのフェールオーバーは、ホストからの iSCSI セッションに影響することなく透過的に実行されます。プライマリ ポートに障害が発生すると状況確認のステータスになるため、未処理のすべての I/O は終了します。フェールオーバー中に受信した新規 I/O は完了せず、ビジー ステータスを受信します。

**ヒント**　LU 番号が異なる場合は、LUN マッピングを使用することで、別のセカンダリ ファイバ チャネル LUN を定義できます。

プライマリ ポートが再びアップの状態になったときに IPS ポートをプライマリ ポートにスイッチバックさせるには、任意の **revert-primary-port** オプションをイネーブルにします。このオプションがディセーブルで（デフォルト）、スイッチオーバーの後にプライマリ ポートが再びアップ状態になった場合は、古いセッションはセカンダリ ポートに残り、プライマリ ポートにスイッチバックすることはありません。ただし、新しいセッションはいずれもプライマリ ポートを使用します。プライマリ ポートとセカンダリ ポートが同時に使用されるのは、この状況のときだけです。

Device Manager を使用してファイバ チャネル ターゲット ポート全体に対してスタティック iSCSI 仮想ターゲットを作成する手順は、次のとおりです。

**ステップ 1**　[IP] > [iSCSI] をクリックします。

iSCSI 設定が表示されます（図 4-12 を参照）。

**ステップ 2**　[Targets] タブをクリックして、既存の iSCSI ターゲットのリストを表示します（図 4-13 を参照）。

**ステップ 3**　[Create] をクリックして iSCSI ターゲットを作成します。

[Create iSCSI Targets] ダイアログボックスが表示されます（図 4-15 を参照）。

**ステップ 4**　[iSCSI Name] フィールドに iSCSI ターゲット ノード名を IQN フォーマットで設定します。

**ステップ 5**　[Port WWN] フィールドにマッピングするファイバ チャネル ターゲット ポートを設定します。

**ステップ 6**　[Select from List] オプション ボタンをクリックして、この仮想 iSCSI ターゲットをアクセスさせる iSCSI イニシエータ ノード名または IP アドレスを設定するか、または、[All] オプション ボタンをクリックして、この仮想 iSCSI ターゲットをすべての iSCSI イニシエータにアクセスさせるようにします。「iSCSI アクセス コントロール」（P.4-26）を参照してください。

**ステップ 7**　[Select from List] オプション ボタンをクリックして、iSCSI ターゲットをアドバタイズするインターフェイスをそれぞれ選択するか、[All] オプション ボタンを選択して、すべてのインターフェイスをアドバタイズします。

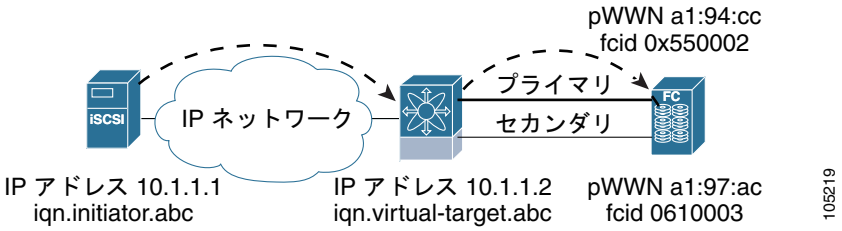
**ステップ 8**　[Apply] をクリックして、この変更を保存します。

## ストレージ ポート フェールオーバーの LUN trespass

スタティックにインポートされた iSCSI ターゲットのハイ アベイラビリティの他に、アクティブ ポートの障害時に、スタティックにインポートした iSCSI ターゲットのアクティブ ポートからパッシブ ポートに LU を移動できる trespass 機能を使用できます。

2 つのファイバ チャネル N ポート間で LU を可視化するように物理ファイバ チャネル ターゲットでは、アクティブ ポートに障害が発生するとパッシブ ポートに引き継がれます。物理ファイバ チャネル ターゲットの中には、trespass 機能を使用してアクティブ ポートからパッシブ ポートへの LU の移動を必要とするものもあります。スタティックにインポートされた iSCSI ターゲットのセカンダリ pWWN オプション、および trespass 機能をイネーブルにする追加のオプションは、冗長ポートを持つ物理ファイバ チャネル ターゲットで使用できます。アクティブ ポートに障害が発生した場合、パッシブ ポートがアクティブになり、trespass 機能がイネーブルの場合は、Cisco MDS スイッチは LU を新しいアクティブ ポートに移動するようにターゲットに要求を送信します。iSCSI セッションは、新しいアクティブ ポートを使用するように切り替わり、移動した LU には新しいアクティブ ポートを介したアクセスが行われます（図 4-40 を参照）。

図 4-40　アクティブ プライマリ ポートを持つ仮想ターゲット




スタティック iSCSI 仮想ターゲットの trespass 機能をイネーブルにするには、Device Manager で [IP] > [iSCSI] を選択し、[Targets] タブを選択して [Trespass Mode] チェックボックスをオンにします。

# 同一 IP ネットワークに接続された複数の IPS ポート

図 4-41 に、同一 IP ネットワーク内で複数のギガビット イーサネット インターフェイスを使用する設定例を示します。

図 4-41　同一 IP ネットワーク内のギガビット イーサネット インターフェイス

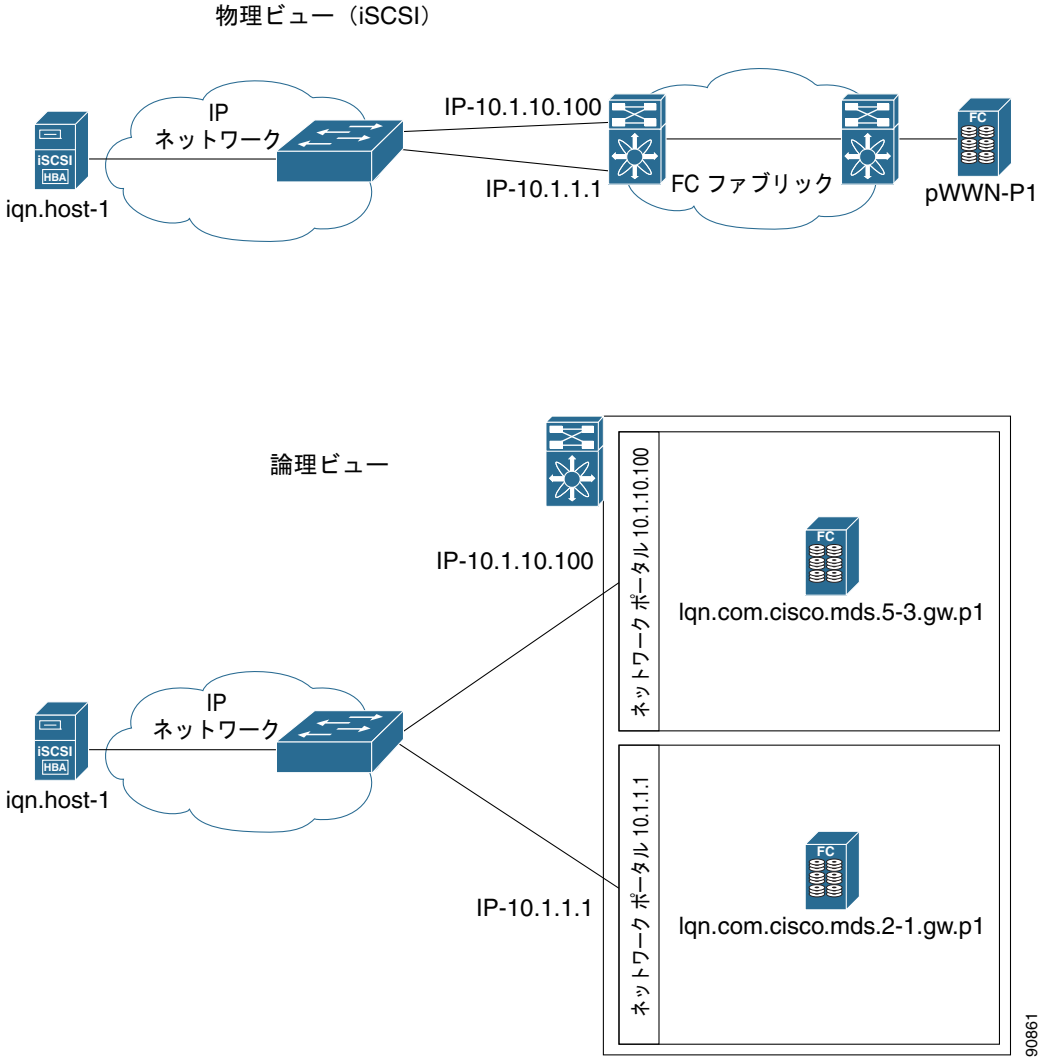



図 4-41 では、各 iSCSI ホストは、各物理ファイバ チャネル ターゲットごとに（異なる名前を持つ）2 つの iSCSI ターゲットを検出します。ホスト上のマルチパス ソフトウェアは、両方のパスを介してロード バランシングを提供します。一方のギガビット イーサネット インターフェイスに障害が発生しても、ホストのマルチパス ソフトウェアは別のパスを使用できるので影響を受けません。

# VRRP ベースのハイ アベイラビリティ

図 4-42 に、VRRP ベースのハイ アベイラビリティ iSCSI の設定例を示します。

**図 4-42　VRRP ベースの iSCSI ハイ アベイラビリティ**

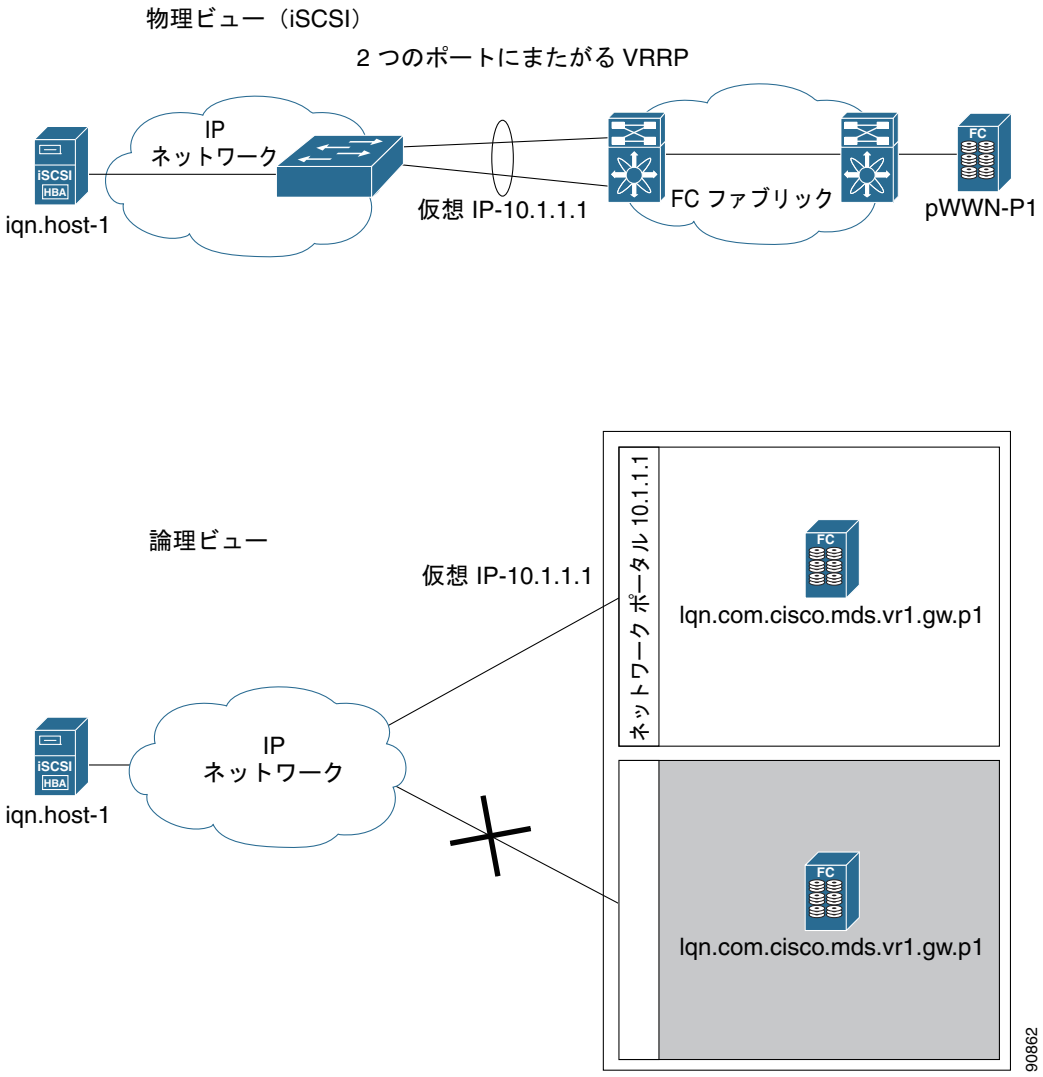



図 4-42 では、各 iSCSI ホストは、各物理ファイバ チャネル ターゲットごとに 1 つの iSCSI ターゲットを検出します。VRRP マスターのギガビット イーサネット インターフェイスに障害が発生すると、iSCSI セッションは終了します。次にホストがターゲットに再接続すると、別のギガビット イーサネット インターフェイスが新しいマスターとして仮想 IP アドレスを引き継いでいるため、セッションが発生します。

# イーサネット PortChannel ベースのハイ アベイラビリティ

（注）　1 つの iSCSI リンクに対するすべての iSCSI データ トラフィックは、1 つの TCP 接続で実行されます。結果として、その iSCSI リンクに対する集約帯域幅は 1 Gbps となります。

図 4-43 に、サンプルのイーサネット PortChannel ベースのハイ アベイラビリティ iSCSI 構成を示します。

**図 4-43　イーサネット PortChannel ベース iSCSI ハイ アベイラビリティ**

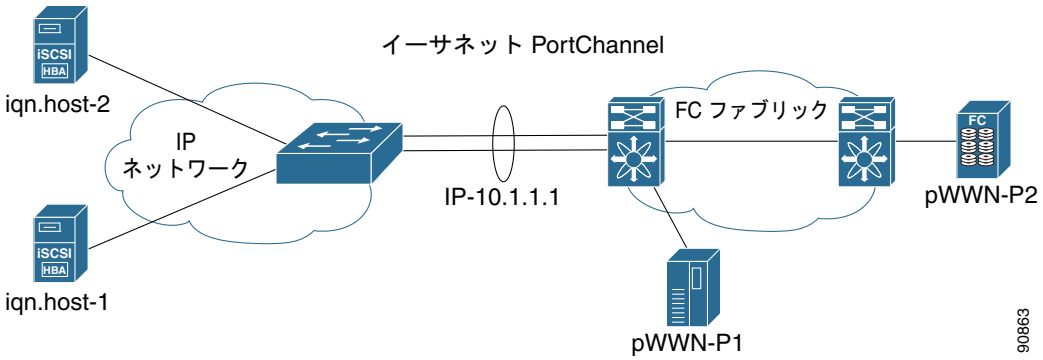



図 4-43 では、各 iSCSI ホストは、各物理ファイバ チャネル ターゲットごとに 1 つの iSCSI ターゲットを検出します。iSCSI ホストから IPS ポート上の iSCSI 仮想ターゲットへの iSCSI セッションは、2 つの物理インターフェイスのいずれかを使用します（iSCSI セッションが使用する TCP 接続は 1 つであるため）。ギガビット イーサネット インターフェイスで障害が発生すると、IPS モジュールとイーサネット スイッチは透過的にすべてのフレームを 2 番目のギガビット イーサネット インターフェイスに転送します。

（注）　イーサネット PortChannel が IPS モジュールとイーサネット スイッチ間に設定されている場合、VRRP を設定したロード バランシングを正常に動作させるためには、イーサネット スイッチ上のロード バランシング ポリシーは、ポート番号ではなく、送信元および宛先 IP アドレスだけに基づいている必要があります。

# iSCSI 認証セットアップに関する注意事項とシナリオ

ここでは、設定可能な各種 iSCSI 認証、セットアップ要件、およびサンプル シナリオに関する注意事項について説明します。次の認証セットアップに関する注意事項を説明します。

- 「認証なしの設定」（P.4-61）
- 「ローカル パスワード データベースを使用した CHAP の設定」（P.4-61）
- 「外部 RADIUS サーバを使用した CHAP の設定」（P.4-62）
- 「iSCSI トランスペアレント モード イニシエータ」（P.4-63）
- 「ターゲット ストレージ デバイスで必要な LUN マッピング」（P.4-67）

**注意**　iSLB VRRP グループの一部である iSCSI インターフェイスの認証を変更すると、インターフェイス上のロード バランシングに影響をおよぼします。「iSCSI インターフェイス パラメータの変更とロード バランシングに対するその影響」（P.4-48）を参照してください。

# 認証なしの設定

iSCSI 認証方法を **none** に設定すると、認証なしのネットワークが構成されます。

Fabric Manager で、[Physical Attributes] ペインの [End Devices] > [iSCSI] を選択します。[Globals] タブを選択して、[AuthMethod] ドロップダウン メニューを [none] に設定してから、[Apply Changes] をクリックします。

# ローカル パスワード データベースを使用した CHAP の設定

ローカル パスワード データベースの CHAP オプションを使用して認証を設定する場合は、次の手順に従います。

**ステップ 1**　iSCSI プロトコルでローカル パスワード データベースを使用するように AAA 認証を設定します。

**a.** Fabric Manager で、[Physical Attributes] ペインの [Switches] > [Security] > [AAA] を選択します。

**b.** [Information] ペインで、[Applications] タブをクリックします。

**c.** iSCSI 行の [Local] チェックボックスをオンにして、[Apply Changes] をクリックします。

**ステップ 2**　すべての iSCSI クライアントで CHAP を要求するように iSCSI 認証方法を設定します。

**a.** Fabric Manager で、[Physical Attributes] ペインの [End Devices] > [iSCSI] を選択します。

**b.** [Information] ペインで、[Globals] タブをクリックします。

**c.** [AuthMethod] ドロップダウン メニューを [chap] に設定して、[Apply Changes] をクリックします。

**ステップ 3**　iSCSI ユーザのユーザ名とパスワードを設定します。

**a.** Device Manager で、[Security] > [iSCSI] を選択します。

**b.** [Username]、[Password]、および [Confirm Password] フィールドを設定します。

**c.** [Create] をクリックして変更を保存します。

**ステップ 4**　グローバル iSCSI 認証セットアップを確認します。

**a.** Fabric Manager で、[Physical Attributes] ペインの [End Devices] > [iSCSI] を選択します。

**b.** [Information] ペインで、[Globals] タブをクリックします。

# 外部 RADIUS サーバを使用した CHAP の設定

外部 RADIUS サーバで CHAP オプションを使用して認証を設定する場合は、次の手順に従います。

**ステップ 1**　Cisco MDS スイッチのパスワードを RADIUS サーバへの RADIUS クライアントとして設定します。

a. Fabric Manager で、[Physical Attributes] ペインの [Switches] > [Security] > [AAA] > [RADIUS] を選択します。

b. [Information] ペインで、[Default] タブをクリックします。

c. [AuthKey] フィールドをデフォルトのパスワードに設定して、[Apply Changes] アイコンをクリックします。

**ステップ 2**　RADIUS サーバ IP アドレスの設定

a. Fabric Manager で、[Physical Attributes] ペインの [Switches] > [Security] > [AAA] > [RADIUS] を選択します。

b. [Information] ペインで、[Server] タブをクリックして、[Create Row] をクリックします。

c. [Index] フィールドを一意の数に設定します。

d. [IP Type] オプション ボタンを [ipv4] または [ipv6] に設定します。

e. [Name] または [IP Address] フィールドを RADIUS サーバの IP アドレスに設定し、[Create] をクリックします。

**ステップ 3**　RADIUS サーバ グループを作成し、そのグループに RADIUS サーバを追加します。

a. Fabric Manager で、[Physical Attributes] ペインの [Switches] > [Security] > [AAA] を選択します。

b. [Information] ペインで、[Server Groups] タブをクリックして、[Create Row] を選択します。

c. [Index] フィールドを一意の数に設定します。

d. [Protocol] オプション ボタンを [radius] に設定します。

e. [Name] フィールドをサーバ グループ名に設定します。

f. [ServerIDList] を RADIUS サーバのインデックス値に設定し（作成方法については、ステップ 2 c. を参照してください）、[Create] をクリックします。

**ステップ 4**　RADIUS サーバに向かうように iSCSI プロトコルの認証確認をセットアップします。

a. Fabric Manager で、[Physical Attributes] ペインの [Switches] > [Security] > [AAA] を選択します。

b. [Information] ペインで、[Applications] タブをクリックします。

c. [Type]、[SubType]、および [Function] カラムの iSCSI 行を右クリックします。

d. [ServerGroup IDList] を [Server Group] のインデックス値に設定し（作成方法については、ステップ 3 を参照してください）、[Create] をクリックします。

**ステップ 5**　すべての iSCSI クライアントで CHAP を要求するように iSCSI 認証方法を設定します。

a. Fabric Manager で、[Physical Attributes] ペインの [End Devices] > [iSCSI] を選択します。

b. [AuthMethod] ドロップダウン メニューから、[chap] を選択します。

c. [Apply Changes] アイコンをクリックします。

**ステップ 6**　Fabric Manager で、[Physical Attributes] ペインの [End Devices] > [iSCSI] を選択します。

**ステップ 7**　[Information] ペインで [Globals] タブをクリックして、グローバル iSCSI 認証セットアップが CHAP になっていることを確認します。

**ステップ 8**　Fabric Manager で、[Physical Attributes] ペインの [Switches] > [Security] > [AAA] を選択します。

**ステップ 9**　[Information] ペインで、[Applications] タブをクリックして、iSCSI の AAA 認証情報を確認します。

iSCSI RADIUS サーバを設定する手順は、次のとおりです。

**ステップ 1**　Cisco MDS スイッチの管理イーサネット IP アドレスからのアクセスを許可するように RADIUS サーバを設定します。

**ステップ 2**　Cisco MDS スイッチを認証する RADIUS サーバの共有秘密を設定します。

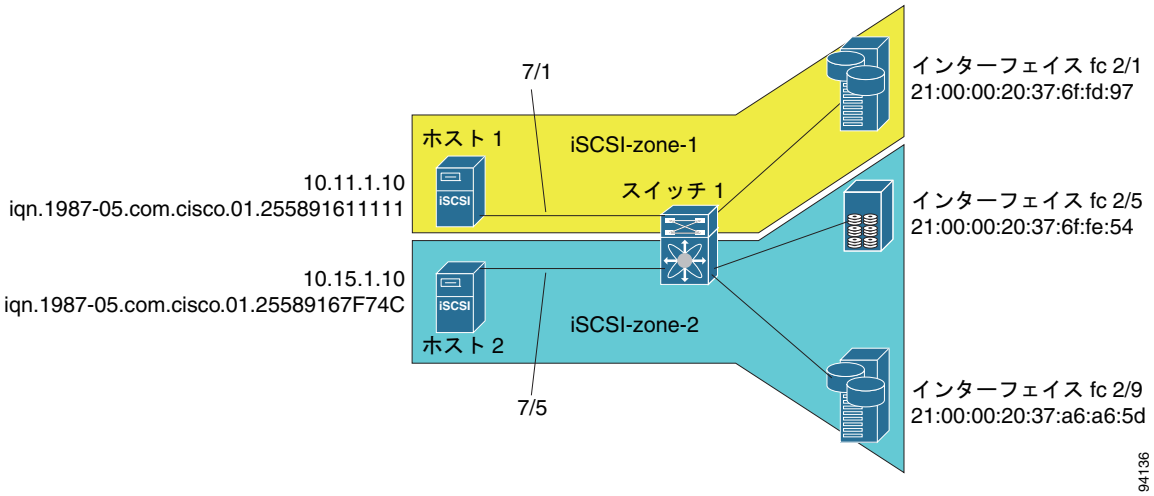
**ステップ 3**　RADIUS サーバで iSCSI ユーザとパスワードを設定します。

# iSCSI トランスペアレント モード イニシエータ

このシナリオでは、次の構成を想定しています（図 4-44 を参照）。

- LUN マッピングまたは LUN マスキング、あるいはターゲット デバイスのその他のホストのアクセスコントロールがない
- iSCSI ログイン認証がない（つまりログイン認証が [none] に設定されている）
- トポロジは次のとおりです。
  - iSCSI インターフェイス 7/1 は、IP アドレスによりイニシエータを特定するように設定されています。
  - iSCSI インターフェイス 7/5 は、ノード名によりイニシエータを特定するように設定されています。
  - IPv4 アドレス 10.11.1.10、名前 iqn.1987-05.com.cisco:01.255891611111 の iSCSI イニシエータ ホスト 1 は、IPS ポート 7/1 に接続し、IPv4 アドレス（ホスト 1 = 10.11.1.10）によって識別されます。
  - IPv4 アドレス 10.15.1.10、ノード名 iqn.1987-05.com.cisco:01.25589167f74c の iSCSI イニシエータ ホスト 2 は、IPS ポート 7/5 に接続します。

**図 4-44　iSCSI シナリオ 1**



シナリオ 1 を設定する場合は、次の手順に従います（図 4-44 を参照）。

**ステップ 1**　Cisco MDS スイッチのすべての iSCSI ホストの null 認証を設定します。

**a.** Fabric Manager で、[Physical Attributes] ペインの [End Devices] > [iSCSI] を選択します。

**b.** [Information] ペインで、[AuthMethod] ドロップダウン メニューから [none] を選択します。

**c.** [Apply Changes] アイコンをクリックします。

**ステップ 2**　自動生成された iSCSI ターゲット名を使用して、すべてのファイバ チャネル ターゲットを iSCSI SAN に動的にインポートするように iSCSI を設定します。

**a.** Device Manager で、[IP] > [iSCSI] をクリックします。

**b.** [Targets] タブをクリックします。

**c.** [Dynamically Import FC Targets] チェックボックスをオンにします。

**d.** [Apply] をクリックします。

**ステップ 3**　IPv4 アドレスを持つスロット 7 ポート 1 のギガビット イーサネット インターフェイスを設定して、インターフェイスをイネーブルにします。

**a.** Fabric Manager で、[Physical Attributes] ペインの [Switches] > [Interfaces] > [Gigabit Ethernet] を選択します。

**b.** [Information] ペインで、[IP Address] タブをクリックして、[Create Row] を選択します。

**c.** スロット 7 ポート 1 のギガビット イーサネット インターフェイスの IP アドレスとサブネット マスクを設定します。

**d.** [Create] をクリックします。

**e.** [General] タブを選択して、スロット 7 ポート 1 のギガビット イーサネット インターフェイスの [Admin] ドロップダウン メニューから [up] を選択します。

**f.** [Apply Changes] アイコンをクリックします。

**（注）**　ホスト 2 はこのポートに接続しています。

**ステップ 4**　IP アドレスによってすべての動的 iSCSI イニシエータを特定するようにスロット 7 ポート 1 の iSCSI インターフェイスを設定し、インターフェイスをイネーブルにします。

**a.** Fabric Manager で、[Physical Attributes] ペインの [Switches] > [Interfaces] > [FC Logical] を選択します。

**b.** [Information] ペインで、[iSCSI] タブをクリックします。

**c.** [Initiator ID Mode] ドロップダウン メニューから [ipaddress] を選択して、[Apply Changes] アイコンをクリックします。

**d.** Device Manager で、[Interfaces] > [Ethernet and iSCSI] を選択します。

**e.** [iSCSI] タブをクリックします。

**f.** スロット 7 ポート 1 の iSCSI インターフェイスの [Admin] ドロップダウン メニューから [up] を選択します。

**g.** [Apply] をクリックします。

**ステップ 5**　IPv4 アドレスを持つスロット 7 ポート 5 のギガビット イーサネット インターフェイスを設定して、インターフェイスをイネーブルにします。

**a.** Fabric Manager で、[Physical Attributes] ペインの [Switches] > [Interfaces] > [Gigabit Ethernet] を選択します。

**b.** [Information] ペインで、[IP Address] タブをクリックして、[Create Row] をクリックします。

**c.** スロット 7 ポート 5 のギガビット イーサネット インターフェイスの IP アドレスとサブネット マスクを設定します。

**d.** [Create] をクリックします。

**e.** [General] タブを選択して、スロット 7 ポート 5 のギガビット イーサネット インターフェイスの [Admin] ドロップダウン メニューから [up] を選択します。

**f.** [Apply Changes] アイコンをクリックします。

**ステップ 6**　ノード名によってすべての動的 iSCSI イニシエータを特定するようにスロット 7 ポート 5 の iSCSI インターフェイスを設定し、インターフェイスをイネーブルにします。

**a.** Fabric Manager で、[Physical Attributes] ペインの [Switches] > [Interfaces] > [FC Logical] を選択します。

**b.** [Information] ペインで、[iSCSI] タブをクリックします。

**c.** [Initiator ID Mode] ドロップダウン メニューから [name] を選択して、[Apply Changes] アイコンをクリックします。

**d.** Device Manager で、[Interfaces] > [Ethernet and iSCSI] を選択します。

**e.** [iSCSI] タブをクリックします。

**f.** スロット 7 ポート 5 の iSCSI インターフェイスの [Admin] ドロップダウン メニューから [up] を選択します。

**g.** [Apply] をクリックします。

**（注）**　ホスト 1 はこのポートに接続しています。

**ステップ 7**　利用可能なファイバ チャネル ターゲットを確認します。

**a.** Device Manager で、[FC] > [Name Server] を選択します。

**b.** [General] タブをクリックします。

**ステップ 8**　ホスト 1 とその中に 1 つのファイバ チャネル ターゲットを入れた *iscsi-zone-1* という名前のゾーンを作成します。

**（注）**　iSCSI インターフェイスは IP に基づいてすべてのホストを特定するように設定されているため、ゾーン メンバシップ設定のホストの IP アドレスを使用します。

**a.** Fabric Manager で、[Zones] > [Edit Local Full Zone Database] を選択します。

**b.** [Edit Local Full Zone Database] ダイアログボックスの [VSAN] ドロップダウン メニューから [VSAN 1] を選択します。

**c.** 左側のナビゲーション ペインで [Zones] フォルダを選択して、[Insert] をクリックします。

**d.** [Zone Name] フィールドを [iscsi-zone-1] に設定して、[OK] をクリックします。

**e.** 左側のナビゲーション ペインで [iscsi-zone-1] フォルダを選択して、[Insert] をクリックします。

**f.** [ZoneBy] オプション ボタンを [WWN] に設定します。

**g.** Port WWN をファイバ チャネル ターゲットの pWWN（つまり、21:00:00:20:37:6f:fd:97）に設定して、[Add] をクリックします。

**h.** [ZoneBy] オプション ボタンを [iSCSI IP Address/Subnet] に設定します。

**i.** [IP Address/Mask] フィールドをホスト 1 iSCSI イニシエータ（10.11.1.10）の IP アドレスに設定して、[Add] をクリックします。

**ステップ 9**　ホスト 2 とその中に 2 つのファイバ チャネル ターゲットを入れた *iscsi-zone-2* という名前のゾーンを作成します。

**（注）** iSCSI インターフェイスはノード名に基づいてすべてのホストを特定するように設定されているため、ゾーン メンバシップ設定の iSCSI ホストのシンボリック ノード名を使用します。

**a.** Fabric Manager で、メイン メニューから、[Zones] > [Edit Local Full Zone Database] を選択します。

**b.** [Edit Local Full Zone Database] ダイアログボックスの [VSAN] ドロップダウン メニューから [VSAN 2] を選択します。

**c.** 左側のナビゲーション ペインで [Zones] フォルダを選択して、[Insert] をクリックします。

**d.** [Zone Name] フィールドを [iscsi-zone-2] に設定して、[OK] をクリックします。

**e.** 左側のナビゲーション ペインで [iscsi-zone-2] フォルダを選択して、[Insert] をクリックします。

**f.** [ZoneBy] オプション ボタンを [WWN] に設定します。

**g.** Port WWN をファイバ チャネル ターゲットのいずれかの pWWN（例 : 21:00:00:20:37:6f:fe:5）に設定します。次に、[Add] をクリックします。

**h.** Port WWN をファイバ チャネル ターゲットの別の pWWN（例 : 21:00:00:20:37:a6:a6:5d）に設定します。次に、[Add] をクリックします。

**i.** [ZoneBy] オプション ボタンを [iSCSI name] に設定します。

**j.** [Port Name] フィールドをホスト 2 のシンボリック名（iqn.1987-05.com.cisco:01.25589167f74c）に設定して、[Add] をクリックします。

**ステップ 10**　ゾーン セットを作成して、メンバーとして 2 つのゾーンを追加し、ゾーン セットを有効にします。

**（注）** iSCSI インターフェイスは、ノード名に基づいてすべてのホストを特定するように設定されています。

**a.** Fabric Manager で、[Zones] > [Edit Local Full Zone Database] を選択します。

**b.** [Edit Local Full Zone Database] ダイアログボックスの [VSAN] ドロップダウン メニューから [VSAN 1] を選択します。

**c.** 左側のナビゲーション ペインで [Zoneset] フォルダを選択して、[Insert] をクリックします。

**d.** [Zoneset Name] を [zonset-iscsi] に設定して、[OK] をクリックします。

**e.** [zoneset-iscsi] フォルダをクリックして、[Insert] をクリックします。

**f.** [Zone Name] フィールドを [iscsi-zone-1] に設定して、[OK] をクリックします。

**g.** [Zone Name] フィールドを [iscsi-zone-2] に設定して、[OK] をクリックします。

**h.** [Activate] をクリックして、新しいゾーン セットをアクティブにします。

**i.** [Continue Activation] をクリックして、アクティブ化を完了します。

**ステップ 11**　iSCSI ホスト（ホスト 1 とホスト 2）を構築します。

**ステップ 12**　すべての iSCSI セッションを表示します。

**a.** Device Manager で、[Interfaces] > [Monitor] > [Ethernet] を選択します。

**b.** [iSCSI connections] タブをクリックして、すべての iSCSI セッションを表示します。

**c.** Device Manager で、[IP] > [iSCSI] を選択して、[Session Initiators] タブを選択します。

**d.** [Details] をクリックします。

**ステップ 13**　Fabric Manager で、[Physical Attributes] ペインで、[End Devices] > [iSCSI] を選択して、2 つの iSCSI イニシエータの詳細を確認します。

**ステップ 14**　Fabric Manager で、[Zones] > [Edit Local Full Zone Database] を選択して、アクティブなゾーン セットを表示します。iSCSI イニシエータの FC ID が解決されます。

**ステップ 15**　Device Manager で、[FC] > [Name Server] を選択します。ファイバ チャネル ネーム サーバには、iSCSI ホストに対して作成された仮想 N ポートが表示されます。

**ステップ 16**　Device Manager で、[FC] > [Name Server] を選択します。

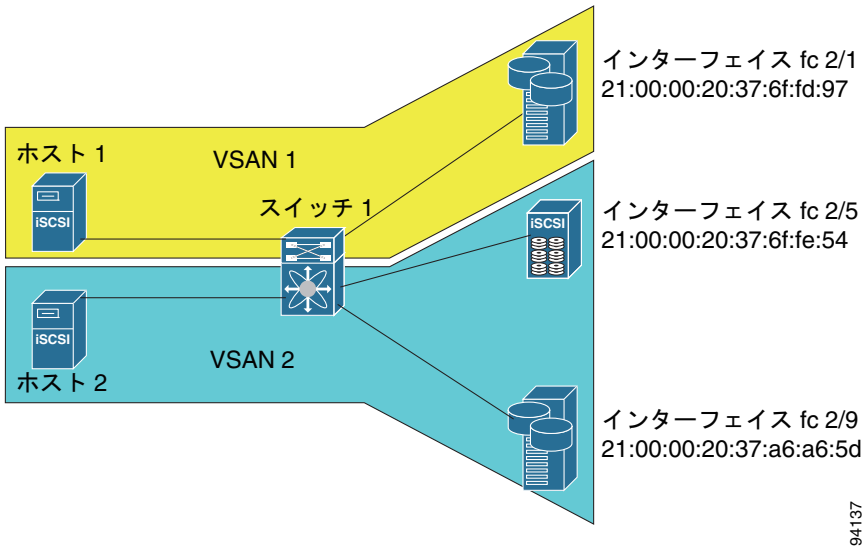
**ステップ 17**　[Advanced] タブをクリックします。ファイバ チャネル ネーム サーバの iSCSI イニシエータ ノードの詳細出力を確認します。

# ターゲット ストレージ デバイスで必要な LUN マッピング

サンプル シナリオ 2 は、次の構成を想定しています（図 4-45 を参照）。

- アクセス コントロールがファイバ チャネル ゾーニングに基づいている。
- ターゲット ベースの LUN マッピングまたは LUN マスキングがある。
- iSCSI 認証がない（none）。
- iSCSI イニシエータは異なる VSAN に割り当てられている。

**図 4-45　iSCSI シナリオ 2**



シナリオ 2 を設定する場合は、次の手順に従います（図 4-45 を参照）。

**ステップ 1**　すべての iSCSI ホストに対して null 認証を設定します。

a. Fabric Manager で、[Physical Attributes] ペインの [End Devices] > [iSCSI] を選択します。

b. [Information] ペインで、[AuthMethod] ドロップダウン メニューから [none] を選択します。

c. [Apply Changes] アイコンをクリックします。

**ステップ 2**　自動生成された iSCSI ターゲット名を使用して、すべてのファイバ チャネル ターゲットを iSCSI SAN に動的にインポートするように iSCSI を設定します。

a. Device Manager で、[IP] > [iSCSI] をクリックします。

b. [Targets] タブをクリックします。

c. [Dynamically Import FC Targets] チェックボックスをオンにします。

d. [Apply] をクリックします。

**ステップ 3**　IPv4 アドレスを持つスロット 7 ポート 1 のギガビット イーサネット インターフェイスを設定して、インターフェイスをイネーブルにします。

a. Fabric Manager で、[Physical Attributes] ペインの [Switches] > [Interfaces] > [Gigabit Ethernet] を選択します。

b. [Information] ペインで、[IP Address] タブをクリックして、[Create Row] を選択します。

c. スロット 7 ポート 1 のギガビット イーサネット インターフェイスの IP アドレスとサブネット マスクを設定します。

d. [Create] をクリックします。

e. [General] タブをクリックして、スロット 7 ポート 1 のギガビット イーサネット インターフェイスの [Admin] ドロップダウン メニューから [up] を選択します。

f. [Apply Changes] アイコンをクリックします。

**ステップ 4**　IP アドレスによってすべての動的 iSCSI イニシエータを特定するようにスロット 7 ポート 1 の iSCSI インターフェイスを設定し、インターフェイスをイネーブルにします。

a. Fabric Manager で、[Physical Attributes] ペインの [Switches] > [Interfaces] > [FC Logical] を選択します。

b. [Information] ペインで、[iSCSI] タブを選択します。

c. [Initiator ID Mode] ドロップダウン メニューから [ipaddress] を選択して、[Apply Changes] アイコンをクリックします。

d. Device Manager で、[Interfaces] > [Ethernet and iSCSI] を選択します。

e. [iSCSI] タブをクリックします。

f. スロット 7 ポート 1 の iSCSI インターフェイスの [Admin] ドロップダウン メニューから [up] を選択します。

g. [Apply] をクリックします。

**ステップ 5**　IPv4 アドレスを持つスロット 7 ポート 5 のギガビット イーサネット インターフェイスを設定して、インターフェイスをイネーブルにします。

a. Fabric Manager で、[Physical Attributes] ペインの [Switches] > [Interfaces] > [Gigabit Ethernet] を選択します。

b. [Information] ペインで、[IP Address] タブをクリックして、[Create Row] をクリックします。

**c.** スロット 7 ポート 5 のギガビット イーサネット インターフェイスの IP アドレスとサブネット マスクを設定します。

**d.** [Create] をクリックします。

**e.** [General] タブを選択して、スロット 7 ポート 5 のギガビット イーサネット インターフェイスの [Admin] ドロップダウン メニューから [up] を選択します。

**f.** [Apply Changes] アイコンをクリックします。

**ステップ 6**　IP アドレスによってすべての動的 iSCSI イニシエータを特定するようにスロット 7 ポート 5 の iSCSI インターフェイスを設定し、インターフェイスをイネーブルにします。

**a.** Fabric Manager で、[Physical Attributes] ペインの [Switches] > [Interfaces] > [FC Logical] を選択します。

**b.** [Information] ペインで、[iSCSI] タブをクリックします。

**c.** [Initiator ID Mode] ドロップダウン メニューから [ipaddress] を選択して、[Apply Changes] アイコンをクリックします。

**d.** Device Manager で、[Interfaces] > [Ethernet and iSCSI] を選択します。

**e.** [iSCSI] タブをクリックします。

**f.** スロット 7 ポート 5 の iSCSI インターフェイスの [Admin] ドロップダウン メニューから [up] を選択します。

**g.** [Apply] をクリックします。

**ステップ 7**　ホスト 1 の静的 pWWN と nWWN の設定を行います。

**a.** Device Manager で、[IP] > [iSCSI] を選択します。

**b.** [Initiators] タブをクリックします。

**c.** ホスト 1 iSCSI イニシエータの [Node Address Persistent] および [Node Address System-assigned] チェックボックスをオンにします。

**d.** [Apply] をクリックします。

**ステップ 8**　ホスト 2 の静的 pWWN の設定を行います。

**a.** Device Manager で、[IP] > [iSCSI] を選択します。

**b.** [Initiators] タブをクリックします。

**c.** ホスト 2 iSCSI イニシエータを右クリックして、[Edit pWWN] をクリックします。

**d.** [System-assigned Num] フィールドで [1] を選択して、[Apply] をクリックします。

**ステップ 9**　設定した WWN を表示します。

**（注）**　WWN はシステムで割り当てられます。イニシエータは異なる VSAN のメンバーです。

**a.** Fabric Manager で、[Physical Attributes] ペインの [End Devices] > [iSCSI] を選択します。

**b.** [Initiators] タブをクリックします。

**ステップ 10**　VSAN 1 のホスト 1 と iSCSI ターゲットを作成します。

**（注）**　iSCSI インターフェイスは IP に基づいてすべてのホストを特定するように設定されているため、ゾーン メンバシップ設定のホストの IP アドレスを使用します。

**a.** Fabric Manager で、[Zones] > [Edit Local Full Zone Database] を選択します。

**b.** [Edit Local Full Zone Database] ダイアログボックスの [VSAN] ドロップダウン メニューから [VSAN 1] を選択します。

**c.** 左側のナビゲーション ペインで [Zones] フォルダを選択して、[Insert] をクリックします。

**d.** [Zone Name] フィールドを [iscsi-zone-1] に設定して、[OK] をクリックします。

**e.** 左側のナビゲーション ペインで [iscsi-zone-1] フォルダを選択して、[Insert] をクリックします。

**f.** [ZoneBy] オプション ボタンを [WWN] に設定します。

**g.** Port WWN をファイバ チャネル ターゲットの pWWN（つまり、21:00:00:20:37:6f:fd:97）に設定します。次に、[Add] をクリックします。

**h.** [ZoneBy] オプション ボタンを [iSCSI IP Address/Subnet] に設定します。

**i.** [IP Address/Mask] フィールドをホスト 1 iSCSI イニシエータ（10.11.1.10）の IP アドレスに設定して、[Add] をクリックします。

**（注）** iSCSI シンボリック ノード名または pWWN のいずれかで、iSCSI イニシエータのゾーン メンバシップのファイバ チャネル ストレージを使用できます。この場合は、pWWN は固定的です。

**ステップ 11** VSAN 1 で設定されたゾーンを作成し、アクティブ化します。

**a.** Fabric Manager で、[Zones] > [Edit Local Full Zone Database] を選択します。

**b.** [Edit Local Full Zone Database] ダイアログボックスの [VSAN] ドロップダウン メニューから [VSAN 1] を選択します。

**c.** 左側のナビゲーション ペインで [Zoneset] フォルダを選択して、[Insert] をクリックします。

**d.** [Zoneset Name] を [zonset-iscsi-1] に設定して、[OK] をクリックします。

**e.** [zoneset-iscsi-1] フォルダをクリックして、[Insert] をクリックします。

**f.** [Zone Name] フィールドを [iscsi-zone-1] に設定して、[OK] をクリックします。

**g.** [Activate] をクリックして、新しいゾーン セットをアクティブにします。

**h.** [Continue Activation] をクリックして、アクティブ化を完了します。

**ステップ 12** ホスト 2 と 2 つのファイバ チャネル ターゲットを含むゾーンを作成します。

**（注）** ホストが VSAN 2 にある場合、ファイバ チャネル ターゲットとゾーンも、VSAN 2 になければなりません。

**（注）** iSCSI インターフェイスは、ノード名に基づいてすべてのホストを特定するように設定されています。

**a.** Fabric Manager で、[Zones] > [Edit Local Full Zone Database] を選択します。

**b.** [Edit Local Full Zone Database] ダイアログボックスの [VSAN] ドロップダウン メニューから [VSAN 2] を選択します。

**c.** 左側のナビゲーション ペインで [Zones] フォルダを選択して、[Insert] をクリックします。

**d.** [Zone Name] フィールドを [iscsi-zone-2] に設定して、[OK] をクリックします。

**e.** 左側のナビゲーション ペインで [iscsi-zone-2] フォルダを選択して、[Insert] をクリックします。

**f.** [ZoneBy] オプション ボタンを [WWN] に設定します。

**g.** Port WWN をファイバ チャネル ターゲットのいずれかの pWWN（例 : 21:00:00:20:37:6f:fe:5）に設定して、[Add] をクリックします。

**h.** Port WWN をファイバ チャネル ターゲットの別の pWWN（例 : 21:00:00:20:37:a6:a6:5d）に設定して、[Add] をクリックします。

**i.** [ZoneBy] オプション ボタンを [iSCSI IP Address/Subnet] に設定します。

**j.** [IP Address/Mask] フィールドをホスト 2 iSCSI イニシエータ（10.15.1.11）の IP アドレスに設定して、[Add] をクリックします。

**ステップ 13**　VSAN 2 で設定されたゾーンを作成し、アクティブ化します。

**a.** Fabric Manager で、[Zones] > [Edit Local Full Zone Database] を選択します。

**b.** [Edit Local Full Zone Database] ダイアログボックスの [VSAN] ドロップダウン メニューから [VSAN 2] を選択します。

**c.** 左側のナビゲーション ペインで [Zoneset] フォルダを選択して、[Insert] をクリックします。

**d.** [Zoneset Name] を [zonset-iscsi-2] に設定して、[OK] をクリックします。

**e.** [zoneset-iscsi-2] フォルダをクリックして、[Insert] をクリックします。

**f.** [Zone Name] フィールドを [iscsi-zone-2] に設定して、[OK] をクリックします。

**g.** [Activate] をクリックして、新しいゾーン セットをアクティブにします。

**h.** [Continue Activation] をクリックして、アクティブ化を完了します。

**ステップ 14**　両方のホストで、iSCSI クライアントを起動します。

**ステップ 15**　すべての iSCSI セッションを表示します。

**a.** Device Manager で、[Interface] > [Monitor] > [Ethernet] を選択し、[iSCSI connections] タブをクリックして、すべての iSCSI セッションを表示します。

**b.** Device Manager で、[IP] > [iSCSI] を選択して、[Session Initiators] タブを選択します。

**c.** [Details] をクリックします。

**ステップ 16**　Fabric Manager で、[Physical Attributes] ペインで、[End Devices] > [iSCSI] を選択して、2 つの iSCSI イニシエータの詳細を確認します。

**ステップ 17**　Fabric Manager で、[Zones] > [Edit Local Full Zone Database] を選択して、アクティブなゾーン セットを表示します。iSCSI イニシエータの FC ID が解決されます。

**ステップ 18**　Device Manager で、[FC] > [Name Server] を選択します。ファイバ チャネル ネーム サーバには、iSCSI ホストに対して作成された仮想 N ポートが表示されます。

**ステップ 19**　Device Manager で、[FC] > [Name Server] を選択します。

**ステップ 20**　[Advanced] タブをクリックします。ファイバ チャネル ネーム サーバの iSCSI イニシエータ ノードの詳細出力を確認します。

# iSNS

インターネット ストレージ ネーム サービス（iSNS）では、iSCSI デバイスの検出、管理、および設定を自動化することで、既存の TCP/IP ネットワークを SAN としてより効果的に機能させることができます。このような機能を容易に動作させるために、iSNS サーバとクライアントは次のように機能します。

- iSNS クライアントは、iSNS サーバでアクセスできる iSCSI ポータルとすべての iSCSI デバイスを登録します。
- iSNS サーバは iSNS クライアントに次のサービスを提供します。
  - デバイス登録
  - 状態変更通知
  - リモート ドメイン検出サービス

iSNS クライアントとして動作するすべての iSCSI デバイス（イニシエータとターゲット）は、iSNS サーバで登録できます。iSCSI イニシエータは、次に、ターゲットのリストの iSNS サーバに問い合せます。iSNS サーバは、設定されたアクセス制御パラメータに基づいて問い合せクライアントがアクセスできるターゲットのリストで応答します。

Cisco MDS 9000 ファミリ スイッチは、iSNS クライアントとして動作し、外部 iSNS サーバですべての利用可能な iSCSI ターゲットを登録します。IPS モジュールまたは MPS-14/2 モジュールがインストールされている Cisco MDS 9000 ファミリのすべてのスイッチは、iSNS サーバ機能をサポートします。これによって、iSCSI などの外部 iSNS クライアントは、スイッチを登録し、SAN のすべての利用可能な iSCSI ターゲットを検出できます。

ここで説明する内容は、次のとおりです。



## iSNS クライアント機能の概要

各 IPS インターフェイスの iSNS クライアント機能（ギガビット イーサネット インターフェイスまたはサブインターフェイス、あるいは PortChannel）は、iSNS サーバで情報を登録します。iSNS プロファイルを作成し、サーバの IP アドレスをプロファイルに追加し、プロファイルをインターフェイスに割り当て（タギング）することで、iSNS サーバの IP アドレスを指定する必要があります。iSNS プロファイルは、1 つ以上のインターフェイスにタギングできます。

プロファイルがインターフェイスにタギングされると、スイッチはプロファイルの iSNS サーバの IP アドレス（一般的な iSNS ポート番号 3205 を使用）への TCP 接続を開き、ネットワーク エンティティとポータル オブジェクトを登録します。一意のエンティティは各 IPS インターフェイスに関連付けられます。次に、スイッチは Fibre Channel Name Server（FCNS; ファイバ チャネル ネーム サーバ）データベースとスイッチ設定を検索して、iSNS サーバで登録するストレージ ノードを検索します。

関連付けられたファイバ チャネル pWWN が FCNS データベースにあり、アクセス コントロール設定がそれを防止しない場合、静的にマッピングされた仮想ターゲットが登録されます。動的なターゲット インポートがイネーブルになっている場合は、動的にマッピングされたターゲットが登録されます。iSCSI によるファイバ チャネル ターゲットのインポート方法に関する詳細については、「iSCSI ターゲットとしてのファイバ チャネル ターゲットの提示」（P.4-9）を参照してください。

設定が変更（アクセス コントロール変更または動的インポートのディセーブル化など）された場合や、ファイバ チャネル ストレージ ポートがオフラインになったときに、ストレージ ノードが利用できなくなると、ストレージ ノードは iSNS サーバから登録解除されます。ノードがオンラインになると、再登録されます。

iSNS クライアントが iSNS サーバでオブジェクトを登録または登録解除できないとき（たとえば、クライアントが iSNS サーバに対する TCP 接続を作成できない場合）には、毎分再試行して、iSNS サーバに影響するインターフェイスのすべての iSNS オブジェクトを再登録しようとします。iSNS クライアントが使用する登録間隔は 15 分です。クライアントがこの時間の間に登録を更新できない場合、サーバはエントリを登録解除します。

プロファイルのタギングを解除しても、ネットワーク エンティティとポータルは、そのインターフェイスから登録解除されます。

（注）　iSNS クライアントは VRRP インターフェイスではサポートされていません。

# iSNS クライアント プロファイルの作成

Fabric Manager を使用して iSNS プロファイルを作成する場合は、次の手順に従います。

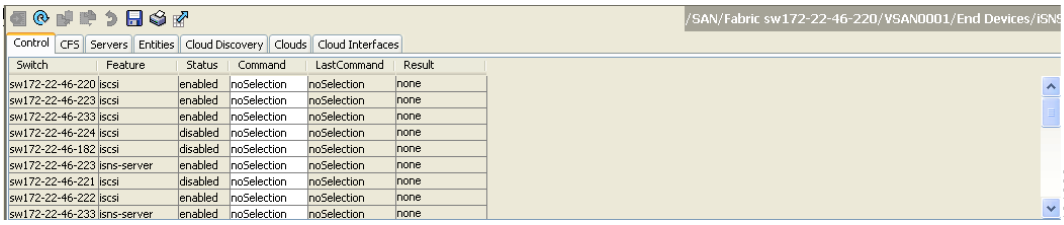
**ステップ 1**　[Physical Attributes] ペインで [End Devices] > [iSCSI] を選択します。

[Information] ペインに iSCSI 設定が表示されます（図 4-12 を参照）。

**ステップ 2**　[iSNS] タブを選択します。

**ステップ 3**　設定された iSNS プロファイルが表示されます（図 4-46 を参照）。

**図 4-46　Fabric Manager の iSNS プロファイル**




**ステップ 4**　[Create Row] アイコンをクリックします。

[Create iSNS Profiles] ダイアログボックスが表示されます。

**ステップ 5**　[ProfileName] フィールドを作成する iSNS プロファイル名に設定します。

**ステップ 6**　[ProfileAddr] フィールドを iSNS サーバの IP アドレスに設定します。

**ステップ 7**　[Create] をクリックして変更を保存します。

Fabric Manager を使用して iSNS プロファイルを削除する場合は、次の手順に従います。

**ステップ 1**　[Physical Attributes] ペインの [End Devices] > [iSCSI] を選択します。

[Information] ペインに iSCSI 設定が表示されます（図 4-12 を参照）。

**ステップ 2**　[iSNS] タブを選択します。

設定された iSNS プロファイルが表示されます（図 4-46 を参照）。

**ステップ 3**　削除するプロファイルを右クリックして、[Delete Row] アイコンをクリックします。

Fabric Manager を使用してインターフェイスにプロファイルをタギングする場合は、次の手順に従います。

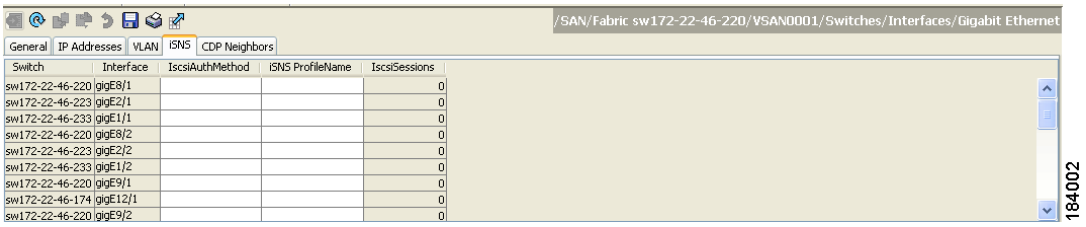
**ステップ 1**　[Physical Attributes] ペインで [Switches] > [Interfaces] > [Gigabit Ethernet] を選択します。

[Information] ペインにギガビット イーサネットの設定が表示されます。

**ステップ 2**　[iSNS] タブをクリックします。

これらのインターフェイスに設定された iSNS プロファイルが表示されます（図 4-47 を参照）。

**図 4-47　Fabric Manager の iSNS プロファイル**




**ステップ 3**　[iSNS ProfileName] フィールドをこのインターフェイスに追加する iSNS プロファイル名に設定します。

**ステップ 4**　[Apply Changes] アイコンをクリックして、これらの変更を保存します。

Fabric Manager を使用してインターフェイスからプロファイルのタギングを解除する場合は、次の手順に従います。

**ステップ 1**　[Physical Attributes] ペインで [Switches] > [Interfaces] > [Gigabit Ethernet] を選択します。

[Information] ペインにギガビット イーサネットの設定が表示されます。

**ステップ 2**　[iSNS] タブをクリックします。

これらのインターフェイスに設定された iSNS プロファイルが表示されます（図 4-47 を参照）。

**ステップ 3**　タグを解除する [iSNS ProfileName] フィールドを右クリックして、そのフィールドのテキストを削除します。

**ステップ 4**　[Apply Changes] アイコンをクリックして、これらの変更を保存します。

# iSNS サーバ機能の概要

イネーブルにすると、Cisco 9000 ファミリ MDS スイッチの iSNS サーバは、すべての登録された iSCSI デバイスを追跡します。結果として、iSNS クライアントは、iSNS サーバに問い合せて、その他の iSNS クライアントを検索できます。iSNS サーバは次の機能も提供します。

- iSNS クライアントは、iSNS サーバで登録されたその他の iSNS クライアントの登録、登録解除、および問い合せができます。
- アクセス コントロールの実行を一元的に管理し、特定のイニシエータからターゲットへのアクセスを許可または拒否します。
- 登録された iSNS クライアントに通知メカニズムを提供し、他の iSNS クライアントのステータス変更に関する変更通知を受信します。
- ファイバ チャネルと iSCSI デバイスの両方に単一のアクセス コントロール設定を提供します。
- iSCSI イニシエータへの直接 IP 接続がない iSCSI ターゲットを検出します。

## シナリオの例

iSNS サーバは、ファイバ チャネル ゾーニング情報と iSCSI アクセス コントロール情報と設定の両方を使用して、ファイバ チャネルと iSCSI デバイス全体で均一のアクセス コントロールを提供します。iSNS クライアントとして動作する iSCSI イニシエータだけが、アクセス コントロール情報の両方のセットに基づいてアクセスできるデバイスを検出できます。図 4-48 に、このシナリオの例を示します。

**図 4-48　Cisco MDS 環境における iSNS サーバの使用方法**

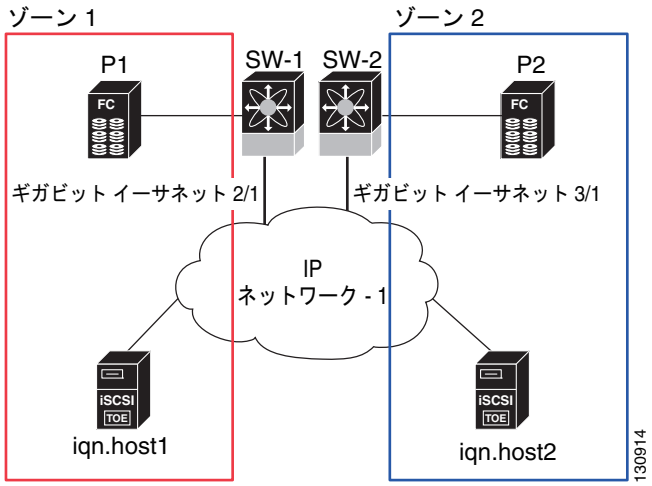



図 4-48 では、iqn.host1 および iqn.host2 が iSCSI イニシエータです。P1 および P2 はファイバ チャネル ターゲットです。2 つのイニシエータは別のゾーンにあります。ゾーン 1 は iqn.host1 とターゲット P1 から構成され、ゾーン 2 は iqn.host2 とターゲット P2 から構成されます。iSNS サーバ機能は、SW-1 と SW-2 の両方のスイッチでイネーブルになっています。登録処理は次の方法で実行されます。

1. Initiator iqn.host1 は SW-1、ポート Gigabitethernet2/1 で登録します。
2. Initiator iqn.host2 は SW-2、ポート Gigabitethernet3/1 で登録します。
3. Initiator iqn.host1 は SW-1 に対して iSNS クエリを発行して、すべてのアクセス可能なターゲットを判断します。

4. 次に、iSNS サーバがファイバ チャネル ネーム サーバ（FCNS）に問い合せ、クエリ送信側からアクセスできる同じゾーンにあるデバイスのリストを取得します。このクエリは P1 だけを生成します。
5. 次に、iSNS サーバは独自のデータベースに問い合せ、ファイバ チャネル デバイスを対応する iSCSI ターゲットに変換します。これは、仮想ターゲットおよびアクセス コントロール設定、あるいは動的ファイバ チャネル ターゲット インポート機能がイネーブルかディセーブルかなどの iSCSI 設定に基づいています。
6. iSNS サーバはクエリ送信側に応答を送信します。この応答には iSNS サーバが認識しているすべての iSCSI ポータルのリストが含まれています。つまり、iqn.host1 は、SW-1（Gigabitethernet 2/1）または SW-2（Gigabitethernet 3/1）経由で、ターゲット P1 へのログインを選択できます。
7. イニシエータが SW-1 にログインすることを選択し、後からそのポートがアクセスできなくなった場合（たとえば、Gigabitethernet 2/1 がダウンした場合）は、イニシエータは代わりに SW-2 のポート Gigabitethernet 3/1 経由でターゲット P1 に接続することを選択できます。
8. ターゲットがダウンしているか、ゾーンから削除されている場合は、iSNS サーバは iSNS State Change Notification（SCN）メッセージをイニシエータに送信するため、イニシエータはセッションを削除できます。

# iSNS サーバの設定

ここでは、Cisco MDS 9000 ファミリ スイッチの iSNS サーバの設定方法について説明します。

ここで説明する内容は、次のとおりです。



## iSNS サーバのイネーブル化

iSNS サーバ機能をイネーブルにするには、iSCSI をイネーブルにする必要があります（「iSCSI のイネーブル化」（P.4-5）を参照）。iSCSI をディセーブルにすると、iSNS が自動的にディセーブルになります。iSNS サーバがスイッチ上でイネーブルになると、対応する iSCSI インターフェイスが起動しているすべての IPS ポートでは、外部 iSNS クライアントからの iSNS 登録とクエリ要求を処理できます。

Fabric Manager を使用して iSNS サーバをイネーブルにする場合は、次の手順に従います。

**ステップ 1**　[End Devices] > [iSNS] を選択します。

[Information] ペインに iSNS 設定が表示されます。

**ステップ 2**　[Control] タブをクリックして、iSNS サーバ機能の [Command] ドロップダウン メニューから [enable] を選択します。

**ステップ 3**　[Apply Changes] アイコンをクリックして、この変更を保存します。

（注）　iSNS クライアントからターゲットを検出するときに、VRRP IPv4 アドレスを使用している場合は、[secondary] オプションを使用して、IP アドレスを作成していることを確認します。

## iSNS 設定配布

CFS インフラストラクチャを使用して、ファブリック全体の iSNS サーバに iSCSI イニシエータ設定を配布できます。これによって、すべてのスイッチで稼動中の iSNS サーバが、問い合せ側の iSNS クライアントに対し、ファブリックの任意の場所にある利用可能な iSCSI デバイスのリストを提供できます。CFS については、『*Cisco Fabric Manager System Management Configuration Guide*』を参照してください。

Fabric Manager を使用して iSNS 設定配布をイネーブルにする場合は、次の手順に従います。

**ステップ 1**　[End Devices] > [iSNS] を選択します。

[Information] ペインに iSNS 設定が表示されます。

**ステップ 2**　[CFS] タブをクリックして、iSNS の [Admin] ドロップダウン メニューから [enable] を選択します。

**ステップ 3**　iSNS の [Global] ドロップダウン メニューから、[enable] を選択します。

**ステップ 4**　[Apply Changes] アイコンをクリックして、この変更を保存します。

## ESI 再試行カウントの設定

iSNS クライアントは、iSNS プロファイルを使用して、設定した iSNS サーバに情報を登録します。登録時には、クライアントは 60 秒以上の Entity Status Inquiry（ESI; エンティティ ステータス照会）間隔を示すことができます。クライアントが ESI 間隔をゼロ（0）に設定して登録する場合は、サーバは ESI を使用してクライアントを監視しません。このような場合、明示的に登録解除されるか、iSNS サーバ機能がディセーブルになるまで、クライアントの登録は有効なままです。

ESI 再試行カウントは、iSNS サーバがエンティティ ステータスについて iSNS クライアントに問い合せる回数です。デフォルトの ESI 再試行カウントは 3 です。クライアントはサーバにまだ有効であることを示す応答を送信します。設定した再試行回数を超えてもクライアントが応答できない場合は、クライアントはサーバから登録解除されます。

## 登録期間の設定

iSNS クライアントは、iSNS サーバで登録期間を指定します。iSNS サーバは、この期間が終了するまで、登録をアクティブな状態に保ちます。この期間中に iSNS クライアントからのコマンドがない場合は、iSNS サーバはデータベースからクライアント登録を削除します。

iSNS クライアントが登録期間を指定しない場合は、iSNS サーバはデフォルト値の 0 を取り、登録を無制限にアクティブに保ちます。MDS iSNS サーバで手動で登録期間を設定することもできます。

Fabric Manager を使用して iSNS サーバの登録期間を設定する場合は、次の手順に従います。

**ステップ 1**　[End Devices] > [iSNS] を選択します。

[Information] ペインに iSNS 設定が表示されます。

**ステップ 2**　[Servers] タブをクリックします。

設定した iSNS サーバが表示されます。

**ステップ 3**　[ESI NonResponse Threshold] フィールドを ESI 再試行カウント値に設定します。

**ステップ 4**　[Apply Changes] アイコンをクリックして、この変更を保存します。

## iSNS クライアント登録および登録解除

iSNS クライアントは登録されるまで、iSNS サーバに問い合せできません。

iSNS クライアントの登録解除は明示的に、あるいは（ESI 監視によって）iSNS サーバがクライアントに到達できないことを検出するときに発生します。

iSNS クライアント登録と登録解除を行うと、すべての関連する iSNS クライアントに State Change Notification（SCN）が送信されます。

## ターゲット検出

iSCSI イニシエータは、iSNS サーバにクエリを発行して、ターゲットを検出します。サーバはターゲットのリストを検索する *DevGetNext* 要求と、IP アドレスや接続先ポート番号などのターゲットとポータル詳細情報を判定する *DevAttrQuery* をサポートしています。

iSCSI クライアントからクエリ要求を受信すると、iSNS サーバはファイバ チャネル ネーム サーバ（FCNS）に問い合せ、問い合せ側のイニシエータからアクセスできるファイバ チャネル ターゲットのリストを取得します。このクエリの結果は、現在アクティブなゾーニング設定および現在のイニシエータの設定に依存します。iSNS サーバは続いて iSCSI ターゲット設定を使用して、ファイバ チャネル ターゲット設定（仮想ターゲットと動的インポート設定）を同等の iSCSI ターゲットに変換します。この段階では、仮想ターゲットに対して設定されたアクセス コントロールに適用されます。次に、ターゲット詳細に関する応答メッセージが問い合せのイニシエータに送信されます。

iSNS サーバは、問い合せ側のイニシエータに、すべての可能なターゲットとポータルを含む包括的な応答を送信します。たとえば、ファイバ チャネル ターゲットが別の iSCSI ターゲットとして異なる IPS インターフェイスにエクスポートされる場合は、iSNS サーバはすべての可能な iSCSI ターゲットとポータルのリストで応答します。

ターゲットのリストを最新の状態に保つために、iSNS サーバは、iSCSI ターゲットが到達可能か到達不可能になると、必ず State Change Notification（SCN）をクライアントに送信します。これで、クライアントは、別の iSNS クエリを開始して、アクセス可能なターゲットのリストを再検出できるようになります。次のいずれかが発生すると、iSCSI ターゲットの到達可能性が変わります。

- ターゲットが起動またはダウンした。
- FC ターゲット設定の動的インポートが変更された。
- ゾーン セットが変更された。
- デフォルト ゾーン アクセス コントロールが変更された。
- IPS インターフェイス状態が変更された。
- イニシエータ設定変更により、ターゲットがアクセス可能または不可能になった。

# iSNS クラウド検出

IP ネットワークの iSNS サーバを検出するプロセスを自動化するように iSNS クラウド検出を設定できます。

ここで説明する内容は、次のとおりです。



## クラウド検出の概要

（注）　iSNS クラウド検出は、IBM BladeCenter および Cisco Fabric Switch for HP c-Class BladeSystem の Cisco ファブリック スイッチではサポートされていません。

iSNS サーバがクエリ要求を受信すると、iSNS サーバはイニシエータがターゲットに到達できる利用可能なターゲットとポータルのリストで応答します。MDS スイッチ外の IP ネットワーク設定により、イニシエータから到達可能なのがギガビット イーサネット インターフェイスのサブセットだけになる場合があります。イニシエータに返されるポータルのセットが到達可能であることを保証するためには、iSNS サーバがそのイニシエータから到達可能な一連のギガビット イーサネット インターフェイスについて認識している必要があります。

iSNS クラウド検出機能では、スイッチ上のインターフェイスを分割された IP クラウドにパーティショニングすることで、イニシエータから到達可能なさまざまなインターフェイスについての情報を iSNS サーバに提供します。この検出では、現在起動しているすべての既知の IPS ポートにメッセージを送信し、応答の有無に基づいて、リモート IPS ポートが同じ IP ネットワークにあるか異なる IP ネットワークにあるかを判断します。

次のイベントの発生時に、クラウド検出が開始されます。

- CLI からの手動要求が CLI からのクラウド検出を開始した。このアクションを実行すると、既存のメンバシップが破壊され、新しいメンバシップが作成されます。
- インターフェイスの自動検出では、正しいクラウドにインターフェイスが割り当てられます。その他のすべてのクラウド メンバーは影響を受けません。各クラウドのメンバシップは増分的に構築され、次のイベント時に開始されます。
  - ギガビット イーサネット インターフェイスが起動した。これは、ローカルとリモートのいずれのギガビット イーサネット インターフェイスも該当します。
  - ギガビット イーサネット インターフェイスの IP アドレスが変更された。
  - ポート上の VRRP 設定が変更された。

iSNS サーバは CFS を使用してすべてのスイッチにクラウドおよびメンバシップ情報を配信します。したがって、クラウド メンバシップ表示は、ファブリックのすべてのスイッチで同じになります。

（注）　CFS 配布が iSNS クラウド検出で正常に動作するためには、ファブリックのすべてのスイッチで Cisco SAN-OS リリース 3.0(1) または NX-OS 4.1(1b) 以上が稼動していなければなりません。

# iSNS クラウド検出の設定

ここでは、iSNS クラウド検出の設定方法について説明します。ここで説明する内容は、次のとおりです。



## iSNS クラウド検出のイネーブル化

Fabric Manager を使用して iSNS クラウド検出をイネーブルにする場合は、次の手順に従います。

**ステップ 1**　[End Devices] > [iSNS] を選択します。

[Information] ペインに iSNS 設定が表示されます。

**ステップ 2**　[Control] タブをクリックして、クラウド検出機能の [Command] ドロップダウン メニューから [enable] を選択します。

**ステップ 3**　[Apply Changes] アイコンをクリックして、この変更を保存します。

## オンデマンド iSNS クラウド検出の開始

Fabric Manager を使用してオンデマンド iSNS クラウド検出を開始する場合は、次の手順に従います。

**ステップ 1**　[End Devices] > [iSNS] を選択します。

[Information] ペインに iSNS 設定が表示されます。

**ステップ 2**　[Cloud Discovery] タブをクリックして、[Manual Discovery] チェックボックスをオンにします。

**ステップ 3**　[Apply Changes] アイコンをクリックして、この変更を保存します。

## 自動 iSNS クラウド検出の設定

Fabric Manager を使用して自動 iSNS クラウド検出をイネーブルにする場合は、次の手順に従います。

**ステップ 1**　[End Devices] > [iSNS] を選択します。

[Information] ペインに iSNS 設定が表示されます。

**ステップ 2**　[Cloud Discovery] タブをクリックして、[AutoDiscovery] チェックボックスをオンにします。

**ステップ 3**　[Apply Changes] アイコンをクリックして、この変更を保存します。

## iSNS クラウド検出配布の設定

Fabric Manager を使用して iSNS クラウド検出 CFS 配布をイネーブルにする場合は、次の手順に従います。

**ステップ 1**　[End Devices] > [iSNS] を選択します。

[Information] ペインに iSNS 設定が表示されます。

**ステップ 2**　[CFS] タブをクリックして、クラウド検出機能の [Admin] ドロップダウン メニューから [enable] を選択します。

**ステップ 3**　クラウド検出機能の [Global] ドロップダウン メニューから、[enable] を選択します。

**ステップ 4**　[Apply Changes] アイコンをクリックして、この変更を保存します。

# デフォルト設定

表 4-2 に、iSCSI パラメータのデフォルト設定を示します。

**表 4-2　デフォルト iSCSI パラメータ**

| パラメータ | デフォルト |
|---|---|
| TCP 接続数 | iSCSI セッションごとに 1 つ |
| **minimum-retransmit-time** | 300 ミリ秒 |
| **keepalive-timeout** | 60 秒 |
| **max-retransmissions** | 4 回の再送信 |
| PMTU 検出 | イネーブル |
| **pmtu-enable reset-timeout** | 3600 秒 |
| SACK | イネーブル |
| **max-bandwidth** | 1 Gbps |
| **min-available-bandwidth** | 70 Mbps |
| **round-trip-time** | 1 ミリ秒 |
| バッファ サイズ | 4096 KB |
| 制御 TCP およびデータ接続 | パケット送信なし |
| TCP 輻輳ウィンドウの監視 | イネーブル |
| バースト サイズ | 50 KB |
| ジッタ | 500 マイクロ秒 |
| TCP 接続モード | アクティブ モードがイネーブル |
| iSCSI へのターゲット ファイバ チャネル | 未インポート |
| iSCSI ターゲットのアドバタイズ | すべてのギガビット イーサネット インターフェイス、サブインターフェイス、PortChannel インターフェイス、および PortChannel サブインターフェイスでアドバタイズ |
| 仮想ファイバ チャネル ホストへの iSCSI ホスト マッピング | 動的マッピング |

表 4-2　デフォルト iSCSI パラメータ （続き）

| パラメータ | デフォルト |
|---|---|
| 動的 iSCSI イニシエータ | VSAN 1 のメンバー |
| イニシエータの識別 | iSCSI ノード名 |
| 静的仮想ターゲットのアドバタイズ | 仮想ターゲットへのアクセスを許可されているイニシエータはありません（明示的に設定されている場合を除く） |
| iSCSI ログイン認証 | CHAP または非認証メカニズム |
| **revert-primary-port** | ディセーブル |
| ヘッダーおよびデータ ダイジェスト | iSCSI イニシエータが要求を送信するときに自動的にイネーブル。この機能は store-and-forward モードでは設定および使用できません。 |
| iSNS 登録間隔 | 60 秒（設定不可） |
| iSNS 登録間隔の再試行 | 3 |
| ファブリック配信 | ディセーブル |

表 4-3 に、iSLB パラメータのデフォルト設定を示します。

表 4-3　デフォルト iSLB パラメータ

| パラメータ | デフォルト |
|---|---|
| ファブリック配信 | ディセーブル |
| ロード バランシング メトリック | 1000 |