iSCSI の構成

Cisco MDS 9000 ファミリの IP ストレージ（IPS）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することによって、ファイバ チャネル SAN の到達距離を延長します。IP ホストは Internet Small Computer Systems Interface（iSCSI）プロトコルを使用して、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 ポートを搭載したファイバ チャネル モジュール固有で、Cisco MDS 9200 スイッチまたは Cisco MDS 9500 ディレクタで使用可能です。Cisco MDS NX-OS リリース 7.3(0)DY(1) 以降で iSCSI は 24/10 ポート SAN の拡張モジュールを搭載した Cisco MDS 9700 Director でサポートされていません。

Cisco MDS 9216i スイッチと 14/2 マルチプロトコル サービス（MPS-14/2）モジュールでは、ファイバ チャネル、FCIP、および iSCSI 機能も使用できます。MPS-14/2 モジュールは、Cisco MDS 9200 シリーズまたは Cisco MDS 9500 シリーズのすべてのスイッチで使用できます。

この章は、次の項で構成されています。

iSCSI の概要

Cisco MDS 9000 ファミリの IP ストレージ（IPS）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することによって、ファイバ チャネル SAN の到達距離を延長します。iSCSI 機能は、IP ネットワーク内の iSCSI ホストと、Cisco MDS 9000 ファミリ スイッチの任意のファイバ 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 のファイバ チャネル ストレージ デバイス間で、iSCSI 要求および応答をルーティングします。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。iSCSI 機能を使用するには、ファブリック内の目的のスイッチ上で iSCSI を明示的にイネーブルにする必要があります。

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

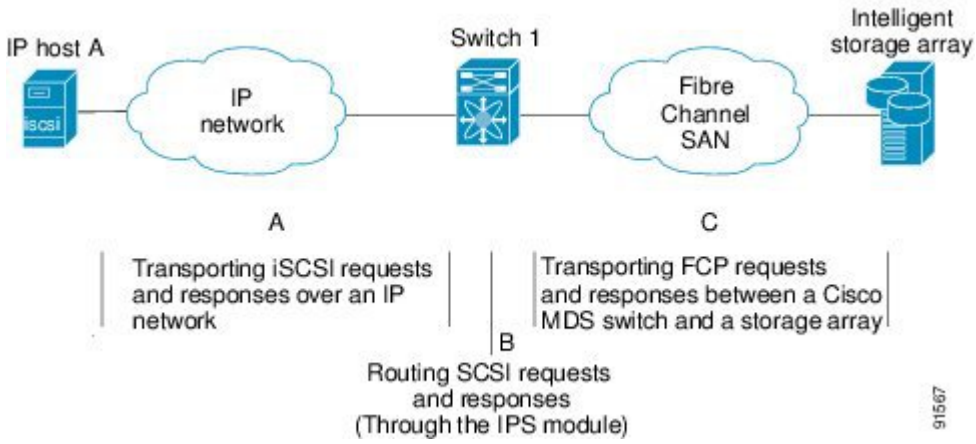
iSCSI 機能は、IP ネットワーク内の iSCSI ホストと、Cisco MDS 9000 ファミリ スイッチの任意のファイバ チャネル インターフェイスからアクセス可能なファイバ チャネル SAN のファイバ チャネル ストレージ デバイス間で、iSCSI 要求および応答をルーティングします。

IPS ポートを搭載したファイバ チャネル 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がある 各 iSCSI ホストには、互換性のある iSCSI ドライバをインストールしておく必要があります。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 ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールは、透過型 SCSI ルーティングを実行します。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。

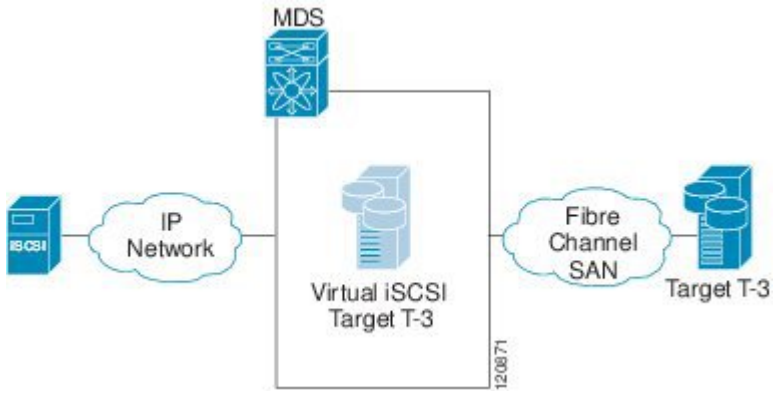
IP ネットワークを介して IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールに接続し、ファイバ チャネル SAN 上のファイバ チャネル ストレージにアクセスする、iSCSI ホストの一般的な構成例を示します（ 次の図を参照）。

図 *1 : iSCSI* 要求および応答の転送（透過型 *iSCSI* ルーティングの場合）



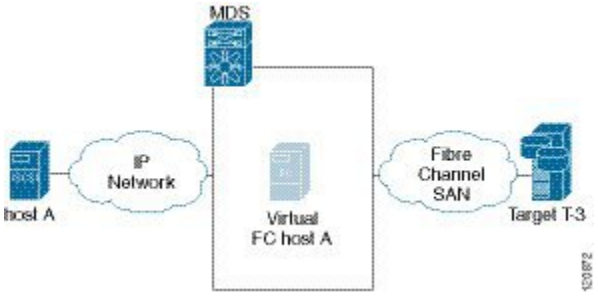
IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールは、独立した iSCSI SAN ビューおよびファイバ チャネル SAN ビューを作成します。iSCSI SAN ビューの場合、IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールが iSCSI 仮想ターゲットを作成し、それをファイバ チャネル SAN で使用できる物理ファイバ チャネル ターゲットに対応付けます。これらのモジュールは、物理 iSCSI ターゲットが IP ネットワークに接続されているかのように、ファイバ チャネル ターゲットを IP ホストに提示します。

図 *2 : iSCSI SAN* ビュー：*iSCSI* 仮想ターゲット



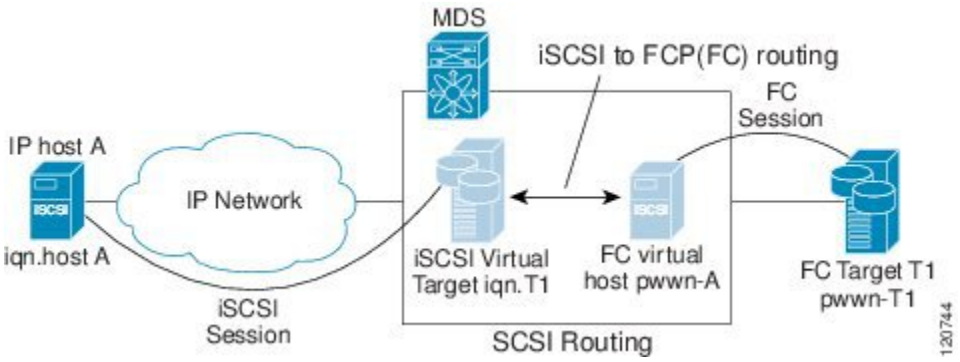
ファイバ チャネル SAN ビューの場合、IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールが仮想ファイバ チャネル ホストとして iSCSI ホストを提示します。ストレージ デバイスは、実ファイバ チャネル ホストで実行される通信と同様に、仮想ファイバ チャネル ホストと通信します。

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



IPS ポートを搭載したファイバ チャネル 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 ホスト間で、コマンドを透過的にマッピングします。

図 *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 デバイスへのルーティングでは、主に次の処理が実行されます。

- IP ネットワークを介して、ホストと IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュール間で iSCSI 要求および応答が転送されます。
- 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間で、SCSI 要求および応答がルーティングされます（iSCSI を FCP に変換したり、その逆の変換を行ったりします）。IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールで、この変換とルーティングを実行します。
- IPS ポートを搭載したファイバ チャネル 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 デバイス間で、FCP 要求または応答が転送されます。

（注） iSCSI に相当するファイバ チャネル(FCP)は、ファイバ チャネル SAN を介して SCSI コマンドを伝送します。iSCSI プロトコルの詳細については、http://www.ietf.org で IP ストレージに関する IETF 標準規格を参照してください。

iSCSI の設定制限

iSCSI の設定に関しては、次の限度があります。

- ファブリックでサポートされる iSCSI および iSLB 発信側の最大数は 2000 です。
- サポートされる iSCSI および iSLB 発信側の最大数はポートごとに 200 です。
- 透過型またはプロキシイニシエータ モードで IPS ポートがサポートする iSCSI および iSLB セッションの最大数は 500 です。
- スイッチがサポートする iSCSI および iSLB セッションの最大数は 5000 です。
- ファブリックでサポートされる iSCSI および iSLB ターゲットの最大数は 6000 です。

iSCSI の構成

Cisco MDS 9000 ファミリの IP ストレージ（IPS）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することによって、ファイバ チャネル SAN の到達距離を延長します。IP ホストは Internet Small Computer Systems Interface（iSCSI）プロトコルを使用して、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 ポートを搭載したファイバ チャネル モジュール固有で、Cisco MDS 9200 スイッチまたは Cisco MDS 9500 ディレクタで使用可能です。Cisco MDS NX-OS リリース 7.3(0)DY(1) 以降で iSCSI は 24/10 ポート SAN の拡張モジュールを搭載した Cisco MDS 9700 Director でサポートされていません。

Cisco MDS 9216i スイッチと 14/2 マルチプロトコル サービス（MPS-14/2）モジュールでは、ファイバ チャネル、FCIP、および iSCSI 機能も使用できます。MPS-14/2 モジュールは、Cisco MDS 9200 シリーズまたは Cisco MDS 9500 シリーズのすべてのスイッチで使用できます。

（注） ギガビット イーサネット インターフェイスの構成については、「IPv4 の基本的なギガビット イーサネット構成」のセクションを参照してください。

この章は、次の項で構成されています。

iSCSI のイネーブル化

iSCSI 機能を使用するには、ファブリック内の目的のスイッチ上で iSCSI を明示的に有効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、この機能は Cisco MDS 9000 ファミリのすべてのスイッチでディセーブルになっています。

参加させるスイッチの iSCSI を有効にするには、次のステップを実行します。

始める前に

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。

手順

ステップ 1 構成コマンドを1行に1つずつ入力します。CNTL/Z で終了します

switch# **config terminalerminal**

ステップ 2 スイッチ上で iSCSI を有効にします。

switch(config)# **feature iscsi**

ステップ 3 現在のスイッチ上で iSCSI を無効（デフォルト）にします。

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

ステップ 4 スイッチ上で iSCSI モジュールを有効にします。

switch(config)# **iscsi enable module <x>**

（注）
SME と iSCSI を同一スイッチ上で使用可能にする新しいコマンドが追加されました。

ステップ 5 スイッチの iSCSI モジュールを無効にします。

switch(config)# **no iscsi enable module <x>**

仮想ファイバ チャネル ホストとしての iSCSI ホストの提示

IPS ポートまたは MPS-14/2 モジュールを搭載したファイバ チャネルは、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、ストレージ デバイスにコマンドを送信し、ストレージデバイスと相互にデータを転送します。これらのモジュールでは、仮想ファイバ チャネル N ポートを使用して、iSCSI ホストに代わってファイバ 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 アドレスにより識別されます。

iSCSI インターフェイスの作成

IPS ポートを搭載したファイバチャネルモジュール、MPS-14/2 モジュール、または Cisco MDS 9250i マルチサービス ファブリック スイッチの 1/10Gbps IP ストレージ ポート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すると、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できます。反対方向では、応答を変換してルーティングできま

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 ステートでなければなりません。

iSCSI インターフェイスを有効にするには、次のステップを実行します。

始める前に

tcp maximum-bandwidth-kbps および **tcp maximum-bandwidth-mbps** コマンドを使用して iSCSI の速度を構成し、**switchport speed** コマンドを使用して物理 IP ストレージ ポートの速度を 1Gbps または 10Gbps に設定します。Cisco MDS スイッチは、基盤となる物理ギガビット イーサネット ポートまたは IP ストレージ ポートの速度に基づいて iSCSI tcp maximum-bandwidth-kbps と maximum-bandwidth-mbps を制限しません。したがって、iSCSI **tcp maximum-bandwidth-kbps** および **tcp maximum-bandwidth-mbps** コマンドを、速度 1 Gbps で実行している物理 IP ストレージ ポートで 10Gbps に相当する速度に構成できてしまいます。TCP 最大帯域幅を構成するときには、物理 IP ストレージ ポートの最大速度を超えないようにしてください。

手順

ステップ 1 必要なギガビット イーサネット インターフェイスをイネーブルにします。

```
switch# config terminal
switch(config)# interface gigabitethernet 2/1
switch(config-if)# no shutdown
switch(config-if)# exit
switch(config)#
```

ステップ 2 必要な iSCSI インターフェイスを作成し、このインターフェイスを有効にします。

```
switch(config)# interface iscsi 2/1
switch(config-if)# no shutdown
```

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 ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールは、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提示し、 iSCSI ホストからこれらへのアクセスを許可します。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 デバイスまたはポートを iSCSI デバイスとして、自動的に対応付けます。このマッピングを使用して、自動 iSCSI ターゲット名が作成されます。

  。
- スタティック マッピング：手動で iSCSI ターゲット デバイスを作成し、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 LUN のサブセットに対応付けます。このマッピングの場合は、ユーザー側で一意の iSCSI ターゲット名を指定する必要があります。

スタティック マッピングは、iSCSI ホストをファイバ チャネル ターゲット内の LU のサブセットに限定する必要がある場合、iSCSI アクセス コントロールが必要な場合、またはその両方が当てはまる場合に使用します（「iSCSI アクセス コントロール」を参照）。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を構成できます（「透過的なフェールオーバ」を参照）。

（注） IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールはデフォルトで、iSCSI にファイバ チャネル ターゲットをインポートしません。IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールで iSCSI 発信側からファイバ チャネル ターゲットを使用できるようにするには、ダイナミック マッピングまたはスタティック マッピングを構成しておく必要があります。

ダイナミック マッピング

ダイナミック マッピングを構成すると、IPS ポートを搭載したファイバ チャネル 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、各物理ファイバ チャネル ターゲット ポートを 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 ポートを介してアクセス可能なすべての LU は、物理ファイバ チャネル ターゲット ポートの場合と同じ論理ユニット番号（LUN）を持つ iSCSI LU として使用できます。

iSCSI ターゲット ノード名は、iSCSI 修飾名 （IQN）フォーマットを使用して、自動的に作成されます。iSCSI 修飾名の長さは、最大 223、最小 16 の英数字に制限されています。

名前は SAN 内で一意である必要があるため、IPS ポートを搭載したファイバチャネルモジュールまたは MPS-14/2 モジュールでは次の規則に従って、IQN フォーマットの iSCSI ターゲット ノード名を作成します。

- Virtual Router Redundancy Protocol（VRRP）グループまたはポートチャネルに属していない IPS ギガビット イーサネット ポートでは、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 ポートでは、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>
  ```

- ポート チャネルの一部であるポートではこのフォーマットを使用します。

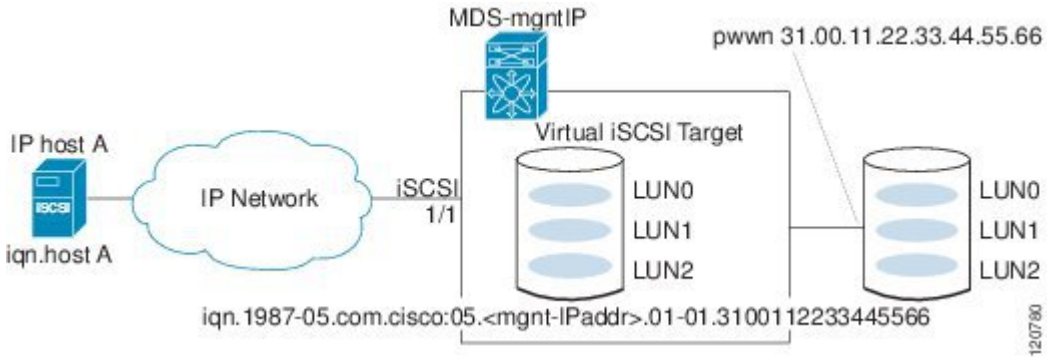
  ```
  iqn.1987-02.com.cisco:02.<mgmt-ip-address>.pc-<port-ch-sub-intf#>.<Target-pWWN>
  ```

（注） スイッチ名が設定されている場合、スイッチ名は管理 IP アドレスの代わりに使用されます。スイッチ名が設定されていない場合は、管理 IP アドレスが使用されます。

Cisco MDS 9000 ファミリ スイッチ内の各 IPS ポートはこの規則に従って、SAN 内の同じファイバ チャネル ターゲット ポートに対して一意の iSCSI ターゲット ノード名を作成します。

たとえば、pWWN が 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 ターゲットが作成され、その pWWN に LUN 0、LUN 1、および LUN 2 が含まれる場合、これらの LUN は、iSCSI ターゲット ノード名 iqn.1987-05.com.cisco:05.*MDS_switch_management_IP_address* .

図 *5:* ダイナミック ターゲット マッピング



（注） 構成されているアクセス コントロール メカニズムによっては、個々の iSCSI イニシエータで一部のターゲットにアクセスできない場合があります（「iSCSI アクセス コントロール」を参照）。

ファイバ チャネル ターゲットから *iSCSI* へのダイナミック マッピングを有効にする

ファイバ チャネル ターゲットから iSCSI へのダイナミック マッピングを有効にするには、次のステップを実行します。

手順

ステップ 1 コンフィギュレーション モードを入力します。

```
switch# config terminal
switch(config)#
```

ステップ 2 IPS ポートを搭載したファイバ チャネル モジュールと MPS-14/2 モジュールは、ファイバ チャネル SAN のファイバチャネル ターゲットをすべて IP ネットワークにダイナミックにインポートします。

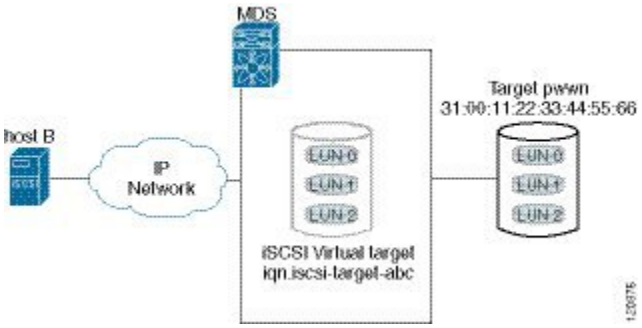
```
switch(config)# iscsi import target fc
```

スタティック マッピング

ユーザーが定義した一意の iSCSI ノード名を割り当てることによって、 iSCSI ターゲットを手動で（スタティックに）作成できます。iSCSI 修飾名の長さは、最小 16 文字、最大 223 文字に制限されています。スタティック マッピングの iSCSI ターゲットでは、ファイバチャネル ターゲット ポート全体をマッピング（ターゲット ポート内のすべての LUN を iSCSI ターゲットに

マッピング）することも、ファイバ チャネル ターゲット ポートの 1 つまたは複数の LU を含めることもできます。

図 *6:* スタティック マッピングの *iSCSI* ターゲット



（注） 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。ファイバ チャネル ターゲット ポート全体をすでにマッピングしている場合、LUN マッピング オプションは使用できません。

スタティックにマッピングされたターゲットへのアクセスを制御する手順については、「iSCSI ベース アクセス コントロール」セクション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ズ

スタティック iSCSI ターゲットをアドバタイズする場合に経由するギガビット イーサネット インターフェイスを制限できます。デフォルトでは、iSCSI ターゲットは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、ポートチャネルインターフェイス、およびポート チャネル サブインターフェイスでアドバタイズされます。

iSCSI 仮想ターゲットをアドバタイズするインターフェイスを構成する

iSCSI 仮想ターゲットをアドバタイズする特定のインターフェイスを構成するステップは、次のとおりです。

手順

ステップ 1 指定されたインターフェイスでのみ、仮想ターゲットをアドバタイズします。デフォルトでは、すべての IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールのすべてのインターフェイスでアドバタイズされます。

```
switch(config-iscsi-tgt)# advertise interface GigabitEthernet 2/5
```

（注）
仮想ターゲットを複数インターフェイスでアドバタイズするには、インターフェイスごとに次のコマンドを発行します。

ステップ 2 ターゲットのアドバタイズ元インターフェイスのリストから、このインターフェイスを削除します。

```
switch(config-iscsi-tgt)# no advertise interface GigabitEthernet 2/5
```

iSCSI 仮想ターゲットの設定例

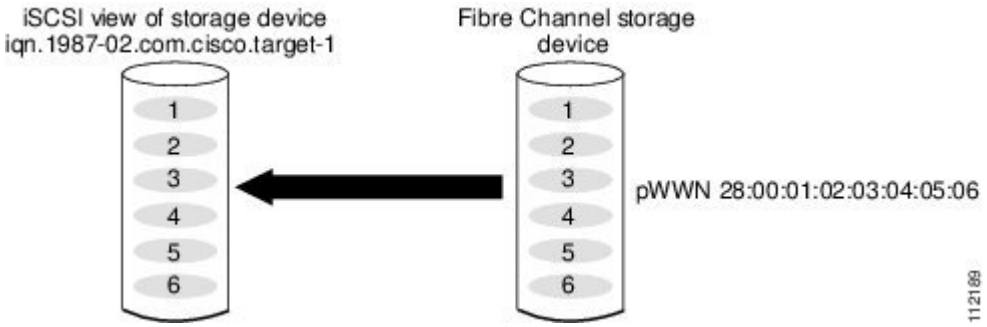
ここでは、3 種類の iSCSI 仮想ターゲット設定例を示します。

例 1

iSCSI 仮想ターゲットとしてファイバ チャネル ターゲット全体を割り当てる例を示します。ファイバ チャネル ターゲットに属しているすべての LUN を iSCSI ターゲットの一部として使用できます。

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

図 *7: iSCSI* ノード名の割り当て

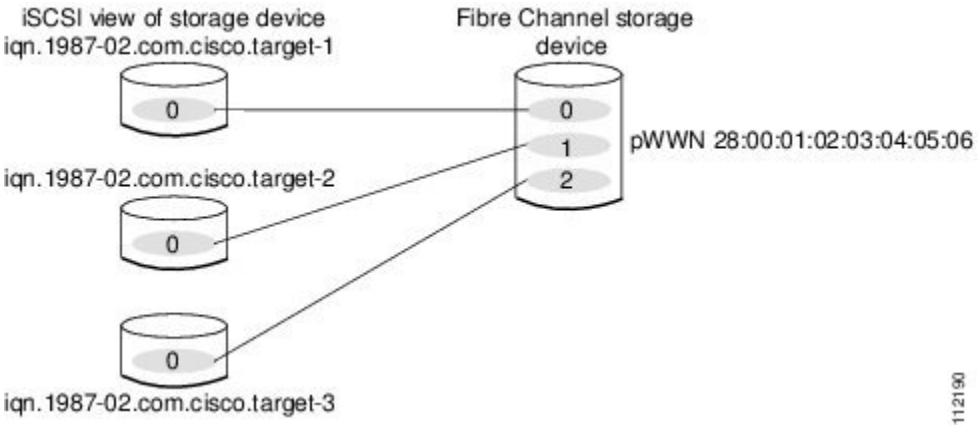


例 2

ファイバ チャネル ターゲットの LUN のサブセットを 3 つの iSCSI 仮想ターゲットにマッピングする例を示します。各 iSCSI ターゲットが所有する LUN は 1 つのみです。

```
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
```

図 *8 : iSCSI* ノード名への *LUN* のマッピング

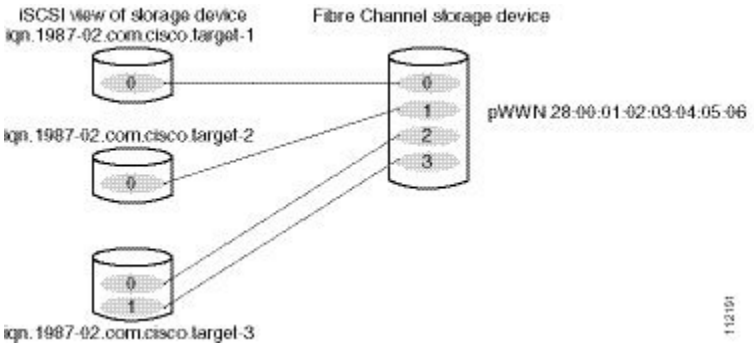


例 3

ファイバ チャネル LUN ターゲットの 3 つのサブセットを 3 つの iSCSI 仮想ターゲットにマッピングする例を示します。2 つの iSCSI ターゲットで LUN を 1 つ使用し、3 つ目の iSCSI ターゲットで LUN を 2 つ使用します。

```
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
```

図 *9 :* 複数の *iSCSI* ノード名への *LUN* のマッピング



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 ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールは、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提示し、 iSCSI ホストからこれらへのアクセスを許可します。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 デバイスまたはポートを iSCSI デバイスとして、自動的に対応付けます。このマッピングを使用して、自動 iSCSI ターゲット名が作成されます。

。

- スタティック マッピング：手動で iSCSI ターゲット デバイスを作成し、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 LUN のサブセットに対応付けます。このマッピングの場合は、ユーザー側で一意の iSCSI ターゲット名を指定する必要があります。

スタティック マッピングは、iSCSI ホストをファイバ チャネル ターゲット内の LU のサブセットに限定する必要がある場合、iSCSI アクセス コントロールが必要な場合、またはその両方が当てはまる場合に使用します（「iSCSI アクセス コントロール」を参照）。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を構成できます（「透過的なフェールオーバ」を参照）。

（注） IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールはデフォルトで、iSCSI にファイバ チャネル ターゲットをインポートしません。IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールで iSCSI 発信側からファイバ チャネル ターゲットを使用できるようにするには、ダイナミック マッピングまたはスタティック マッピングを構成しておく必要があります。

ダイナミック マッピング

ダイナミック マッピングを構成すると、IPS ポートを搭載したファイバ チャネル 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、各物理ファイバ チャネル ターゲット ポートを 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 ポートを介してアクセス可能なすべての LU は、物理ファイバ チャネル ターゲット ポートの場合と同じ論理ユニット番号（LUN）を持つ iSCSI LU として使用できます。

iSCSI ターゲット ノード名は、iSCSI 修飾名 （IQN）フォーマットを使用して、自動的に作成されます。iSCSI 修飾名の長さは、最大 223、最小 16 の英数字に制限されています。

名前は SAN 内で一意である必要があるため、IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールでは次の規則に従って、IQN フォーマットの iSCSI ターゲット ノード名を作成します。

- Virtual Router Redundancy Protocol（VRRP）グループまたはポートチャネルに属していない IPS ギガビット イーサネット ポートでは、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 ポートでは、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>
```

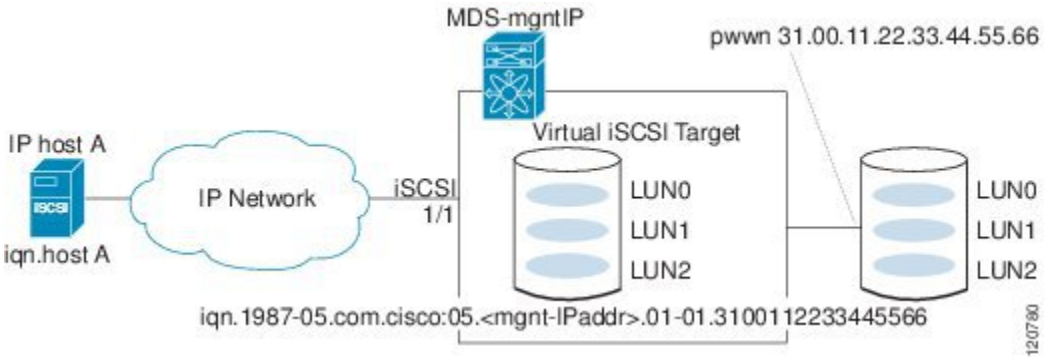
- ポート チャネルの一部であるポートではこのフォーマットを使用します。
  `iqn.1987-02.com.cisco:02.<mgmt-ip-address>.pc-<port-ch-sub-intf#>.<Target-pWWN>`

（注） スイッチ名が設定されている場合、スイッチ名は管理 IP アドレスの代わりに使用されます。スイッチ名が設定されていない場合は、管理 IP アドレスが使用されます。

Cisco MDS 9000 ファミリ スイッチ内の各 IPS ポートはこの規則に従って、SAN 内の同じファイバ チャネル ターゲット ポートに対して一意の iSCSI ターゲット ノード名を作成します。

たとえば、pWWN が 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 ターゲットが作成され、その pWWN に LUN 0、LUN 1、および LUN 2 が含まれる場合、これらの LUN は、iSCSI ターゲット ノード名 iqn.1987-05.com.cisco:05.*MDS_switch_management_IP_address* .

図 *10*: ダイナミック ターゲット マッピング

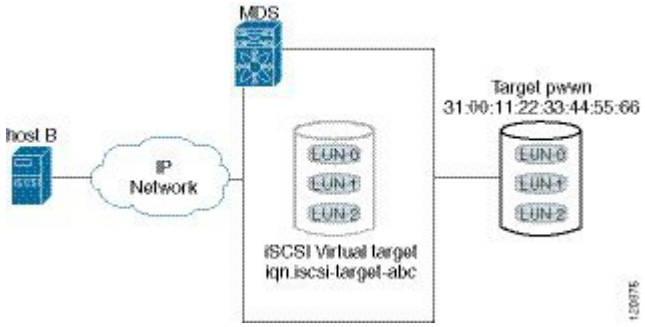


（注） 構成されているアクセス コントロール メカニズムによっては、個々の iSCSI イニシエータで一部のターゲットにアクセスできない場合があります（「iSCSI アクセス コントロール」を参照）。

スタティック マッピング

ユーザーが定義した一意の iSCSI ノード名を割り当てることによって、 iSCSI ターゲットを手動で（スタティックに）作成できます。iSCSI 修飾名の長さは、最小 16 文字、最大 223 文字に制限されています。スタティック マッピングの iSCSI ターゲットでは、ファイバ チャネル ターゲット ポート全体をマッピング（ターゲット ポート内のすべての LUN を iSCSI ターゲットにマッピング）することも、ファイバ チャネル ターゲット ポートの 1 つまたは複数の LU を含めることもできます。

図 *11* : スタティック マッピングの *iSCSI* ターゲット



（注） 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。ファイバ チャネル ターゲット ポート全体をすでにマッピングしている場合、LUN マッピング オプションは使用できません。

スタティックにマッピングされたターゲットへのアクセスを制御する手順については、「iSCSI ベース アクセス コントロール」セクション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ズ

スタティック iSCSI ターゲットをアドバタイズする場合に経由するギガビット イーサネット インターフェイスを制限できます。デフォルトでは、iSCSI ターゲットは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、ポートチャネルインターフェイス、およびポート チャネル サブインターフェイスでアドバタイズされます。

iSCSI 仮想ターゲットをアドバタイズするインターフェイスを構成する

iSCSI 仮想ターゲットをアドバタイズする特定のインターフェイスを構成するステップは、次のとおりです。

手順

ステップ 1 指定されたインターフェイスでのみ、仮想ターゲットをアドバタイズします。デフォルトでは、すべての IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールのすべてのインターフェイスでアドバタイズされます。

```
switch(config-iscsi-tgt)# advertise interface GigabitEthernet 2/5
```

（注）
仮想ターゲットを複数インターフェイスでアドバタイズするには、インターフェイスごとに次のコマンドを発行します。

ステップ 2 ターゲットのアドバタイズ元インターフェイスのリストから、このインターフェイスを削除します。

```
switch(config-iscsi-tgt)# no advertise interface GigabitEthernet 2/5
```

仮想ファイバ チャネル ホストとしての iSCSI ホストの提示

IPS ポートまたは MPS-14/2 モジュールを搭載したファイバ チャネルは、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、ストレージ デバイスにコマンドを送信し、ストレージデバイスと相互にデータを転送します。これらのモジュールでは、仮想ファイバ チャネル N ポートを使用して、iSCSI ホストに代わってファイバ 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 アドレスにより識別されます。

イニシエータ識別モードの指定

イニシエータ識別モードを指定するには、次のステップを実行します。

手順

ステップ 1 すべてのイニシエータを識別するスイッチ上の iSCSI インターフェイスを選択します。

```
switch# config terminal
switch(config)# interface iscsi 4/1
switch(config-if)#
```

ステップ 2 IP アドレスに基づいて iSCSI イニシエータを識別します。

```
switch(config-if)# switchport initiator id ip-address
```

ステップ 3 イニシエータ ノード名に基づいて iSCSI イニシエータを識別します。これはデフォルトの動作です。

```
switch(config-if)# switchport initiator id name
```

iSCSI 仮想ターゲットの設定例

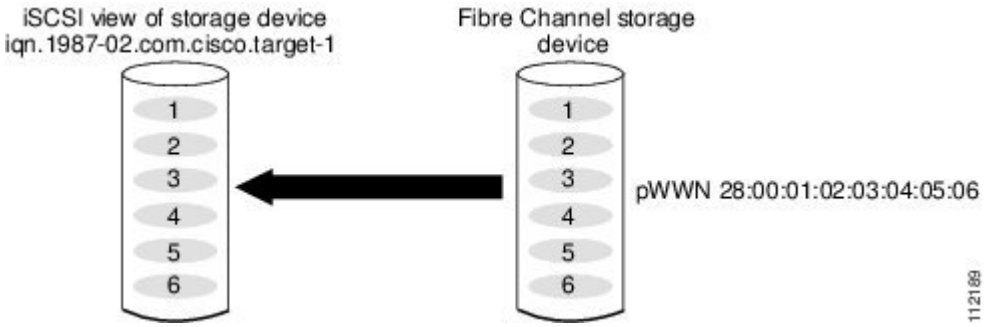
ここでは、3 種類の iSCSI 仮想ターゲット構成例を示します。

iSCSI 仮想ターゲットとしてファイバ チャネル ターゲット全体を割り当てます。

iSCSI 仮想ターゲットとしてファイバ チャネル ターゲット全体を割り当てる例を示します。ファイバ チャネル ターゲットに属しているすべての LUN を iSCSI ターゲットの一部として使用できます。

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

図 *12* : *iSCSI* ノード名の割り当て

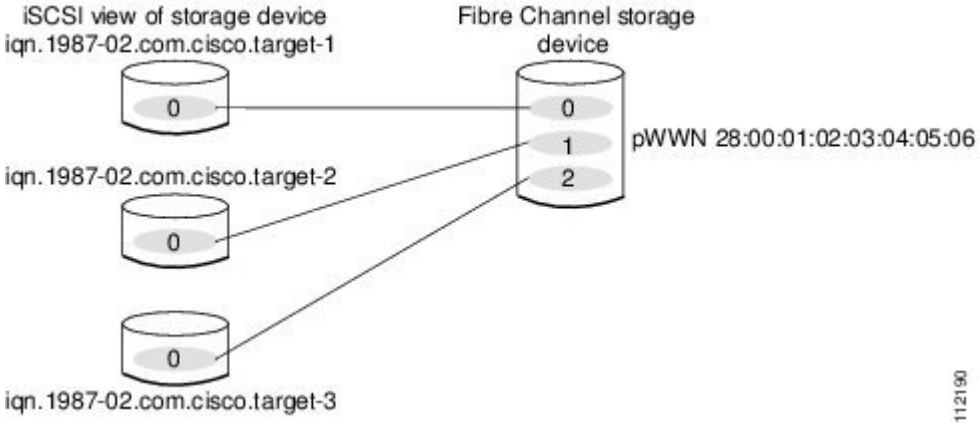


ファイバ チャネル ターゲットの LUN のサブセットを 3 つの iSCSI 仮想ターゲットにマッピング

ファイバ チャネル ターゲットの LUN のサブセットを 3 つの iSCSI 仮想ターゲットにマッピングする例を示します。各 iSCSI ターゲットが所有する LUN は 1 つのみです。

```
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
```

図 *13* : *iSCSI* ノード名への *LUN* のマッピング



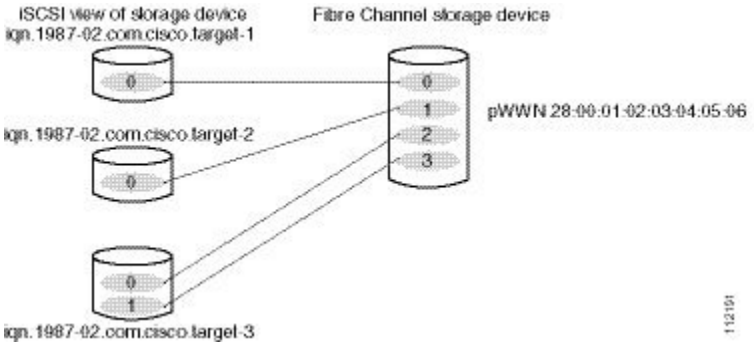
ファイバ チャネル LUN ターゲットの 3 つのサブセットを 3 つの iSCSI 仮想ターゲットにマッピング

ファイバ チャネル LUN ターゲットの 3 つのサブセットを 3 つの iSCSI 仮想ターゲットにマッピングする例を示します。2 つの iSCSI ターゲットで LUN を 1 つ使用し、3 つ目の iSCSI ターゲットで LUN を 2 つ使用します。

```
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
```

図 *14* : 複数の *iSCSI* ノード名への *LUN* のマッピング



発信側提供モード

ファイバ チャネル ファブリックの iSCSI ホストは、透過型イニシエータ モードおよびプロキシ イニシエータ モードの 2 種類のモードで提供できます。

- 透過型イニシエータ モードでは、各 iSCSI ホストが 1 つの仮想ファイバ チャネル ホストとして提供されます。トランスペアレント モードの利点は、ファイバ チャネル アクセス コントロールを「実」ファイバ チャネル ホストを管理する場合と同様に、きめ細かく設定できることです。iSCSI からファイバ チャネルへの 1 対 1 のマッピングなので、ファイバ チャネル ストレージ デバイスに関して、ホストごとに異なるゾーン分割または LUN アクセス コントロールを設定できます。
- プロキシ イニシエータ モードでは、1 つの IPS ポートに与えられる仮想ファイバ チャネル ホストは 1 つだけであり、すべての iSCSI ホストがその仮想ファイバ チャネル ホストを使用して、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 デバイスでホストごとに明示的な LUN アクセス コントロールを必要とするシナリオでは、iSCSI 発信側ごとのスタティックな設定は大きな負担となる可能性があります。このような状況では、プロキシ イニシエータ モードを使用すると、設定が簡素化されます。

（注） iSLB VRRP グループに属している iSCSI インターフェイスについて、プロキシ イニシエータ モードをイネーブルにすると、インターフェイスのロード バランシングが影響を受けます。「iSCSI インターフェイス パラメータの変更およびロード バランシングへの影響」セクションを参照してください

Cisco MDS スイッチは、次の iSCSI セッション制限をサポートします。

- スイッチ上の最大 iSCSI セッション数は 5000 です。
- 透過型イニシエータ モードの場合、各 IPS ポートの最大 iSCSI セッション数は 500 です。

- プロキシ イニシエータ モードの場合、各 IPS ポートの最大 iSCSI セッション数は 500 です。
- IPS ポートで作成できる同時セッションの最大数は 5 です（サポート可能なセッションの合計数は 500）。

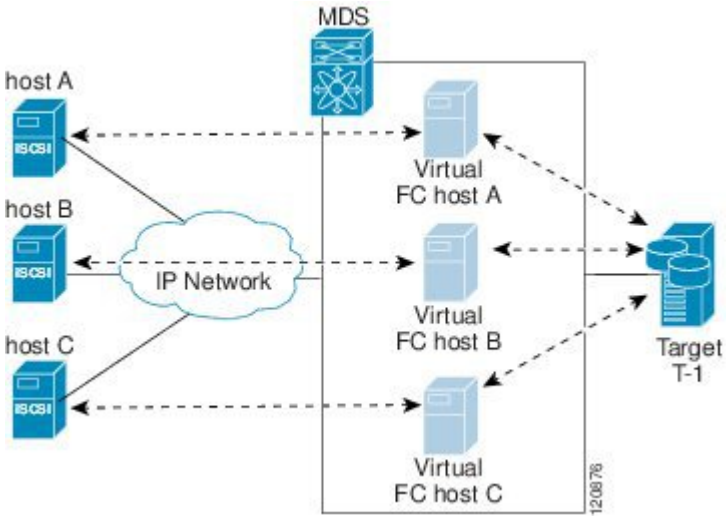
（注） ポート上で 6 つ以上の iSCSI セッションを同時にアクティブにしようとすると、発信側に一時的なエラーが伝えられ、あとでセッションの作成を再試行することになります。

透過型イニシエータ モード

個々の iSCSI ホストが、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）として提供されます。トランスペアレント モードの利点は、ファイバ チャネル アクセス コントロールをきめ細かく設定できることです。iSCSI からファイバ チャネルへの 1 対 1 のマッピングなので、ファイバ チャネル ストレージ デバイスに関して、ホストごとに異なるゾーン分割または LUN アクセス コントロールを設定できます。

iSCSI ホストから IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールに接続すると、そのホスト用の仮想ホスト N ポート（HBA ポート）が作成されます。ファイバ チャネル N ポートごとに、一意の Node WWN および Port WWN が 1 つずつ必要です。

図 *15* : 仮想ホスト *HBA* ポート



WWN を指定して仮想 N ポートを作成したあとで、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）を行います。FLOGI の完了後、ファイバ チャネル SAN で仮想 N ポートがオンラインになり、ファイバ チャネル ネーム サーバーで仮想 N ポートが登録されます。IPS ポートを搭載したファイバ チャネル 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 サーバーの IP-address フィールドに iSCSI ホストの IP アドレス

- ネーム サーバーの symbolic-node-name フィールドに iSCSI ホストの IQN
- ネーム サーバーの FC-4 type フィールドに SCSI_FCP
- ネーム サーバーの FC-4 feature に発信側フラグ
- ネーム サーバーの N ポート デバイスを iSCSI ゲートウェイ デバイスとして指定する FC-4 type フィールドに、ベンダー固有の iSCSI GW フラグ

iSCSI ホストからのすべての iSCSI セッションが終了すると、IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールが明示的なファブリック ログアウト（FLOGO）を実行し、ファイバ チャネル SAN から仮想 N ポート デバイスを除去します（間接的に、ファイバ チャネル ネーム サーバからデバイスを登録解消することになります）。

ホストから iSCSI 仮想ターゲットへの iSCSI セッションごとに、実ファイバ 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。3 つの iSCSI ホストがあり、その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 ホストのそれぞれからターゲットに、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 発信側アイドル タイムアウトでは、発信側が最後の iSCSI セッションからログアウトするまでに、仮想ファイバ チャネル N ポートのアイドル状態が続く時間を指定します。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 に対してログインとログオフを繰り返さないようにするために有用です。ファイバ チャネル SAN で不必要に RSCN が生成される可能性が少なくなります。

アイドル タイムアウトを構成する

発信側のアイドル タイムアウトを設定するには、次のステップを実行します。

手順

ステップ 1 コンフィギュレーション モードを開始します。

```
switch# config terminal
switch(config)#
```

ステップ 2 iSCSI イニシエータのアイドル タイムアウト値を 10 秒に構成します。

```
switch(config)# iscsi initiator idle-timeout 10
```

iSCSI イニシエータへの WWN の割り当て

iSCSI ホストは次のいずれかのメカニズムで、N ポートの WWN に対応付けられます。

- 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 ホストはダイナミックに生成されたポート WWN（pWWN）およびノード WWN（nWWN）に対応付けられます。iSCSI ホストは接続のたびに、異なる WWN に対応付けられる可能性があります。このオプションは、ファイバ チャネル ターゲット デバイス上でアクセス コントロールが不要な場合に使用します。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 を使用して設定するからです。

WWN は、MDS スイッチの WWN プールから割り当てられます。iSCSI ホストへの WWN マッピングは、iSCSI ホストに IPS ポートとの iSCSI セッションが 1 つ以上あるかぎり維持されます。ホストからのすべての iSCSI セッションが終了し、IPS ポートを搭載したファイバ チャネル 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 プールに戻ります。戻されたアドレスは、ファイバ チャネル ファブリックにアクセスする必要がある他の iSCSI ホストに割り当てることができます。

次の 3 種類のダイナミック イニシエータ モードがサポートされます。

- iSCSI：ダイナミック発信側は iSCSI 発信側として扱われ、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。
- 拒否：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の動作モードです。この構成は、CFS を使用して配信されます。

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 に対応付けられます。このマッピングは、永続ストレージで維持され、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 デバイス上でアクセス コントロールを使用する場合は、このモードが必要です。

スタティック マッピングは、次の 2 つの方法のいずれかで実装できます。

- ユーザー割り当て：構成プロセス中に、一意の WWN を独自に指定できます。
- システム割り当て：スイッチのファイバ チャネル WWN プールから WWN を提供し、スイッチ構成でマッピングを維持することをスイッチに要求できます。

system-assign オプションの使用を推奨します。手動でWWNを割り当てる場合は、固有の割り当てにする必要があります（詳細については、『Cisco Fabric Manager ファブリック構成ガイド』『Cisco MDS 9000 ファミリ NX-OS ファブリック構成ガイド』を参照してください）。すでに割り当てられている WWN は使用できません。

ダイナミック iSCSI 発信側 WWN マッピングをスタティックにする方法

ダイナミック iSCSI 発信側のログイン後に、その発信側で次回ログイン時にも同じマッピングが使用されるように、自動的に割り当てられたnWWN/pWWNマッピングを維持することがあります。

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。

（注） ダイナミック iSCSI 発信側をスタティック iSLB 発信側に変換したり、ダイナミック iSLB 発信側をスタティック iSCSI 発信側に変換したりはできません。

（注） イニシエータの作成後にダイナミック pWWN をスタティックにできるのは、CLI を使用した場合だけです。Device Manager または Fabric Manager ではできません。Fabric Manager または Device Manager で pWWN をスタティックにするには、この発信側を削除してから作成し直す必要があります。

WWN の衝突チェック

アップグレードに失敗した場合、またはシステム ソフトウェアをダウングレードした場合に、システムによってスタティック iSCSI 発信側に割り当てられた WWN がシステムに偶発的に戻されることがあります（**install all** コマンドを使用せずに、旧来の Cisco MDS SAN-OS を手動でブート）。このような場合、システムはそれらの WWN をあとで他の iSCSI 発信側（ダイナミックまたはスタティック）に割り当て、衝突を引き起こす可能性があります。

このような状況になったときには常に、システムに属している設定済みのWWNを調べて削除することによって、この問題に対処できます。

iSCSI イニシエータの名 name プションを使用したダイナミック マッピングを構成する

iSCSI イニシエータに（**name** オプションを使用して） ダイナミック マッピングを構成するには、次のステップを実行します。

手順

ステップ 1 コンフィギュレーション モードを入力します。

```
switch# config terminal
switch(config)#
```

ステップ 2 iSLB ダイナミック イニシエータ モードを指定します。

```
switch(config)# iscsi dynamic initiator islb
```

ステップ 3 ダイナミック イニシエータの MDS スイッチへのログインを禁止する

```
switch(config)# iscsi dynamic initiator deny
```

ステップ 4 iSCSI モード（デフォルト）に戻します。

```
switch(config)# no iscsi dynamic initiator islb
```

iSCSI イニシエータの名 name プションを使用したスタティック マッピングを構成する

iSCSI イニシエータ に（**[name]** オプションを使用して）スタティック マッピングを構成するには、次のステップを実行します。

手順

ステップ 1 コンフィギュレーション モードを入力します。

```
switch# config terminal
switch(config)#
```

ステップ 2 イニシエータ ノードの iSCSI 名を使用して iSCSI イニシエータを構成します。名前の最大長は英数字 223 文字です。最小長は 16 です。

```
switch(config)# iscsi initiator name iqn.1987-02.com.cisco.initiator
switch(config-iscsi-init)#
```

ステップ 3 構成済み iSCSI イニシエータを削除します。

```
switch(config)# no iscsi initiator name iqn.1987-02.com.cisco.initiator
```

iSCSI イニシエータの名 IP アドレス プションを使用したスタティック マッピングを構成する

iSCSI イニシエータに（**ip-address** オプションを使用して）スタティック マッピングを構成するには、次のステップを実行します。

手順

ステップ 1 コンフィギュレーション モードを入力します。

```
switch# config terminal
switch(config)#
```

ステップ 2 イニシエータ ノードの IPv4 アドレスを使用して iSCSI イニシエータを構成します。

```
switch(config)# iscsi initiator ip-address 10.50.0.0
switch(config-iscsi-init)#
```

ステップ 3 イニシエータ ノードの IPv6 ユニキャスト アドレスを使用して iSCSI イニシエータを構成します。

```
switch(config)# iscsi initiator ip-address 2001:0DB8:800:200C::417A
switch(config-iscsi-init)#
```

ステップ 4 （オプション）設定済み iSCSI イニシエータを削除します。

```
switch(config)# no iscsi initiator ip-address 2001:0DB8:800:200C::417A
```

iSCSI イニシエータに対する WWN の割り当て

iSCSI イニシエータに WWN を割り当てるには、次のステップを実行します。

始める前に

system-assign オプションを使用して iSCSI イニシエータに WWN を設定した場合、設定を ASCII ファイルに保存すると、システムによって割り当てられた WWN も保存されます。以後、write erase コマンドを実行する場合は、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。この作業を怠ると、ASCII 設定ファイルをスイッチ上で再適用した場合に、WWN を二重に割り当てることになる可能性があります。

手順

ステップ 1 スイッチの WWN プールを使用してこの iSCSI イニシエータに nWWN を割り当て、それを永続的に保持します。

```
switch(config-iscsi-init)# static nWWN system-assign
```

ステップ 2 ユーザーが指定した WWN を、iSCSI イニシエータの nWWN として割り当てます。iSCSI ノードごとに 1 つの nWWN だけを指定できます。

```
switch(config-iscsi-init)# static nWWN 20:00:00:05:30:00:59:11
```

ステップ 3 スイッチの WWN プールを使用して、この iSCSI イニシエータに 2 つの pWWN を割り当て、それらを永続的に保持します。範囲は 1 ～ 64 です。

```
switch(config-iscsi-init)# static pWWN system-assign 2
```

ステップ 4 ユーザーが指定した WWN を iSCSI イニシエータの pWWN として割り当てます。

```
switch(config-iscsi-init)# static pWWN 21:00:00:20:37:73:3b:20
```

自動的に割り当てられた nWWN/pWWN マッピングの保存

自動的に割り当てられた nWWN/pWWN マッピングを永続的に維持するには、次のステップを実行します。

手順

ステップ 1 コンフィギュレーション モードを入力します。

```
switch# config terminal
switch(config)#
```

ステップ 2 名前で指定された iSCSI イニシエータに自動的に割り当てられた pWWN および nWWN を保存します。

```
switch(config)# iscsi save-initiator name iqn.1987-02.com.cisco.initiator
```

ステップ 3 IPv4 アドレスで指定された iSCSI イニシエータに自動的に割り当てられた pWWN および nWWN を保存します。

```
switch(config)# iscsi save-initiator ip-address 10.10.100.11
```

ステップ 4 IPv6 ユニキャスト アドレスで指定された iSCSI イニシエータに自動的に割り当てられた pWWN および nWWN を保存します。

```
switch(config)# iscsi save-initiator ip-address 2001:0DB8:800:200C::417A
```

ステップ 5 すべてのイニシエータに自動的に割り当てられた nWWN および pWWN を保存します。

```
switch(config)# iscsi save-initiator
```

ステップ 6 EXEC モードに戻ります。

```
switch(config)# exit

switch#
```

ステップ 7 システム リブート後も nWWN/pWWN マッピング構成を保存します。

```
switch# copy running-config startup-config
```

WWN の競合の確認と削除

WWN の競合を調べて削除するには、次のステップを実行します。

手順

ステップ 1 コンフィギュレーション モードを入力します。

```
switch# config terminal
switch(config)#
```

ステップ 2 WWN 競合を確認します。

```
switch(config)# iscsi duplicate-wwn-check

List of Potential WWN Conflicts:
--------------------------------
Node : iqn.test-local-nwwn:1-local-pwwn:1
nWWN : 22:03:00:0d:ec:02:cb:02
pWWN : 22:04:00:0d:ec:02:cb:02
```

ステップ 3 iqn.test-local-nwwn:1-local-pwwn:1 というイニシエータの iSCSI イニシエータ コンフィギュレーション モードを開始します。

```
switch(config)# iscsi initiator name iqn.test-local-nwwn:1-local-pwwn:1
```

ステップ 4 競合する nWWN が削除されます。

```
switch(config-iscsi-init)# no static nWWN 22:03:00:0d:ec:02:cb:02
```

ステップ 5 競合する pWWN が削除されます。

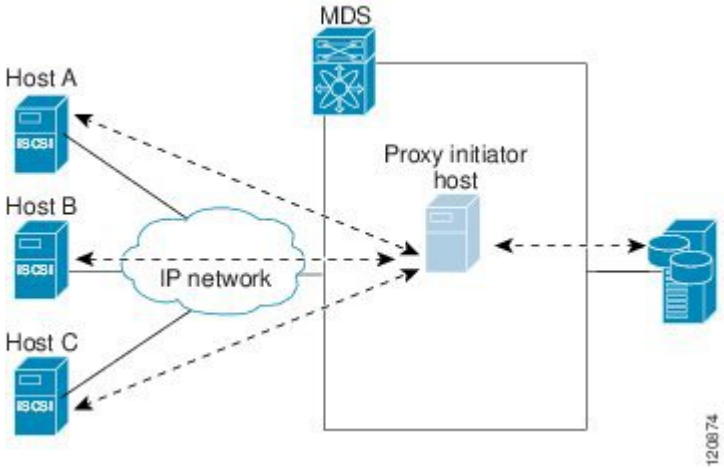
```
switch(config-iscsi-init)# no static pWWN 22:04:00:0d:ec:02:cb:02
```

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、あらゆるホストに関して明示的な LUN アクセス コントロールが必要な場合、透過型イニシエータ モードを使用します（1 つの iSCSI ホストを 1 つのファイバ チャネル ホストとして提供）。各 iSCSI ホストは静的に設定する必要があります。この場合、iSCSI ホストごとにいくつもの設定作業が必要です。明示的な LUN アクセス コントロールが必要ない場合、プロキシ イニシエータ モードを使用すると、構成が簡略化されます。

このモードでは、作成される仮想ホスト N ポート（HBA ポート）は IPS ポートごとに 1 つだけです。その IPS ポートに接続するすべての iSCSI ホストは同じ仮想ホスト N ポートを使用して多重化されます。このモードを使用すると、WWN をスタティックにバインドする作業が簡単になります。この IPS ポートを介して接続する各 iSCSI イニシエータで使用されるすべての LUN について、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 アレイ上の 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。さらに、LUN マッピングおよび iSCSI アクセス コントロール（「スタティック マッピング」セクションを参照）を指定して iSCSI 仮想ターゲットを構成することによって、各 iSCSI イニシエータに LUN が割り当てられます。

図 *16 : IPS* ポートの多重化



プロキシ イニシエータ モードは IPS ポート単位で設定できますが、その場合にこのモードになるのは、その IPS ポートで終端する iSCSI イニシエータのみです。

プロキシ イニシエータ モードで IPS ポートを設定した場合、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）を行います。FLOGI の完了後、ファイバ チャネル ファブリックでプロキシ発信側仮想 N ポートがオンラインになり、ファイバ チャネル ネーム サーバーで仮想 N ポートが登録されます。IPS ポートを搭載したファイバ チャネル 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 サーバーに次のエントリを登録します。

- ネーム サーバーの symbolic-node-name フィールドに iSCSI インターフェイス名 iSCSI スロット/ポート
- ネーム サーバーの FC-4 type フィールドに SCSI_FCP
- ネーム サーバーの FC-4 feature に発信側フラグ
- ネーム サーバ]の N ポート デバイスを iSCSI ゲートウェイ デバイスとして指定する FC-4 type フィールドに、ベンダー固有のフラグ（iscsi-gw）

透過型イニシエータ モードと同様、ユーザーは pWWN および nWWN を指定することも、またはプロキシ発信側 N ポートへの WWN 割り当てをシステムに要求することもできます。

（注） iSLB VRRP グループに属している iSCSI インターフェイスについて、プロキシ イニシエータ モードをイネーブルにすると、インターフェイスのロード バランシングが影響を受けます。「iSCSIインターフェイスパラメータの変更およびロードバランシングへの影響」セクションを参照してください。

（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（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）のみを設定できます。iSCSI 発信側の IP アドレス、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 アクセス コントロールを使用します。

プロキシ イニシエータの構成

プロキシ イニシエータを構成するには、次のステップを実行します。

手順

ステップ 1 コンフィギュレーション モードを入力します。

```
switch# config terminal
switch(config)#
```

ステップ 2 イニシエータの接続先となるスイッチの iSCSI インターフェイスを選択します。

```
switch(config)# interface iscsi 4/1
switch(config-if)#
```

ステップ 3 システム割り当て nWWN および pWWN を使用してプロキシ イニシエータ モードを構成します。

```
switch(config-if)# switchport proxy-initiator
```

ステップ 4 （オプション）プロキシ イニシエータ モードを無効にします。

```
switch(config-if)# no switchport proxy-initiator
```

ステップ 5 （オプション）指定された WWN を使用してプロキシ イニシエータ モードを構成します。

```
switch(config-if)# switchport proxy-initiator nWWN 11:11:11:11:11:11:11:11 pwwn 22:22:22:22:22:22:22:22
```

ステップ 6 （オプション）プロキシ イニシエータ モードを無効にします。

```
switch(config-if)# no switchport proxy-initiator nWWN 11:11:11:11:11:11:11:11 pwwn
22:22:22:22:22:22:22:22
```

iSCSI の VSAN メンバーシップ

iSCSI インターフェイスにはポート VSAN という VSAN メンバーシップを構成できます。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 内で明示的に設定されていない場合には、自動的にこの VSAN のメンバーになります。iSCSI インターフェイスのデフォルト ポート VSAN は、VLAN 1 です。iSCSI デバイスもファイバ チャネル デバイスと同様、2 種類の方式で VSAN メンバーシップを定義できます。

- iSCSI ホスト：iSCSI ホストに対する VSAN メンバーシップ。（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 メンバーシップ（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 メンバーシップを継承します）。

個々の iSCSI ホストを特定の VSAN に属すように設定できます。指定した VSAN によって、iSCSI インターフェイスの VSAN メンバーシップが上書きされます。

iSCSI ホストの VSAN メンバーシップの割り当て

iSCSI ホストの VSAN メンバーシップを割り当てるには、次のステップを実行します。

始める前に

その他の VSAN（VSAN 1 以外）内に発信側を設定すると（VSAN 2 など）、発信側は自動的に VSAN 1 から削除されます。VSAN 1 にもこの発信側を存続させる場合は、この発信側を VSAN 1 内に明示的に設定する必要があります。

手順

ステップ 1 コンフィギュレーション モードを入力します。

```
switch# config terminal
switch(config)#
```

ステップ 2 iSCSI イニシエータを構成します。

```
switch(config)# iscsi initiator name iqn.1987-02.com.cisco.initiator
switch(config-iscsi-init)#
```

ステップ 3 指定された VSAN に iSCSI イニシエータ ノードを割り当てます。

```
switch(config-iscsi-init)# vsan 3
```

（注）
1 つ以上の VLAN にこのホストを割り当てることができます。

ステップ 4 指定された VSAN から iSCSI ノードを削除します。

```
switch(config-iscsi-init)# no vsan 5
```

iSCSI インターフェイスのデフォルト ポート VSAN の設定

iSCSI インターフェイスにはポート *VSAN* という VSAN メンバーシップを構成できます。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 内で明示的に設定されていない場合には、自動的にこの VSAN のメンバーになります。言い換えると、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 発信側のデフォルト VSAN になります。iSCSI インターフェイスのデフォルト ポート VSAN は、VLAN 1 です。

iSCSI インターフェイスのデフォルト ポート VSAN を変更するステップは、次のとおりです。

始める前に

iSLB VRRP グループに属している iSCSI インターフェイスの VSAN メンバー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が影響を受けます。「iSCSI インターフェイス パラメータの変更およびロード バランシングへの影響」セクションを参照してください。

手順

ステップ 1 コンフィギュレーション モードを入力します。

```
switch# config terminal
switch(config)#
```

ステップ 2 iSCSI インターフェイスの VSAN メンバーシップを構成します。

```
switch(config)# iscsi interface vsan-membership
```

ステップ 3 VSAN に対するデータベースを構成します。アプリケーション特有の VSAN パラメータは、このプロンプトから設定できません。

```
switch(config)# vsan database
switch(config-vsan-db)#
```

ステップ 4 指定された VSAN（VSAN 2）に、iscsi 2/1 インターフェイスのメンバーシップを割り当てます。

```
switch(config - vsan-db)# vsan 2 interface iscsi 2/1
```

ステップ 5 iSCSI インターフェイスのポート VSAN としてデフォルトの VSAN を使用するように設定を戻します。

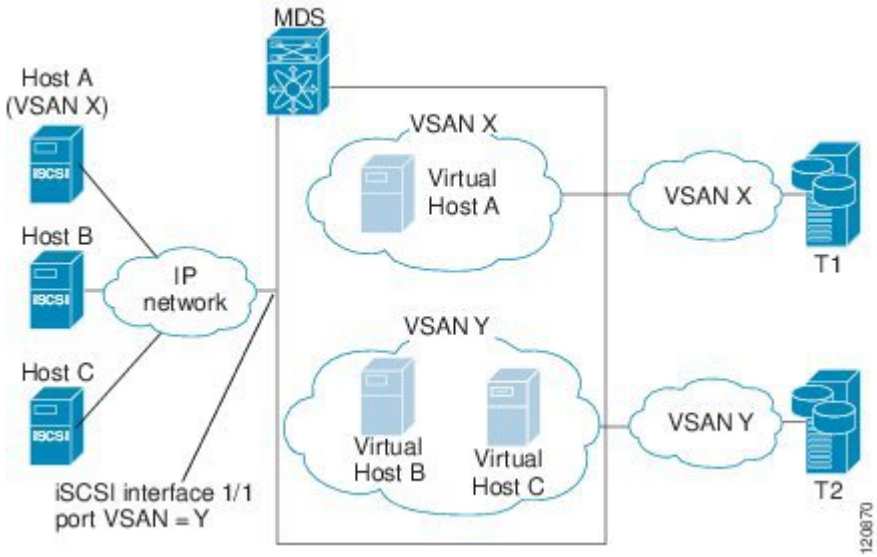
```
switch(config - vsan-db)# no vsan 2 interface iscsi 2/1
```

iSCSI デバイスの VSAN メンバーシップ

以下のような iSCSI デバイスの VSAN メンバーシップの例：

- SCSI インターフェイス 1/1 は VSAN Y のメンバーです。
- iSCSI 発信側ホスト A は、VSAN X に対する明示的 VSAN メンバーシップが与えられています。
- 3 つの iSCSI 発信側（ホスト A、ホスト B、およびホスト C）が iSCSI インターフェイス 1/1 に接続します。

図 *17 : iSCSI* インターフェイスの *VSAN* メンバーシップ



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メンバーシップが設定されているので、VSAN X に追加されます。仮想ホスト B およびホスト C の N ポートは、明示的メンバーシップが設定されていないので、iSCSI インターフェイスの VSAN メンバーシップを引き継ぎ、VSAN Y に属します。

iSCSI ホストの拡張 VSAN メンバーシップ

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 デバイスなどのリソースをさまざまな VSAN 間で共有しなければならない場合に便利です。

iSCSI のアクセス コントロール

iSCSI デバイスでは 2 種類のアクセス コントロール方式を使用できます。ファイバ チャネル ファブリックに iSCSI ホストを提供するイニシエータ モードに応じて、一方または両方のアクセス コントロール方式を使用できます。

- 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：ファイバ チャネル ゾーン分割は、iSCSI デバイスをサポートできるように拡張されました。この拡張により、SAN 全体にわたって、統一された柔軟性の高いアクセス コントロール方式を使用する利点が得られます。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あるすべての iSCSI デバイスが自動的に同じゾーンに含まれるので、役に立たない場合があります。
- iSCSI ACL ベースのアクセス コントロール：iSCSI ベースのアクセス コントロールが適用されるのは、スタティック iSCSI 仮想ターゲットを作成した場合だけです。スタティック iSCSI ターゲットの場合は、ターゲットにアクセス可能な iSCSI 発信側のリストを設定で

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 iSCSI ホストにアクセスできません。

ファイバ チャネル ファブリックに iSCSI ホストを提供するイニシエータ モードに応じて、一方または両方のアクセス コントロール方式を使用できます。

この項では、次の項目について説明します。

- 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 ベースのアクセス コントロール
- アクセス コントロールの実行

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 デバイスの標準アクセス コントロール方式であり、VSAN のコンテキストの中で適用されます。ファイバチャネル ゾーン分割は、iSCSI デバイスをサポートできるように拡張されました。この拡張により、SAN 全体にわたって、統一された柔軟性の高いアクセス コントロール方式を使用する利点が得られます。

ファイバ チャネル ゾーンのメンバーを識別する共通メカニズムは、次のとおりです。

- 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。そのインターフェイス経由で接続するデバイスはゾーン内にあります。

ファイバ チャネル ゾーン分割の詳細については、『Cisco Fabric Manager ファブリック構成ガイド』『Cisco MDS 9000 ファミリ NX-OS ファブリック構成ガイド』を参照してください。

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あるすべての iSCSI デバイスが自動的に同じゾーンに含まれるので、役に立たない場合があります。

透過型イニシエータ モード（「透過型イニシエータ モード」で説明したとおり、iSCSI ホストごとに 1 つずつファイバチャネル仮想 N ポートが作成される）では、iSCSI ホストにスタティックな WWN マッピングが設定されている場合に、標準のファイバ チャネル デバイス pWWN ベースのゾーン分割メンバーシップ メカニズムを使用できます。

ゾーン分割メンバーシップ 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ています。

- IPv4 アドレス/サブネット マスク
- IPv6 アドレス/プレフィックス長
- 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、この機能を使用すると、ゾーン メンバーとして IP アドレスまたは iSCSI ノード名を指定できます。スタティック WWN マッピングが設定されている iSCSI ホストでも、これらの機能を使用できます。サブネットマスクを指定することにより、1 つのコマンドで複数のデバイスを IP アドレス ベースのゾーン メンバーシップに指定できます。

（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 デバイスが、単一の仮想ファイバ チャネル N ポート経由でファイバ 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。WWN ベースのゾーン分割を使用した場合、その IPS ポートに接続するすべての iSCSI デバイスが同じゾーンに組み込まれます。プロキシ イニシエータ モードで個別のイニシエータ アクセス コントロールを実施するには、仮想ターゲットに iSCSI ACL を構成します（「iSCSI ベース アクセス コントロール」を参照）。

*iSCSI:*ゾーン データベースへのイニシエータの追加

ゾーン データベースに iSCSI イニシエータを追加するには、次のステップを実行します。

手順

ステップ 1 コンフィギュレーション モードを入力します。

```
switch# config terminal
switch(config)#
```

ステップ 2 IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールの iSCSI デバイスを含めるゾーン名を作成します。

```
switch(config)# zone name iSCSIzone vsan 1
switch(config-zone)
```

ステップ 3 ゾーンに iSCSI ノード名ベースのメンバーシップを割り当てます。

```
switch(config-zone)# member symbolic-nodename iqn.1987-02.com.cisco.initiator1
```

ステップ 4 （オプション）ゾーンから指定したデバイスを削除します。

```
switch(config-zone)# no member symbolic-nodename iqn.1987-02.com.cisco.init1
```

ステップ 5 ゾーンに iSCSI IPv4 アドレス ベースのメンバーシップを割り当てます。

```
switch(config-zone)# member ip-address 10.50.1.1
```

ステップ 6 （オプション）ゾーンから指定したデバイスを削除します。

```
switch(config-zone)# no member ip-address 10.50.1.1
```

ステップ 7 ゾーンに iSCSI IPv6 アドレス ベースのメンバーシップを割り当てます。

```
switch(config-zone)# member ipv6-address 2001:0DB8:800:200C::417A
```

ステップ 8 ゾーンから指定したデバイスを削除します。

```
switch(config-zone)# no member ipv6-address 2001:0DB8:800:200C::417A
```

ステップ 9 ゾーンに iSCSI ポート WWN ベースのメンバーシップを割り当てます。

```
switch(config-zone)# member pwwn 20:00:00:05:30:00:59:11
```

ステップ 10 ポート WWN によって識別されたデバイスをゾーンから削除します。

```
switch(config-zone)# no member pwwn 20:00:00:05:30:00:59:11
```

iSCSI ベースのアクセス コントロール

iSCSI ベース のアクセス コントロールが適用されるのは、スタティック iSCSI 仮想ターゲットを作成した場合だけです（「スタティック マッピング」 を参照）。スタティック iSCSI ターゲットの場合は、ターゲットにアクセス可能な iSCSI 発信側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 iSCSI ホストにアクセスできません。すべてのホストから iSCSI 仮想ターゲットにアクセスできるようにするには、アクセス可能性を明示的に設定する必要があります。発信側アクセス リストには、発信側を 1 つまたは複数指定できます。iSCSI 発信側は、次のいずれかの方式で指定できます。

- iSCSI ノード名
- IPv4 アドレスおよびサブネット
- IPv6 アドレス

iSCSI のアクセス コントロールを構成するには、次のステップを実行します。

始める前に

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、iSCSI ホストにアクセス可能なスタティック iSCSI ターゲットごとに、イニシエータの仮想 N ポートをファイバ チャネル ターゲットと同じファイバ チャネル ゾーンに含める必要があります。

手順

ステップ 1 コンフィギュレーション モードを入力します。

```
switch# config terminal
switch(config)#
```

ステップ 2 iSCSI ターゲット（iqn.1987-02.com.cisco.initiator）を作成します。

```
switch(config)# iscsi virtual-target name iqn.1987-02.com.cisco.initiator
switch(config-iscsi-tgt)#
```

ステップ 3 仮想ターゲット ノードをファイバ チャネル ターゲットにマップします。

```
switch(config-iscsi-tgt)# pWWN 26:00:01:02:03:04:05:06
switch(config-iscsi-tgt)#
```

ステップ 4 指定の iSCSI イニシエータ ノードがこの仮想ターゲットにアクセスできるようにします。複数のイニシエータにこの操作を許可するには、このコマンドを複数回発行します。

```
switch(config-iscsi-tgt)# initiator iqn.1987-02.com.cisco.initiator1 permit
```

ステップ 5 （オプション）指定されたイニシエータ ノードが仮想ターゲットにアクセスするのを防止します。

```
switch(config-iscsi-tgt)# no initiator iqn.1987-02.com.cisco.initiator1 permit
```

ステップ 6 指定された IPv4 アドレスが仮想ターゲットにアクセスするのを防止します。

```
switch(config-iscsi-tgt)# no initiator ip address 10.50.1.1 permit
```

ステップ 7 この IPv4 サブネットワーク（10.50.1/24）内のすべてのイニシエータに、この仮想ターゲットへのアクセスを許可します。

```
switch(config-iscsi-tgt)# initiator ip address 10.50.1.0 255.255.255.0 permit
```

ステップ 8 この IPv4 サブネットワーク内のすべてのイニシエータが仮想ターゲットにアクセスするのを防止します。

```
switch(config-iscsi-tgt)# no initiator ip address 10.50.1.0 255.255.255.0 permit
```

ステップ 9 この IPv6 サブネットワーク内のすべてのイニシエータ（2001:0DB8:800:200C::/64）にこの仮想ターゲットへのアクセスを許可します。

```
switch(config-iscsi-tgt)# initiator ip address 2001:0DB8:800:200C::/64 permit
```

ステップ 10 この IPv6 サブネットワーク内のすべてのイニシエータが仮想ターゲットにアクセスするのを防止します。

```
switch(config-iscsi-tgt)# no initiator ip address 2001:0DB8:800:200C::/64 permit
```

ステップ 11 すべてのイニシエータ ノードにこの仮想ターゲットへのアクセスを許可します。

```
switch(config-iscsi-tgt)# all-initiator-permit
```

ステップ 12 イニシエータが仮想ターゲットにアクセスするのを防止します（デフォルト）。

```
switch(config-iscsi-tgt)# no all-initiator-permit
```

アクセス コントロールの実行

IPS ポートを搭載したファイバ チャネル モジュールおよび MPS-14/2 モジュールでは、iSCSI および 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 検出フェーズおよびiSCSIセッション作成フェーズの両方で実行されます。入出力フェーズでは、アクセス コントロールの実行は不要です。IPS ポートを搭載したファイバ チャネルまたは MPS-14/2 モジュールがiSCSIトラフィックのファイバチャネルへのルーティングを引き受けるためです。

- 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 ターゲットにクエリを送信すると、IPS ポートを搭載したファイバ チャネルまたは MPS-14/2

モジュールは直前の項に記載されたアクセス コントロール ポリシーに基づいて、この iSCSI ターゲットホストからアクセス可能な iSCSI ターゲット リストだけを戻します。IPS ポートを搭載したファイバ チャネルまたは MPS-14/2 モジュールは、ファイバ チャネル ネーム サーバにクエリを送信し、すべての VSAN で発信側と同じゾーンに含まれているすべてのデバイスを要求することによって、これを実行します。さらに、FCNS エントリの FC4-feature フィールドを調べることによって、発信側デバイスを除外します。（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 ポートを搭載したファイバ チャネルまたは 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。各ターゲットには、ユーザーが構成したスタティックな iSCSI ターゲット名または IPS モジュールまたは MPS-14/2 モジュールによって作成されたダイナミックな iSCSI ターゲット名が与えられます（「ダイナミック マッピング」を参照）。

- iSCSI セッションの作成：IP ホストが iSCSI セッションを開始すると、IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールが、「iSCSI ベース アクセス コントロール」で説明した両方のアクセス コントロール方式を使用して、（セッション ログイン要求で）指定された iSCSI ターゲットにアクセスが許可されているかどうかを検証します。

iSCSI ターゲットがスタティックに対応付けられたターゲットの場合、IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールは、iSCSI ターゲットのアクセス リスト内で、iSCSI ホストが許可されているかどうかを検証します。IP ホストからアクセスできない場合は、ログインが拒否されます。iSCSI ホストからアクセスできる場合は、iSCSI ホストが使用する仮想ファイバ チャネル N ポートと、スタティック仮想ターゲットに対応付けられたファイバ チャネル ターゲットが同じファイバ チャネル ゾーンに属しているかどうかが検証されます。

iSCSI ターゲットが自動生成の iSCSI ターゲットの場合、IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールが iSCSI ターゲット名からファイバ チャネル ターゲットの WWN を抽出して、発信側とファイバ チャネル ターゲットが同じファイバ チャネル ゾーンに属しているかどうかを検証します。属している場合は、アクセスが許可されます。

IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールでは、iSCSI ホストのファイバ チャネル N ポートを使用して、ゾーン適用ネーム サーバー クエリーによって、ファイバ チャネル ターゲット WWN を調べます。FC ID がネーム サーバーから戻された場合は、iSCSI セッションが許可されます。これ以外の場合、ログイン要求は拒否されます。

iSCSI セッション認証

IPS ポートを搭載したファイバ チャネル 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 ポートを搭載したファイバチャネルモジュールおよび MPS-14/2 モジュールは、iSCSI 発信側に関する CHAP または None 認証を許可します。認証を必ず使用する場合は、CHAP 認証だけが許可されるようにスイッチを設定する必要があります。

CHAP のユーザー名またはシークレット検証では、Cisco MDS AAA インフラストラクチャでサポートおよび許可されている任意の方式を使用できます。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。『Cisco Fabric Manager セキュリティ構成ガイド』を参照してください。

aaa authentication iscsi コマンドは、iSCSI ホストの AAA 認証を有効にして、使用する方式を指定します。『Cisco MDS 9000 Family NX-OS Security Configuration Guide』を参照してください。

iSCSI ユーザーの AAA 認証の構成

iSCSI ユーザーの AAA 認証を構成するには、次のステップを実行します。

手順

ステップ 1 コンフィギュレーション モードを入力します。

```
switch# config terminal
switch(config)#
```

ステップ 2 iSCSI CHAP 認証に RadServerGrp と呼ばれるグループに追加された RADIUS サーバを使用します。

```
switch(config)# aaa authentication iscsi default group RadServerGrp
```

ステップ 3 iSCSI CHAP 認証には、TacServerGrp と呼ばれるグループに追加された TACACS+ サーバを使用します。

```
switch(config)# aaa authentication iscsi default group TacServerGrp
```

ステップ 4 ローカル パスワード データベースを使用して iSCSI CHAP の認証を行います。

```
switch(config)# aaa authentication iscsi default local
```

iSCSI の認証 メカニズムの構成

iSCSI の認証メカニズムを構成するには、次のステップを実行します。

手順

ステップ 1 コンフィギュレーション モードを入力します。

```
switch# config terminal
switch(config)#
```

ステップ 2 CHAP をデフォルトの認証メカニズムとして Cisco MDS スイッチ用にグローバルに構成します。CHAP 認証はすべての iSCSI セッションで必要です。

```
switch(config)# iscsi authentication chap
```

インターフェイスで iSCSI セッションの認証メカニズムの構成

特定のインターフェイスに対する iSCSI セッションの認証メカニズムを構成するには、次のステップを実行します。

手順

ステップ 1 コンフィギュレーション モードを入力します。

```
switch# config terminal
switch(config)#
```

ステップ 2 ギガビット イーサネット インターフェイスを選択します。

```
switch(config)# interface GigabitEthernet 2/1.100
switch(config-if)#
```

ステップ 3 選択されているインターフェイスへの iSCSI セッションに認証が不要であることを指定します。

```
switch(config-if)# iscsi authentication none
```

ローカル認証の構成

ローカル認証のための iSCSI ユーザーを構成するには、次のステップを実行します。

手順

ステップ 1 構成モード に入ります

```
switch# config terminal
switch(config)#
```

ステップ 2 iSCSI ログイン認証用に、ローカル データベースでユーザー名（iscsiuser）とパスワード（ffsffsfsffs345353554535）を構成します。

```
switch(config)# username iscsiuser password ffsffsfsffs345353554535 iscsi
```

iSCSI イニシエータ認証の制限

iSCSI イニシエータはデフォルトで、IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールに対する自身の認証用に、RADIUS サーバーまたはローカル データベースの任意のユーザー名を使用できます（CHAP ユーザー名は iSCSI イニシエータ名と無関係です）。IPS ポートを搭載したファイバ チャネル 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たCHAPチャレンジに有効な応答があった場合にかぎり、発信側にログインを許可します。ただし、CHAPユーザー名およびパスワードが信用できないものであると、問題が生じる可能性があります。

イニシエータがCHAP認証に特定のユーザー名を使用するように制限するには、次のステップを実行します。

手順

ステップ 1 コンフィギュレーション モードを入力します。

```
switch# config terminal
switch(config)#
```

ステップ 2 イニシエータ iqn.1987-02.com.cisco.init のコンフィギュレーション サブモードを開始します。

```
switch(config)# iscsi initiator name iqn.1987-02.com.cisco.init
switch(config-iscsi-init)#
```

ステップ 3 イニシエータ iqn.1987-02.com.cisco.init を、CHAP ユーザー名として user1 を使用する認証だけに制限します。

```
switch(config-iscsi-init)# username user1
```

（注）
ローカル AAA データベースまたは RADIUS サーバーで user1 を iSCSI ユーザーとして必ず定義してください。

相互 CHAP 認証の設定

IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールは、iSCSI イニシエータが iSCSI ログイン フェーズで Cisco MDS スイッチの iSCSI ターゲットを認証するメカニズムをサポートします。iSCSI 発信側の IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュール認証に加えて、この認証を使用できます。

iSCSIイニシエータに関するIPSポートを搭載したファイバチャネルモジュールまたはMPS-14/2モジュールの認証に加え、IPSポートを搭載したファイバチャネルモジュールまたはMPS-14/2モジュールは、iSCSI ログイン フェーズで Cisco MDS スイッチの iSCSI ターゲットを認証する、iSCSI イニシエータのメカニズムもサポートします。この認証には、ユーザー側で iSCSI 発信側に提示するスイッチ用のユーザー名およびパスワードを設定する必要があります。提供されたパスワードを使用して、発信側が IPS ポートに送信する CHAP チャレンジへの CHAP 応答が計算されます。

スイッチが発信側に対する自身の認証に使用するグローバルiSCSIターゲットユーザー名およびパスワードを設定する手順は、次のとおりです。

手順

ステップ 1 コンフィギュレーション モードを入力します。

```
switch# config terminal
switch(config)#
```

ステップ 2 すべてのイニシエータに対し、スイッチのユーザー アカウント（testuser）をクリア テキスト（デフォルト）で指定されたパスワード（abc123）とともに構成します。パスワードは 128 文字に制限されています。

```
switch(config)# iscsi authentication username testuser password abc123
```

ステップ 3 すべてのイニシエータに対し、スイッチのユーザ アカウント（user1）を 7 で指定された暗号化パスワード（!@*asdsfsdfjh!@df）とともに設定します。

```
switch(config)# iscsi authentication username user1 password 7!@*asdsfsdfjh!@df
```

ステップ 4 すべてのイニシエータに対し、スイッチのユーザー アカウント（user1）をクリア テキスト（デフォルトで 0 で示される）で指定されたパスワード（abcd12AAA）とともに構成します。パスワードは 128 文字に制限されています。

```
switch(config)# iscsi authentication username user1 password 0 abcd12AAA
```

ステップ 5 すべてのイニシエータのグローバル構成を削除します。

```
switch(config)# no iscsi authentication username testuser
```

認証用のイニシエータごとの iSCSI ターゲット ユーザ名とパスワードの構成

スイッチがイニシエータに対する自身の認証に使用するイニシエータ単位の iSCSI ターゲットのユーザー名およびパスワードを設定するには、次の手順を実行します。

始める前に

グローバル構成を表示するには、 **show running-config** および **show iscsi global** コマンドを使用します。**show running-config** および **show iscsi initiator configured** コマンドを使用して、イニシエータ固有の構成を表示します（コマンドの出力例については「iSCSI 情報の表示 」セクションを参照してください）。

手順

ステップ 1 コンフィギュレーション モードを入力します。

```
switch# config terminal
switch(config)#
```

ステップ 2 イニシエータ ノードの iSCSI 名を使用して iSCSI イニシエータを構成します。

```
switch(config)# iscsi initiator name iqn.1987-02.com.cisco.initiator
switch(config-iscsi-init)#
```

ステップ 3 スイッチのユーザー アカウント（testuser）をクリア テキスト（デフォルト）で指定されたパスワード（abcd12AAA）とともに設定します。パスワードは 128 文字に制限されています。

```
switch(config-iscsi-init)# mutual-chap username testuser password abcd12AAA
```

ステップ 4 スイッチのユーザー アカウント（user1）および 7（!@*asdsfsdfjh!@df）で指定された暗号化パスワードを構成します。

```
switch(config-iscsi-init)# mutual-chap username user1 password 7!@*asdsfsdfjh!@df
```

ステップ 5 スイッチ認証構成を削除します。

```
switch(config-iscsi-init)# no mutual-chap username testuser
```

iSCSI 即時データ機能および割り込みデータ機能

Cisco MDS スイッチは、ログイン ネゴシエーション フェーズで発信側が要求した場合に、iSCSI 即時データ機能および割り込みデータ機能をサポートします。即時データは、iSCSI コマンド プロトコル データ ユニット（PDU）のデータ セグメントに格納された iSCSI 書き込みデータで、1 つの PDU に書き込みコマンドと書き込みデータが結合されたものなどです。割り込みデータは、発信側が MSD スイッチなどの iSCSI ターゲットに送信する iSCSI 書き込みデータで、ターゲットから明示的な Ready To Transfer（R2T）PDU を受信する必要のない、iSCSI 送信データ PDU として送信されます。

この 2 つの機能は、発信側とターゲット間で R2T PDU の往復が 1 つ少なくなるため、小規模な書き込みコマンドでは入出力時間の短縮に有効です。MSD スイッチは iSCSI ターゲットとして、1 つのコマンドで最大 64 KB の割り込みデータを使用できます。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 発信側が即時データ機能および割り込みデータ機能をサポートする場合、MDS スイッチ上でこれらの機能が自動的にイネーブルになるので、設定は不要です。

iSCSI インターフェイス拡張機能

iSCSI インターフェイスでは IPS ポート単位で拡張設定オプションを使用できます。これらの構成は詳細な FCIP 構成と同様であり、該当する項ですでに説明されています（「詳細な FCIP プロファイル構成」

iSCSI インターフェイスからこれらのコマンドにアクセスするには、次の例を活用します。

```
switch# config terminal
switch(config)# interface iscsi 4/1
switch(config-if)#
```

Cisco MDS スイッチ向け iSCSI インターフェイスの拡張機能

Cisco MDS スイッチが iSCSI インターフェイスに関してサポートする拡張機能は、次のとおりです。

- iSCSI リスナー ポート
- TCP 調整パラメータ
- iSCSI ルーティング モード
- QoS 値の設定

iSCSI リスナー ポート

新しい TCP 接続を待ち受ける 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、iSCSI ポートは以後、新しく設定されたポート上の TCP 接続だけを許可します。

TCP 調整パラメータ

次の TCP パラメータを構成できます。

- 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」セクションを参照）。
- 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」セクションを 参照）。
- 最大再送信回数（詳細については、「最大再送信回数」セクションを参照 ）。
- パス MTU（詳細については、 「パス MTU」を参照）。
- 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」を参照）。
- 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、「FCIP プロファイル情報の表示」 を参照）。
- ウィンドウ輻輳モニタリング（デフォルトで有効で、デフォルト バースト サイズは 50 KB）（詳細については、「輻輳モニタリング」 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）。

iSCSI ルーティング モード

Cisco MDS 9000 ファミリ 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。モードごとにネゴシエーションを行う動作パラメータが異なり、長所も短所も異なります。また、適切な用途も異なります。

- パススルー モード：パススルー モードでは、IPS ポートを搭載したファイバ チャネル モジュールまたは MPS 14/2 モジュールのポートがファイバ チャネル ターゲットから読み取ったデータ フレームを変換し、バッファリングしないで 1 フレームずつ iSCSI ホストに転送します。したがって、着信フレームを 1 つ受信すると、ただちに 1 つの iSCSI 着信データ PDU として送信されます。

  反対方向では、IPS ポートを搭載したファイバ チャネル モジュールまたは MPS 14/2 モジュールのポートが、iSCSI ホストから送信できる iSCSI 書き込み送信データ PDU の最大サイズを、それを受信できるファイバ チャネル ターゲットで指定された最大データ サイズに制限します。その結果、iSCSI 送信データ PDU を 1 つ受信すると、1 つのファイバ チャネル データ フレームとしてファイバ チャネル ターゲットに送信されます。

  どちらの方向でもバッファリングが行われないので、転送遅延が短縮される利点があります。しかし、最大データ セグメント長が小さいので、ホスト システムの処理のオーバーヘッドが大きくなり、ホストからのデータ転送パフォーマンスが下がるのが一般的です。このモードのもう 1 つの利点は、iSCSI データ ダイジェストが可能になることです。これは TCP チェックサムで得られる以上に、PDU で伝送される iSCSI データの完全性保護に有効です。

- 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 ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールのポートが交換されたすべてのファイバ チャネル データ フレームを組み立て、1 つの大きい iSCSI 受信データ PDU にしてから、iSCSI クライアントに転送します。

  反対方向では、IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールのポートがホストに小さいデータ セグメント サイズを適用しないので、iSCSI ホストは任意のサイズ（最大 256 KB）の iSCSI 送信データ PDU を送信できます。ポートはさらに、iSCSI 送信データ PDU 全体を受信するまで待機し、PDU 全体を受信してから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 ターゲットに転送します。

  このモードの利点は、ホストからのデータ転送パフォーマンスが向上することです。欠点は、転送遅延が大きくなることと、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、デフォルトの転送モードです。

- カットスルー モード：カットスルー モードを使用すると、ストア アンド フォワード モードより読み取り処理のパフォーマンスが向上します。IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールのポートは、各ファイバ チャネル受信データ フレームを受信すると、交換全体の完了を待たずに、ただちに iSCSI ホストに転送することによって、パフォーマンスの向上を実現します。書き込み送信データの処理に関しては、ストア アンド フォワード モードと差はありません。

図 *18 : iSCSI* ルーティング モード

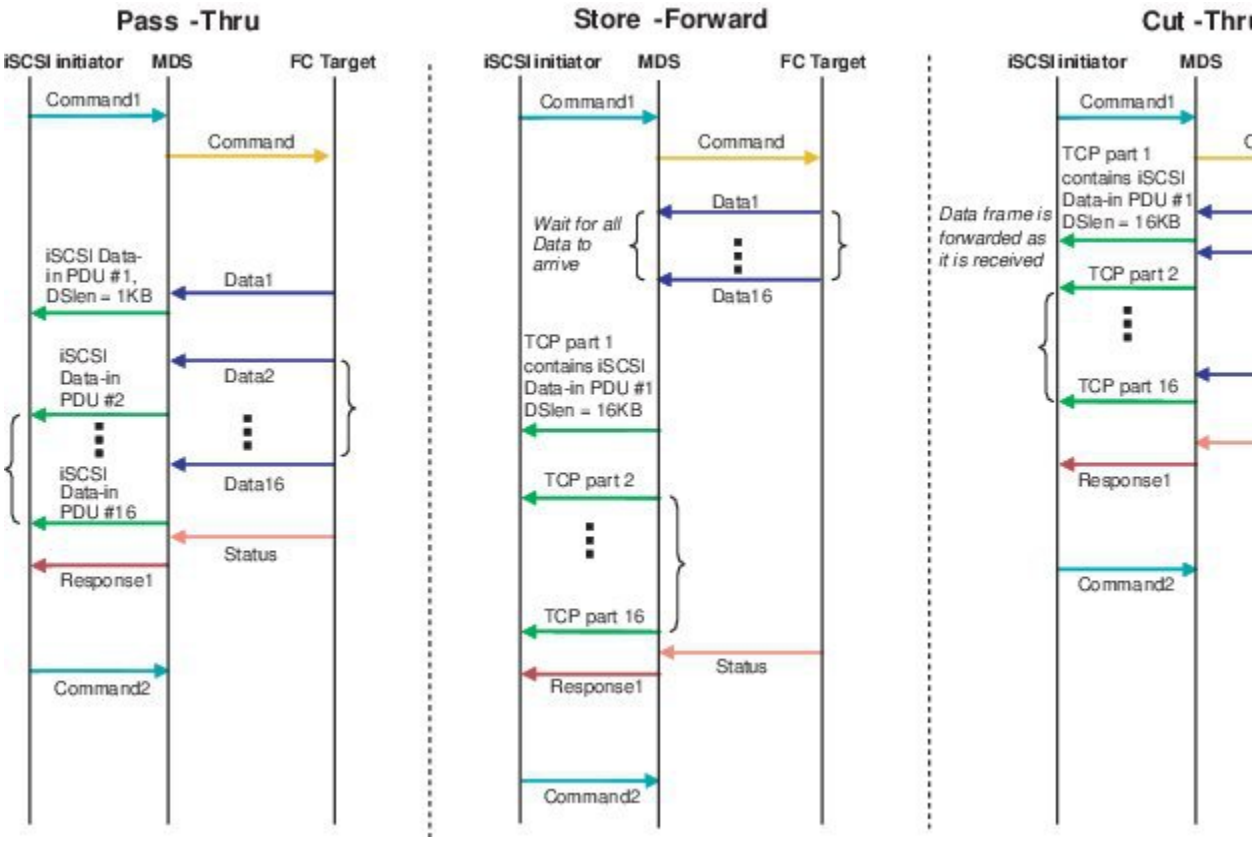


表 *1 : iSCSI* ルーティング モードの比較

モード	利点	欠点
パススルー	遅延が小さい。 データ ダイジェストが使用可能。	データ転送パフォーマンスが低い。
ストア アンド フォワード	データ転送パフォーマンスが高い。	データ ダイジェストが使用不可。

モード	利点	欠点
カットスルー	読み取りパフォーマンスがストア アンド フォワードより向上。	ファイバチャネル ターゲットが置換可能なさまざまなコマンド用の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 モードで転送されるが、後続コマンドのデータはバッファリングされ、動作はストア アンド フォワード モードと同じになる。 データ ダイジェストが使用不可。

（注） iSLB VRRP グループに属している iSCSI インターフェイスの転送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が影響を受けます。「iSCSIインターフェイス パラメータの変更およびロード バランシングへの影響」セクションを参照してください。

QoS 値の設定

QoS 値を設定するには、次のステップを実行します。

手順

ステップ 1 この iSCSI インターフェイスのすべての発信 IP パケットに適用される Differentiated Services Code Point（DSCP）値を 3 に構成します。iSCSI DSCP 値の有効範囲は 0～63 です。

```
switch(config-if)# qos 3
```

ステップ 2 スイッチを工場出荷時設定に戻します（すべてのパケットが DSCP 値 0 でマークされます）。

```
switch(config-if)# no qos 5
```

iSCSI 情報の表示

iSCI の構成に関する詳細情報を取得するには、**show iscsi** コマンドを使用します。

この項では、次のトピックについて取り上げます。

- iSCSI インターフェイスの表示
- iSCSI 統計情報の表示

- プロキシ イニシエータ情報の表示
- グローバル iSCSI 情報の表示
- iSCSI セッションの表示
- iSCSI イニシエータの表示
- iSCSI 仮想ターゲットの表示
- iSCSI ユーザー情報の表示

iSCSI インターフェイスの表示

iSCSI インターフェイスの概要、カウンタ、説明、およびステータスを表示するには、**show iscsi interface** コマンドを使用します。この出力を使用して、管理モード、インターフェイスのステータス、現在使用中の TCP パラメータ、および短い統計情報を確認します。

iSCSI インターフェイス情報の表示例

```
switch# show interface iscsi 4/1
iscsi4/1 is up
Hardware is GigabitEthernet
Port WWN is 20:cf:00:0c:85:90:3e:80
Admin port mode is ISCSI
Port mode is ISCSI
Speed is 1 Gbps
iSCSI initiator is identified by name
Number of iSCSI session: 0 (discovery session: 0)
Number of TCP connection: 0
Configured TCP parameters
Local Port is 3260
PMTU discover is enabled, reset timeout is 3600 sec
Keepalive-timeout is 60 sec
Minimum-retransmit-time is 300 ms
Max-retransmissions 4
Sack is enabled
QOS code point is 0
Maximum allowed bandwidth is 1000000 kbps
Minimum available bandwidth is 70000 kbps
Estimated round trip time is 1000 usec
Send buffer size is 4096 KB
Congestion window monitoring is enabled, burst size is 50 KB
Configured maximum jitter is 500 us
Forwarding mode: store-and-forward
TMF Queueing Mode : disabled
Proxy Initiator Mode : disabled
5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
iSCSI statistics
Input 0 packets, 0 bytes
Command 0 pdus, Data-out 0 pdus, 0 bytes
Output 0 packets, 0 bytes
Response 0 pdus (with sense 0), R2T 0 pdus
Data-in 0 pdus, 0 bytes
```

iSCSI 統計情報の表示

iSCSI インターフェイスごとの短い iSCSI 統計情報または詳細な iSCSI 統計情報を表示するには、 **show iscsi stats** コマンドを使用します。詳細については、次の例を参照してください。

次の例は、IPS ポートでのインバウンドおよびアウトバウンドの両方向の iSCSI スループットを示します。また、この IPS ポートが送受信する異なる種類の iSCSI PDU の数を示します

iSCSI インターフェイスの短い iSCSI 統計情報の表示例

```
switch# show iscsi stats iscsi 2/1
iscsi2/1
5 minutes input rate 704 bits/sec, 88 bytes/sec, 1 frames/sec
5 minutes output rate 704 bits/sec, 88 bytes/sec, 1 frames/sec
iSCSI statistics
974756 packets input, 142671620 bytes
Command 2352 pdus, Data-out 44198 pdus, 92364800 bytes, 0 fragments, unsolicited 0 bytes
output 1022920 packets, 143446248 bytes
Response 2352 pdus (with sense 266), R2T 1804 pdus
Data-in 90453 pdus, 92458248 bytes
```

次の例は、IPS ポートの詳細な iSCSI 統計情報を表示します。トラフィック レートおよび各タイプの iSCSI PDU の数とともに、受信および転送した FCP フレームの数、iSCSI ログインの試行回数、成功回数、および失敗回数が表示されます。また、送受信された各種 iSCSI PDU のうち、重大ではないかまたは頻繁には発生しない iSCSI PDU の数（受信 NOP および送信 NOP（NOP-In および NOP-Out）、テキスト リクエストおよび応答（Text-REQ および Text-RESP）、およびタスク管理リクエストおよび応答（TMF-REQ および TMF-RESP）など）も表示されます。

さまざまなエラー タイプと PDU またはフレーム ドロップ発生回数もカウントされ、表示されます。たとえば、Bad ヘッダーダイジェストは、CRC 検証に失敗したヘッダー ダイジェストがある受信 iSCSI PDU の数を示します。iSCSI Drop セクションには、ターゲットの停止、LUN マッピングの失敗、データ CRC エラー、予想外の即時または非請求データなどの原因でドロップされた PDU の数が示されます。これらの統計情報は、機能が予期したように動作しない場合のデバッグに役立ちます。

最後の [Buffer Stats] セクションは、内部 IPS パケット バッファ動作に関する統計情報を表示します。このセクションはデバッグだけを目的としています。

iSCSI インターフェイスの詳細な iSCSI 統計情報の表示例

```
switch# show iscsi stats iscsi 2/1 detail
iscsi2/1
5 minutes input rate 704 bits/sec, 88 bytes/sec, 1 frames/sec
5 minutes output rate 704 bits/sec, 88 bytes/sec, 1 frames/sec
iSCSI statistics
974454 packets input, 142656516 bytes
Command 2352 pdus, Data-out 44198 pdus, 92364800 bytes, 0 fragments, unsolicited 0 bytes
output 1022618 packets, 143431144 bytes
Response 2352 pdus (with sense 266), R2T 1804 pdus
Data-in 90453 pdus, 92458248 bytes
iSCSI Forward:
Command:2352 PDUs (Rcvd:2352)
Data-Out (Write):16236 PDUs (Rcvd 44198), 0 fragments, 92364800 bytes, unsolicited 0
bytes
FCP Forward:
Xfer_rdy:1804 (Rcvd:1804)
Data-In:90453 (Rcvd:90463), 92458248 bytes
```

```
Response:2352 (Rcvd:2362), with sense 266
TMF Resp:0

iSCSI Stats:
Login:attempt:13039, succeed:110, fail:12918, authen fail:0
Rcvd:NOP-Out:914582, Sent:NOP-In:914582
NOP-In:0, Sent:NOP-Out:0
TMF-REQ:0, Sent:TMF-RESP:0
Text-REQ:18, Sent:Text-RESP:27
SNACK:0
Unrecognized Opcode:0, Bad header digest:0
Command in window but not next:0, exceed wait queue limit:0
Received PDU in wrong phase:0
SCSI Busy responses:0
Immediate data failure::Separation:0
Unsolicited data failure::Separation:0, Segment:0
Add header:0
Sequence ID allocation failure:0
FCP Stats:
Total:Sent:47654
Received:96625 (Error:0, Unknown:0)
Sent:PLOGI:10, Rcvd:PLOGI_ACC:10, PLOGI_RJT:0
PRLI:10, Rcvd:PRLI_ACC:10, PRLI_RJT:0, Error:0, From initiator:0
LOGO:4, Rcvd:LOGO_ACC:0, LOGO_RJT:0
PRLO:4, Rcvd:PRLO_ACC:0, PRLO_RJT:0
ABTS:0, Rcvd:ABTS_ACC:0
TMF REQ:0
Self orig command:10, Rcvd:data:10, resp:10
Rcvd:PLOGI:156, Sent:PLOGI_ACC:0, PLOGI_RJT:156
LOGO:0, Sent:LOGO_ACC:0, LOGO_RJT:0
PRLI:8, Sent:PRLI_ACC:8, PRLI_RJT:0
PRLO:0, Sent:PRLO_ACC:0, PRLO_RJT:0
ADISC:0, Sent:ADISC_ACC:0, ADISC_RJT:0
ABTS:0

iSCSI Drop:
Command:Target down 0, Task in progress 0, LUN map fail 0
CmdSeqNo not in window 0, No Exchange ID 0, Reject 0
No task:0
Data-Out:0, Data CRC Error:0
TMF-Req:0, No task:0
Unsolicited data:0, Immediate command PDU:0
FCP Drop:
Xfer_rdy:0, Data-In:0, Response:0

Buffer Stats:
Buffer less than header size:0, Partial:45231, Split:322
Pullup give new buf:0, Out of contiguous buf:0, Unaligned m_data:0
```

プロキシ イニシエータ情報の表示

プロキシイニシエータ機能がiSCSIインターフェイスで有効になっている場合、設定されているプロキシ イニシエータの情報を表示するには、**show interface iscsi** コマンドを使用します。

システムにより割り当てられたWWNを持つiSCSIインターフェイスのプロキシイニシエータ情報の表示例：

```
switch# show interface iscsi 4/1
iscsi4/1 is up
Hardware is GigabitEthernet
Port WWN is 20:c1:00:05:30:00:a7:9e
Admin port mode is ISCSI
Port mode is ISCSI
```

```
Speed is 1 Gbps
iSCSI initiator is identified by name
Number of iSCSI session: 0, Number of TCP connection: 0
Configured TCP parameters
Local Port is 3260
PMTU discover is enabled, reset timeout is 3600 sec
Keepalive-timeout is 60 sec
Minimum-retransmit-time is 300 ms
Max-retransmissions 4
Sack is disabled
QOS code point is 0
Forwarding mode: pass-thru
TMF Queueing Mode : disabled
Proxy Initiator Mode : enabled<----------------------------Proxy initiator is enabled
nWWN is 28:00:00:05:30:00:a7:a1 (system-assigned)<----System-assigned nWWN
pWWN is 28:01:00:05:30:00:a7:a1 (system-assigned)<---- System-assigned pWWN
5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
iSCSI statistics
Input 7 packets, 2912 bytes
Command 0 pdus, Data-out 0 pdus, 0 bytes
Output 7 packets, 336 bytes
Response 0 pdus (with sense 0), R2T 0 pdus
Data-in 0 pdus, 0 bytes
```

ユーザーによって割り当てられたWWNを持つiSCSIインターフェイスのプロキシイニシエータ情報の表示例：

```
switch# show interface iscsi 4/2
iscsi4/2 is up
Hardware is GigabitEthernet
Port WWN is 20:c1:00:05:30:00:a7:9e
Admin port mode is ISCSI
Port mode is ISCSI
Speed is 1 Gbps
iSCSI initiator is identified by name
Number of iSCSI session: 0, Number of TCP connection: 0
Configured TCP parameters
Local Port is 3260
PMTU discover is enabled, reset timeout is 3600 sec
Keepalive-timeout is 60 sec
Minimum-retransmit-time is 300 ms
Max-retransmissions 4
Sack is disabled
QOS code point is 0
Forwarding mode: pass-thru
TMF Queueing Mode : disabled
Proxy Initiator Mode : enabled
nWWN is 11:11:11:11:11:11:11:11 (manually-configured)<----User-assigned nWWN
pWWN is 22:22:22:22:22:22:22:22 (manually-configured)<----User-assigned pWWN
5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
iSCSI statistics
Input 7 packets, 2912 bytes
Command 0 pdus, Data-out 0 pdus, 0 bytes
Output 7 packets, 336 bytes
Response 0 pdus (with sense 0), R2T 0 pdus
Data-in 0 pdus, 0 bytes
```

グローバル iSCSI 情報の表示

全体的な設定と iSCSI ステータスを表示するには、**show iscsi global** コマンドを使用します。

現在のグローバル iSCSI 構成とステータスの表示例：

```
switch# show iscsi global
iSCSI Global information
Authentication: CHAP, NONE
Import FC Target: Enabled
Initiator idle timeout: 300 seconds
Number of target node: 0
Number of portals: 11
Number of session: 0
Failed session: 0, Last failed initiator name:
```

iSCSI セッションの表示

スイッチの現在の iSCSI セッションに関する詳細を表示するには、**show iscsi session** コマンドを使用します。パラメータを指定しない場合、このコマンドはすべてのセッションを表示します。イニシエータ、ターゲット、またはこの両方を指定して出力をフィルタリングできます。次の例では、IQN（iqn.1987-05.com.cisco:02.3021b0f2fda0.avanti12-w2k）に基づいて構成されている iSCSI イニシエータと、IPv4 アドレス（10.10.100.199）に基づいて構成されている別の iSCSI イニシエータを示します。

すべての iSCSI セッションの短い情報の表示例

```
switch# show iscsi session
Initiator iqn.1987-05.com.cisco:02.3021b0f2fda0.avanti12-w2k
Initiator ip addr (s): 10.10.100.116
Session #1
Discovery session, ISID 00023d000043, Status active
Session #2
Target VT1
VSAN 1, ISID 00023d000046, Status active, no reservation
Session #3
Target VT2
VSAN 1, ISID 00023d000048, Status active, no reservation
Initiator 10.10.100.199
Initiator name iqn.1987-05.com.cisco.01.7e3183ae458a94b1cd6bc168cba09d2e
Session #1
Target VT2
VSAN 1, ISID 246700000000, Status active, no reservation
Session #2
Target VT1
VSAN 1, ISID 246b00000000, Status active, no reservation
Session #3
Target iqn.1987-05.com.cisco:05.switch.04-01.2100002037a6be32
VSAN 1, ISID 246e00000000, Status active, no reservation
```

次の例は、IPv4 アドレス（10.10.100.199）に基づいて設定された iSCSI イニシエータを示します。

指定した iSCSI セッション短い情報の表示例：

```
switch# show iscsi session initiator 10.10.100.199 target VT1
Initiator 10.10.100.199
Initiator name iqn.1987-05.com.cisco.01.7e3183ae458a94b1cd6bc168cba09d2e
Session #1
Target VT1
VSAN 1, ISID 246b00000000, Status active, no reservation
```

指定した iSCSI セッションの詳細情報の表示例：

```
switch# show iscsi session initiator 10.10.100.199 target VT1 detail
Initiator 10.10.100.199 (oasis-qa)
Initiator name iqn.1987-05.com.cisco.01.7e3183ae458a94b1cd6bc168cba09d2e
Session #1 (index 3)
Target VT1
VSAN 1, ISID 246b00000000, TSIH 384, Status active, no reservation
Type Normal, ExpCmdSN 39, MaxCmdSN 54, Barrier 0
MaxBurstSize 0, MaxConn 0, DataPDUInOrder No
DataSeqInOrder No, InitialR2T Yes, ImmediateData No
Registered LUN 0, Mapped LUN 0
Stats:
PDU: Command: 38, Response: 38
Bytes: TX: 8712, RX: 0
Number of connection: 1
Connection #1
Local IP address: 10.10.100.200, Peer IP address: 10.10.100.199
CID 0, State: LOGGED_IN
StatSN 62, ExpStatSN 0
MaxRecvDSLength 1024, our_MaxRecvDSLength 1392
CSG 3, NSG 3, min_pdu_size 48 (w/ data 48)
AuthMethod none, HeaderDigest None (len 0), DataDigest None (len 0)
Version Min: 2, Max: 2
FC target: Up, Reorder PDU: No, Marker send: No (int 0)
Received MaxRecvDSLen key: No
```

iSCSI イニシエータの表示

スイッチの iSCSI インターフェイスに接続されているすべてのイニシエータに関する情報を表示するには、**show iscsi initiator** コマンドを使用します。目的の iSCSI 発信側だけを表示するように情報をフィルタリングするには、発信側名を指定します。iSCSI イニシエータの詳細出力を取得するには、**detail** オプションを指定します。**iscsi-session**（およびオプションで **detail**）パラメータを指定すると、iSCSI セッション情報だけが表示されます。**fcp-session**（およびオプションで **detail**）パラメータを指定すると、FCP セッション情報だけが表示されます。出力には、スタティック イニシエータとダイナミック イニシエータが含まれます。

接続されている iSCSI イニシエータの情報の表示例

```
switch# show iscsi initiator
iSCSI Node name is iqn.1987-05.com.cisco:02.3021b0f2fda0.avanti12-w2k
Initiator ip addr (s): 10.10.100.116
iSCSI alias name: AVANTI12-W2K
Node WWN is 22:01:00:05:30:00:10:e1 (configured)
Member of vsans: 1, 2, 10
Number of Virtual n_ports: 1
Virtual Port WWN is 22:04:00:05:30:00:10:e1 (configured)
Interface iSCSI 4/1, Portal group tag: 0x180
VSAN ID 1, FCID 0x6c0202
VSAN ID 2, FCID 0x6e0000
VSAN ID 10, FCID 0x790000

iSCSI Node name is 10.10.100.199
iSCSI Initiator name: iqn.1987-05.com.cisco.01.7e3183ae458a94b1cd6bc168cba09d2e
iSCSI alias name: oasis-qa
Node WWN is 22:03:00:05:30:00:10:e1 (configured)
Member of vsans: 1, 5
Number of Virtual n_ports: 1
Virtual Port WWN is 22:00:00:05:30:00:10:e1 (configured)
Interface iSCSI 4/1, Portal group tag: 0x180
VSAN ID 5, FCID 0x640000
VSAN ID 1, FCID 0x6c0203
```

iSCSI イニシエータの詳細情報の表示例

```
switch# show iscsi initiator iqn.1987-05.com.cisco:02.3021b0f2fda0.avanti12-w2k detail
iSCSI Node name is iqn.1987-05.com.cisco:02.3021b0f2fda0.avanti12-w2k
Initiator ip addr (s): 10.10.100.116
iSCSI alias name: AVANTI12-W2K
Node WWN is 22:01:00:05:30:00:10:e1 (configured)
Member of vsans: 1, 2, 10
Number of Virtual n_ports: 1

Virtual Port WWN is 22:04:00:05:30:00:10:e1 (configured)
Interface iSCSI 4/1, Portal group tag is 0x180
VSAN ID 1, FCID 0x6c0202
1 FC sessions, 1 iSCSI sessions
iSCSI session details <-------------------iSCSI session details
Target: VT1
Statistics:
PDU: Command: 0, Response: 0
Bytes: TX: 0, RX: 0
Number of connection: 1
TCP parameters
Local 10.10.100.200:3260, Remote 10.10.100.116:4190
Path MTU: 1500 bytes
Retransmission timeout: 310 ms
Round trip time: Smoothed 160 ms, Variance: 38
Advertized window: Current: 61 KB, Maximum: 62 KB, Scale: 0
Peer receive window: Current: 63 KB, Maximum: 63 KB, Scale: 0
Congestion window: Current: 1 KB

FCP Session details <-------------------FCP session details
Target FCID: 0x6c01e8 (S_ID of this session: 0x6c0202)
pWWN: 21:00:00:20:37:62:c0:0c, nWWN: 20:00:00:20:37:62:c0:0c
Session state: CLEANUP
1 iSCSI sessions share this FC session
Target: VT1
Negotiated parameters
RcvDataFieldSize 1392 our_RcvDataFieldSize 1392
MaxBurstSize 0, EMPD: FALSE
Random Relative Offset: FALSE, Sequence-in-order: Yes
Statistics:
PDU: Command: 0, Response: 0
```

SAN の iSCSI イニシエータ用に作成されたファイバ チャネル N ポートのファイバ チャネル ネーム サーバ エントリを表示するには、**show fcns database**（およびオプションで **detail**）コマンドを使用します。

FCNS データベースの内容の表示例

```
switch# show fcns database
VSAN 1:
------------------------------------------------------------------------
FCID TYPE PWWN (VENDOR) FC4-TYPE:FEATURE
------------------------------------------------------------------------
0x020101 N 22:04:00:05:30:00:35:e1 (Cisco) scsi-fcp:init isc..w <--iSCSI
0x020102 N 22:02:00:05:30:00:35:e1 (Cisco) scsi-fcp:init isc..w initiator
0x0205d4 NL 21:00:00:04:cf:da:fe:c6 (Seagate) scsi-fcp:target
0x0205d5 NL 21:00:00:04:cf:e6:e4:4b (Seagate) scsi-fcp:target
...
Total number of entries = 10

VSAN 2:
------------------------------------------------------------------------
FCID TYPE PWWN (VENDOR) FC4-TYPE:FEATURE
------------------------------------------------------------------------
```

```
0xef0001 N 22:02:00:05:30:00:35:e1 (Cisco) scsi-fcp:init isc..w
Total number of entries = 1

VSAN 3:
--------------------------------------------------------------------------
FCID TYPE PWWN (VENDOR) FC4-TYPE:FEATURE
--------------------------------------------------------------------------
0xed0001 N 22:02:00:05:30:00:35:e1 (Cisco) scsi-fcp:init isc..w
Total number of entries = 1
```

FCNS データベースの詳細表示例

```
switch# show fcns database detail
------------------------
VSAN:1 FCID:0x020101
------------------------
port-wwn (vendor) :22:04:00:05:30:00:35:e1 (Cisco)
node-wwn :22:03:00:05:30:00:35:e1
class :2,3
node-ip-addr :10.2.2.12 <--- iSCSI initiator's IPv4 address
ipa :ff ff ff ff ff ff ff ff
fc4-types:fc4_features:scsi-fcp:init iscsi-gw
symbolic-port-name :
symbolic-node-name :iqn.1991-05.com.microsoft:oasis2-dell <--- iSCSI initiator's IQN
port-type :N
port-ip-addr :0.0.0.0
fabric-port-wwn :22:01:00:05:30:00:35:de
hard-addr :0x000000
------------------------
VSAN:1 FCID:0x020102
------------------------
port-wwn (vendor) :22:02:00:05:30:00:35:e1 (Cisco)
node-wwn :22:01:00:05:30:00:35:e1
class :2,3
node-ip-addr :10.2.2.11
ipa :ff ff ff ff ff ff ff ff
fc4-types:fc4_features:scsi-fcp:init iscsi-gw
symbolic-port-name :
symbolic-node-name :iqn.1987-05.com.cisco.01.14ac33ba567f986f174723b5f9f2377
port-type :N
port-ip-addr :0.0.0.0
fabric-port-wwn :22:01:00:05:30:00:35:de
hard-addr :0x000000
...
Total number of entries = 10
==========================================================================
------------------------
VSAN:2 FCID:0xef0001
------------------------
port-wwn (vendor) :22:02:00:05:30:00:35:e1 (Cisco)
node-wwn :22:01:00:05:30:00:35:e1
class :2,3
node-ip-addr :10.2.2.11
ipa :ff ff ff ff ff ff ff ff
fc4-types:fc4_features:scsi-fcp:init iscsi-gw
symbolic-port-name :
symbolic-node-name :iqn.1987-05.com.cisco.01.14ac33ba567f986f174723b5f9f2377
port-type :N
port-ip-addr :0.0.0.0
fabric-port-wwn :22:01:00:05:30:00:35:de
hard-addr :0x000000
Total number of entries = 1
...
```

構成されたすべての iSCSI イニシエータに関する情報を表示するには、**show iscsi initiator configured** を使用します。名前を指定すると、目的のイニシエータに関する情報が表示されます。

構成したイニシエータに関する情報の表示例

```
switch# show iscsi initiator configured
iSCSI Node name is iqn.1987-05.com.cisco:02.3021b0f2fda0.avanti12-w2k
Member of vsans: 1, 2, 10
Node WWN is 22:01:00:05:30:00:10:e1
No. of PWWN: 5
Port WWN is 22:04:00:05:30:00:10:e1
Port WWN is 22:05:00:05:30:00:10:e1
Port WWN is 22:06:00:05:30:00:10:e1
Port WWN is 22:07:00:05:30:00:10:e1
Port WWN is 22:08:00:05:30:00:10:e1

iSCSI Node name is 10.10.100.199
Member of vsans: 1, 5
Node WWN is 22:03:00:05:30:00:10:e1
No. of PWWN: 4
Port WWN is 22:00:00:05:30:00:10:e1
Port WWN is 22:09:00:05:30:00:10:e1
Port WWN is 22:0a:00:05:30:00:10:e1
Port WWN is 22:0b:00:05:30:00:10:e1

User Name for Mutual CHAP: testuser
```

iSCSI 仮想ターゲットの表示

iSCSI イニシエータに iSCSI 仮想ターゲットとしてエクスポートされたファイバ チャネル ターゲットに関する情報を表示するには、 **show iscsi virtual-target** を使用します。出力には、スタティック ターゲットとダイナミック ターゲットが含まれます。

エクスポートされたターゲットの表示例

```
switch# show iscsi virtual-target
target: VT1
* Port WWN 21:00:00:20:37:62:c0:0c
Configured node
all initiator permit is enabled
target: VT2
Port WWN 21:00:00:04:cf:4c:52:c1
Configured node
all initiator permit is disabled
target: iqn.1987-05.com.cisco:05.switch.04-01.2100002037a6be32
Port WWN 21:00:00:20:37:a6:be:32 , VSAN 1
Auto-created node
```

iSCSI ユーザー情報の表示

構成されたすべての iSCSI ユーザー名を表示するには、**show user-account iscsi** コマンドを使用します。

iSCSI ユーザー名の表示例

```
switch# show user-account iscsi
username:iscsiuser
secret: dsfffsffsffasffsdffg
username:user2
secret:cshadhdhsadadjajdjas
```

iSLB の構成

iSCSI サーバ ロードバランシング（iSLB）機能を使用すると、百単位、場合によっては千単位のイニシエータからなる大規模な iSCSI 環境を容易に構成できます。iSLB には次の機能があります。

- 発信側ターゲットおよび自動ゾーンがサポートされるので、iSLB 発信側の設定が簡素化されます。
- Cisco Fabric Services（CFS）によって、ファブリックのすべての MDS スイッチに iSLB 発信側設定が配信されるので、手動設定が不要になります。
- iSCSI ログイン リダイレクトおよび VRRP を使用することによって、iSLB 発信側のダイナミック ロード バランシングが使用できます。

iSLB を使用しない場合、iSCSI を設定するために次の作業が必要になります。

- 次の作業を含め、MDS スイッチ上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 を使用した発信側の設定
  - 発信側およびターゲットのゾーン分割設定
  - （任意）仮想ターゲットの作成および発信側へのアクセス権付与
  - MDS スイッチ上で発信側に作成したスタティック pWWN に基づく、発信側に関するストレージ システム上でのターゲット LUN マッピングおよびマスクの設定
- 複数の MDS スイッチに、設定を手動でコピーする必要があります。
- IPS ポートにロード バランシングはありません。次に例を示します。
  - 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しません。
  - 複数の VRRP グループを使用し、さまざまな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。

- 発信側ターゲットおよび自動ゾーンがサポートされるので、iSLB 発信側の設定が簡素化されます。
- Cisco Fabric Services（CFS）によって、ファブリックのすべての MDS スイッチに iSLB 発信側設定が配信されるので、手動設定が不要になります。

（注） CFS を使用した場合、ファブリック全体に配信されるのは、スタティック マッピングの iSLB 発信側設定だけです。ダイナミックおよびスタティック マッピングの iSCSI 発信側設定は配信されません。

- iSCSI ログイン リダイレクトおよび VRRP を使用することによって、iSLB 発信側のダイナミック ロード バランシングが使用できます。

（注） iSLB を構成する前に、iSCSI を有効にする必要があります（「iSCSI の有効化」セクションを参照）。

iSLB を使用するには、ファブリック内のすべてのスイッチで、Cisco MDS SAN-OS Release 2.1(1a) 以降が稼働している必要があります。

この項では、次のトピックについて取り上げます。

iSLB の設定制限

iSLB の設定に関しては、次の限度があります。

- ファブリックでサポートされる iSLB および iSCSI 発信側の最大数は 2000 です。
- 透過型またはプロキシイニシエータ モードで IPS ポートがサポートする iSLB および iSCSI セッションの最大数は 500 です。
- ファブリックでサポートされる iSLB イニシエータの最大数は 2000 です。
- スイッチがサポートする iSLB イニシエータおよび iSCSI セッションの最大数は 5000 です。
- 透過型またはプロキシ イニシエータ モードにおいて、各 IPS ポートの最大 iSLB セッション数は 500 です。
- ファブリックでサポートされる iSLB および iSCSI ターゲットの最大数は 6000 です。
- CFS 配信が有効な iSLB を使用できるファブリック内のスイッチの最大数は 4 です。
- 保留中の設定に追加できる新規 iSLB 発信側の最大数は 200 です。発信側をそれ以上追加する場合は、設定をいったんコミットする必要があります。
- 実行コンフィギュレーションで 200 を超える iSLB 発信側を設定している場合、iSCSI をディセーブルにできません。iSLB 発信側を 200 未満に減らしてから、iSCSI をディセーブルにしてください。
- CFS の配信を使用しないで iSLB を使用することは可能ですが、iSLB 自動ゾーン機能を使用した場合、ゾーンセットがアクティブになった時点で、トラフィックが中断されます。

- IVR および iSLB 機能が同じファブリックでイネーブルの場合、ファブリック内に両方の機能がイネーブルのスイッチが少なくとも 1 つは必要です。ゾーン分割関連の設定およびアクティブ化（標準ゾーン、IVR ゾーン、または iSLB ゾーン）は、このスイッチ上で実行する必要があります。そうしないと、ファブリック内のトラフィックが中断することがあります。

iSLB 構成の前提条件

iSLB を設定する前に、次の前提作業を実行します。

- iSCSI を有効にします（詳細については、「iSCSI の有効化」セクションを参照してください）。
- ギガビット イーサネット インターフェイスを構成します（「IPv4 のギガビット イーサネットの基本構成」セクションを参照）。
- VRRP グループを構成します（「VRRP を使用したロードバランシングを構成」セクションを参照）。
- ゾーン セットを設定してアクティブにします（詳細については、『Cisco Fabric Manager ファブリック構成ガイド』『Cisco MDS 9000 Family NX-OS ファブリック構成ガイド』を参照してください）。
- iSLB の CFS 配信を有効にします（「iSLB 構成の配信の有効化」セクションを参照）。

iSLB イニシエータ

iSLBイニシエータは、iSCSIイニシエータが提供する機能のほかに、次の機能を提供します。

- iSLB 発信側は、iSLB 仮想ターゲットもサポートします。
- イニシエータ ターゲット：これらのターゲットは、特定のイニシエータに対して設定されます。
- 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：iSCSI ログイン リダイレクトが有効な場合、IPS Manager はインターフェイスごとに計算した負荷に基づいて、最良のインターフェイスに着信セッションをリダイレクトします。
- CFS を使用して行う他のスイッチへの設定配信

iSLBイニシエータは、iSCSIイニシエータが提供する機能のほかに、次の機能を提供します。

- iSLB 発信側は、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 仮想ターゲットときわめて類似していますが、アドバタイズ インターフェイス オプションがないので、CFS を使用して配信可能であることが異なります。
- 発信側ターゲット：これらのターゲットは、特定の発信側に対して設定されます。

- 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いて、最良のインターフェイスに着信セッションをリダイレクトします。
- CFS を使用して行う他のスイッチへの設定配信

iSLB イニシエータの構成

このセクションは、次のトピックで構成されています。

iSLB イニシエータの構成

iSLB イニシエータの **name** オプションを 使用して iSLB イニシエータ構成サブモードを開始するには、次のステップを実行します。

始める前に

iSLB 発信側を設定する前に、その名前または IP アドレスを指定する必要があります。

iSLB 発信側の名前または IP アドレスの指定方法は、iSCSI 発信側の場合と同じです。「スタティック マッピング」を参照してください。

手順

ステップ 1 イニシエータ ノードの iSCSI 名 (iqn.1987-02.com.cisco.initiator) を使用して iSLB イニシエータを設定し、iSLBイニシエータ設定サブモードに入ります。名前の最大長は、英数字223 文字です。最小長は16 です。

```
switch# config terminal
switch(config)#
switch(config)# islb initiator name iqn.1987-02.com.cisco.initiator
switch(config-islb-init)#
```

ステップ 2 構成済み iSLB イニシエータを削除します。

```
switch(config)# no lslb initiator name iqn.1987-02.com.cisco.initiator
```

iSLB イニシエータ IP アドレスの構成

iSLB イニシエータの **ip-address** オプションを使用して iSLB イニシエータ コンフィギュレーション サブモードを開始するには、次の手順を実行します。

始める前に

iSLB 発信側を設定する前に、その名前または IP アドレスを指定する必要があります。

iSLB 発信側の名前または IP アドレスの指定方法は、iSCSI 発信側の場合と同じです。「スタティック マッピング」を参照してください。

手順

ステップ 1 イニシエータ ノードの IPv4 アドレスを使用して iSLB イニシエータを構成し、iSLB イニシエータ構成サブモードを開始します。

```
switch# config terminal
switch(config)# islb initiator ip-address 10.1.1.3
```

ステップ 2 構成済み iSLB イニシエータを削除します。

```
switch(config)# no islb initiator ip-address 10.1.1.3
```

ステップ 3 イニシエータ ノードの IPv6 ユニキャスト アドレスを使用して iSLB イニシエータを構成し、iSLB イニシエータ構成サブモードを開始します。

```
switch(config)# islb initiator ip-address 2001:0DB8:800:200C::417A
switch(config-islb-init)#
```

ステップ 4 構成済み iSLB イニシエータを削除します。

```
switch(config)# no islb initiator ip-address 2001:0DB8:800:200C::417A
```

iSLB 発信側への WWN の割り当て

iSLB ホストは次のいずれかのメカニズムで、N ポートの WWN に対応付けられます。

- 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 発信側の WWN 割り当ては、iSCSI 発信側の場合と同じです。ダイナミック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 割り当て」を参照してください。

SystemAssign system-assign オプションの使用を推奨します。手動で WWN を割り当てる場合は、固有の割り当てにする必要があります（詳細については、『Cisco Fabric Manager ファブリック構成ガイド』『Cisco MDS 9000 ファミリ NX-OS ファブリック構成ガイド』を参照してください）。すでに割り当てられている WWN は使用できません。

ダイナミック iSLB 発信側 WWN マッピングをスタティックにする方法

ダイナミック iSLB イニシエータのログイン後に、そのイニシエータで次回ログイン時にも同じマッピングが使用されるように、自動的に割り当てられた nWWN/pWWN マッピングを維持することがあります（「ダイナミック マッピング」セクションを参照してください）。

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、対応する WWN を固定にすることができます

（注） ダイナミック iSCSI 発信側をスタティック iSLB 発信側に変換したり、ダイナミック iSLB 発信側をスタティック iSCSI 発信側に変換したりはできません。詳細については、「ダイナミック マッピング」を参照してください）。

（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 の場合と同じです。

（注） CFS を使用した場合、ファブリック全体に配信されるのは、スタティック マッピングの iSLB 発信側設定だけです。ダイナミックおよびスタティックに設定された iSCSI 発信側設定は配信されません。

iSLB ターゲット アクセス マッピング

iSLB では、iSCSI 仮想ターゲット アクセスを含むすべてのファブリック配信設定は、iSCSI イニシエータ設定の一部です。アクセスは pWWN またはデバイス エイリアスを使用して付与されます。次のオプション パラメータを 1 つまたは複数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

さらに、自動ゾーン分割を無効にできます。

イニシエータ ターゲットに IQN を設定する場合は、その名前を使用してターゲットを特定する必要があります。そうしないと、イニシエータ ターゲットに一意の IQN が生成されます。

永続的な nWWN/pWWN マッピングの構成

自動的に割り当てられた nWWN/pWWN マッピングを永続的に維持するには、次のステップを実行します。

手順

ステップ 1 名前で指定された iSLB イニシエータに自動的に割り当てられた pWWN および nWWN を保存します。

```
switch# config terminal
switch(config)# islb save-initiator name iqn.1987-02.com.cisco.initiator
```

ステップ 2 IPv4 アドレスで指定された iSLB イニシエータに自動的に割り当てられた pWWN および nWWN を保存します。

```
switch(config)# islb save-initiator 10.10.100.11
```

ステップ 3 IPv6 ユニキャスト アドレスで指定された iSCSI イニシエータに自動的に割り当てられた pWWN および nWWN を保存します。

```
switch(config)# iscsi save-initiator ip-address 2001:0DB8:800:200C::417A
```

ステップ 4 すべての iSLB イニシエータに自動的に割り当てられた nWWN と pWWN を保存します。

```
switch(config)# islb save-initiator
switch(config)# exit
```

ステップ 5 システム リブート後も nWWN/pWWN マッピング構成を保存します。

```
switch# copy running-config startup-config
```

iSCSI 仮想ターゲットへの iSLB イニシエータ アクセスの構成

iSCSI 仮想ターゲットへの iSLB イニシエータ アクセスを構成するには、次のステップを実行します。

手順

ステップ 1 名前を使用してイニシエータを構成し、iSLB イニシエータ コンフィギュレーション サブモードを開始します。

```
switch# config terminal
switch(config)# islb initiator ip-address 10.1.1.3
switch(config-iscsi-islb-init)#
```

ステップ 2 自動ゾーン分割が有効な状態（デフォルト）で pWWN を使用してターゲットへのアクセスを iSLB イニシエータに付与します。

```
switch(config-iscsi-islb-init)# target pwwn 26:00:01:02:03:04:05:06
```

ステップ 3 自動ゾーン分割が無効な状態で pWWN を使用してターゲットへのアクセスを iSLB イニシエータに付与します。

```
switch(config-iscsi-islb-init)# target pwwn 26:00:01:02:03:04:05:06 no-zone
```

ステップ 4 自動ゾーン分割が有効な状態（デフォルト）でデバイス エイリアスを使用してターゲットへのアクセスを iSLB イニシエータに付与します。

```
switch(config-iscsi-islb-init)# target device-alias SampleAlias
```

ステップ 5 デバイス エイリアスとオプションの LUN マッピングを使用して、ターゲットへのアクセスを iSLB イニシエータに許可します。

```
switch(config-iscsi-islb-init)# target device-alias SampleAlias fc-lun 0x1234 iscsi-lun 0x2345
```

ステップ 6 デバイス エイリアスとオプションの IQN を使用して、iSLB イニシエータがターゲットにアクセスすることを許可します。

```
switch(config-iscsi-islb-init)# target device-alias SampleAlias iqn-name
iqn.1987-01.com.cisco.initiator
```

ステップ 7 デバイスエイリアスとオプションのセカンダリデバイスエイリアスを使用して、iSLBイニシエータにターゲットへのアクセスを許可します。

```
switch(config-iscsi-islb-init)# target device-alias SampleAlias sec-device-alias SecondaryAlias
```

ステップ 8 デバイス エイリアスとオプションのセカンダリ pWWN を使用して、iSLB イニシエータ ターゲットへのアクセスを許可します。

```
switch(config-iscsi-islb-init)# target device-alias SampleAlias sec-pwwn 26:01:02:03:04:05:06:07
```

ステップ 9 ターゲット アクセスを削除します。

```
switch(config-iscsi-init)# no target pwwn 26:00:01:02:03:04:05:06
```

iSLB ターゲットの構成の確認

iSLB ターゲット構成を確認するには、**show islb initiator configured** コマンドを使用します。

```
switch# show islb initiator configured
iSCSI Node name is 10.1.1.3
Number of Initiator Targets: 1
Initiator Target: iqn.1987-05.com.cisco:05.ips-hac4
Port WWN 50:06:04:82:ca:e1:26:8d
Zoning Enabled
No. of LU mapping: 3
iSCSI LUN: 0x0001, FC LUN: 0x0001
iSCSI LUN: 0x0002, FC LUN: 0x0002
iSCSI LUN: 0x0003, FC LUN: 0x0003
```

iSLB イニシエータへの VSAN メンバーシップの割り当て

特定の VSAN に属すように、個々の iSLB ホストを設定できます（ファイバチャネルの DPVM 機能と同様）。指定した VSAN によって、iSCSI インターフェイスの VSAN メンバーシップが上書きされます。

詳細については、『Cisco MDS 9000 ファミリ NX-OS Fabric Manager ファブリック構成ガイド』を参照してください。

iSLB 発信側の VSAN メンバーシップを割り当てるには、次の手順を実行します。

始める前に

iSLB 発信側 VSAN の指定方法は、iSCSI 発信側の場合と同じです。「iSCSI の VSAN メンバーシップ」を参照してください。

その他の VSAN（デフォルトの VSAN である VSAN 1 以外）内に iSLB 発信側を設定すると（VSAN 2 など）、発信側は自動的に VSAN 1 から削除されます。VSAN 1 にもこの発信側を存続させる場合は、この発信側を VSAN 1 内に明示的に設定する必要があります。

手順

ステップ 1 IPv4 アドレスを使用して iSLB イニシエータを構成し、iSLB イニシエータ構成サブモードを開始します

```
switch# config terminal
switch(config)# islb initiator ip-address 10.1.1.3
switch(config-islb-init)#
```

ステップ 2 指定された VSAN に iSLB 発信側ノードを割り当てます。1 つ以上の VLAN にこのホストを割り当てることができます。

```
switch(config-islb-init)# vsan 3
```

ステップ 3 指定された VSAN から iSLB イニシエータを削除します。

```
switch(config-islb-init)# no vsan 3
```

ロード バランシングのメトリック設定

重み付け ロード バランシングのために、各発信側にロード メトリックを 割り当てることができます。算出される負荷は、所定の iSCSI インターフェイス上の発信側の数に基づいて決まります。この機能を使用すると、発信側間で帯域幅要件が異なる状況に対応できます。たとえば、データベース サーバーには Web サーバーよりも大きいロード メトリックを割り当てることができます。重み付けロードバランシングは、発信側間でリンク速度の異なる状況にも対応できます。

また、デバイス エイリアスまたは pWWN を使用することによって、発信側ターゲットを設定することもできます。発信側ターゲットに IQN を設定する場合は、その名前を使用して発信側ターゲットを特定する必要があります。そうしないと、イニシエータ ターゲットに一意の IQN が生成されます。

ロード バランシングの詳細については、「VRRP を使用したロード バランシング」を参照してください。

ロード バランシングの重みを設定するには、次の手順を実行します。

手順

ステップ 1 イニシエータ ノードの名前を使用して iSLB イニシエータを構成し、iSLB イニシエータ構成サブモードを開始します。

```
switch# config terminal
switch(config)# islb initiator name iqn.1987-02.com.cisco.initiator
switch(config-iscsi-init)#
```

ステップ 2 この iSLB イニシエータの重みメトリックとして 100 を割り当てます。

```
switch(config-iscsi-init)# metric 100
```

ステップ 3 デフォルト値（1000）に戻します。

```
switch(config-iscsi-init)# no metric 100
```

iSLB イニシエータ構成の確認

iSLB イニシエータ構成を確認するには、**show islb initiator configured** コマンドを使用します。

```
switch# show islb initiator configured
iSCSI Node name is 10.1.1.2
Member of vsans: 10
Node WWN is 23:02:00:0c:85:90:3e:82
Load Balance Metric: 100
Number of Initiator Targets: 1
Initiator Target: test-targt
Port WWN 01:01:01:01:02:02:02:02
Primary PWWN VSAN 1
Zoning support is enabled
Trespass support is disabled
Revert to primary support is disabled
```

iSLB イニシエータ ターゲットの構成

デバイス エイリアスまたは pWWN を使用することによって、発信側ターゲットを設定できます。次のオプション パラメータを 1 つまたは複数指定することもできます（任意）。

- 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

さらに、auto-zoning を無効にできます。発信側ターゲットに IQN を設定する場合は、その名前を使用して発信側ターゲットを特定する必要があります。そうしないと、発信側ターゲットに一意の IQN が生成されます。

iSLB イニシエータ ターゲットを構成するには、次のステップを実行します。

始める前に

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。

手順

ステップ 1 IPv4 アドレスを使用して iSLB イニシエータを構成し、iSLB イニシエータ構成サブモードを開始します

```
switch# config terminal
switch(config)# islb initiator ip-address 10.1.1.3
switch(config-islb-init)#
```

ステップ 2 自動ゾーニングが有効になった状態（デフォルト）で pWWN を使用して、iSLB イニシエータターゲットを構成します。

```
switch(config-iscsi-islb-init)# target pwwn 26:00:01:02:03:04:05:06
```

ステップ 3 自動ゾーニングが無効になっている pWWN を使用して、iSLB イニシエータターゲットを構成します。

```
switch(config-iscsi-islb-init)# target pwwn 26:00:01:02:03:04:05:06 no-zone
```

ステップ 4 自動ゾーニングが有効になった状態（デフォルト）でデバイスエイリアスを使用して、iSLBイニシエータ ターゲットを構成します。

```
switch(config-iscsi-islb-init)# target device-alias SampleAlias
```

ステップ 5 デバイス エイリアスとオプションの LUN マッピングを使用して iSLB イニシエータ ターゲットを構成します。CLI は、**0x** プレフィックスが含まれているかどうかに関係なく、LUN ID の値を 16 進値として解釈します。

```
switch(config-iscsi-islb-init)# target device-alias SampleAlias fc-lun 0x1234 iscsi-lun 0x2345
```

ステップ 6 デバイス エイリアスとオプションの IQN を使用して iSLB イニシエータ ターゲットを構成します。

```
switch(config-iscsi-islb-init)# target device-alias SampleAlias iqn-name
iqn.1987-01.com.cisco.initiator
```

ステップ 7 デバイス エイリアスとオプションのセカンダリ デバイス エイリアスを使用して、iSLB イニシエータ ターゲットを構成します。

```
switch(config-iscsi-islb-init)# target device-alias SampleAlias sec-device-alias SecondaryAlias
```

ステップ 8 デバイス エイリアスとオプションのセカンダリ pWWN を使用して、iSLB イニシエータ ターゲットを構成します。

```
switch(config-iscsi-islb-init)# target device-alias SampleAlias sec-pwwn 26:01:02:03:04:05:06:07
```

ステップ 9 デバイス エイリアスと VSAN 識別子を使用して iSLB イニシエータ ターゲットを構成します。

```
switch(config-iscsi-islb-init)# target device-alias SampleAlias vsan 10
```

ステップ 10 iSLB イニシエータ ターゲットを削除します。

```
switch(config-iscsi-init)# no target pwwn 26:00:01:02:03:04:05:06
```

iSLB発信側および発信側ターゲット用のゾーンの設定およびアクティブ化

iSLB 発信側および発信側ターゲットを追加するゾーンの名前を設定できます。ゾーン名を指定しなかった場合、IPS マネージャによってダイナミックに作成されます。iSLB ゾーン セットに関する次の考慮事項があります。

- 発信側ターゲットが設定された発信側の自動ゾーン分割は、デフォルトでイネーブルになります。
- VSAN で自動ゾーンを作成するには、その VSAN でゾーン セットをアクティブにする必要があります。
- 別のゾーン セットがアクティブ化の途中にある場合、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、iSLB ゾーン セットのアクティブ化に失敗する可能性があります。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ために、ゾーン分割関連の処理（標準ゾーン、IVR ゾーン、または iSLB ゾーン）は、一度に 1 つだけ実行してください。
- 自動ゾーンが作成されるのは、ゾーン セットがアクティブで、そのゾーン セットに少なくとも 1 つ変更があった場合です。自動ゾーンだけが変化した場合、アクティブ化は無効です。

iSLB イニシエータのオプションの自動ゾーン名を構成し、ゾーン セットをアクティブ化するには、次のステップを実行します。

始める前に

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

手順

ステップ 1 IPv4 アドレスを使用して iSLB イニシエータを構成し、iSLB イニシエータ構成サブモードを開始します

```
switch# config terminal
switch(config)# islb initiator ip-address 10.1.1.3
switch(config-islb-init)#
```

ステップ 2 （オプション）イニシエータとイニシエータターゲットを追加するゾーン名を指定します。

```
switch(config-islb-init)# zonename IslbZone
```

ステップ 3 （デフォルト）イニシエータとイニシエータ ターゲットをゾーンから削除し、動的に作成されたゾーンに追加します。

```
switch(config-islb-init)# no zonename IslbZone
```

ステップ 4 コンフィギュレーション モードに戻ります。

```
switch(config-islb-init)# exit
```

ステップ 5 ゾーン分割が有効になっている iSLB イニシエータおよびイニシエータ ターゲットのゾーン分割をアクティブにし、ゾーン名が構成されていない場合は自動ゾーンを作成します。

CFS が有効な場合は、このステップは不要です。CFS は、設定変更が確定されると、自動的にゾーンをアクティブにします。

```
switch(config)# islb zoneset activate
```

iSLB ゾーン分割設定の確認

次に、動的に生成されたゾーン名を使用した場合の **show zoneset active** コマンドの出力例を示します。

```
switch# show zoneset active
zoneset name zoneset-1 vsan 1
zone name ips_zone_5d9603bcff68008a6fc5862a6670ca09 vsan 1
* fcid 0x010009 [ip-address 10.1.1.3]
pwwn 22:00:00:04:cf:75:28:4d
pwwn 22:00:00:04:cf:75:ed:53
pwwn 22:00:00:04:cf:75:21:d5
pwwn 22:00:00:04:cf:75:ee:59
.
.
.
```

次に、設定されたゾーン名 IslbZone を使用した場合の **show zoneset active** コマンドの出力例を示します。

```
switch# show zoneset active
zoneset name zoneset-1 vsan 1
zone name ips_zone_IslbZone vsan 1
ip-address 10.1.1.3
pwwn 22:00:00:04:cf:75:28:4d
pwwn 22:00:00:04:cf:75:ed:53
pwwn 22:00:00:04:cf:75:21:d5
pwwn 22:00:00:04:cf:75:ee:59
.
.
.
```

iSLB セッション認証の設定

IPS ポートを搭載したファイバ チャネル モジュールおよび 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 iSLB 認証メカニズムをサポートします。デフォルトでは、IPS ポートを搭載したファイバ チャネル モジュールおよび MPS-14/2 モジュールは、iSCSI 発信側に関する CHAP または None 認証を許可します。認証を必ず使用する場合は、CHAP 認証だけが許可されるようにスイッチを設定する必要があります。

CHAP ユーザー名または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および許可されている方法を使用できます（詳細については、『Cisco Fabric Manager セキュリティ構成ガイド』『Cisco MDS 9000 Family NX-OS セキュリティ構成ガイド』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 セッション認証の指定方法は、iSCSI の場合と同じです。「iSCSI セッション 認証」を参照してください。

iSLB イニシエータ認証の制限

iSLB イニシエータはデフォルトで、IPS ポートを搭載したファイバ チャネルまたは MPS-14/2 モジュールに対する自身の認証用に、RADIUS またはローカル AAA データベースの任意のユーザー名を使用できます（CHAP ユーザー名は iSLB 発信側名と無関係です）。IPS ポートを搭載したファイバ チャネル 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た CHAP チャレンジに有効な応答があった場合にかぎり、発信側にログインを許可します。ただし、CHAP ユーザー名およびパスワードが信用できないものであると、問題が生じる可能性があります。

イニシエータが CHAP 認証に特定のユーザー名を使用するように制限するには、次のステップを実行します。

手順

ステップ 1 イニシエータ ノードの IQN を使用して iSLB イニシエータを構成し、iSLB イニシエータ構成サブモードを開始します。

```
switch# config terminal
switch(config)# islb initiator name iqn.1987-02.com.cisco.init
switch(config-islb-init)#
```

ステップ 2 イニシエータ `iqn.1987-02.com.cisco.init` を、CHAP ユーザー名として `user1` を使用する認証だけに制限します。

（注）
ローカル AAA データベースまたは RADIUS サーバーで user1 を iSCSI ユーザーとして必ず定義してください。

```
switch(config-islb-init)#
switch(config-islb-init)# username user1
```

相互 CHAP 認証

iSLB イニシエータに関する IPS ポートを搭載したファイバ チャネル モジュールおよび MPS-14/2 モジュールの認証に加え、IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールは、iSCSI ログイン フェーズで Cisco MDS スイッチのイニシエータ ターゲットを認証する、iSLB イニシエータのメカニズムもサポートします。この認証には、ユーザー側で iSLB 発信側に提示するスイッチ用のユーザー名およびパスワードを設定する必要があります。

提供されたパスワードを使用して、発信側がIPSポートに送信するCHAPチャレンジへのCHAP応答が計算されます。

スイッチが発信側に対する自身の認証に使用する発信側単位のユーザー名およびパスワードを設定するには、次の手順を実行します。

手順

ステップ 1 イニシエータ ノードの名前を使用して iSLB イニシエータを構成し、iSLB イニシエータ構成サブモードを開始します。

```
switch# config terminal
switch(config)# islb initiator name iqn.1987-02.com.cisco.initiator
switch(config-islb-init)#
```

ステップ 2 クリア テキスト（デフォルト）で指定されたパスワード（dcba12LKJ）とともに、スイッチのユーザ アカウント（testuser）を構成します。パスワードは 128 文字に制限されています。

```
switch(config-islb-init)# mutual-chap username testuser password dcba12LKJ
```

ステップ 3 7 (!@*asdsfsdfjh!@df) で指定された暗号化パスワードとともに、スイッチのユーザーアカウント（testuser）を構成します。

```
switch(config-islb-init)# mutual-chap username testuser password 7!@*asdsfsdfjh!@df
```

ステップ 4 スイッチ認証構成を削除します。

```
switch(config-iscsi-init)# no mutual-chap username testuser
```

iSLB ゾーン認証設定の確認

グローバル構成を表示するには、**show running-config** および **show iscsi global** コマンドを使用します。イニシエータ固有の設定を表示するには、 **show running-config** コマンドと **show islb initiator configured** コマンドを使用します。

iSLB ユーザー名と相互 CHAP 構成を確認するには、**show islb initiator configured** コマンドを使用します。

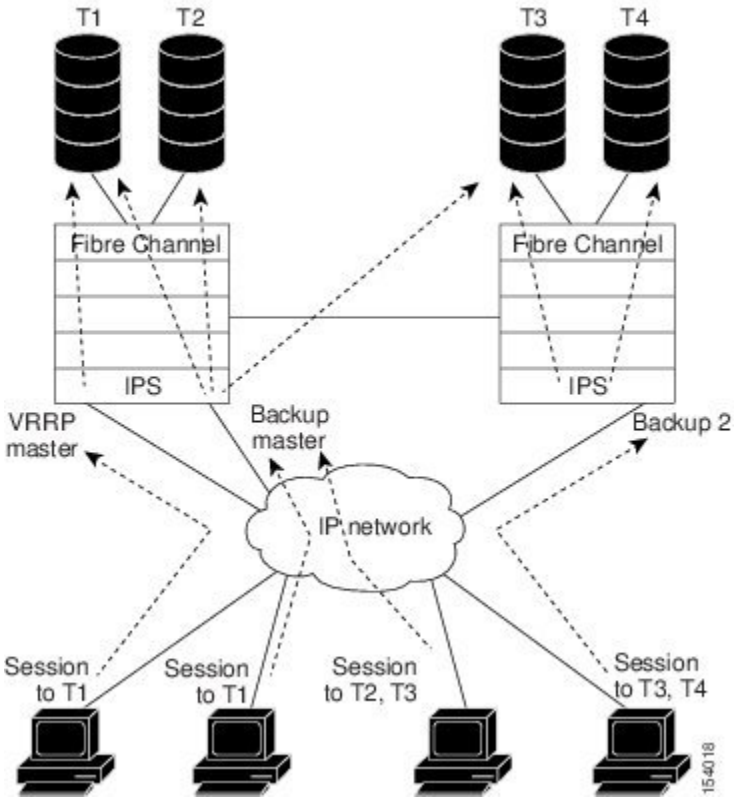
```
switch# show islb initiator configured
iSCSI Node name is 10.1.1.3
Member of vsans: 3
User Name for login authentication: user1
User Name for Mutual CHAP: testuser
Load Balance Metric: 1000 Number of Initiator Targets: 1
Number of Initiator Targets: 1
Initiator Target: iqn.1987-05.com.cisco:05.ips-hac4
Port WWN 50:06:04:82:ca:e1:26:8d
Zoning Enabled
No. of LU mapping: 3
iSCSI LUN: 0x0001, FC LUN: 0x0001
iSCSI LUN: 0x0002, FC LUN: 0x0002
iSCSI LUN: 0x0003, FC LUN: 0x0003
```

VRRP を使用するロード バランシング

iSLB に仮想ルータ冗長プロトコル（VRRP）ロードバランシングを設定できます。ホストは、ポータル アドレスとして VRRP アドレスを指定して設定されています。VRRP マスター ポートは発信側から最初の iSCSI セッションを受信すると、そのホスト用のバックアップ ポートを割り当てます。マスター ポートの障害時に回復が必要な場合は、CFS によってこの情報がすべてのスイッチで同期化されます。発信側には、一時リダイレクト iSCSI ログイン応答が与えられます。ホストはその後、対応する物理 IP アドレスでバックアップ ポートにログインします。VRRP グループ内で、ロード バランシングがイネーブルに設定されているすべての iSCSI インターフェイスに、同じインターフェイス VSAN、認証、プロキシ イニシエータ モード、および転送モードを設定する必要があります。

iSLB に仮想ルータ冗長プロトコル（VRRP）ロードバランシングを設定できます。次の図に、iSLB を使用したロード バランシングの例を示します。

図 *19 : iSLB* 発信側のロード バランシング例



ホストは、ポータルアドレスとしてVRRPアドレスを指定して設定されています。VRRPマスターポートは発信側から最初のiSCSIセッションを受信すると、そのホスト用のバックアップポートを割り当てます。マスター ポートの障害時に回復が必要な場合は、CFS によってこの情報がすべてのスイッチで同期化されます。発信側には、一時リダイレクト iSCSI ログイン応答が与えられます。ホストはその後、対応する物理 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 ポートが停止した場合、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 によって、バックアップ ポートが停止したことを認識し、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） IPS ポートを搭載したファイバ チャネル モジュールとイーサネット スイッチ間にイーサネット ポート チャネルが構成されている場合は、VRRP によるロード バランシングを正常に動作させるために、イーサネット スイッチ上のロード バランシング ポリシーをポート番号ではなく、送信元/宛先 IP アドレスだけに基づいたものにする必要があります。

（注） 発信側をマスター 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。

iSLB VRRP ロード バランシングは、セッション数ではなく iSLB 発信側の数に基づいて実行されます。ターゲットの多い iSLB 発信側は（セッション数が結果的に多くなるので）、他の iSLB 発信側より大きいロード 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 発信側のロード メトリックをデフォルト値の 1000 から 3000 に引き上げることができます。

iSLB 対応として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。これは、リダイレクトされたセッションが VRRP IP アドレスまたはグループに関する情報を伝達しないからです。この制限によって、スレーブ バックアップ ポートは所属先の VRRP グループを一意のものとして識別できます。

iSCSI インターフェイス パラメータの変更およびロード バランシングへの影響

VRRP グループ内で、ロード バランシングがイネーブルに設定されているすべての iSCSI インターフェイスに、同じインターフェイス VSAN、認証、プロキシ イニシエータ モード、および転送モードを設定する必要があります。VRRP グループ内の iSCSI インターフェイスで、これらのパラメータのいずれかを変更しなければならない場合は、一度に 1 つずつ、インターフェイスを処理する必要があります。VRRP グループの一部のインターフェイスでパラメータが変更され、他のインターフェイスでは変更されていない移行期の間、マスター ポートは新しい発信側をリダイレクトする代わりにローカルで処理します。

VRRP グループに含まれる iSCSI インターフェイスの VSAN、プロキシ発信側、認証、および転送モードを変更すると、セッションが繰り返し停止することがあります。

ギガビット イーサネット インターフェイスを選択する VRRP ロード バランシング アルゴリズム

発信側から iSCSI セッション要求を受信した VRRP マスターは、VRRP グループに含まれるインターフェイスの 1 つに対して既存のマッピングがあるかどうかを最初に調べます。該当するマッピングがある場合、VRRP マスターは発信側をそのインターフェイスにリダイレクトします。該当するマッピングがない場合、VRRP マスターは負荷が最小のインターフェイスを選択

し、イニシエータの iSLB メトリック（重み）を使用して、選択したインターフェイスの負荷を更新します。

（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、セッションごとにマスターインターフェイスがリダイレクト作業を実行するためです。新しいイニシエータは、他のすべてのインターフェイスで次の条件が満たされている場合のみ、マスターインターフェイスに割り当てられます。 VRRP backup interface load > [2 * VRRP master interface load + 1]

この次の例は、次の構成に基づいています。

- GigabitEthernet2/1.441 は Switch1 の VRRP マスター インターフェイスです。
- GigabitEthernet2/2.441 は Switch1 の VRRP バックアップ インターフェイスです。
- GigabitEthernet1/1.441 は Switch2 の VRRP バックアップ インターフェイスです。
- GigabitEthernet1/2.441 は Switch2 の VRRP バックアップ インターフェイスです。

デフォルト メトリックを使用した負荷分散

次の出力例は、デフォルトのロードメトリック値を使用した3台のイニシエータへの初期負荷分散を示しています。

```
switch# show islb vrrp summary
.
.
.
--------------------------------------------------------------------------------
VR Id VRRP IP Switch WWN Ifindex Load
--------------------------------------------------------------------------------
M 1 10.10.122.115 20:00:00:0b:5f:3c:01:80 GigabitEthernet2/1.441 0
1 10.10.122.115 20:00:00:0b:5f:3c:01:80 GigabitEthernet2/2.441 1000
1 10.10.122.115 20:00:00:0c:ce:5c:5b:c0 GigabitEthernet1/1.441 1000
1 10.10.122.115 20:00:00:0c:ce:5c:5b:c0 GigabitEthernet1/2.441 1000
-- Initiator To Interface Assignment --
--------------------------------------------------------------------------------
Initiator VR Id VRRP IP Switch WWN Ifindex
--------------------------------------------------------------------------------
iqn.cisco.test-linux.init0 1 10.10.122.115 20:00:00:0b:5f:3c:01:80 GigabitEthernet2/2.441
iqn.cisco.test-linux.init1 1 10.10.122.115 20:00:00:0c:ce:5c:5b:c0 GigabitEthernet1/1.441
iqn.cisco.test-linux.init 1 10.10.122.115 20:00:00:0c:ce:5c:5b:c0 GigabitEthernet1/2.441
```

次の出力例は、4 台の発信側の負荷分散を示しています。マスター インターフェイスのインターフェイス ロード メトリック値が 0 から 1000 に変更されています。

```
switch# show islb vrrp summary
.
.
.
--------------------------------------------------------------------------------
VVR Id VRRP IP Switch WWN Ifindex Load
--------------------------------------------------------------------------------
M 1 10.10.122.115 20:00:00:0b:5f:3c:01:80 GigabitEthernet2/1.441 1000
1 10.10.122.115 20:00:00:0b:5f:3c:01:80 GigabitEthernet2/2.441 1000
1 10.10.122.115 20:00:00:0c:ce:5c:5b:c0 GigabitEthernet1/1.441 1000
```

```
1 10.10.122.115 20:00:00:0c:ce:5c:5b:c0 GigabitEthernet1/2.441 1000
-- Initiator To Interface Assignment --
--------------------------------------------------------------------------------
Initiator VR Id VRRP IP Switch WWN Ifindex
--------------------------------------------------------------------------------
iqn.cisco.test-linux.init0 1 10.10.122.115 20:00:00:0b:5f:3c:01:80 GigabitEthernet2/2.441
iqn.cisco.test-linux.init1 1 10.10.122.115 20:00:00:0c:ce:5c:5b:c0 GigabitEthernet1/1.441
iqn.cisco.test-linux.init2 1 10.10.122.115 20:00:00:0c:ce:5c:5b:c0 GigabitEthernet1/2.441
iqn.cisco.test-linux.init3 1 10.10.122.115 20:00:00:0b:5f:3c:01:80 GigabitEthernet2/1.441
```

次の出力例は、9台のイニシエータの負荷分散を示しています。バックアップ インターフェイスのインターフェイス ロード メトリック値が変更されています。

```
switch# show islb vrrp summary
.
.
.
--------------------------------------------------------------------------------
VVR Id VRRP IP Switch WWN Ifindex Load
--------------------------------------------------------------------------------
M 1 10.10.122.115 20:00:00:0b:5f:3c:01:80 GigabitEthernet2/1.441 1000
1 10.10.122.115 20:00:00:0b:5f:3c:01:80 GigabitEthernet2/2.441 3000
1 10.10.122.115 20:00:00:0c:ce:5c:5b:c0 GigabitEthernet1/1.441 3000
1 10.10.122.115 20:00:00:0c:ce:5c:5b:c0 GigabitEthernet1/2.441 2000
-- Initiator To Interface Assignment --
--------------------------------------------------------------------------------
Initiator VR Id VRRP IP Switch WWN Ifindex
--------------------------------------------------------------------------------
iqn.cisco.test-linux.init0 1 10.10.122.115 20:00:00:0b:5f:3c:01:80 GigabitEthernet2/2.441
iqn.cisco.test-linux.init1 1 10.10.122.115 20:00:00:0c:ce:5c:5b:c0 GigabitEthernet1/1.441
iqn.cisco.test-linux.init2 1 10.10.122.115 20:00:00:0c:ce:5c:5b:c0 GigabitEthernet1/2.441
iqn.cisco.test-linux.init3 1 10.10.122.115 20:00:00:0b:5f:3c:01:80 GigabitEthernet2/1.441
iqn.cisco.test-linux.init4 1 10.10.122.115 20:00:00:0b:5f:3c:01:80 GigabitEthernet2/2.441
iqn.cisco.test-linux.init5 1 10.10.122.115 20:00:00:0c:ce:5c:5b:c0 GigabitEthernet1/1.441
iqn.cisco.test-linux.init6 1 10.10.122.115 20:00:00:0c:ce:5c:5b:c0 GigabitEthernet1/2.441
iqn.cisco.test-linux.init7 1 10.10.122.115 20:00:00:0b:5f:3c:01:80 GigabitEthernet2/2.441
iqn.cisco.test-linux.init8 1 10.10.122.115 20:00:00:0c:ce:5c:5b:c0 GigabitEthernet1/1.441
```

1 台のイニシエータでメトリックが 3000 に設定された負荷分散

次の出力例は、1台のイニシエータでロードメトリックが3000に設定され、残りのイニシエータでデフォルトのメトリック値が設定されている3台のイニシエータの初期負荷分散を示します。

```
switch# show islb vrrp summary
.
.
.
--------------------------------------------------------------------------------
VVR Id VRRP IP Switch WWN Ifindex Load
--------------------------------------------------------------------------------
M 1 10.10.122.115 20:00:00:0b:5f:3c:01:80 GigabitEthernet2/1.441 0
1 10.10.122.115 20:00:00:0b:5f:3c:01:80 GigabitEthernet2/2.441 1000
1 10.10.122.115 20:00:00:0c:ce:5c:5b:c0 GigabitEthernet1/1.441 3000
1 10.10.122.115 20:00:00:0c:ce:5c:5b:c0 GigabitEthernet1/2.441 1000
-- Initiator To Interface Assignment --
--------------------------------------------------------------------------------
Initiator VR Id VRRP IP Switch WWN Ifindex
--------------------------------------------------------------------------------
iqn.cisco.test-linux.init0 1 10.10.122.115 20:00:00:0c:ce:5c:5b:c0 GigabitEthernet1/1.441
iqn.cisco.test-linux.init1 1 10.10.122.115 20:00:00:0b:5f:3c:01:80 GigabitEthernet2/2.441
iqn.cisco.test-linux.init2 1 10.10.122.115 20:00:00:0c:ce:5c:5b:c0 GigabitEthernet1/2.441
```

次の出力例は、4 台の発信側の負荷分散を示しています。マスター インターフェイスのインターフェイス ロード メトリック値が 0 から 1000 に変更されています。

```
switch# show islb vrrp summary
.
.
.
--------------------------------------------------------------------------------
VVR Id VRRP IP Switch WWN Ifindex Load
--------------------------------------------------------------------------------
M 1 10.10.122.115 20:00:00:0b:5f:3c:01:80 GigabitEthernet2/1.441 1000
1 10.10.122.115 20:00:00:0b:5f:3c:01:80 GigabitEthernet2/2.441 3000
1 10.10.122.115 20:00:00:0c:ce:5c:5b:c0 GigabitEthernet1/1.441 1000
1 10.10.122.115 20:00:00:0c:ce:5c:5b:c0 GigabitEthernet1/2.441 1000
-- Initiator To Interface Assignment --
--------------------------------------------------------------------------------
Initiator VR Id VRRP IP Switch WWN Ifindex
--------------------------------------------------------------------------------
iqn.cisco.test-linux.init0 1 10.10.122.115 20:00:00:0b:5f:3c:01:80 GigabitEthernet2/2.441
iqn.cisco.test-linux.init1 1 10.10.122.115 20:00:00:0c:ce:5c:5b:c0 GigabitEthernet1/2.441
iqn.cisco.test-linux.init2 1 10.10.122.115 20:00:00:0c:ce:5c:5b:c0 GigabitEthernet1/1.441
iqn.cisco.test-linux.init3 1 10.10.122.115 20:00:00:0b:5f:3c:01:80 GigabitEthernet2/1.441
```

次の出力例は、9台のイニシエータの負荷分散を示しています。バックアップインターフェイスのインターフェイス ロード メトリック値が変更されています。

```
switch# show islb vrrp summary
.
.
.
--------------------------------------------------------------------------------
VVR Id VRRP IP Switch WWN Ifindex Load
--------------------------------------------------------------------------------
M 1 10.10.122.115 20:00:00:0b:5f:3c:01:80 GigabitEthernet2/1.441 2000
1 10.10.122.115 20:00:00:0b:5f:3c:01:80 GigabitEthernet2/2.441 3000
1 10.10.122.115 20:00:00:0c:ce:5c:5b:c0 GigabitEthernet1/1.441 3000
1 10.10.122.115 20:00:00:0c:ce:5c:5b:c0 GigabitEthernet1/2.441 3000
-- Initiator To Interface Assignment --
--------------------------------------------------------------------------------
Initiator VR Id VRRP IP Switch WWN Ifindex
--------------------------------------------------------------------------------
iqn.cisco.test-linux.init0 1 10.10.122.115 20:00:00:0b:5f:3c:01:80 GigabitEthernet2/2.441
iqn.cisco.test-linux.init1 1 10.10.122.115 20:00:00:0c:ce:5c:5b:c0 GigabitEthernet1/1.441
iqn.cisco.test-linux.init2 1 10.10.122.115 20:00:00:0c:ce:5c:5b:c0 GigabitEthernet1/2.441
iqn.cisco.test-linux.init3 1 10.10.122.115 20:00:00:0b:5f:3c:01:80 GigabitEthernet2/1.441
iqn.cisco.test-linux.init4 1 10.10.122.115 20:00:00:0c:ce:5c:5b:c0 GigabitEthernet1/1.441
iqn.cisco.test-linux.init5 1 10.10.122.115 20:00:00:0c:ce:5c:5b:c0 GigabitEthernet1/2.441
iqn.cisco.test-linux.init6 1 10.10.122.115 20:00:00:0c:ce:5c:5b:c0 GigabitEthernet1/1.441
iqn.cisco.test-linux.init7 1 10.10.122.115 20:00:00:0c:ce:5c:5b:c0 GigabitEthernet1/2.441
iqn.cisco.test-linux.init8 1 10.10.122.115 20:00:00:0b:5f:3c:01:80 GigabitEthernet2/1.441
```

VRRP を使用したロード バランシングの構成

iSLB 用の VRRP を設定する前に、IP ネットワークに接続するスイッチのギガビット イーサネットインターフェイス上で、VRRPを設定しておく必要があります。ギガビットイーサネットインターフェイス上で VRRP を構成する方法については、「仮想 ルータの冗長性プロトコル」を参照してください。

ロード バランシング用の VRRP の有効化

iSLB の VRRP を有効または無効にするには、次のステップを実行します。

手順

ステップ 1 IPv4 VR グループ 10 用に iSLB VRRP をイネーブルにします。

```
switch# config terminal
switch(config)# islb vrrp 10 load-balance
```

ステップ 2 IPv4 VR グループ 10 用に iSLB VRRP をディセーブルにします。

```
switch(config)# no islb vrrp 10 load-balance
```

ステップ 3 IPv6 VR グループ 20 用に iSLB VRRP をイネーブルにします。

```
switch(config)# islb vrrp ipv6 20 load-balance
```

ステップ 4 IPv6 VR グループ 20 用に iSLB VRRP をディセーブルにします。

```
switch(config)# no islb vrrp ipv6 20 load-balance
```

iSLB VRRP ロード バランシング構成の確認

IPv4 用の iSLB VRRP ロード バランシング構成を確認するには、**show vrrp vr** コマンドを使用します。

```
switch# show vrrp vr 1
Interface VR IpVersion Pri Time Pre State VR IP addr
---------------------------------------------------------------------------
GigE1/5 1 IPv4 100 1 s master 10.10.10.1
GigE1/6 1 IPv4 100 1 s master 10.10.10.1
```

IPv6 用の iSLB VRRP ロード バランシング構成を確認するには、**show vrrp ipv6 vr** コマンドを使用します。

```
switch# show vrrp ipv6 vr 1
Interface VR IpVersion Pri Time Pre State VR IP addr
---------------------------------------------------------------------
GigE6/2 1 IPv6 100 100cs master 5000:1::100
PortCh 4 1 IPv6 100 100cs master 5000:1::100
```

iSLB VRRP 情報の表示

VRRP ロード バランシング情報を表示するには、**show islb vrrp summary vr** コマンドを使用します。

```
switch# show islb vrrp summary vr 30

-- Groups For Load Balance --
-------------------------------------------------------------------------------------------
VR Id VRRP Address Type Configured Status
-------------------------------------------------------------------------------------------
30 IPv4 Enabled
```

```
-- Interfaces For Load Balance --
------------------------------------------------------------------------------------------
VR Id VRRP IP Switch WWN Ifindex Load
------------------------------------------------------------------------------------------
30 192.168.30.40 20:00:00:0d:ec:02:cb:00 GigabitEthernet3/1 2000
30 192.168.30.40 20:00:00:0d:ec:02:cb:00 GigabitEthernet3/2 2000
30 192.168.30.40 20:00:00:0d:ec:0c:6b:c0 GigabitEthernet4/1 2000
M 30 192.168.30.40 20:00:00:0d:ec:0c:6b:c0 GigabitEthernet4/2 1000
```

CFS を使用した iSLB 構成の配信

iSLB 発信側および MDS スイッチ上の発信側ターゲットに設定を配信できます。この機能を使用すると、1 台の MDS スイッチのコンソールから、ファブリック全体で iSLB の設定を同期化できます。iSCSI 発信側アイドル タイムアウト、グローバル認証、および iSCSI ダイナミック イニシエータ モード パラメータも配信されます。CFS 配信は、デフォルトではディセーブルになっています。

MDS スイッチにおける iSLB 発信側および発信側ターゲットの設定は、Cisco Fabric Services（CFS）を使用して配信できます。この機能を使用すると、1 台の MDS スイッチのコンソールから、ファブリック全体で iSLB の設定を同期化できます。iSCSI 発信側アイドル 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パラメータも配信されます。CFS 配信はデフォルトで無効になっています（詳細については『Cisco Fabric Manager システム管理構成ガイド』『Cisco MDS 9000 ファミリ NX-OS システム管理構成ガイド』を参照してください）。

配信をイネーブルにすると、最初の設定によって暗黙セッションが開始されます。それ以降に入力されたすべてのサーバー設定変更は、一時データベースに保存され、データベースを明示的にコミットしたときに、ファブリック内のすべてのスイッチ（送信元スイッチを含む）に適用されます。

iSLB に対して CFS がイネーブルの場合は、最初の iSLB 設定処理によって CFS セッションが開始され、ファブリック内の iSLB コンフィギュレーションがロックされます。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。その後、スイッチごとにコンフィギュレーションが検証されます。このチェックによって、次の保証が得られます。

- iSLB 発信側に割り当てられた VSAN は、すべてのスイッチ上で設定されている。
- iSLB 発信側に設定されたスタティック WWN は一意であり、すべてのスイッチで使用できる。
- iSLB 発信側ノード名は、すべてのスイッチ上の iSCSI 発信側と衝突しない。

チェック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コミットします。チェックが失敗した場合は、コミット全体が失敗します。

（注） iSLB が全面的にサポートされるのは、CFS がイネーブルの場合だけです。CFS モードを有効にしないで iSLB 自動ゾーン分割を使用すると、ゾーン セットをアクティブにしたときに、トラフィックが中断することがあります。

CFS は非 iSLB 発信側設定を配信しません。また、ファイバ チャネル ターゲット設定をインポートしません。

非 iSLB 仮想ターゲットは引き続き、アドバタイズされたインターフェイス オプションをサポートします。

（注） 保留中の変更はvolatileディレクトリだけで使用でき、スイッチを再起動すると廃棄されます。

CFS を使用した iSLB 構成の配信

この項の内容は、次のとおりです。

iSLB 構成配信の有効化

CFS による iSLB 設定の配信を有効にするには、次のステップを実行します。

手順

ステップ 1 構成モードに入ります。

```
switch# config terminal
```

ステップ 2 iSLB 設定の配信をイネーブルにします。

```
switch(config)# islb distribute
```

ステップ 3 iSLB 設定の配信をディセーブル（デフォルト）にします。

```
switch(config)# no islb distribute
```

ファブリックのロック

既存の設定を変更するときの最初のアクションによって、保留中の設定が作成され、ファブリック内の機能がロックされます。ファブリックをロックすると、次の条件が適用されます。

- 他のユーザーがこの機能の設定に変更を加えることができなくなります。

- アクティブな設定をコピーすると保留中の設定が作成されます。これ以後の変更は保留設定に対して行われ、アクティブな設定（およびファブリック内の他のスイッチ）に変更をコミットするか、または変更を廃棄するまで、保留設定にとどまります。

（注） iSLB CFS セッションがアクティブな場合は、iSCSI の設定変更は認められません。

ファブリックへの変更のコミット

保留中の iSLB 設定変更をアクティブ コンフィギュレーションおよびファブリック内のその他の MDS スイッチに適用するには、その変更をコミットする必要があります。保留中の設定変更が配信され、コミットが正常に完了した時点で、ファブリック全体の MDS スイッチでアクティブ コンフィギュレーションに設定変更が適用されます。さらに、自動ゾーンがアクティブになり、ファブリックのロックが解除されます。

ファブリック内の他の MDS スイッチに iSLB の設定変更をコミットし、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には、次の手順を実行します。

手順

ステップ 1 構成モードに入ります。

```
switch# config terminal
```

ステップ 2 iSLB 構成の配布をコミットし、iSLB 自動ゾーンをアクティブにして、ファブリック ロックをリリースします。

```
switch(config)# islb commit
```

保留中の変更の廃棄

いつでも iSLB コンフィギュレーションに対する保留中の変更を廃棄し、ファブリックのロックを解除できます。このアクションによって、ファブリック内のスイッチのアクティブ コンフィギュレーションが影響を受けることはありません。

保留中の iSLB の構成変更を廃棄し、ファブリックのロックを解除するには、次のステップを実行します。

手順

ステップ 1 構成モードに入ります。

```
switch# config terminal
```

ステップ 2 iSLB 設定の配信をコミットします。

```
switch(config)# islb abort
```

ファブリックのロックのクリア

ユーザーが iSLB の設定作業を実行し、変更をコミットまたは廃棄することによってロックを解除しなかった場合は、管理者がファブリックの任意のスイッチからロックを解除できます。管理者がこのタスクを実行すると、保留中の変更は廃棄され、ファブリック ロックが解除されます。

始める前に

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

手順

ファブリック ロックを解除するには、管理者権限を持つログイン ID を使用して EXEC モードで **clear islb session**コマンドを発行します。

```
switch# clear islb session
```

CFS マージ プロセス

2 つのファブリックでマージする場合、CFS は両方のファブリックから iSLB のコンフィギュレーションをマージしようとします。一方のファブリックの指定スイッチ（上位スイッチ）が自身の iSLB 構成を他方のファブリックの指定スイッチ（下位スイッチ）に送信します。下位スイッチは自身の実行コンフィギュレーションと受信したコンフィギュレーションを比較し、矛盾の有無を調べます。矛盾が見つからなかった場合は、2つのコンフィギュレーションをマージして、両方のファブリックのすべてのスイッチに送信します。その後、スイッチごとにコンフィギュレーションが検証されます。このチェックによって、次の保証が得られます。

- iSLB 発信側に割り当てられた VSAN は、すべてのスイッチ上で設定されている。
- iSLB 発信側に設定されたスタティック WWN は一意であり、すべてのスイッチで使用できる。
- iSLB 発信側ノード名は、すべてのスイッチ上の iSCSI 発信側と衝突しない。

このチェック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、マージされたコンフィギュレーションを実行コンフィギュレーションにコミットするように指示します。チェックに失敗した場合は、マージが失敗します。

show islb merge status コマンドは、失敗の正確な理由を表示します。マージの失敗後に最初に正常終了するコミット要求により、ファブリックはマージ失敗状態から解放されます。

保留中の iSLB 設定変更の表示

保留中の構成変更は **show islb pending** コマンドを使用して表示できます。

```
switch# show islb pending
iscsi initiator idle-timeout 10
islb initiator ip-address 10.1.1.1
static pWWN 23:01:00:0c:85:90:3e:82
static pWWN 23:06:00:0c:85:90:3e:82
username test1
islb initiator ip-address 10.1.1.2
static nWWN 23:02:00:0c:85:90:3e:82
```

保留中の構成と現在の構成の違いは、 **show islb pending-diff** コマンドを使用して表示できます。

```
switch# show islb pending-diff
+iscsi initiator idle-timeout 10
islb initiator ip-address 10.1.1.1
+ static pWWN 23:06:00:0c:85:90:3e:82
+islb initiator ip-address 10.1.1.2
+ static nWWN 23:02:00:0c:85:90:3e:82
```

iSLB CFS ステータスの表示

iSLB CFS ステータスは、 show islb session statuss コマンドを使用して表示する：

iSLB CFS ステータスは、**show islb session status** コマンドを使用して表示できます。

```
switch# show islb status
iSLB Distribute is enabled
iSLB CFS Session exists
```

iSLB CFS 配信セッション ステータスの表示

iSLB CFS 配信セッションのステータスは、**show islb cfs-session status** コマンドを使用して表示できます。

```
switch# show islb cfs-session status
last action : fabric distribute enable
last action result : success
last action failure cause : success
```

iSLB CFS マージ ステータスの表示

iSLB CFS マージ ステータスは、**show islb merge status** コマンドを使用して表示できます。

```
switch# show islb merge status
Merge Status: Success
```

iSLB CFS マージ ステータスの矛盾

マージで矛盾が生じる場合があります。マージで次の矛盾が生じた場合は、ユーザーの介入が必要です。

- iSCSI グローバル認証または iSCSI 発信側アイドル タイムアウトのパラメータが、2 つのファブリックで同じ設定になっていない。
- 同じ iSLB 発信側の設定が 2 つのファブリックでそれぞれ異なる。
- 一方のファブリックの iSLB 発信側に、他方のファブリックの iSCSI 発信側と同じ名前が与えられている。
- 2 つのファブリックで重複する pWWN/nWWN の設定が見つかった。たとえば、一方のファブリックの iSLB 発信側に設定された pWWN/nWWN が、他方のファブリックの iSCSI 発信側または別の iSLB 発信側に設定されているなどです。
- 一方のファブリックの iSLB 発信側に設定された VSAN が他方のファブリックに存在しない。

マージの矛盾の詳細については、Syslog を調べてください。同じ iSLB 発信側に、衝突しない別の発信側ターゲット セットがある場合は、ユーザーの介入は不要です。マージされたコンフィギュレーションは、すべての発信側ターゲットの和集合です。

iSCSI ハイ アベイラビリティ

iSCSI 設定で使用できるハイ アベイラビリティ機能は、次のとおりです。

透過型ターゲット フェールオーバー

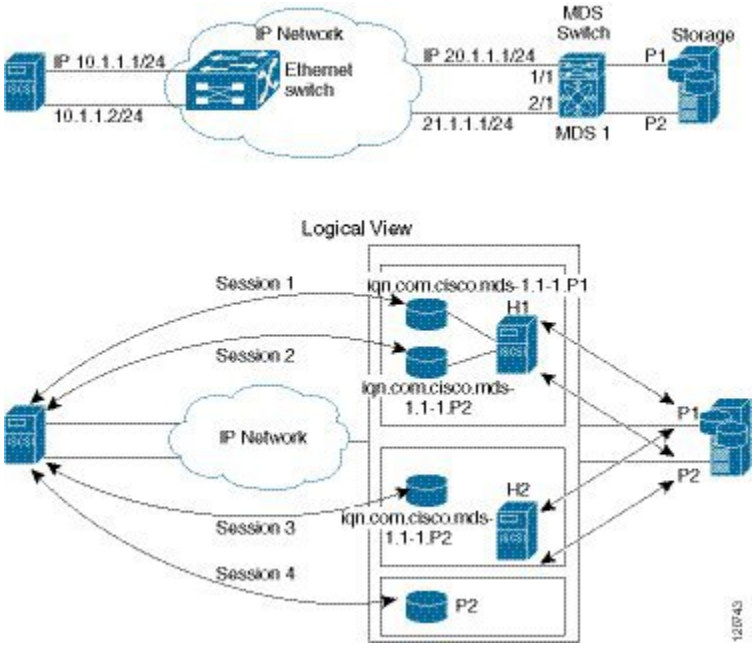
iSCSI 設定で使用できるハイ アベイラビリティ機能は、次のとおりです。

- マルチパス ソフトウェアが稼働しているホストでの iSCSI ハイ アベイラビリティ：このトポロジでは、あらゆるコンポーネントの障害から回復できます。ホストのマルチパス ソフトウェアがストレージにアクセスする別のパスで、ロードバランシングまたはフェールオーバーを処理します。
- マルチパス ソフトウェアのないホストでの iSCSI ハイ アベイラビリティ：マルチパス ソフトウェアのないホストは、同じストレージへの複数のパスについて、情報が得られません。

マルチパス ソフトウェアが稼働しているホストでの iSCSI ハイ アベイラビリティ

以下の図に、マルチパス ソフトウェアが稼働しているホストの iSCSI HA ソリューションに対応する物理および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 NIC から 2 つの IPS ポートへの iSCSI セッションが 2 つあります。

図 *20 :* マルチパス ソフトウェアが稼働しているホスト



各 IPS ポートはストレージの 2 つの同じファイバ チャネル ターゲット ポートを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、iSCSI ターゲット名は異なります。したがって、2 つの IPS ポートで合計 4 つの iSCSI ターゲット デバイスをエクスポートします。この 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。各 IPS ポートは 2 つの iSCSI ターゲットをエクスポートするので、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 で障害が発生した場合、セッション 1 および 2 は失敗しますが、セッション 3 および 4 がまだ残っています。

IPS ポート 1 で障害が発生した場合、iSCSI ホストは IPS ポートに接続できないので、セッション 1 および 2 が失敗します。しかし、セッション 3 および 4 はそのまま使用できます。

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）。しかし、セッション 2 および 4 はそのまま使用できます。

このトポロジでは、あらゆるコンポーネントの障害から回復できます。ホストのマルチパス ソフトウェアがストレージにアクセスする別のパスで、ロードバランシングまたはフェールオーバーを処理します。

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

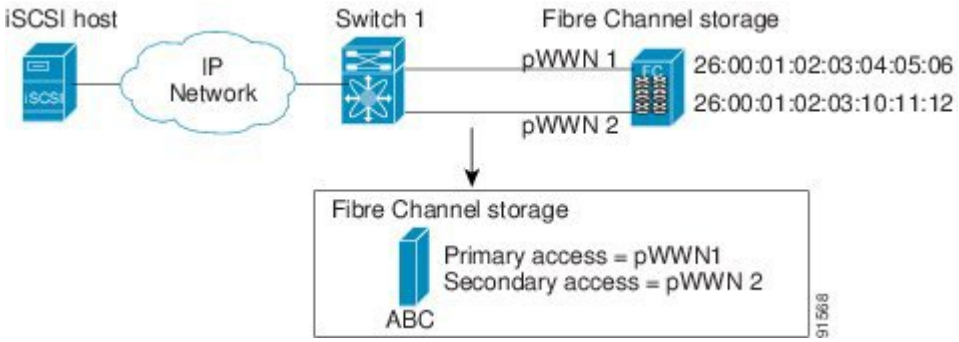
ホストにマルチパス ソフトウェアがない場合、ホストは同じストレージに複数のセッションを実行するので、上記のトポロジは当てはまりません。マルチパス ソフトウェアを使用していないホストは、同じストレージへの複数のパスについて、情報が得られません。

IP ストレージには、このシナリオで HA ソリューションを提供する機能が、他に 2 つあります。

- IPS ポートは VRRP 機能をサポートし（「IPStorage インターフェイスの VRRP の構成」セクションを参照）、IPS ポートのフェールオーバーを提供します。
- IPS には、iSCSI スタティック仮想ターゲットに関して、透過型のファイバ チャネル ターゲット フェールオーバー機能があります。

スタティックにインポートされた iSCSI ターゲットは、別の方法でファイバ チャネル ターゲットにセカンダリ pWWN を提供することもできます。この方法は、複数の冗長ポートで LU を認識できるように物理ファイバ チャネル ターゲットが設定されている場合に使用できます。アクティブ ポートに障害が発生した場合は、セカンダリ ポートがアクティブになり、新しいアクティブ ポートを使用するように iSCSI セッションが切り替わります。

図 *21 : 2* つのファイバ チャネル ポートを介したスタティック ターゲット インポート



上の図では、pWWN1 および 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 ターゲットに冗長アクセスを行うことができます。

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 セッションに影響を与えることなく、IPS ポートから透過的に実行されます。プライマリ ポートに障害が発生した場合は、すべての未処理入出力が終了し、状態確認ステータスになります。フェールオーバーが未完了の間に受信された新規入出力は、ビジー ステータスを受け取ります。

LUN マッピングを使用すると、別のセカンダリ ファイバ チャネル LUN を定義できます（LU 番号が異なる場合）。

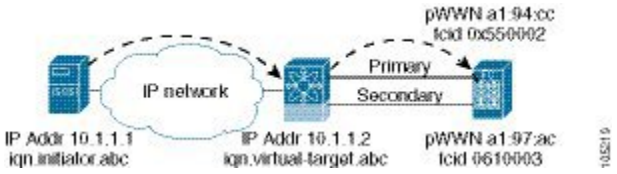
プライマリ ポートが再起動した場合に、IPS ポートがプライマリ ポートに再び切り替わるようにするには、**revert-primary port** オプションをイネーブルにします。このオプションがディセーブル（デフォルト）の場合は、スイッチオーバーのあとにプライマリ ポートを再起動しても、元のセッションは引き続きセカンダリ ポートにとどまり、プライマリ ポートに切り替わりません。ただし、新規セッションはプライマリ ポートを使用します。これは、プライマリおよびセカンダリ ポートが同時に使用される唯一の状況です。

ストレージ ポート フェールオーバー用の LUN トレスパス

スタティックにインポートされた iSCSI ターゲットにハイ アベイラビリティをもたらす以外に、アクティブ ポートで障害が発生した場合に、トレスパス機能を使用して、スタティックにインポートされた 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 を移動できます。

2 つのファイバ チャネル N ポートで LU を認識できるように設定された物理ファイバ 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した場合、パッシブ ポートが処理を引き継ぎます。一部の物理ファイバ チャネル ターゲットでは、アクティブ ポートからパッシブ ポートに LU を移動する場合に、トレスパス機能を使用する必要があります。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、およびトレスパス機能をイネーブルにする追加オプションは、冗長ポートを持つ物理ファイバ チャネル ターゲットに使用できます。アクティブ ポートに障害が発生すると、パッシブ ポートがアクティブになります。トレスパス機能がイネーブルの場合、Cisco MDS スイッチは、LU を新規アクティブ ポート上に移動するようターゲットに要求を送信します。新しいアクティブ ポートを使用するように iSCSI セッションが切り替わり、移動した LU は新しいアクティブ ポートを介してアクセスされます。

図 *22:* アクティブ プライマリ ポートを含む仮想ターゲット



スタティック iSCSI 仮想ターゲットの作成

スタティック iSCSI 仮想ターゲットを作成するには、次のステップを実行します。

手順

ステップ 1 iSCSI ターゲット（iqn.1987-02.com.cisco.initiator）を作成します。

```
switch# config terminal
switch(config)# iscsi virtual-target name iqn.1987-02.com.cisco.initiator
```

ステップ 2 この仮想ターゲットのプライマリ ポートを構成します。

```
switch(config-iscsi-tgt)# pwwn 26:00:01:02:03:04:05:06
```

ステップ 3 この仮想ターゲットのプライマリ ポートとセカンダリ ポートを構成します。

```
switch(config-iscsi-tgt)# pwwn 26:00:01:02:03:04:05:06 secondary-pwwn 26:00:01:02:03:10:11:12
```

ステップ 4 LUN マッピングと、セカンダリ ファイバ チャネル ポート上の異なる LUN を使用して、この仮想ターゲットのプライマリ ポートを構成します。

```
switch(config-iscsi-tgt)# pwwn 26:00:01:02:03:04:05:06 fc-lun 0x1 iscsi-lun 0x0 sec-lun 0x3
```

ステップ 5 この仮想ターゲットのプライマリ ポート、セカンダリ ポート、およびLUNマッピング構成を削除します。

```
switch(config-iscsi-tgt)# no pwwn 26:00:01:02:03:04:05:06
```

ステップ 6 プライマリ ポートがアクティブになったときにセッションをすべてプライマリ ポートに戻すように、この仮想ターゲットのセッション フェールオーバー冗長性を構成します。

```
switch(config-iscsi-tgt)# revert-primary-port
```

ステップ 7 既存のセッションに対してセカンダリ ポートを引き続き使用し、新しいセッションに対してプライマリ ポートを使用するようにスイッチを設定します（デフォルト）。

```
switch(config-iscsi-tgt)# no revert-primary-port
```

スタティック iSCSI 仮想ターゲットのトレスパス機能を有効にする

スタティック iSCSI 仮想ターゲットのトレスパス機能を有効にするには、次のステップを実行します。

手順

ステップ 1 iSCSI ターゲット（iqn.1987-02.com.cisco.initiator）を作成します。

```
switch# config terminal
switch(config)# iscsi virtual-target name iqn.1987-02.com.cisco.initiator
switch(config-iscsi-tgt)#
```

ステップ 2 ファイバ チャネル ターゲットに仮想ターゲット ノードをマッピングし、セカンダリ pWWN を構成します。

```
switch(config-iscsi-tgt)# pwwn 50:00:00:a1:94:cc secondary-pwwn 50:00:00:a1:97:ac
```

ステップ 3 トレスパス機能を有効にします。

```
switch(config-iscsi-tgt)# trespass
```

ステップ 4 トレスパス機能を無効にします（デフォルト）。

```
switch(config-iscsi-tgt)# no trespass
```

スタティック iSCSI 仮想ターゲットのトレスパス機能の確認

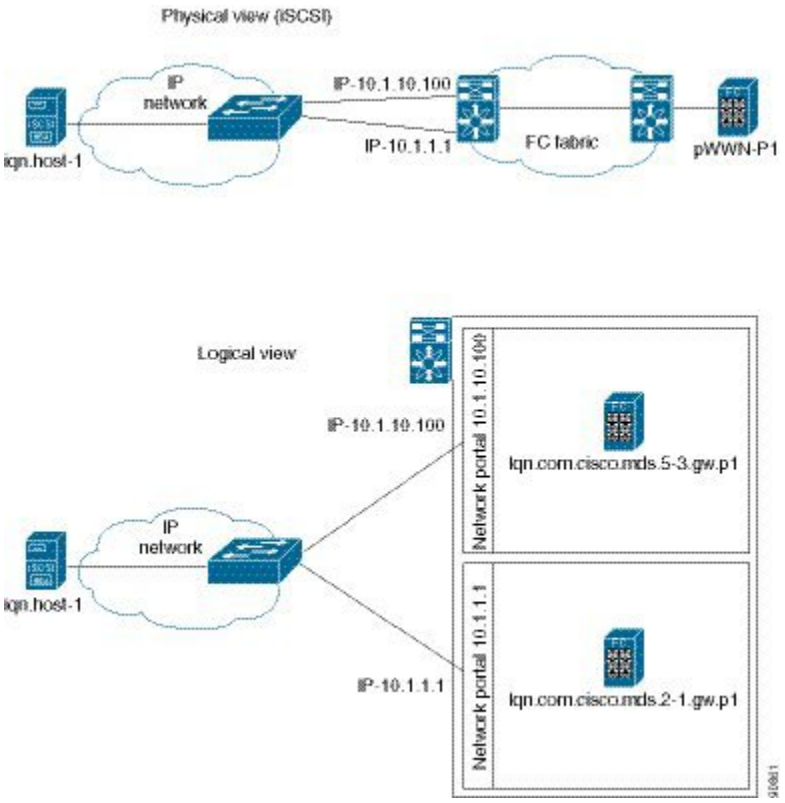
show iscsi virtual-target コマンドを使用して、スタティック iSCSI 仮想ターゲットのトレスパス機能を確認します。

```
switch# show iscsi virtual-target iqn.1987-02.com.cisco.initiator
target: 1987-02.com.cisco.initiator
Port WWN 10:20:10:00:56:00:70:50
Configured node
all initiator permit is disabled
trespass support is enabled
```

同じ IP ネットワークに接続された複数の IPS ポート

次の図では、各 iSCSI ホストは物理ファイバ チャネル ターゲット（異なる名前のターゲット）ごとに 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、両方のパスでロード バランシングを行います。いずれかのギガビット 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対応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。

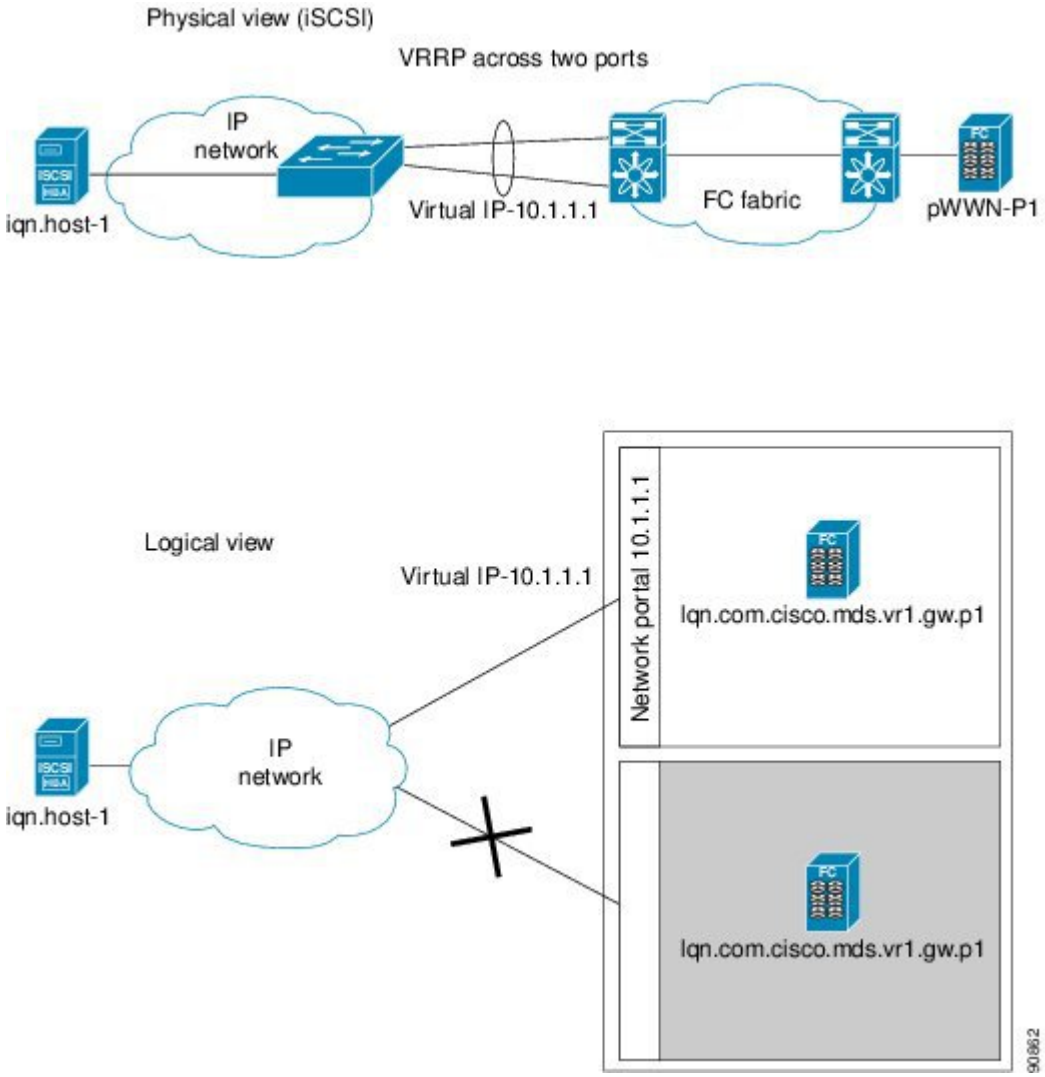
図 *23*：同じ *IP* ネットワーク内の複数のギガビット イーサネット インターフェイス



VRRP ベースのハイ アベイラビリティ

次の図では、各 iSCSI ホストは物理ファイバ 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 セッションが終了します。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 アドレスを引き継ぐため、ホストはターゲットに再接続し、セッションが起動します。

図 *24 : VRRP* ベースの *iSCSI* ハイ アベイラビリティ



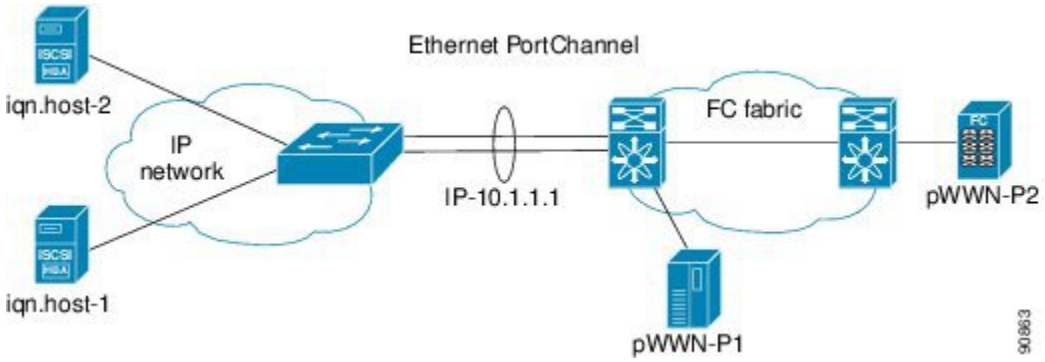
イーサネット ポート チャネル ベースのハイ アベイラビリティ

次の図では、各 iSCSI ホストは物理ファイバ 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 iSCSI 仮想ターゲット（IPS ポート上）への iSCSI セッションでは、2 つの物理インターフェイスのうちの 1 つを使用します（1 つの iSCSI セッションが 1 つの TCP 接続を使用するため）。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、IPS ポートを搭載したファイバ チャネル モジュールおよびイーサネット スイッチはすべてのフレームを別のギガビット イーサネット インターフェイスに透過的に転送します。

（注） 1 つの iSCSI リンクのすべての iSCSI データ トラフィックは、1 つの TCP 接続上で伝送されます。したがって、この iSCSI リンクの集約帯域幅は 1 Gbps になります。

（注） IPS ポートを搭載したファイバ チャネル モジュールとイーサネット スイッチ間にイーサネット ポート チャネルが構成されている場合は、VRRP によるロード バランシングを正常に動作させるために、イーサネット スイッチ上のロード バランシング ポリシーをポート番号ではなく、送信元/宛先 IP アドレスだけに基づいたものにする必要があります。

図 *25 :* イーサネット ポート チャネル ベースの *iSCSI* ハイ アベイラビリティ



iSCSI 認証設定時の注意事項およびシナリオ

ここでは、iSCSI 認証に関する注意事項および設定要件について説明し、シナリオの例を示します。

（注） この項の内容は、EXEC モード、コンフィギュレーション モード、およびすべてのサブモードを開始、終了する手順を指定するものではありません。いずれかのコマンドを入力する前に、プロンプトを確認する必要があります。

（注） iSLB VRRP グループに属している iSCSI インターフェイスの認証を変更すると、インターフェイスのロードバランシングが影響を受けます。「iSCSI インターフェイス パラメータの変更およびロード バランシングへの影響」セクションを参照してください。

取り上げる認証設定時の注意事項は、次のとおりです。

認証なしの構成

iSCSI 認証を **[none]** に設定して、ネットワークを認証なしに構成します。認証なしを構成するには、次のコマンドを使用します。

```
switch(config)# iscsi authentication none
```

ローカル パスワード データベースを使用した CHAP の構成

ローカル パスワード データベースで CHAP オプションを 使用して認証 を構成するには、次のステップを実行します。

手順

ステップ 1 iSCSI プロトコルにローカル 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。

```
switch(config)# aaa authentication iscsi default local
```

ステップ 2 すべての iSCSI クライアントに CHAP を要求するように、iSCSI 認証方式を設定します。

```
switch(config)# iscsi authentication chap
```

ステップ 3 iSCSI ユーザーのユーザー名およびパスワードを設定します。

```
switch(config)# username iscsi-user password abcd iscsi
```

（注）
iscsi オプションを指定しない場合、iSCSI ユーザーの代わりにユーザー名が Cisco MDS スイッチ ユーザーと見なされます。

ステップ 4 グローバル iSCSI 認証の設定を確認します。

```
switch# show iscsi global
iSCSI Global information Authentication: CHAP <----Verify
Import FC Target: Disabled
.
.
.
```

外部 RADIUS サーバを使用した CHAP の構成

外部 RADIUS サーバで CHAP オプションを使用して認証を構成するステップは、次のとおりです。

始める前に

手順

ステップ 1 RADIUS サーバに対する RADIUS クライアントとしての Cisco MDS スイッチのパスワードを構成します。

```
switch(config)# radius-server key mds-1
```

ステップ 2 次のいずれかを実行して RADIUS サーバーの IP アドレスを設定します。

a) IPv4 アドレスを設定します。

```
switch(config)# radius-server host 10.1.1.10
```

b) IPv6 アドレスを設定します。

```
switch(config)# radius-server host 2001:0DB8:800:200C::417A
```

ステップ 3 次のいずれかを実行して、RADIUS サーバー グループ IP アドレスを設定します。

a) IPv4 アドレスを設定します。

```
switch(config)# aaa group server radius iscsi-radius-group
switch(config-radius)# server 10.1.1.1
```

b) IPv6 アドレスを設定します。

```
switch(config)# aaa group server radius iscsi-radius-group
switch(config-radius)# server 001:0DB8:800:200C::4180
switch(config)# aaa authentication iscsi default group iscsi-radius-group
```

ステップ 4 すべての iSCSI クライアントに CHAP を要求するように、iSCSI 認証方式を設定します。

```
switch(config)# iscsi authentication chap
```

ステップ 5 グローバル iSCSI 認証設定が CHAP 用であることを確認します。

```
switch# show iscsi global
iSCSI Global information
Authentication: CHAP <---------------- Verify CHAP
.
.
.
```

ステップ 6 AAA 許可情報が iSCSI 用であることを確認します。

```
switch# show aaa authentication
default: local
console: local
iscsi: group iscsi-radius-group <--------- Group name
dhchap: local

switch# show radius-server groups
total number of groups:2

following RADIUS server groups are configured:
group radius:
server: all configured radius servers
group iscsi-radius-group:
server: 10.1.1.1 on auth-port 1812, acct-port 1813

switch# show radius-server
Global RADIUS shared secret:mds-1 <-------- Verify secret
.
.
.
.

following RADIUS servers are configured:
10.1.1.1: <----------- Verify the server IPv4 address
available for authentication on port:1812
available for accounting on port:1813
```

iSCSI トランスペアレント モード イニシエータ

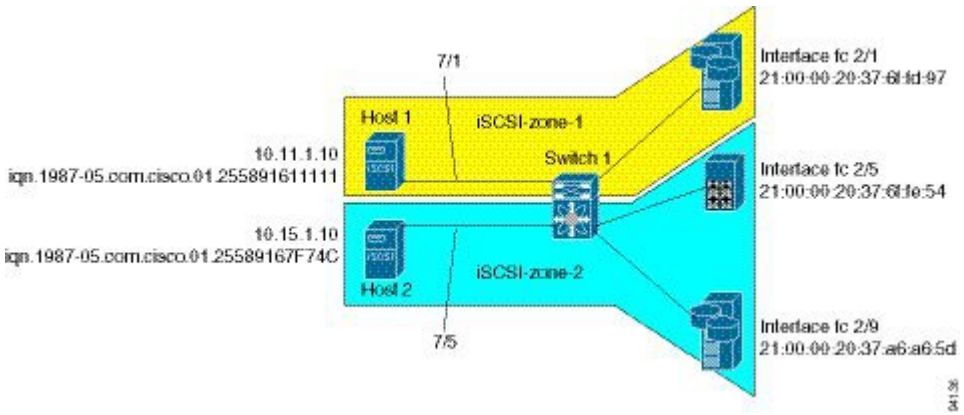
この構成は、次の構成を前提としています。

- ターゲット デバイス上に LUN マッピング、LUN マスキング、またはその他のホスト アクセス コントロールを設定しない。
- iSCSI ログイン認証を行わない（ログイン認証は none に設定）。
- トポロジは次のとおり。
  - iSCSI インターフェイス 7/1 は、IP アドレスで発信側を識別するように設定する。
  - iSCSI インターフェイス 7/5 は、ノード名で発信側を識別するように設定する。
  - IPS ポート 7/1 に接続する、IPv4 アドレスが 10.11.1.10 で名前が iqn.1987-05.com.cisco:01.255891611111 の iSCSI 発信側ホスト 1 を IPv4 アドレス（ホスト 1 = 10.11.1.10）で指定する。
  - IPv4 アドレスが 10.15.1.10 でノード名が iqn.1987-05.com.cisco:01.25589167f74c の iSCSI 発信側ホスト 2 を、IPS ポート 7/5 に接続する。

iSCSI の構成シナリオ 1

次の図は、シナリオ 1 を表しています。シナリオ 1 を構成するステップは、次のとおりです。

図 *26 : iSCSI* のシナリオ *1*



手順

ステップ 1 Cisco MDS スイッチのすべての iSCSI ホストにヌル認証を構成します。

```
switch(config)# iscsi authentication none
```

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 にダイナミックにインポートするように、iSCSI を設定します。

```
switch(config)# iscsi import target fc
```

ステップ 3 IPv4 アドレスを指定してスロット 7 ポート 1 のギガビット イーサネット インターフェイスを設定し、インターフェイスを有効にします。

```
switch(config)# interface gigabitethernet 7/1
switch(config-if)# ip address 10.11.1.1 255.255.255.0
switch(config-if)# no shutdown
```

（注）
ホスト 2 はこのポートに接続します。

ステップ 4 すべてのダイナミック iSCSI イニシエータを IP アドレスで識別するように、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有効にします。

```
switch(config)# interface iscsi 7/1
switch(config-if)# switchport initiator id ip-address
switch(config-if)# no shut
```

ステップ 5 IPv4 アドレスを指定してスロット 7 ポート 5 のギガビット イーサネット インターフェイスを設定し、インターフェイスを有効にします。

```
switch(config)# interface gigabitethernet 7/5
switch(config-if)# ip address 10.15.1.1 255.255.255.0
switch(config-if)# no shutdown
```

ステップ 6 すべてのダイナミック iSCSI イニシエータをノード名で識別するように、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有効にします。

```
switch(config)# interface iscsi 7/5
switch(config-if)# switchport initiator id name
switch(config-if)# no shutdown
```

（注）
ホスト 1 はこのポートに接続します。

ステップ 7 使用可能なファイバ チャネル ターゲットを確認します。

```
switch# show fcns database
VSAN 1:
--------------------------------------------------------------------------
FCID TYPE PWWN (VENDOR) FC4-TYPE:FEATURE
--------------------------------------------------------------------------
0x6d0001 NL 21:00:00:20:37:6f:fd:97 (Seagate) scsi-fcp:target
0x6d0101 NL 21:00:00:20:37:6f:fe:54 (Seagate) scsi-fcp:target
0x6d0201 NL 21:00:00:20:37:a6:a6:5d (Seagate) scsi-fcp:target
Total number of entries = 3
```

ステップ 8 ホスト 1 および 1 つのファイバ チャネル ターゲットが所属している *iscsi-zone-1* という名前のゾーンを作成します。

```
switch(config)# zone name iscsi-zone-1 vsan 1
switch(config-zone)# member pwwn 21:00:00:20:37:6f:fd:97
switch(config-zone)# member ip-address 10.11.1.10
```

（注）
iSCSI インターフェイスはすべてのホストを IP アドレスで識別するように設定されているので、ゾーン メンバーシップの設定には IP アドレスを使用します。

ステップ 9 ホスト 2 および 2 つのファイバ チャネル ターゲットが所属している *iscsi-zone-2* という名前のゾーンを作成します。

```
switch(config)# zone name iscsi-zone-2 vsan 1
switch(config-zone)# member pwwn 21:00:00:20:37:6f:fe:54
switch(config-zone)# member pwwn 21:00:00:20:37:a6:a6:5d
switch(config-zone)# member symbolic-nodename iqn.1987-05.com.cisco:01.25589167f74c
```

（注）
すべてのホストをノード名で識別するように iSCSI インターフェイスが設定されているので、ゾーン メンバーシップの設定には、iSCSI ホストのシンボリック ノード名を使用します。

ステップ 10 ゾーン セットを作成し、2 つのゾーンをメンバーとして追加します。

```
switch(config)# zoneset name zoneset-iscsi vsan 1
switch(config-zoneset)# member iscsi-zone-1
switch(config-zoneset)# member iscsi-zone-2
```

ステップ 11 ゾーン セットをアクティブにします。

```
switch(config)# zoneset activate name zoneset-iscsi vsan 1
```

ステップ 12 アクティブ ゾーン セットを表示します。

```
switch# show zoneset active
zoneset name zoneset-iscsi vsan 1
zone name iscsi-zone-1 vsan 1
* fcid 0x6d0001 [pwwn 21:00:00:20:37:6f:fd:97] <-----------Target
symbolic-nodename 10.11.1.10 <---------------------------------- iSCSI host (host 1, not online)

zone name iscsi-zone-2 vsan 1
* fcid 0x6d0101 [pwwn 21:00:00:20:37:6f:fe:54] <------------Target
* fcid 0x6d0201 [pwwn 21:00:00:20:37:a6:a6:5d] <------------Target
symbolic-nodename iqn.1987-05.com.cisco:01.25589167f74c <-iSCSI host (host 2, not online)
```

ステップ 13 iSCSI ホスト（ホスト 1 およびホスト 2）を起動します。

ステップ 14 すべての iSCSI セッションを表示します（詳細情報を表示する場合は **detail** オプションを使用します）。

```
switch# show iscsi session
Initiator iqn.1987-05.com.cisco:01.25589167f74c <-----Host 2
Initiator ip addr (s): 10.15.1.11
Session #1
Target iqn.1987-05.com.cisco:05.172.22.92.166.07-05.21000020376ffe54
VSAN 1, ISID 00023d000001, Status active, no reservation

Session #2
Target iqn.1987-05.com.cisco:05.172.22.92.166.07-05.2100002037a6a65d
VSAN 1, ISID 00023d000001, Status active, no reservation

Initiator 10.11.1.10 <----------------------------------Host 1
Initiator name iqn.1987-05.com.cisco:01.e41695d16b1a
Session #1
Target iqn.1987-05.com.cisco:05.172.22.92.166.07-01.21000020376ffd97
VSAN 1, ISID 00023d000001, Status active, no reservation
```

（注）
自動作成されたターゲット名の最後の部分は、ファイバ チャネル ターゲットの pWWN です。

ステップ 15 2 つの iSCSI イニシエータの詳細を確認します。

ホスト 2：ノード名に基づくイニシエータ ID（イニシエータは iSCSI インターフェイス 7/5 に入るため）：

```
switch# show iscsi initiator

iSCSI Node name is iqn.1987-05.com.cisco:01.25589167f74c
Initiator ip addr (s): 10.15.1.11
iSCSI alias name: oasis11.cisco.com
Node WWN is 20:02:00:0b:fd:44:68:c2 (dynamic)
Member of vsans: 1
Number of Virtual n_ports: 1
Virtual Port WWN is 20:03:00:0b:fd:44:68:c2 (dynamic)
Interface iSCSI 7/5 , Portal group tag: 0x304
VSAN ID 1, FCID 0x6d0300
```

ホスト 1：IPv4 アドレスに基づくイニシエータ ID（イニシエータは iSCSI インターフェイス 7/1 に入るため）：

```
iSCSI Node name is 10.11.1.10
iSCSI Initiator name: iqn.1987 - 05.com.cisco:01.e41695d16b1a
iSCSI alias name: oasis10.cisco.com
Node WWN is 20:04:00:0b:fd:44:68:c2 (dynamic)
Member of vsans: 1
Number of Virtual n_ports: 1
Virtual Port WWN is 20:05:00:0b:fd:44:68:c2 (dynamic)
Interface iSCSI 7/1 , Portal group tag: 0x300
VSAN ID 1, FCID 0x6d0301
```

ステップ 16 アクティブ 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。

ホスト 1 の解決された FC ID：

```
switch# show zoneset active
zoneset name zoneset-iscsi vsan 1
zone name iscsi-zone-1 vsan 1
* fcid 0x6d0001 [pwwn 21:00:00:20:37:6f:fd:97]
* fcid 0x6d0301 [symbolic-nodename 10.11.1.10]
```

ホスト 2 の FC ID：

```
zone name iscsi-zone-2 vsan 1
* fcid 0x6d0101 [pwwn 21:00:00:20:37:6f:fe:54]
* fcid 0x6d0201 [pwwn 21:00:00:20:37:a6:a6:5d]
* fcid 0x6d0300 [symbolic-nodename iqn.1987-05.com.cisco:01.25589167f74c] <-------------------------
```

ステップ 17 ファイバ チャネル ネーム サーバーによって、iSCSI ホスト用に作成された仮想 N ポートが表示されます。

```
switch# show fcns database
VSAN 1:
--------------------------------------------------------------------------
FCID TYPE PWWN (VENDOR) FC4-TYPE:FEATURE
--------------------------------------------------------------------------
0x6d0001 NL 21:00:00:20:37:6f:fd:97 (Seagate) scsi-fcp:target
0x6d0101 NL 21:00:00:20:37:6f:fe:54 (Seagate) scsi-fcp:target
0x6d0201 NL 21:00:00:20:37:a6:a6:5d (Seagate) scsi-fcp:target
0x6d0300 N 20:03:00:0b:fd:44:68:c2 (Cisco) scsi-fcp:init isc..w
0x6d0301 N 20:05:00:0b:fd:44:68:c2 (Cisco) scsi-fcp:init isc..w
```

ステップ 18 ファイバ チャネル ネーム サーバーの iSCSI イニシエータ ノードに関する詳細出力を確認します。

```
switch# show fcns database fcid 0x6d0300 detail vsan 1
------------------------
VSAN:1 FCID:0x6d0300
```

```
-----------------------
port-wwn (vendor) :20:03:00:0b:fd:44:68:c2 (Cisco)
node-wwn :20:02:00:0b:fd:44:68:c2
class :2,3
node-ip-addr :10.15.1.11
ipa :ff ff ff ff ff ff ff ff
fc4-types:fc4_features:scsi-fcp:init iscsi-gw
symbolic-port-name :
symbolic-node-name :iqn.1987-05.com.cisco:01.25589167f74c <--------------------
port-type :N
port-ip-addr :0.0.0.0
fabric-port-wwn :21:91:00:0b:fd:44:68:c0
hard-addr :0x000000
Total number of entries = 1
```

```
switch# show fcns database fcid 0x6d0301 detail vsan 1
-----------------------
VSAN:1 FCID:0x6d0301
-----------------------
port-wwn (vendor) :20:05:00:0b:fd:44:68:c2 (Cisco)
node-wwn :20:04:00:0b:fd:44:68:c2
class :2,3
node-ip-addr :10.11.1.10
ipa :ff ff ff ff ff ff ff ff
fc4-types:fc4_features:scsi-fcp:init iscsi-gw
symbolic-port-name :
symbolic-node-name :10.11.1.10
port-type :N
port-ip-addr :0.0.0.0
fabric-port-wwn :21:81:00:0b:fd:44:68:c0
hard-addr :0x000000
```

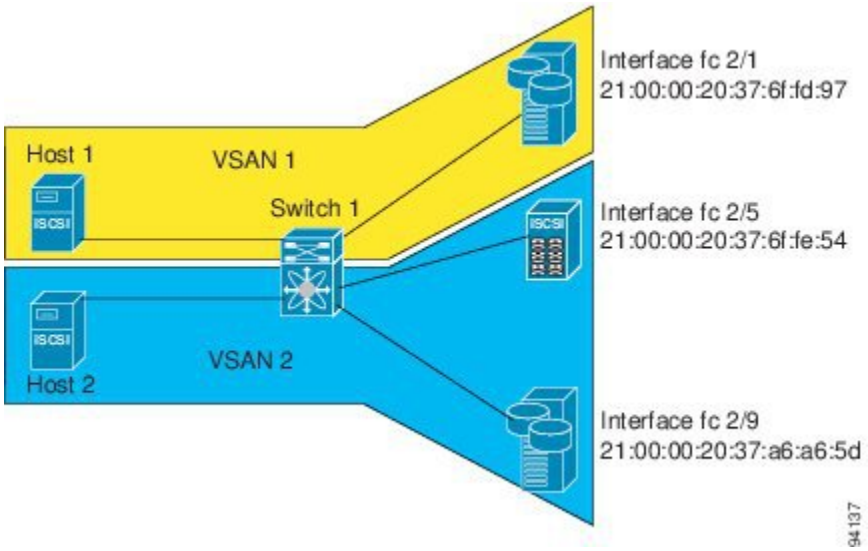
iSCSI の構成シナリオ 2

シナリオ 2 の例で想定されている構成は、次のとおりです。

- アクセス コントロールはファイバ チャネル ゾーン分割に基づく。
- ターゲットベースの LUN マッピングまたは LUN マスキングを使用する。
- iSCSI 認証は行わない（none）。
- iSCSI 発信側を個別の VSAN に割り当てる。

次の図は、シナリオ 2 を表します。シナリオ 2 を構成するステップは、次のとおりです。

図 *27 : iSCSI* のシナリオ *2*



手順

ステップ 1 すべての iSCSI ホストにヌル認証を設定します。

```
switch(config)# iscsi authentication none
```

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 にダイナミックにインポートするように、iSCSI を設定します。

```
switch(config)# iscsi import target fc
```

ステップ 3 IPv4 アドレスを指定してスロット 7 ポート 1 のギガビット イーサネット インターフェイスを設定し、インターフェイスを有効にします。

```
switch(config)# interface gigabitethernet 7/1
switch(config-if)# ip address 10.11.1.1 255.255.255.0
switch(config-if)# no shutdown
```

ステップ 4 すべてのダイナミック iSCSI イニシエータを IP アドレスで識別するように、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有効にします。

```
switch(config)# interface iscsi 7/1
switch(config-if)# switchport initiator id ip-address
switch(config-if)# no shutdown
```

ステップ 5 IPv4 アドレスを指定してスロット 7 ポート 5 のギガビット イーサネット インターフェイスを設定し、インターフェイスを有効にします。

```
switch(config)# interface gigabitethernet 7/5
switch(config-if)# ip address 10.15.1.1 255.255.255.0
switch(config-if)# no shutdown
```

ステップ 6 すべてのダイナミック iSCSI イニシエータを IP アドレスで識別するように、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有効にします。

```
switch(config)# interface iscsi 7/5
switch(config-if)# switchport initiator id ip-address
switch(config-if)# no shutdown
```

ステップ 7 iSCSI イニシエータごとにスタティック設定を追加します。

```
switch(config)# iscsi initiator name iqn.1987-05.com.cisco:01.e41695d16b1a <-----Host 2
switch(config-iscsi-init)# static pWWN system-assign 1
switch(config-iscsi-init)# static nWWN system-assign
switch(config)# iscsi initiator ip address 10.15.1.11 <----------------------------------Host 1
switch(config-iscsi-init)# static pwwn system-assigned 1
switch(config-iscsi-init)# vsan 2
```

（注）
ホスト 1 は VSAN 2 で設定されます。

ステップ 8 設定済みの WWN を表示します。

```
switch# show iscsi initiator configured
iSCSI Node name is iqn.1987-05.com.cisco:01.e41695d16b1a
Member of vsans: 1
Node WWN is 20:03:00:0b:fd:44:68:c2
No. of PWWN: 1
Port WWN is 20:02:00:0b:fd:44:68:c2

iSCSI Node name is 10.15.1.11
Member of vsans: 2
No. of PWWN: 1
Port WWN is 20:06:00:0b:fd:44:68:c2
```

（注）
WWN はシステムによって割り当てられています。発信側はさまざまな VSAN に所属しています。

ステップ 9 ホスト 1 を含むゾーンを作成します。

```
switch(config)# zone name iscsi-zone-1 vsan 1
```

ステップ 10 *iscsi-zone-1* という名前のゾーンに 3 つのメンバーを追加します。

a) 次のコマンドは、シンボリック ノード名に基づいています。

```
switch(config-zone)# member symbolic-nodename iqn.1987-05.com.cisco:01.e41695d16b1a
```

b) 次のコマンドは、発信側に割り当てられた固定 pWWN に基づいています。pWWN は **show iscsi initiator** 出力から取得できます。

```
switch(config-zone)# member pwwn 20:02:00:0b:fd:44:68:c2
```

ステップ 11 ホスト 2 および 2 つのファイバ チャネル ターゲットがあるゾーンを作成します。

```
switch(config)# zone name iscsi-zone-2 vsan 2
```

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

ステップ 12 VSAN 2 のゾーン セットをアクティブにします。

```
switch(config)# zoneset activate name iscsi-zoneset-v2 vsan 2
Zoneset activation initiated. check zone status
switch# show zoneset active vsan 2
zoneset name iscsi-zoneset-v2 vsan 2
zone name iscsi-zone-2 vsan 2
* fcid 0x750001 [pwwn 21:00:00:20:37:6f:fe:54]
* fcid 0x750101 [pwwn 21:00:00:20:37:a6:a6:5d]
pwwn 20:06:00:0b:fd:44:68:c2
```

ステップ 13 両方のホストで iSCSI クライアントを起動し、該当するセッションが開始されたことを確認します。

ステップ 14 iSCSI セッションを表示し、ファイバ チャネル ターゲットおよび構成された WWN を確認します。

```
switch# show iscsi session
Initiator iqn.1987-05.com.cisco:01.e41695d16b1a
Initiator ip addr (s): 10.11.1.10
Session #1
Discovery session, ISID 00023d000001, Status active
Session #2
Target iqn.1987-05.com.cisco:05.172.22.92.166.07-01.21000020376ffd97 <----
VSAN 1, ISID 00023d000001, Status active, no reservation
```

ステップ 15 iSCSI イニシエータを表示し、設定された pWWN および nWWN を確認します。

```
switch# show iscsi initiator
iSCSI Node name is iqn.1987-05.com.cisco:01.e41695d16b1a
Initiator ip addr (s): 10.11.1.10
iSCSI alias name: oasis10.cisco.com
Node WWN is 20:03:00:0b:fd:44:68:c2 (configured) <----------
Member of vsans: 1
Number of Virtual n_ports: 1
Virtual Port WWN is 20:02:00:0b:fd:44:68:c2 (configured) <----
Interface iSCSI 7/1, Portal group tag: 0x300
VSAN ID 1, FCID 0x680102
```

ステップ 16 ファイバ チャネルのネーム サーバーを確認します。

```
switch# show fcns database vsan 1
VSAN 1:
--------------------------------------------------------------------
FCID TYPE PWWN (VENDOR) FC4-TYPE:FEATURE
--------------------------------------------------------------------
0x680001 NL 21:00:00:20:37:6f:fd:97 (Seagate) scsi-fcp:target
0x680102 N 20:02:00:0b:fd:44:68:c2 (Cisco) scsi-fcp:init iscw
```

ステップ 17 ネーム サーバーの iSCSI イニシエータ ノードの FC ID に関する詳細を確認します。

```
switch(config)# show fcns database fcid 0x680102 detail vsan 1
------------------------
VSAN:1 FCID:0x680102
------------------------
port-wwn (vendor) :20:02:00:0b:fd:44:68:c2 (Cisco)
node-wwn :20:03:00:0b:fd:44:68:c2
class :2,3
node-ip-addr :10.11.1.10
ipa :ff ff ff ff ff ff ff ff
fc4-types:fc4_features:scsi-fcp:init iscsi-gw
symbolic-port-name :
symbolic-node-name :iqn.1987-05.com.cisco:01.e41695d16b1a
port-type :N
port-ip-addr :0.0.0.0
```

```
fabric-port-wwn :21:81:00:0b:fd:44:68:c0
iSCSI alias name: oasis10.cisco.com
```

ステップ 18 ファイバ チャネルのネーム サーバーを確認します。

```
switch# show fcns database vsan 1

VSAN 1:
--------------------------------------------------------------------
FCID TYPE PWWN (VENDOR) FC4-TYPE:FEATURE
--------------------------------------------------------------------
0x680001 NL 21:00:00:20:37:6f:fd:97 (Seagate) scsi-fcp:target
0x680102 N 20:02:00:0b:fd:44:68:c2 (Cisco) scsi-fcp:init isc..w
```

ステップ 19 ネーム サーバーの iSCSI イニシエータ ノードの FC ID に関する詳細を確認します。

```
switch(config)# show fcns database fcid 0x680102 detail vsan 1
------------------------
VSAN:1 FCID:0x680102
------------------------
port-wwn (vendor) :20:02:00:0b:fd:44:68:c2 (Cisco)
node-wwn :20:03:00:0b:fd:44:68:c2
class :2,3
node-ip-addr :10.11.1.10
ipa :ff ff ff ff ff ff ff ff
fc4-types:fc4_features:scsi-fcp:init iscsi-gw
symbolic-port-name :
symbolic-node-name :iqn.1987-05.com.cisco:01.e41695d16b1a
port-type :N
port-ip-addr :0.0.0.0
fabric-port-wwn :21:81:00:0b:fd:44:68:c0
hard-addr :0x000000
```

ステップ 20 iSCSI クライアントの FC ID がゾーン分割によって解決されたことを確認します。

```
switch# show zoneset active vsan 1
zoneset name iscsi-zoneset-v1 vsan 1
zone name iscsi-zone-1 vsan 1
* fcid 0x680001 [pwwn 21:00:00:20:37:6f:fd:97]
* fcid 0x680102 [pwwn 20:02:00:0b:fd:44:68:c2]
```

ステップ 21 2 番目のイニシエータが VSAN 2 の 2 つのファイバ チャネル ターゲットに接続されていることを確認します。

次のコマンドは、最初のターゲットへのセッションと2番目のターゲットへのセッションを表示します。

```
switch# show iscsi session initiator 10.15.1.11
Initiator 10.15.1.11
Initiator name iqn.1987-05.com.cisco:01.25589167f74c
Session #1
Target iqn.1987-05.com.cisco:05.172.22.92.166.07-05.21000020376ffe54 <--
VSAN 2, ISID 00023d000001, Status active, no reservation
Session #2
Target iqn.1987-05.com.cisco:05.172.22.92.166.07-05.2100002037a6a65d <--
VSAN 2, ISID 00023d000001, Status active, no reservation
```

次のコマンドを実行すると、ダイナミック WWN が割り当てられていないスタティック WWN およびスタティック pWWN としてイニシエータに表示されます。

```
switch# show iscsi initiator
iSCSI Node name is 10.15.1.11
iSCSI Initiator name: iqn.1987-05.com.cisco:01.25589167f74c
iSCSI alias name: oasis11.cisco.com
```

```
Node WWN is 20:04:00:0b:fd:44:68:c2 (dynamic)
Member of vsans: 2
Number of Virtual n_ports: 1
Virtual Port WWN is 20:06:00:0b:fd:44:68:c2 (configured)
Interface iSCSI 7/5, Portal group tag: 0x304
VSAN ID 2, FCID 0x750200
```

次の出力には、ネームサーバの iSCSI イニシエータ エントリが表示されています。

```
switch# show fcns database vsan 2
VSAN 2:
FCID TYPE PWWN (VENDOR) FC4-TYPE:FEATURE
0x750001 NL 21:00:00:20:37:6f:fe:54 (Seagate) scsi-fcp:target
0x750101 NL 21:00:00:20:37:a6:a6:5d (Seagate) scsi-fcp:target
0x750200 N 20:06:00:0b:fd:44:68:c2 (Cisco) scsi-fcp:init isc..w
Total number of entries = 3
```

```
switch# show fcns database fcid 0x750200 detail vsan 2
-----------------------
VSAN:2 FCID:0x750200
-----------------------
port-wwn (vendor) :20:06:00:0b:fd:44:68:c2 (Cisco)
node-wwn :20:04:00:0b:fd:44:68:c2
class :2,3
node-ip-addr :10.15.1.11
ipa :ff ff ff ff ff ff ff ff
fc4-types:fc4_features:scsi-fcp:init iscsi-gw
symbolic-port-name :
symbolic-node-name :10.15.1.11
port-type :N
port-ip-addr :0.0.0.0
fabric-port-wwn :21:91:00:0b:fd:44:68:c0
hard-addr :0x000000
Total number of entries = 1
```

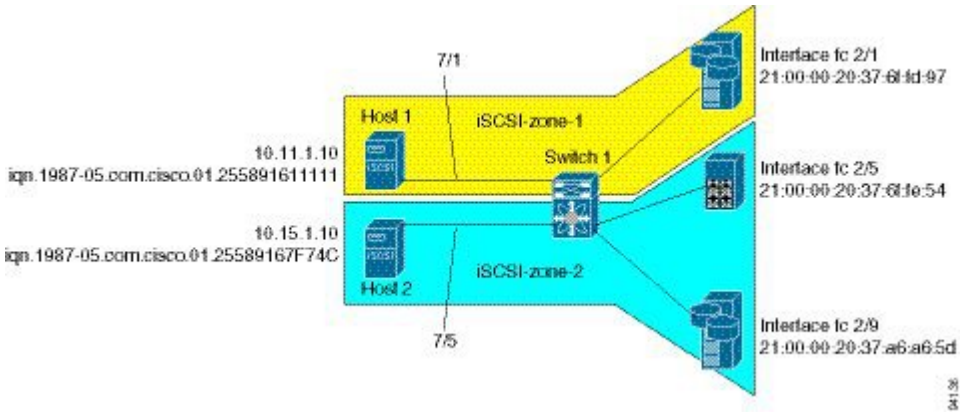
次のコマンドは、iSCSI イニシエータに解決された FC ID を表示します。

```
switch# show zoneset active vsan 2
zoneset name iscsi-zoneset-v2 vsan 2
zone name iscsi-zone-2 vsan 2
* fcid 0x750001 [pwwn 21:00:00:20:37:6f:fe:54]
* fcid 0x750101 [pwwn 21:00:00:20:37:a6:a6:5d]
```

iSCSI の構成シナリオ 1

次の図は、シナリオ 1 を表しています。シナリオ 1 を構成するステップは、次のとおりです。

図 *28 : iSCSI* のシナリオ *1*



手順

ステップ 1 Cisco MDS スイッチのすべての iSCSI ホストにヌル認証を構成します。

```
switch(config)# iscsi authentication none
```

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 にダイナミックにインポートするように、iSCSI を設定します。

```
switch(config)# iscsi import target fc
```

ステップ 3 IPv4 アドレスを指定してスロット 7 ポート 1 のギガビット イーサネット インターフェイスを設定し、インターフェイスを有効にします。

```
switch(config)# interface gigabitethernet 7/1
switch(config-if)# ip address 10.11.1.1 255.255.255.0
switch(config-if)# no shutdown
```

（注）
ホスト 2 はこのポートに接続します。

ステップ 4 すべてのダイナミック iSCSI イニシエータを IP アドレスで識別するように、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有効にします。

```
switch(config)# interface iscsi 7/1
switch(config-if)# switchport initiator id ip-address
switch(config-if)# no shut
```

ステップ 5 IPv4 アドレスを指定してスロット 7 ポート 5 のギガビット イーサネット インターフェイスを設定し、インターフェイスを有効にします。

```
switch(config)# interface gigabitethernet 7/5
switch(config-if)# ip address 10.15.1.1 255.255.255.0
switch(config-if)# no shutdown
```

ステップ 6 すべてのダイナミック iSCSI イニシエータをノード名で識別するように、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有効にします。

```
switch(config)# interface iscsi 7/5
switch(config-if)# switchport initiator id name
switch(config-if)# no shutdown
```

（注）
ホスト 1 はこのポートに接続します。

ステップ 7 使用可能なファイバ チャネル ターゲットを確認します。

```
switch# show fcns database
VSAN 1:
--------------------------------------------------------------------------
FCID TYPE PWWN (VENDOR) FC4-TYPE:FEATURE
--------------------------------------------------------------------------
0x6d0001 NL 21:00:00:20:37:6f:fd:97 (Seagate) scsi-fcp:target
0x6d0101 NL 21:00:00:20:37:6f:fe:54 (Seagate) scsi-fcp:target
0x6d0201 NL 21:00:00:20:37:a6:a6:5d (Seagate) scsi-fcp:target
Total number of entries = 3
```

ステップ 8 ホスト 1 および 1 つのファイバ チャネル ターゲットが所属している *iscsi-zone-1* という名前のゾーンを作成します。

```
switch(config)# zone name iscsi-zone-1 vsan 1
switch(config-zone)# member pwwn 21:00:00:20:37:6f:fd:97
switch(config-zone)# member ip-address 10.11.1.10
```

（注）
iSCSI インターフェイスはすべてのホストを IP アドレスで識別するように設定されているので、ゾーン メンバーシップの設定には IP アドレスを使用します。

ステップ 9 ホスト 2 および 2 つのファイバ チャネル ターゲットが所属している *iscsi-zone-2* という名前のゾーンを作成します。

```
switch(config)# zone name iscsi-zone-2 vsan 1
switch(config-zone)# member pwwn 21:00:00:20:37:6f:fe:54
switch(config-zone)# member pwwn 21:00:00:20:37:a6:a6:5d
switch(config-zone)# member symbolic-nodename iqn.1987-05.com.cisco:01.25589167f74c
```

（注）
すべてのホストをノード名で識別するように iSCSI インターフェイスが設定されているので、ゾーン メンバーシップの設定には、iSCSI ホストのシンボリック ノード名を使用します。

ステップ 10 ゾーン セットを作成し、2 つのゾーンをメンバーとして追加します。

```
switch(config)# zoneset name zoneset-iscsi vsan 1
switch(config-zoneset)# member iscsi-zone-1
switch(config-zoneset)# member iscsi-zone-2
```

ステップ 11 ゾーン セットをアクティブにします。

```
switch(config)# zoneset activate name zoneset-iscsi vsan 1
```

ステップ 12 アクティブ ゾーン セットを表示します。

```
switch# show zoneset active
zoneset name zoneset-iscsi vsan 1
zone name iscsi-zone-1 vsan 1
* fcid 0x6d0001 [pwwn 21:00:00:20:37:6f:fd:97] <-----------Target
symbolic-nodename 10.11.1.10 <--------------------------------- iSCSI host (host 1, not online)
```

```
zone name iscsi-zone-2 vsan 1
* fcid 0x6d0101 [pwwn 21:00:00:20:37:6f:fe:54] <------------Target
* fcid 0x6d0201 [pwwn 21:00:00:20:37:a6:a6:5d] <------------Target
symbolic-nodename iqn.1987-05.com.cisco:01.25589167f74c <-iSCSI host (host 2, not online)
```

ステップ 13 iSCSI ホスト（ホスト 1 およびホスト 2）を起動します。

ステップ 14 すべての iSCSI セッションを表示します（詳細情報を表示する場合は **detail** オプションを使用します）。

```
switch# show iscsi session
Initiator iqn.1987-05.com.cisco:01.25589167f74c <-----Host 2
Initiator ip addr (s): 10.15.1.11
Session #1
Target iqn.1987-05.com.cisco:05.172.22.92.166.07-05.21000020376ffe54
VSAN 1, ISID 00023d000001, Status active, no reservation

Session #2
Target iqn.1987-05.com.cisco:05.172.22.92.166.07-05.2100002037a6a65d
VSAN 1, ISID 00023d000001, Status active, no reservation

Initiator 10.11.1.10 <----------------------------------Host 1
Initiator name iqn.1987-05.com.cisco:01.e41695d16b1a
Session #1
Target iqn.1987-05.com.cisco:05.172.22.92.166.07-01.21000020376ffd97
VSAN 1, ISID 00023d000001, Status active, no reservation
```

（注）
自動作成されたターゲット名の最後の部分は、ファイバ チャネル ターゲットの pWWN です。

ステップ 15 2 つの iSCSI イニシエータの詳細を確認します。

ホスト 2：ノード名に基づくイニシエータ ID（イニシエータは iSCSI インターフェイス 7/5 に入るため）：

```
switch# show iscsi initiator

iSCSI Node name is iqn.1987-05.com.cisco:01.25589167f74c
Initiator ip addr (s): 10.15.1.11
iSCSI alias name: oasis11.cisco.com
Node WWN is 20:02:00:0b:fd:44:68:c2 (dynamic)
Member of vsans: 1
Number of Virtual n_ports: 1
Virtual Port WWN is 20:03:00:0b:fd:44:68:c2 (dynamic)
Interface iSCSI 7/5 , Portal group tag: 0x304
VSAN ID 1, FCID 0x6d0300
```

ホスト 1：IPv4 アドレスに基づくイニシエータ ID（イニシエータは iSCSI インターフェイス 7/1 に入るため）：

```
iSCSI Node name is 10.11.1.10
iSCSI Initiator name: iqn.1987 - 05.com.cisco:01.e41695d16b1a
iSCSI alias name: oasis10.cisco.com
Node WWN is 20:04:00:0b:fd:44:68:c2 (dynamic)
Member of vsans: 1
Number of Virtual n_ports: 1
Virtual Port WWN is 20:05:00:0b:fd:44:68:c2 (dynamic)
Interface iSCSI 7/1 , Portal group tag: 0x300
VSAN ID 1, FCID 0x6d0301
```

ステップ 16 アクティブ 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。

ホスト 1 の解決された FC ID：

```
switch# show zoneset active
zoneset name zoneset-iscsi vsan 1
zone name iscsi-zone-1 vsan 1
* fcid 0x6d0001 [pwwn 21:00:00:20:37:6f:fd:97]
* fcid 0x6d0301 [symbolic-nodename 10.11.1.10]
```

ホスト 2 の FC ID：

```
zone name iscsi-zone-2 vsan 1
* fcid 0x6d0101 [pwwn 21:00:00:20:37:6f:fe:54]
* fcid 0x6d0201 [pwwn 21:00:00:20:37:a6:a6:5d]
* fcid 0x6d0300 [symbolic-nodename iqn.1987-05.com.cisco:01.25589167f74c] <-------------------------
```

ステップ 17 ファイバ チャネル ネーム サーバーによって、iSCSI ホスト用に作成された仮想 N ポートが表示されます。

```
switch# show fcns database
VSAN 1:
--------------------------------------------------------------------------
FCID TYPE PWWN (VENDOR) FC4-TYPE:FEATURE
--------------------------------------------------------------------------
0x6d0001 NL 21:00:00:20:37:6f:fd:97 (Seagate) scsi-fcp:target
0x6d0101 NL 21:00:00:20:37:6f:fe:54 (Seagate) scsi-fcp:target
0x6d0201 NL 21:00:00:20:37:a6:a6:5d (Seagate) scsi-fcp:target
0x6d0300 N 20:03:00:0b:fd:44:68:c2 (Cisco) scsi-fcp:init isc..w
0x6d0301 N 20:05:00:0b:fd:44:68:c2 (Cisco) scsi-fcp:init isc..w
```

ステップ 18 ファイバ チャネル ネーム サーバーの iSCSI イニシエータ ノードに関する詳細出力を確認します。

```
switch# show fcns database fcid 0x6d0300 detail vsan 1
------------------------
VSAN:1 FCID:0x6d0300
------------------------
port-wwn (vendor) :20:03:00:0b:fd:44:68:c2 (Cisco)
node-wwn :20:02:00:0b:fd:44:68:c2
class :2,3
node-ip-addr :10.15.1.11
ipa :ff ff ff ff ff ff ff ff
fc4-types:fc4_features:scsi-fcp:init iscsi-gw
symbolic-port-name :
symbolic-node-name :iqn.1987-05.com.cisco:01.25589167f74c <--------------------
port-type :N
port-ip-addr :0.0.0.0
fabric-port-wwn :21:91:00:0b:fd:44:68:c0
hard-addr :0x000000
Total number of entries = 1

switch# show fcns database fcid 0x6d0301 detail vsan 1
------------------------
VSAN:1 FCID:0x6d0301
------------------------
port-wwn (vendor) :20:05:00:0b:fd:44:68:c2 (Cisco)
node-wwn :20:04:00:0b:fd:44:68:c2
class :2,3
node-ip-addr :10.11.1.10
ipa :ff ff ff ff ff ff ff ff
fc4-types:fc4_features:scsi-fcp:init iscsi-gw
symbolic-port-name :
symbolic-node-name :10.11.1.10
port-type :N
port-ip-addr :0.0.0.0
```

```
fabric-port-wwn :21:81:00:0b:fd:44:68:c0
hard-addr :0x000000
```

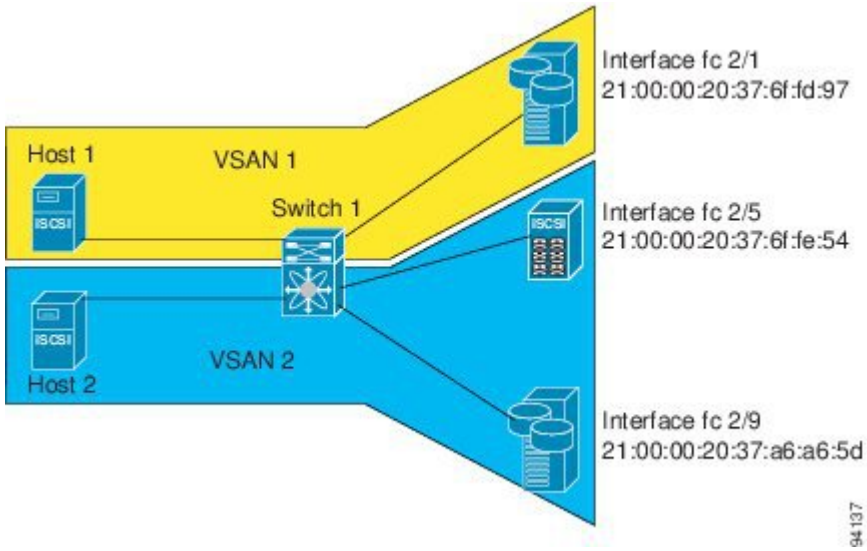
iSCSI の構成シナリオ 2

シナリオ 2 の例で想定されている構成は、次のとおりです。

- アクセス コントロールはファイバ チャネル ゾーン分割に基づく。
- ターゲットベースの LUN マッピングまたは LUN マスキングを使用する。
- iSCSI 認証は行わない（none）。
- iSCSI 発信側を個別の VSAN に割り当てる。

次の図は、シナリオ 2 を表します。シナリオ 2 を構成するステップは、次のとおりです。

図 *29 : iSCSI* のシナリオ *2*



手順

ステップ 1 すべての iSCSI ホストにヌル認証を設定します。

```
switch(config)# iscsi authentication none
```

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 にダイナミックにインポートするように、iSCSI を設定します。

```
switch(config)# iscsi import target fc
```

ステップ 3 IPv4 アドレスを指定してスロット 7 ポート 1 のギガビット イーサネット インターフェイスを設定し、インターフェイスを有効にします。

```
switch(config)# interface gigabitethernet 7/1
switch(config-if)# ip address 10.11.1.1 255.255.255.0
switch(config-if)# no shutdown
```

ステップ 4 すべてのダイナミック iSCSI イニシエータを IP アドレスで識別するように、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有効にします。

```
switch(config)# interface iscsi 7/1
switch(config-if)# switchport initiator id ip-address
switch(config-if)# no shutdown
```

ステップ 5 IPv4 アドレスを指定してスロット 7 ポート 5 のギガビット イーサネット インターフェイスを設定し、インターフェイスを有効にします。

```
switch(config)# interface gigabitethernet 7/5
switch(config-if)# ip address 10.15.1.1 255.255.255.0
switch(config-if)# no shutdown
```

ステップ 6 すべてのダイナミック iSCSI イニシエータを IP アドレスで識別するように、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有効にします。

```
switch(config)# interface iscsi 7/5
switch(config-if)# switchport initiator id ip-address
switch(config-if)# no shutdown
```

ステップ 7 iSCSI イニシエータごとにスタティック設定を追加します。

```
switch(config)# iscsi initiator name iqn.1987-05.com.cisco:01.e41695d16b1a <-----Host 2
switch(config-iscsi-init)# static pWWN system-assign 1
switch(config-iscsi-init)# static nWWN system-assign
switch(config)# iscsi initiator ip address 10.15.1.11 <----------------------------------Host 1
switch(config-iscsi-init)# static pwwn system-assigned 1
switch(config-iscsi-init)# vsan 2
```

（注）
ホスト 1 は VSAN 2 で設定されます。

ステップ 8 設定済みの WWN を表示します。

```
switch# show iscsi initiator configured
iSCSI Node name is iqn.1987-05.com.cisco:01.e41695d16b1a
Member of vsans: 1
Node WWN is 20:03:00:0b:fd:44:68:c2
No. of PWWN: 1
Port WWN is 20:02:00:0b:fd:44:68:c2

iSCSI Node name is 10.15.1.11
Member of vsans: 2
No. of PWWN: 1
Port WWN is 20:06:00:0b:fd:44:68:c2
```

（注）
WWN はシステムによって割り当てられています。発信側はさまざまな VSAN に所属しています。

ステップ 9 ホスト 1 を含むゾーンを作成します。

```
switch(config)# zone name iscsi-zone-1 vsan 1
```

ステップ 10 *iscsi-zone-1* という名前のゾーンに 3 つのメンバーを追加します。

a) 次のコマンドは、シンボリック ノード名に基づいています。

```
switch(config-zone)# member symbolic-nodename iqn.1987-05.com.cisco:01.e41695d16b1a
```

b) 次のコマンドは、発信側に割り当てられた固定 pWWN に基づいています。pWWN は **show iscsi initiator** 出力から取得できます。

```
switch(config-zone)# member pwwn 20:02:00:0b:fd:44:68:c2
```

ステップ 11 ホスト 2 および 2 つのファイバ チャネル ターゲットがあるゾーンを作成します。

```
switch(config)# zone name iscsi-zone-2 vsan 2
```

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

ステップ 12 VSAN 2 のゾーン セットをアクティブにします。

```
switch(config)# zoneset activate name iscsi-zoneset-v2 vsan 2
Zoneset activation initiated. check zone status
switch# show zoneset active vsan 2
zoneset name iscsi-zoneset-v2 vsan 2
zone name iscsi-zone-2 vsan 2
* fcid 0x750001 [pwwn 21:00:00:20:37:6f:fe:54]
* fcid 0x750101 [pwwn 21:00:00:20:37:a6:a6:5d]
pwwn 20:06:00:0b:fd:44:68:c2
```

ステップ 13 両方のホストで iSCSI クライアントを起動し、該当するセッションが開始されたことを確認します。

ステップ 14 iSCSI セッションを表示し、ファイバ チャネル ターゲットおよび構成された WWN を確認します。

```
switch# show iscsi session
Initiator iqn.1987-05.com.cisco:01.e41695d16b1a
Initiator ip addr (s): 10.11.1.10
Session #1
Discovery session, ISID 00023d000001, Status active
Session #2
Target iqn.1987-05.com.cisco:05.172.22.92.166.07-01.21000020376ffd97 <----
VSAN 1, ISID 00023d000001, Status active, no reservation
```

ステップ 15 iSCSI イニシエータを表示し、設定された pWWN および nWWN を確認します。

```
switch# show iscsi initiator
iSCSI Node name is iqn.1987-05.com.cisco:01.e41695d16b1a
Initiator ip addr (s): 10.11.1.10
iSCSI alias name: oasis10.cisco.com
Node WWN is 20:03:00:0b:fd:44:68:c2 (configured) <----------
Member of vsans: 1
Number of Virtual n_ports: 1
Virtual Port WWN is 20:02:00:0b:fd:44:68:c2 (configured) <----
Interface iSCSI 7/1, Portal group tag: 0x300
VSAN ID 1, FCID 0x680102
```

ステップ 16 ファイバ チャネルのネーム サーバーを確認します。

```
switch# show fcns database vsan 1
VSAN 1:
--------------------------------------------------------------------
```

```
FCID TYPE PWWN (VENDOR) FC4-TYPE:FEATURE
--------------------------------------------------------------------
0x680001 NL 21:00:00:20:37:6f:fd:97 (Seagate) scsi-fcp:target
0x680102 N 20:02:00:0b:fd:44:68:c2 (Cisco) scsi-fcp:init iscw
```

ステップ 17 ネーム サーバーの iSCSI イニシエータ ノードの FC ID に関する詳細を確認します。

```
switch(config)# show fcns database fcid 0x680102 detail vsan 1
-----------------------
VSAN:1 FCID:0x680102
-----------------------
port-wwn (vendor) :20:02:00:0b:fd:44:68:c2 (Cisco)
node-wwn :20:03:00:0b:fd:44:68:c2
class :2,3
node-ip-addr :10.11.1.10
ipa :ff ff ff ff ff ff ff ff
fc4-types:fc4_features:scsi-fcp:init iscsi-gw
symbolic-port-name :
symbolic-node-name :iqn.1987-05.com.cisco:01.e41695d16b1a
port-type :N
port-ip-addr :0.0.0.0
fabric-port-wwn :21:81:00:0b:fd:44:68:c0
iSCSI alias name: oasis10.cisco.com
```

ステップ 18 ファイバ チャネルのネーム サーバーを確認します。

```
switch# show fcns database vsan 1

VSAN 1:
--------------------------------------------------------------------
FCID TYPE PWWN (VENDOR) FC4-TYPE:FEATURE
--------------------------------------------------------------------
0x680001 NL 21:00:00:20:37:6f:fd:97 (Seagate) scsi-fcp:target
0x680102 N 20:02:00:0b:fd:44:68:c2 (Cisco) scsi-fcp:init isc..w
```

ステップ 19 ネーム サーバーの iSCSI イニシエータ ノードの FC ID に関する詳細を確認します。

```
switch(config)# show fcns database fcid 0x680102 detail vsan 1
-----------------------
VSAN:1 FCID:0x680102
-----------------------
port-wwn (vendor) :20:02:00:0b:fd:44:68:c2 (Cisco)
node-wwn :20:03:00:0b:fd:44:68:c2
class :2,3
node-ip-addr :10.11.1.10
ipa :ff ff ff ff ff ff ff ff
fc4-types:fc4_features:scsi-fcp:init iscsi-gw
symbolic-port-name :
symbolic-node-name :iqn.1987-05.com.cisco:01.e41695d16b1a
port-type :N
port-ip-addr :0.0.0.0
fabric-port-wwn :21:81:00:0b:fd:44:68:c0
hard-addr :0x000000
```

ステップ 20 iSCSI クライアントの FC ID がゾーン分割によって解決されたことを確認します。

```
switch# show zoneset active vsan 1
zoneset name iscsi-zoneset-v1 vsan 1
zone name iscsi-zone-1 vsan 1
* fcid 0x680001 [pwwn 21:00:00:20:37:6f:fd:97]
* fcid 0x680102 [pwwn 20:02:00:0b:fd:44:68:c2]
```

ステップ 21 2 番目のイニシエータが VSAN 2 の 2 つのファイバ チャネル ターゲットに接続されていることを確認します。

次のコマンドは、最初のターゲットへのセッションと2番目のターゲットへのセッションを表示します。

```
switch# show iscsi session initiator 10.15.1.11
Initiator 10.15.1.11
Initiator name iqn.1987-05.com.cisco:01.25589167f74c
Session #1
Target iqn.1987-05.com.cisco:05.172.22.92.166.07-05.21000020376ffe54 <--
VSAN 2, ISID 00023d000001, Status active, no reservation
Session #2
Target iqn.1987-05.com.cisco:05.172.22.92.166.07-05.2100002037a6a65d <--
VSAN 2, ISID 00023d000001, Status active, no reservation
```

次のコマンドを実行すると、ダイナミック WWN が割り当てられていないスタティック WWN およびスタティック pWWN としてイニシエータに表示されます。

```
switch# show iscsi initiator
iSCSI Node name is 10.15.1.11
iSCSI Initiator name: iqn.1987-05.com.cisco:01.25589167f74c
iSCSI alias name: oasis11.cisco.com
Node WWN is 20:04:00:0b:fd:44:68:c2 (dynamic)
Member of vsans: 2
Number of Virtual n_ports: 1
Virtual Port WWN is 20:06:00:0b:fd:44:68:c2 (configured)
Interface iSCSI 7/5, Portal group tag: 0x304
VSAN ID 2, FCID 0x750200
```

次の出力には、ネームサーバの iSCSI イニシエータ エントリが表示されています。

```
switch# show fcns database vsan 2
VSAN 2:
FCID TYPE PWWN (VENDOR) FC4-TYPE:FEATURE
0x750001 NL 21:00:00:20:37:6f:fe:54 (Seagate) scsi-fcp:target
0x750101 NL 21:00:00:20:37:a6:a6:5d (Seagate) scsi-fcp:target
0x750200 N 20:06:00:0b:fd:44:68:c2 (Cisco) scsi-fcp:init isc..w
Total number of entries = 3
```

```
switch# show fcns database fcid 0x750200 detail vsan 2
------------------------
VSAN:2 FCID:0x750200
------------------------
port-wwn (vendor) :20:06:00:0b:fd:44:68:c2 (Cisco)
node-wwn :20:04:00:0b:fd:44:68:c2
class :2,3
node-ip-addr :10.15.1.11
ipa :ff ff ff ff ff ff ff ff
fc4-types:fc4_features:scsi-fcp:init iscsi-gw
symbolic-port-name :
symbolic-node-name :10.15.1.11
port-type :N
port-ip-addr :0.0.0.0
fabric-port-wwn :21:91:00:0b:fd:44:68:c0
hard-addr :0x000000
Total number of entries = 1
```

次のコマンドは、iSCSI イニシエータに解決された FC ID を表示します。

```
switch# show zoneset active vsan 2
zoneset name iscsi-zoneset-v2 vsan 2
zone name iscsi-zone-2 vsan 2
```

```
* fcid 0x750001 [pwwn 21:00:00:20:37:6f:fe:54]
* fcid 0x750101 [pwwn 21:00:00:20:37:a6:a6:5d]
```

Internet Storage Name Service の概要

Internet Storage Name Service（iSNS）を使用すると、iSCSI デバイスの検出、管理、および設定の自動化により、既存の TCP/IP ネットワークが SAN としてより効率的に機能できるようになります。その実現のために、iSNS サーバーおよびクライアントは、次のように動作します。

- iSNS クライアントは、使用するとアクセスできる iSCSI ポータルおよびすべての iSCSI デバイスを iSNS サーバーに登録します。
- 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
  - ステート変更通知
  - 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（イニシエータおよびターゲットの両方）を、iSNS サーバーに登録できます。iSCSI イニシエータはその後 iSNS サーバーに対しターゲットのリストをクエリーできます。iSNS サーバーは応答として、クエリーの送信元クライアントが設定されているアクセス コントロール パラメータに基づいてアクセスできるターゲットのリストを提供します。

Cisco MDS 9000 ファミリ スイッチは、iSNS クライアントとして動作可能であり、使用可能なすべての iSCSI ターゲットを外部 iSNS サーバーに登録できます。IPS ポートを搭載したファイバ チャネル モジュールまたは MPS-14/2 モジュールが搭載されている Cisco MDS 9000 ファミリのスイッチはすべて、iSNS サーバ機能をサポートします。したがって、iSCSI 発信元などの外部 iSNS クライアントをスイッチに登録し、SAN で使用可能なすべての iSCSI ターゲットを検出できます。

このセクションは、次のトピックで構成されています。

iSNS クライアント機能の概要

Internet Storage Name Service（iSNS）を使用すると、iSCSI デバイスの検出、管理、および設定の自動化により、既存の TCP/IP ネットワークが SAN としてより効率的に機能できるようになります。iSNS クライアントは、使用するとアクセスできる iSCSI ポータルおよびすべての iSCSI デバイスを iSNS サーバーに登録します。iSNS クライアントとして動作するすべての iSCSI デバイス（発信側およびターゲットの両方）を、iSNS サーバーに登録できます。iSNS クライアントが iSNS サーバーにオブジェクトを登録/登録解除できない場合（クライアントが iSNS サーバーに TCP 接続できない場合など）、この iSNS クライアントは継続的に、関連するインターフェイスのすべての iSNS オブジェクトを iSNS サーバーに再登録しようとします。

各 IPS インターフェイス（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、またはポート チャネル）の iSNS クライアント機能によって、iSNS サーバーに情報が登録されます。

インターフェイスにプロファイルをタグ付けすると、スイッチはプロファイル内の iSNS サーバー IP アドレスへの TCP 接続を開始し（既知の iSNS ポート番号 3205 を使用）、ネットワーク エンティティおよびポータル オブジェクトを登録します。IPS インターフェイスごとに一意のエンティティが対応付けられます。スイッチはさらに、ファイバ チャネル ネーム サーバー（FCNS）データベースおよびスイッチの設定を検索し、iSNS サーバーに登録するストレージ ノードを検出します。

FCNS データベースにファイバ チャネル pWWN が対応付けられていて、アクセス コントロールが設定されていない場合は、スタティックにマッピングされた仮想ターゲットが登録されます。ダイナミック ターゲット インポートがイネーブルの場合は、ダイナミックにマッピングされたターゲットが登録されます。iSCSI がファイバチャネル ターゲットをインポートする方法の詳細については、「iSCSI ターゲットとしてのファイバ チャネル ターゲットの表示」を参照してください。

設定変更（アクセス コントロールの変更、ダイナミック インポートのディセーブル化など）が発生したために、またはファイバチャネル ストレージ ポートがオフラインになったために、ストレージ ノードを使用できなくなった場合は、ストレージ ノードが iSNS サーバーから登録解除されます。ストレージ ノードがオンラインに戻ると、ストレージ ノードが再登録されます。

iSNS クライアントが iSNS サーバーにオブジェクトを登録/登録解除できない場合（クライアントが iSNS サーバーに TCP 接続できない場合など）、この iSNS クライアントは継続的に、関連するインターフェイスのすべての iSNS オブジェクトを iSNS サーバーに再登録しようとします。iSNS クライアントで使用される登録インターバル値は 15 分です。クライアントがこのインターバルの間に登録を更新できなかった場合、サーバーはエントリの登録を解除します。

プロファイルのタグ付けを解除すると、ネットワーク エンティティおよびポータルも該当する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ません。

iSNS クライアント プロファイルの作成

iSNS プロファイルを作成するには、次のステップを実行します。

手順

ステップ 1 MyIsns と呼ばれるプロファイルを作成します。

```
switch# config terminal
switch(config)# isns profile name MyIsns
switch(config-isns-profile)#
```

ステップ 2 このプロファイルに iSNS サーバの IPv4 アドレスを指定します。

```
switch(config-isns-profile)# server 10.10.100.211
```

ステップ 3 このプロファイルから構成されている iSNS サーバを削除します。

```
switch(config-isns-profile)# no server 10.10.100.211
```

ステップ 4 このプロファイルに iSNS サーバの IPv6 アドレスを指定します。

```
switch(config-isns-profile)# server 2003::11
```

ステップ 5 このプロファイルから構成されている iSNS サーバを削除します。

```
switch(config-isns-profile)# no server 10.20.100.211
```

インターフェイスにプロファイルをタグ付け

インターフェイスにプロファイルをタグ付けするには、次の手順を実行します。

手順

ステップ 1 次の構成モードを入力します。

```
switch# config terminal
switch(config)#
```

ステップ 2 指定されたギガビット イーサネット インターフェイスを構成します。

```
switch(config)# interface gigabitethernet 4/1
switch(config-if)#
```

ステップ 3 インターフェイスにプロファイルをタグ付けします。

```
switch(config-if)# isns MyIsns
```

ステップ 4 インターフェイスからプロファイルのタグ付けを解除します。

```
switch(config-if)# no isns OldIsns
```

iSNS クライアント構成の確認

構成された iSNS プロファイルの表示：

構成された iSNS プロファイルを表示するには、**show isns profile** コマンドを使用します。プロファイル ABC には、iSNS サーバーに登録された 2 つのポータルがあります。各ポータルは、特定のインターフェイスに対応しています。プロファイル XYZ には指定された iSNS サーバがありますが、タグ付けされたインターフェイスは構成されていません。

構成された iSNS プロファイル情報の表示

```
switch# show isns profile
iSNS profile name ABC
tagged interface GigabitEthernet2/3
tagged interface GigabitEthernet2/2
iSNS Server 10.10.100.204

iSNS profile name XYZ
iSNS Server 10.10.100.211
```

指定した iSNS プロファイルの表示

```
switch# show isns profile ABC
iSNS profile name ABC
tagged interface GigabitEthernet2/3
tagged interface GigabitEthernet2/2
iSNS Server 10.10.100.204
```

タグ付きインターフェイスごとの iSNS PDU 統計情報を含む、すべての構成済みプロファイルの表示：

タグ付けされたインターフェイスごとに、設定されたすべてのプロファイルおよび iSNS PDU 統計情報を表示するには、**show isns profile counters** コマンドを使用します。

構成されたプロファイルおよび iSNS 統計情報の表示

```
switch# show isns profile counters
iSNS profile name ABC
tagged interface port-channel 1
iSNS statistics
Input 54 pdus (registration/deregistration pdus only)
Reg pdus 37, Dereg pdus 17
Output 54 pdus (registration/deregistration pdus only)
Reg pdus 37, Dereg pdus 17
iSNS Server 10.10.100.204

iSNS profile name XYZ
tagged interface port-channel 2
iSNS statistics
Input 30 pdus (registration/deregistration pdus only)
Reg pdus 29, Dereg pdus 1
Output 30 pdus (registration/deregistration pdus only)
Reg pdus 29, Dereg pdus 1
iSNS Server 10.1.4.218
```

指定したプロファイルの iSNS 統計情報の表示

```
switch# show isns profile ABC counters
iSNS profile name ABC
tagged interface port-channel 1
iSNS statistics
Input 54 pdus (registration/deregistration pdus only)
Reg pdus 37, Dereg pdus 17
Output 54 pdus (registration/deregistration pdus only)
Reg pdus 37, Dereg pdus 17
iSNS Server 10.10.100.204
```

iSNS サーバに登録されたオブジェクト、および所定のプロファイルで指定されたオブジェクトをすべて表示します。

iSNS サーバに登録されたオブジェクト、および所定のプロファイルで指定されたオブジェクトをすべて表示するには、**show isns** コマンドを使用します。

iSNS クエリの表示：

```
switch# show isns query ABC gigabitethernet 2/3
iSNS server: 10.10.100.204
Init: iqn.1991-05.com.w2k
Alias: <MS SW iSCSI Initiator>
Tgt : iqn.1987-05.com.cisco:05.172.22.94.22.02-03
Tgt : iqn.1987-05.com.cisco:05.172.22.94.22.02-03.210000203762fa34
nWWN: 200000203762fa34
```

インターフェイスがタグ付けされている iSNS プロファイルの表示

インターフェイスがタグ付けされた iSNS プロファイルを表示するには、**show interface** コマンドを使用します。

タグ付けされた iSNS インターフェイスの表示：

```
switch# show interface gigabitethernet 2/3
GigabitEthernet2/3 is up
Hardware is GigabitEthernet, address is 0005.3000.ae94
Internet address is 10.10.100.201/24
MTU 1500 bytes
Port mode is IPS
Speed is 1 Gbps
Beacon is turned off
Auto-Negotiation is turned on
iSNS profile ABC
^^^^^^^^^^^^^^^^
5 minutes input rate 112 bits/sec, 14 bytes/sec, 0 frames/sec
5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
1935 packets input, 132567 bytes
4 multicast frames, 0 compressed
0 input errors, 0 frame, 0 overrun 0 fifo
1 packets output, 42 bytes, 0 underruns
0 output errors, 0 collisions, 0 fifo
0 carrier errors
```

iSNS サーバ機能

イネーブルの場合、Cisco 9000 ファミリ MDS スイッチ上の iSNS サーバーは登録されているすべての iSCSI デバイスを追跡します。その結果、iSNS クライアントは iSNS サーバーにクエリーを送信することによって、他の iSNS クライアントを突き止めることができます。iSNS サーバーは次の機能も提供します。

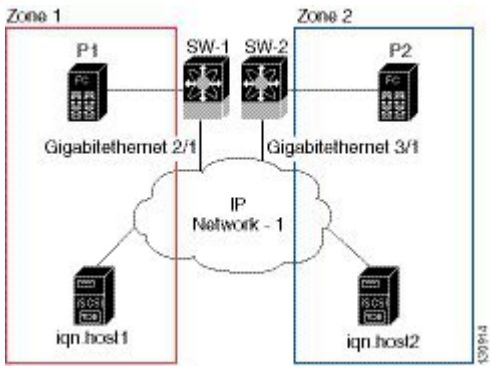
- iSNS クライアントを登録および登録解除できるようにします。また、iSNS クライアントから iSNS サーバーに登録されている他の iSNS クライアントを照会できるようにします。
- 特定の発信側からターゲットへのアクセスを許可または拒否する、アクセス コントロールの実施を集中管理します。

- 登録されている iSNS クライアントが、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け取るための通知方式を提供します。
- ファイバ チャネル デバイスと iSCSI デバイスの両方について、1 つのアクセス コントロール設定で対応できます。
- iSCSI 発信側に直接 IP 接続していない iSCSI ターゲットを検出します。

シナリオ例

iSNS サーバーは、ファイバ チャネルのゾーン分割情報と、iSCSI アクセス コントロール情報および設定の両方を利用することによって、ファイバ チャネル デバイスと iSCSI デバイスにまたがって、統一されたアクセス 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 発信側だけが、両方のアクセス コントロール情報に基づいてアクセスが許可されるデバイスを検出します。次の図は、このシナリオの例を示しています。

図 *30 : Cisco MDS* 環境における *iSNS* サーバーの使用例



上の図で、iqn.host1 および iqn.host2 は 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それぞれ異なるゾーンにあります。ゾーン 1 は iqn.host1 およびターゲット P1 からなり、ゾーン 2 は iqn.host2 およびターゲット P2 からなります。iSNS サーバー機能は両方のスイッチ（SW-1 および SW-2）で有効です。登録処理の流れは、次のとおりです。

1. 発信側 iqn.host1 が SW-1 のポート Gigabitethernet2/1 に登録されます。
2. 発信側 iqn.host2 が SW-2 のポート Gigabitethernet3/1 に登録されます。
3. 発信側 iqn.host1 が SW-1 に iSNS クエリーを送信し、アクセス可能なすべてのターゲットを調べます。
4. 次に iSNS サーバーがファイバ チャネル ネーム サーバー（FCNS）にクエリーを送信し、クエリー元からアクセス可能な（つまり、同じゾーン内の）デバイスのリストを取得します。このクエリーの結果は P1 だけです。
5. iSNS サーバーは次に自身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、そのアクセス コントロールの設定、ダイナミック 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なのかディセーブルなのかといった iSCSI の設定に基づいて行われます。

6. iSNS サーバーはクエリーの発信側に応答を戻します。この応答には、iSNS サーバーが認識しているすべての iSCSI ポータルを記したリストが含まれます。したがって、iqn.host1 は SW-1（Gigabitethernet 2/1）または SW-2（Gigabitethernet 3/1）のどちらからターゲット P1 にログインするかを選択できます。
7. 発信側が SW-1 へのログインを選択し、あとでポートがアクセス不能になった場合（Gigabitethernet 2/1 の停止など）、発信側は代わりに SW-2 のポート Gigabitethernet 3/1 からターゲット P1 への接続に移行することを選択できます。
8. ターゲットが停止するか、またはゾーンから除去された場合、iSNS サーバーは発信側に iSNS State Change Notification（SCN）メッセージを送信し、発信側がセッションを削除できるようにします。

iSNS サーバの構成

ここでは、Cisco MDS 9000 ファミリ スイッチ上で iSNS サーバーを設定する方法について説明します。

このセクションは、次のトピックで構成されています。

iSNS サーバの有効化

iSNS サーバーをイネーブルにするには、次の手順を実行します。

始める前に

iSNS サーバ機能を有効にする前に、iSCSI を有効にする必要があります（「iSCSI の有効化」を参照）。iSCSI をディセーブルにすると、自動的に iSNS がディセーブルになります。スイッチ上で iSNS サーバーがイネーブルになると、対応する iSCSI インターフェイスがアップ状態であるすべての IPS ポートで、外部 iSNS クライアントからの iSNS 登録およびクエリー要求に応じられるようになります。

手順

ステップ 1 iSNS サーバを有効にします。

```
switch# config terminal
switch(config)# isns-server enable
```

ステップ 2 iSNS サーバを無効にします（デフォルト）。

```
switch(config)# no isns-server enable
```

iSNS の構成配信

iSNS 構成の配信を有効にするには、次のステップを実行します。

始める前に

CFS インフラストラクチャを使用すると、ファブリック全域の iSNS サーバーに iSCSI 発信側の設定を配信できます。したがって、どのスイッチ上で動作している iSNS サーバーであっても、クエリーの送信元である iSNS クライアントに、ファブリックの任意の場所で使用できる iSCSI デバイスのリストを提供できます。CFS の詳細については、『Cisco Fabric Manager システム管理構成ガイド』『Cisco MDS 9000 ファミリ NX-OS システム管理構成ガイド』を参照してください。

手順

ステップ 1 CFS インフラストラクチャを使用して、iSCSI 仮想ターゲット構成をファブリック内のすべてのスイッチに配信します。

```
switch# config terminal
switch(config)# isns distribute
```

ステップ 2 iSCSI 仮想ターゲット構成のファブリック内のすべてのスイッチへの配信を停止します（デフォルト）。

```
switch(config)# no isns distribute
```

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、設定されている iSNS サーバーに情報を登録します。クライアントは登録時に、60 秒以上のエンティティ ステータス照会（ESI）インターバルを指定できます。クライアントが ESI インターバルをゼロ（0）に設定して登録した場合、サーバーは ESI を使用したクライアントのモニタリングを行いません。このような場合、クライアントの登録は明示的に登録解除されるまで、または iSNS サーバー機能がディセーブルになるまで有効です。

ESI 再試行カウントは、iSNS サーバーが iSNS クライアントにそれぞれのエンティティ ステータスを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ーに、引き続きアライブ状態であることを伝える応答を送信します。設定された回数だけ再試行しても、クライアントが応答できなかった場合、そのクライアントはサーバーから登録解除されます。

iSNS サーバの ESI 再試行回数を構成するには、次のステップを実行します。

手順

ステップ 1 クライアントへの接続を最大 6 回再試行するように ESI を構成します。指定できる範囲は 1 ～ 10 です。

```
switch# config terminal
switch(config)# isns esi retries 6
```

ステップ 2 デフォルト値の 3 回の再試行に戻します。

```
switch(config)# no isns esi retries 6
```

登録期間の設定

iSNS クライアントは、iSNS サーバーへの登録期間を指定します。iSNS サーバーはこの期間が終了するまで、登録をアクティブなものとして維持します。この期間内に iSNS クライアントからコマンドが送信されなかった場合、iSNS サーバーはデータベースからクライアントの登録を削除します。

iSNS クライアントが登録期間を指定しなかった場合、iSNS サーバーはデフォルトの 0 が指定されたものとして、登録を無限にアクティブにしておきます。MDS iSNS サーバー上で登録期間を手動設定することもできます。

iSNS サーバ上で登録期間を構成するには、次のステップを実行します。

手順

ステップ 1 登録を 300 秒間アクティブに構成します。有効な登録期間の範囲は 0 ～ 65536 秒です。

```
switch# config terminal
switch(config)# isns registration period 300
```

ステップ 2 クライアントが登録したタイムアウト値、またはデフォルト値の 0 に戻します。

```
switch(config)# no isns registration period
```

iSNS クライアントの登録および登録解除

show isns database コマンドを使用すると、登録されているすべての iSNS クライアントとそれらに関連付けられた構成を表示できます。

iSNSクライアントは、登録するまでiSNSサーバに問い合わせることができません。iSNS クライアントの登録解除は、明示的に行うことも、iSNS サーバーが（ESI モニタリングによって）クライアントに到達できないことを検出した時点で行われることもあります。

iSNS クライアントの登録および登録解除によって、ステータス変更通知（SCN）が生成され、関係するすべての iSNS クライアントに送信されます。

ターゲットの検出

iSCSI 発信側は、iSNS サーバーにクエリーを送信することによってターゲットを検出します。サーバはターゲット リストを検索する DevGetNext 要求をサポートします。また、接続先 IP アドレスまたはポート番号など、ターゲットおよびポータルの詳細を調べる DevAttrQuery をサポートします。

iSNS クライアントからクエリー要求を受信した iSNS サーバーは、FCNS に問い合せて、クエリー元である発信側が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。このクエリーの結果は、発信側のその時点でアクティブなゾーン分割の設定および現在の設定（複数可）によって決まります。iSNS サーバーはその後、iSCSI ターゲットの設定（仮想ターゲットおよびダイナミック インポート設定）を使用して、ファイバ チャネル ターゲットを同等の iSCSI ターゲットに変換します。この段階で、仮想ターゲットにアクセス コントロールが設定されている場合は、それも適用されます。さらに、ターゲットの詳細を記した応答メッセージがクエリー発信側に戻されます。

iSNS サーバーは、可能性のあるターゲットおよびポータルをすべて指定し、統合した応答をクエリー元である発信側に送信します。たとえば、ファイバ チャネル ターゲットがさまざまな IPS インターフェイス上で異なる iSCSI ターゲットとしてエクスポートされる場合、iSNS サーバーは可能性のあるすべての iSCSI ターゲットおよびポータルを示したリストで応答します。

最新のターゲット リストを維持するために、iSNS サーバーは iSCSI ターゲットが到達可能または到達不能になるたびに、クライアントにステート変更通知（SCN）を送信します。クライアントはその場合、iSNS クエリーをもう一度開始することによって、アクセス可能なターゲットのリストを再検出することが想定されています。iSCSI ターゲットの到達可能性が変化するのは、次のいずれかが発生した場合です。

- ターゲットがアップまたはダウンする。
- FC ターゲットのダイナミック インポート設定が変更される。
- ゾーン セットが変更される。
- デフォルトのゾーン アクセス コントロールが変更される。
- IPS インターフェイスのステートが変化する。
- イニシエータの構成変更によって、ターゲットがアクセス可能またはアクセス不能になる。

iSNS サーバ構成の確認

iSNS データベースに関する ESI インターバルおよび要約情報の表示

ESI インターバルおよび iSNS データベースの内容に関するサマリ情報を確認するには、**show isns config** コマンドを使用します（ を参照）。

ESI インターバルおよびデータベースの内容の iSNS サーバ構成の表示：

```
switch# show isns config
Server Name: switch1(Cisco Systems) Up since: Fri Jul 30 04:08:16 2004
Index: 1 Version: 1 TCP Port: 3205
fabric distribute (remote sync): ON
ESI
Non Response Threshold: 5 Interval(seconds): 60
Database contents
Number of Entities: 2
Number of Portals: 3
```

```
Number of ISCSI devices: 4
Number of Portal Groups: 0
```

iSNS データベースの内容に関する詳細情報の表示：

iSNS データベースの内容に関する詳細情報を表示するには、**show isns database**コマンドを使用しま。このコマンドは、iSNS データベースの情報（データベースに登録されているすべてのエンティティ、ノード、およびポータル）を表示します。このコマンドでオプションを指定しない場合、明示的に登録されたオブジェクトだけが表示されます。VSAN ID の横のアスタリスクは、iSCSI ノードが VSAN のデフォルト ゾーンにあることを示します。

明示的に登録されているオブジェクトの表示

```
switch# show isns database
Entity Id: dp-204
Index: 2 Last accessed: Fri Jul 30 04:08:46 2004
iSCSI Node Name: iqn.1991-05.comdp-2041
Entity Index: 2
Node Type: Initiator(2) Node Index: 0x1
SCN Bitmap: OBJ_UPDATED|OBJ ADDED|OBJ REMOVED|TARGET&SELF
Node Alias: <MS SW iSCSI Initiator>
VSANS: 1(*), 5(*)
Portal IP Address: 192.168.100.2 TCP Port: 4179
Entity Index: 2 Portal Index: 1
ESI Interval: 0 ESI Port: 4180 SCN Port: 4180
```

登録されたノードとポータル、および構成されたノードとポータルの完全なデータベースの表示

```
switch# show isns database full
Entity Id: isns.entity.mds9000
Index: 1 Last accessed: Fri Jul 30 04:08:16 2004

iSCSI Node Name: iqn.com.cisco.disk1
Entity Index: 1
Node Type: Target(1) Node Index: 0x80000001
WWN(s):
22:00:00:20:37:39:dc:45
VSANS:
iSCSI Node Name: iqn.isns-first-virtual-target
Entity Index: 1
Node Type: Target(1) Node Index: 0x80000002

VSANS:
iSCSI Node Name: iqn.com.cisco.disk2
Entity Index: 1
Node Type: Target(1) Node Index: 0x80000003
WWN(s):
22:00:00:20:37:39:dc:45

VSANS:
Portal IP Address: 192.168.100.5 TCP Port: 3205
Entity Index: 1 Portal Index: 3

Portal IP Address: 192.168.100.6 TCP Port: 3205
Entity Index: 1 Portal Index: 5

Entity Id: dp-204
Index: 2 Last accessed: Fri Jul 30 04:08:46 2004

iSCSI Node Name: iqn.1991-05.com.microsoft:dp-2041
Entity Index: 2
```

```
Node Type: Initiator(2) Node Index: 0x1
SCN Bitmap: OBJ_UPDATED|OBJ ADDED|OBJ REMOVED|TARGET&SELF
Node Alias: <MS SW iSCSI Initiator>

VSANS: 1(*), 5(*)
Portal IP Address: 192.168.100.2 TCP Port: 4179
Entity Index: 2 Portal Index: 1
ESI Interval: 0 ESI Port: 4180 SCN Port: 4180
```

（注） *local option* は、仮想ターゲットにのみ使用可能です。

ローカル スイッチの仮想ターゲット情報の表示：

```
switch# show isns database virtual-targets local
Entity Id: isns.entity.mds9000
Index: 1 Last accessed: Fri Jul 30 04:08:16 2004

iSCSI Node Name: iqn.com.cisco.disk1
Entity Index: 1
Node Type: Target(1) Node Index: 0x80000001
WWN(s):
22:00:00:20:37:39:dc:45

VSANS:
iSCSI Node Name: iqn.isns-first-virtual-target
Entity Index: 1
Node Type: Target(1) Node Index: 0x80000002

VSANS:
iSCSI Node Name: iqn.com.cisco.disk2
Entity Index: 1
Node Type: Target(1) Node Index: 0x80000003
WWN(s):
22:00:00:20:37:39:dc:45

VSANS:
Portal IP Address: 192.168.100.5 TCP Port: 3205
Entity Index: 1 Portal Index: 3

Portal IP Address: 192.168.100.6 TCP Port: 3205
Entity Index: 1 Portal Index: 5
```

指定したスイッチの仮想ターゲットの表示：

```
switch# show isns database virtual-targets switch 20:00:00:0d:ec:01:04:40
Entity Id: isns.entity.mds9000
Index: 1 Last accessed: Fri Jul 30 04:08:16 2004

iSCSI Node Name: iqn.com.cisco.disk1
Entity Index: 1
Node Type: Target(1) Node Index: 0x80000001
WWN(s):
22:00:00:20:37:39:dc:45

VSANS:
iSCSI Node Name: iqn.isns-first-virtual-target
Entity Index: 1
Node Type: Target(1) Node Index: 0x80000002

VSANS:
iSCSI Node Name: iqn.com.cisco.disk2
```

```
Entity Index: 1
Node Type: Target(1) Node Index: 0x80000003
WWN(s):
22:00:00:20:37:39:dc:45

VSANS:
Portal IP Address: 192.168.100.5 TCP Port: 3205
Entity Index: 1 Portal Index: 3

Portal IP Address: 192.168.100.6 TCP Port: 3205
Entity Index: 1 Portal Index: 5
```

iSNS サーバに登録されたノードの属性の表示：

iSNS サーバに登録されているノードの属性を表示するには、**show isns node** コマンドを使用します。オプションを指定しない場合、名前とノードタイプ属性が 1 行に 1 つずつ簡潔に表示されます。

明示的に登録されているオブジェクトの表示：

```
switch# show isns node all
--------------------------------------------------------------------------------
iSCSI Node Name Type
--------------------------------------------------------------------------------
iqn.1987-05.com.cisco:05.switch1.02-03.22000020375a6c8 Target
...
iqn.com.cisco.disk1 Target
iqn.com.cisco.ipdisk Target
iqn.isns-first-virtual-target Target
iqn.1991-05.cw22 Target
iqn.1991-05.cw53 Target
```

指定したノードの表示

```
switch# show isns node name iqn.com.cisco.disk1
iSCSI Node Name: iqn.com.cisco.disk1
Entity Index: 1
Node Type: Target(1) Node Index: 0x80000001
WWN(s):
22:00:00:20:37:39:dc:45
VSANS: 1
```

すべてのノードの属性詳細の表示

```
switch# show isns node all detail
iSCSI Node Name: iqn.1987-05.com.cisco:05.switch1.02-03.22000020375a6c8f
Entity Index: 1
Node Type: Target(1) Node Index: 0x3000003
Configured Switch WWN: 20:00:00:0d:ec:01:04:40
WWN(s):
22:00:00:20:37:5a:6c:8f
VSANS: 1
...
iSCSI Node Name: iqn.com.cisco.disk1
Entity Index: 1
Node Type: Target(1) Node Index: 0x80000001
Configured Switch WWN: 20:00:00:0d:ec:01:04:40
WWN(s):
22:00:00:20:37:39:dc:45
VSANS: 1

iSCSI Node Name: iqn.com.cisco.ipdisk
Entity Index: 1
```

```
Node Type: Target(1) Node Index: 0x80000002
Configured Switch WWN: 20:00:00:0d:ec:01:04:40
WWN(s):
22:00:00:20:37:5a:70:1a
VSANS: 1

iSCSI Node Name: iqn.isns-first-virtual-target
Entity Index: 1
Node Type: Target(1) Node Index: 0x80000003
Configured Switch WWN: 20:00:00:0d:ec:01:04:40

iSCSI Node Name: iqn.parna.121212
Entity Index: 1
Node Type: Target(1) Node Index: 0x80000004
Configured Switch WWN: 20:00:00:0d:ec:01:04:40

iSCSI Node Name: iqn.parna.121213
Entity Index: 1
Node Type: Target(1) Node Index: 0x80000005
Configured Switch WWN: 20:00:00:0d:ec:01:04:40
```

ポータルの属性とそのアクセス可能なノードの表示：

ポータルの属性をアクセス可能なノードとともに表示するには、**show isns portal** コマンドを使用します。スイッチの WWN とインターフェイスの組み合わせ、または IP アドレスとポート番号の組み合わせを使用して、ポータルを指定できます。

すべてのポータルの属性情報の表示：

```
switch# show isns portal all
--------------------------------------------------------------------------------
IPAddress TCP Port Index SCN Port ESI port
--------------------------------------------------------------------------------
192.168.100.5 3205 3 - -
192.168.100.6 3205 5 - -
```

すべてのポータルの詳細な属性情報の表示：

```
switch# show isns portal all detail
Portal IP Address: 192.168.100.5 TCP Port: 3205
Entity Index: 1 Portal Index: 3

Portal IP Address: 192.168.100.6 TCP Port: 3205
Entity Index: 1 Portal Index: 5
```

仮想ポータルの表示：

```
switch# show isns portal virtual
--------------------------------------------------------------------------------
IPAddress TCP Port Index SCN Port ESI port
--------------------------------------------------------------------------------
192.168.100.5 3205 3 - -
192.168.100.6 3205 5 - -
```

指定したスイッチの仮想ポータルの表示：

```
switch# show isns portal virtual switch 20:00:00:0d:ec:01:04:40
--------------------------------------------------------------------------------
IPAddress TCP Port Index SCN Port ESI port
--------------------------------------------------------------------------------
192.168.100.5 3205 3 - -
192.168.100.6 3205 5 - -
```

指定したスイッチの仮想ポータルの詳細情報の表示：

```
switch# show isns portal virtual switch 20:00:00:0d:ec:01:04:40 detail
Portal IP Address: 192.168.100.5 TCP Port: 3205
Entity Index: 1 Portal Index: 3
Switch WWN: 20:00:00:0d:ec:01:04:40
Interface: GigabitEthernet2/3

Portal IP Address: 192.168.100.6 TCP Port: 3205
Entity Index: 1 Portal Index: 5
Switch WWN: 20:00:00:0d:ec:01:04:40
Interface: GigabitEthernet2/5
```

エンティティの属性をエンティティ内のポータルとノードのリストとともに表示します。

エンティティの属性をエンティティ内のポータルとノードのリストとともに表示するには、**show isns entity** コマンドを使用します。オプションを指定しない場合、エンティティに関連付けられたノードまたはポータルのエンティティ ID および番号が、1 行に 1 つずつ簡潔に表示されます

登録されているすべてのエントリの表示：

```
switch1# show isns entity
--------------------------------------------------------------------------------
Entity ID Last Accessed
--------------------------------------------------------------------------------
dp-204 Tue Sep 7 23:15:42 2004
```

データベース内のすべてのエンティティの表示：

```
switch# show isns entity all

--------------------------------------------------------------------------------
Entity ID Last Accessed
--------------------------------------------------------------------------------
isns.entity.mds9000 Tue Sep 7 21:33:23 2004

dp-204 Tue Sep 7 23:15:42 2004
```

指定した ID のエンティティの表示：

```
switch1# show isns entity id dp-204
Entity Id: dp-204
Index: 2 Last accessed: Tue Sep 7 23:15:42 2004
```

データベース内のすべてのエンティティの詳細情報の表示：

```
switch1# show isns entity all detail
Entity Id: isns.entity.mds9000
Index: 1 Last accessed: Tue Sep 7 21:33:23 2004

Entity Id: dp-204
Index: 2 Last accessed: Tue Sep 7 23:16:34 2004
```

仮想エンティティの表示：

```
switch# show isns entity virtual
Entity Id: isns.entity.mds9000
Index: 1 Last accessed: Thu Aug 5 00:58:50 2004

Entity Id: dp-204
Index: 2 Last accessed: Thu Aug 5 01:00:23 2004
```

インポート ターゲットに関する情報の表示

show iscsi global config コマンドを使用して、インポート ターゲットに関する情報を表示します。

指定したスイッチのインポート ターゲット設定の表示：

```
switch# show isns iscsi global config switch 20:00:00:05:ec:01:04:00
iSCSI Global configuration:
Switch: 20:00:00:05:ec:01:04:00 iSCSI Auto Import: Enabled
```

すべてのスイッチのインポート ターゲット設定の表示：

```
switch# show isns iscsi global config all
iSCSI Global configuration:
Switch: 20:00:44:0d:ec:01:02:40 iSCSI Auto Import: Enabled
```

iSNS アプリケーションの CFS ピア スイッチ情報の表示

iSNS アプリケーションに関する CFS ピア スイッチ情報を表示するには、**show cfs peers** コマンドを使用します。

iSNS アプリケーションの CFS ピア スイッチ情報の表示：

```
switch# show cfs peers name isns

Scope : Physical
--------------------------------------------------
Switch WWN IP Address
--------------------------------------------------
20:00:00:00:ec:01:00:40 10.10.100.11 [Local]

Total number of entries = 1
```

iSNS Cloud Discovery

iSNS クラウド検出を設定することによって、IP ネットワーク内の iSNS サーバーを検出する処理を自動化できます。

この項では、次のトピックについて取り上げます。

- クラウド検出
- iSNS クラウド検出の設定
- クラウド検出ステータスの確認
- クラウド検出メンバーシップの確認
- クラウド検出統計情報の表示

クラウド検出

クエリー要求を受信した iSNS サーバーは、発信側がターゲットに到達するために通過できる、使用可能なターゲットおよびポータルのリストで応答します。MDS スイッチ外部の IP ネットワーク設定によって、発信側から到達できるのがギガビット 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。発信側に戻されたポータルセットに到達できるようにするには、所定の発信側から到達できるギガビット イーサネット インターフェイス セットを iSNS サーバーで認識する必要があります。

（注） iSNS クラウド検出は、Cisco Fabric Switch for IBM BladeCenter および Cisco Fabric Switch for HP c-Class BladeSystem ではサポートされません。

iSNS クラウド検出機能は、スイッチ上のインターフェイスをばらばらの IP クラウドに分割することによって、発信側から到達できる各種インターフェイスの情報を iSNS サーバーに提供します。この検出では、その時点でアップしている他のあらゆる既知の IPS ポートにメッセージを送信し、応答（または応答がないこと）によって、リモート IPS ポートが同一 IP ネットワークにあるのか、それとも別の IP ネットワークにあるのかを判別します。

クラウド検出は、次のイベントが発生したときに開始されます。

- CLI からの手動要求によって、CLI からクラウド検出が開始される。この動作によって、既存のメンバーシップが破棄され、新しいメンバーシップが作成されます。
- インターフェイスの自動検出により、インターフェイスが適切なクラウドに割り当てられる。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ーシップは増分方式で作成され、次のイベントによって開始されます。
  - ギガビット イーサネット インターフェイスがアップする（ローカルまたはリモート ギガビット イーサネット インターフェイス）。
  - 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る。
  - ポートの VRRP 設定が変更される。

iSNS サーバーは CFS を使用して、あらゆるスイッチにクラウドおよびメンバーシップ情報を配信します。したがって、ファブリック内のすべてのスイッチでクラウド メンバーシップ ビューが一致します。

（注） iSNS クラウド検出で CFS 配信が正しく行われるようにするには、ファブリック内のすべてのスイッチで Cisco SAN-OS Release 3.0(1) または NX-OS 4.1(1b) 以降が稼働している必要があります。

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。

- iSNS クラウド検出のイネーブル化
- オンデマンド型 iSNS クラウド検出の開始
- iSNS クラウド自動検出の設定

- iSNS クラウド自動検出構成の確認
- iSNS クラウド検出の設定
- iSNS クラウド検出メッセージ タイプの設定

iSNS クラウド検出のイネーブル化

iSNS クラウド検出を有効にするには、次のステップを実行します。

手順

ステップ 1 iSNS クラウド検出を有効にします。

```
switch# config terminal
switch(config)# cloud-discovery enable
```

ステップ 2 iSNS クラウド検出を無効にします（デフォルト）。

```
switch(config)# no cloud-discovery enable
```

オンデマンド型 iSNS クラウド検出の開始

オンデマンドの iSNS クラウド検出を開始するには、EXEC モードで **cloud discover** コマンドを使用します。

次に、ファブリック全体のオンデマンド クラウド検出を開始する例を示します。

```
switch# cloud discover
```

iSNS クラウド自動検出の設定

iSNS クラウド自動検出を構成するステップは、次のとおりです。

手順

ステップ 1 iSNS クラウド自動検出を有効にします（デフォルト）。

```
switch# config terminal
switch(config)# cloud discovery auto
```

ステップ 2 iSNS クラウド自動検出を無効にします。

```
switch(config)# no cloud discovery auto
```

ステップ 3 iSNS クラウド自動検出構成の確認：

```
switch# show cloud discovery config
Auto discovery: Enabled
```

iSNS クラウド検出の配信の構成

CFS を使用した iSNS クラウド検出配信を設定するには、次の手順を実行します。

手順

ステップ 1 iSNS クラウド検出ファブリック配信を有効にします（デフォルト）。

```
switch# config terminal
switch(config)# cloud discovery fabric distribute
```

ステップ 2 iSNS クラウド検出ファブリック配信を無効にします。

```
switch(config)# no cloud discovery fabric distribute
```

iSNS クラウド検出メッセージ タイプの設定

使用する iSNS クラウド検出メッセージのタイプを設定できます。デフォルトで、iSNS クラウド検出では ICMP が使用されます。

iSNS クラウド検出メッセージのタイプを設定するには、次の手順を実行します。

手順

ステップ 1 次の構成モードを入力します。

```
switch# config terminal
switch(config)#
```

ステップ 2 ICMP メッセージを使用する iSNS クラウド検出を有効にします（デフォルト）。

```
switch(config)# cloud discovery message icmp
```

（注）
ICMP メッセージだけがサポートされています。

クラウド検出ステータスの確認

クラウド検出動作のステータスを確認するには、**show cloud discovery status** コマンドを使用します。

```
switch# show cloud discovery status
Discovery status: Succeeded
```

クラウド検出メンバーシップの確認

スイッチのクラウド メンバーシップを確認するには **show cloud membership all** コマンドを使用します。

```
switch# show cloud membership all
Cloud 2
GigabitEthernet1/5[20:00:00:0d:ec:02:c6:c0] IP Addr 10.10.10.5
GigabitEthernet1/6[20:00:00:0d:ec:02:c6:c0] IP Addr 10.10.10.6
#members=2
```

スイッチの未解決メンバーシップを確認するには **show cloud membership unresolved** コマンドを使用します。

```
switch# show cloud membership unresolved
Undiscovered Cloud
No members
```

クラウド検出動作の統計情報を確認するには、**show cloud discovery statistics** コマンドを使用します。

```
switch# show cloud discovery statistics
Global statistics
Number of Auto Discovery = 1
Number of Manual Discovery = 0
Number of cloud discovery (ping) messages sent = 1
Number of cloud discovery (ping) success = 1
```

デフォルト設定

次の表に、iSCSI パラメータのデフォルト設定を示します。

表 *2:* デフォルトの *iSCSI* パラメータ

パラメータ	デフォルト
TCP 接続の数	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
PMTU ディスカバリ	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	パケットの送信なし
TCP 輻輳ウィンドウ モニタリング	イネーブル

パラメータ	デフォルト
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 へのファイバ チャネル ターゲット	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、ポートチャネル インターフェイス、およびポート チャネル 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 ホストのマッピング	ダイナミック マッピング
ダイナミック iSCSI 発信側	VSAN 1 のメンバー
発信側の識別	iSCSI ノード名
スタティック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発信側が要求を送信した時点で自動的にイネーブル。ストアアンドフォワードモードの場合、この機能は設定不可および使用不可
iSNS 登録インターバル	60 秒（設定不可）
iSNS 登録インターバルの再試行回数	3
ファブリック配信	ディセーブル

次の表に、iSLB パラメータのデフォルト設定を示します。

表 *3:* デフォルト *iSLB*

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

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