



ファイバ チャンネル ゲートウェイの 使用方法

この章で説明する内容は、次のとおりです。

- [ファイバ チャンネル ゲートウェイの設定 \(p.5-2\)](#)
- [ファイバ チャンネル ゲートウェイの管理 \(p.5-3\)](#)
- [イニシエータの設定 \(p.5-7\)](#)
- [ターゲットおよび LUN の設定 \(p.5-7\)](#)
- [IT ペアの設定 \(p.5-8\)](#)
- [ITL の設定 \(p.5-10\)](#)
- [既存の IT および ITL へのポート アクセスの設定 \(p.5-26\)](#)
- [ポート アクセス設定の表示 \(p.5-31\)](#)
- [既存 ITL への LUN アクセスの設定 \(p.5-33\)](#)
- [LUN アクセス設定の表示 \(p.5-38\)](#)
- [個々の ITL アトリビュートの設定 \(p.5-40\)](#)
- [ゲートウェイ グルーピング \(p.5-48\)](#)

ファイバチャネル ゲートウェイの設定

この章では、ファイバチャネル ゲートウェイに関連する作業の実行手順について説明します。ここでは、次の作業を行うときに実行する内容について簡単に説明します。

- 新規ゲートウェイの設置
- 既存の設定のアップデート

新規ファイバチャネル ゲートウェイの設定

新規のファイバチャネルゲートウェイを取り付けたときは、次の作業を行います。

-
- ステップ 1** ゲートウェイを起動して、トラフィックを転送できるようにします（「[カードの起動](#)」 [p.5-3] を参照）。
- ステップ 2** 新規 ITL にデフォルトのアトリビュートが割り当てられるように、グローバル SRP/ITL アトリビュートを設定します（「[グローバルアトリビュートの設定](#)」 [p.3-2] を参照）。
- ステップ 3** ITL を検出して、ホストとストレージ間の通信パスを提供します（「[ITL の設定](#)」 [p.5-10] を参照）。
- ステップ 4** ITL および IT をカスタマイズして、デフォルト設定と異なるストレージアクセスの許可または拒否、およびデフォルト設定以外のカスタム動作を設定します（「[個々の ITL アトリビュートの設定](#)」 [p.5-40] を参照）。
-

既存の設定のアップデート

ファイバチャネルゲートウェイの既存の設定を変更する場合には、次のいずれかの作業を行います。

- グローバル ITL アトリビュートを再設定して、新規 ITL のデフォルト設定を変更します（「[グローバルアトリビュートの設定](#)」 [p.3-2] を参照）。



(注)

グローバルなデフォルト設定を変更した場合、変更前のデフォルト設定が適用された既存の ITL には、変更は反映されません。既存の ITL は、個別に再設定する必要があります。

- 既存の ITL を再設定して、SAN のプライオリティおよび要件の変更に応じて、アクセスおよび動作の設定を更新します（「[個々の ITL アトリビュートの設定](#)」 [p.5-40] を参照）。
- ストレージ デバイスおよびホストを追加した場合、ITL を追加します（「[ITL の設定](#)」 [p.5-10] を参照）。

ファイバチャネルゲートウェイの管理

ファイバチャネルゲートウェイカードを管理するには、Element Manager または CLI を使用します。

カードの起動

IB ホストとファイバチャネルストレージ間でトラフィックを転送するには、インターフェイスカードを起動します。

Element Manager を使用する

Element Manager を使用してファイバチャネルゲートウェイカードを起動する手順は、次のとおりです。

ステップ 1 Element Manager を起動して、サーバスイッチに接続します。

ステップ 2 起動したいカードをダブルクリックします。Fibre Channel Card # ウィンドウが開きます。# は、カードが搭載されているスロットの番号です。



(注) カードが正常に起動したかどうかを確認するには、Card Boot Status フィールドを調べます。Card Boot Status フィールドに **success** と表示され、Card Boot Stage フィールドに **done** と表示されるまでは、次の手順に進まないでください。

ステップ 3 Enable/Disable Card フィールドで、**up** オプション ボタンをクリックします。

ステップ 4 Apply ボタンをクリックします。

CLI を使用する

CLI を使用してファイバチャネルゲートウェイカードを起動する手順は、次のとおりです。

ステップ 1 CLI セッションを開き、ファイバチャネル読み書き権限のあるユーザとしてログインします。権限の詳細については、『Cisco SFS Product Family Command Reference』を参照してください。

```
Login: super
Password: xxxxxx
```

ステップ 2 **enable** コマンドを入力して、特権 EXEC モードを開始します。

```
SFS-3012R> enable
SFS-3012R#
```

ステップ 3 **show card** コマンドを入力して、カードが正常に起動していることを確認します。



(注) Boot Stage フィールドに **done** と表示され、Boot Status フィールドに **success** と表示されるまでは、次の手順に進まないでください。

```
SFS-3012R# show card
```

```
=====
                        Card Information
=====
  admin      oper      admin  oper  oper
slot type    type      status status code
-----
 1  controller  controller  up    up    normal
 5  fc2port2G  fc2port2G  down  down  normal
 7  fc2port2G  fc2port2G  up    up    normal
16  ib12port4x  ib12port4x  up    up    normal
=====

  boot      boot      boot
slot stage  status    image
-----
 1  done     success   TopspinOS-2.0.0/build447
 5  none     none
 7  done     success   TopspinOS-2.0.0/build447
16  done     success   TopspinOS-2.0.0/build447
=====

                        Card Seeprom
=====
  product    pca      pca      fru
slot serial-number  serial-number  number  number
-----
 1  PY-0305-000017  PY-0305-000017  95-00005-01-B3  98-00001-01
 5  PY-0309-000023  PY-0309-000023  95-00008-01-C1  0
 7  PY-0244-000007  PY-0244-000007  95-00008-01-B0  0
16  PY-0307-000028  PY-0307-000028  95-00006-01-B1  0
=====
```

ステップ 4 **configure terminal** コマンドを入力して、グローバル コンフィギュレーション モードを開始します。

```
SFS-3012R# configure terminal
SFS-3012R(config)#
```

ステップ 5 **card** コマンドを入力して、ファイバチャネル ゲートウェイが搭載されているスロット番号を指定します。

```
SFS-3012R(config)# card 5
SFS-3012R(config-card-5)#
```

ステップ 6 **no shutdown** コマンドを入力して、カードを起動します。

```
SFS-3012R(config-card-5)# no shutdown
SFS-3012R(config-card-5)#
```

カードの停止

Element Manager を使用してカードを停止するには、前述の手順を実行し、ステップ3で **down** オプション ボタンをクリックします。

CLI を使用してカードを停止するには、前述の手順を実行し、ステップ6で **shutdown** コマンドを入力します。

ポートの起動

ポート上でトラフィックを転送するには、インターフェイス ポートを起動します。

Element Manager を使用する

Element Manager を使用してファイバチャネルゲートウェイ ポートを起動する手順は、次のとおりです。

-
- ステップ1** Element Manager を起動して、サーバスイッチに接続します。
 - ステップ2** 起動したいポートをダブルクリックします。Fibre Channel Port card#/port# ウィンドウが開きます。slot# はファイバチャネルゲートウェイカードが搭載されているスロットの番号、port# はカード上のポート番号です。
 - ステップ3** Enable/Disable Port フィールドで、**up** オプション ボタンをクリックします。
 - ステップ4** Apply ボタンをクリックします。
-

CLI を使用する

CLI を使用してファイバチャネルゲートウェイ ポートを起動する手順は、次のとおりです。

-
- ステップ1** CLI セッションを開き、ファイバチャネル読み書き権限のあるユーザとしてログインします。権限の詳細については、『Cisco SFS Product Family Command Reference』を参照してください。

```
Login: super
Password: xxxxxx
```

- ステップ2** **enable** コマンドを入力して、特権 EXEC モードを開始します。

```
SFS-3012R> enable
SFS-3012R#
```

- ステップ3** **configure terminal** コマンドを入力して、グローバル コンフィギュレーション モードを開始します。

```
SFS-3012R# configure terminal
SFS-3012R(config)#
```

ステップ 4 `interface` コマンドを入力し、次の内容を指定します。

- `fc` キーワード
- ポートのスロット番号 / ポート番号

ファイバチャネル インターフェイス コンフィギュレーション サブモードが開始されます。

```
SFS-3012R(config)# interface fc 5/1  
SFS-3012R(config-if-fc-5/1)#
```

ステップ 5 `no shutdown` コマンドを入力して、ポートを起動します。

```
SFS-3012R(config-if-fc-5/1)# no shutdown  
SFS-3012R(config-if-fc-5/1)#
```

ポートの停止

Element Manager を使用してポートを停止するには、前述の手順を実行し、ステップ 3 で `down` オプション ボタンをクリックします。

CLI を使用してポートを停止するには、前述の手順を実行し、ステップ 5 で `shutdown` コマンドを入力します。

イニシエータの設定

イニシエータを設定するには、SAN でホストが認識されるように、SRP ホストにファイバチャネル WWNN を割り当てます。イニシエータの設定手順についての詳細は、「ITL の設定」(p.5-10) を参照してください。



(注)

イニシエータは、ファブリックに接続していなくても設定できます。CLI または Element Manager を使用してイニシエータの GUID を入力しておく、SRP ホストを接続したときに設定が適用されます。

ターゲットおよび LUN の設定

ストレージは、ファイバチャネルゲートウェイによって自動的に検出され、設定されます。ターゲットおよび LUN の設定手順についての詳細は、「ITL の設定」(p.5-10) を参照してください。ターゲットおよび LUN を手動で設定する場合には、『Cisco SFS Product Family Command Reference』の **fc srp target** コマンドおよび **fc srp lu** コマンドの説明を参照してください。

IT ペアの設定

Initiator-Target (IT; イニシエータ / ターゲット) ペアは、LUN/LU に関係なく、手動で設定できます。具体的には、IT を設定することにより、IB 上のストレージを稼働させる前にステー징 エリアを作成できます。詳細については、『Cisco SFS Product Family Command Reference』の `fc srp it` コマンドの説明を参照してください。

IT ペア モードによる持続的なバインディングの設定

VFrame システムを設定する場合には（詳細は、『Cisco VFrame InfiniBand Director User Guide』および『Cisco VFrame InfiniBand Third-Party Integration Guide』を参照）、テスト モードで IT ペアを設定し、SRP ホストを起動する前に持続的な接続をテストできます。

CLI によるテスト モードの設定

CLI を使用してテスト モードを設定する手順は、次のとおりです。

ステップ 1 サーバスイッチにログインします。

`enable` コマンドを入力して、特権 EXEC モードを開始します。

```
SFS> enable
SFS#
```

ステップ 2 `configure terminal` コマンドを入力して、グローバル コンフィギュレーション モードを開始します。

```
SFS# configure terminal
SFS(config)#
```

ステップ 3 `fc srp it` コマンドを入力して、次の内容を指定します。

- イニシエータの GUID
- イニシエータの GUID 拡張名
- ターゲットの WWPN
- test-mode キーワード

テスト モードの IT ペアが設定されます。

```
SFS(config)# fc srp it 00:05:ad:00:00:00:16:ff 00:00:00:00:00:00:00:00
21:00:00:04:cf:86:a0:1f test-mode
```

Element Manager によるテスト モードの設定

Element Manager を使用してテスト モードを設定する手順は、次のとおりです。

ステップ 1 **FibreChannel** メニューをクリックし、**Storage Manager** を選択します。Storage Manager ウィンドウが開きます。

- ステップ 2** SRP Hosts フォルダの横にあるプラス符号 (+) をクリックして、フォルダを展開します。SRP Hosts フォルダの下に、設定済みのイニシエータの一覧が表示されます。
- ステップ 3** 表示したいターゲットに接続しているイニシエータをクリックし、次に **Targets** タブをクリックします。右側のディスプレイに、Targets Visible to This Host テーブルが表示されます。
- ステップ 4** 設定したい IT ペアのエントリをクリックし、次に **Edit** ボタンをクリックします。IT Properties ウィンドウが開きます。
- ステップ 5** Mode フィールドで、**Normal** オプション ボタンまたは **Test** オプション ボタンをクリックします。



(注) モードを設定するには、Current Access フィールドに何も入力されていない必要があります。

ITL の設定

イニシエータがストレージと通信できるようにするには、ITL を設定する必要があります。ITL は、CLI または Element Manager の GUI を使用して設定できます。

- グローバル アトリビュートの設定時にポート アクセスおよび LUN アクセスを制限した場合には、「[Element Manager による ITL の設定 \(グローバル ポリシーの制限を適用した場合\)](#)」(p.5-12) または「[CLI による ITL の設定 \(グローバル ポリシーによる制限を適用した場合\)、オプション 1](#)」(p.5-14) を参照してください。
- アクセスを設定していない場合には、次のセクションの手順を参照してください。



(注)

Fibre Channel コマンドの入力時に「Operation temporarily failed – try again」(処理に一時的に失敗しました。もう一度、試みてください) というエラー メッセージが表示された場合には、ファイバチャネル ゲートウェイの初期化が完了するまで待機してから、再びコマンドを入力してください。

Element Manager による ITL の設定 (グローバル ポリシーの制限を適用していない場合)

ITL を設定する前に、SRP ホストをすべてのストレージからログアウトする必要があります。設定が終了したら、再びログインします。ここで説明する手順は、Linux ホストの例です。

ホストの種類に応じて、ステップ 1 およびステップ 2 の内容を調整してください。

ポート マスキングおよび LUN マスキングのポリシーが制限されていない場合、Linux SRP ホストで ITL を設定する手順は、次のとおりです。

ステップ 1 ホストにログインします。

ステップ 2 `/usr/local/topspin/bin/vstat --verbose|grep -i guid` コマンドを入力して、ホストの GUID を表示します。



(注) GUID の値を書き留めておいてください。以降で、この値を繰り返し入力します。

ステップ 3 次の手順で、サーバスイッチのファイバチャネル ゲートウェイを起動します。

- Element Manager を開始します。
- 起動したいファイバチャネル ゲートウェイ カードをダブルクリックします。Fibre Channel Card ウィンドウが開きます。
- Enable/Disable Card フィールドで、**up** オプション ボタンをクリックし、**Apply** ボタンをクリックします。
- (任意) 追加のゲートウェイについて、この手順を繰り返します。

ファイバチャネル ゲートウェイが、接続されているすべてのストレージを自動的に検出します。



(注) 検出された LU は、SRP ホストがこれらの LU に接続するまでは、グレー表示 (非アクティブ) のままです。ホストが LU に接続すると、アイコンがブルー (アクティブ) に変わります。

- ステップ 4** Element Manager の FibreChannel メニューで、**Storage Manager** を選択します。Topspin Storage Manager ウィンドウが開きます。
- ステップ 5** インターフェイスの左側フレームにある **Storage** ナビゲーション ツリーで、**SRP Hosts** フォルダをクリックします。インターフェイスの右側フレームに、**SRP Hosts** のディスプレイが表示されます。
- ステップ 6** SRP Hosts ディスプレイの **Define New** ボタンをクリックします。Define New SRP Host ウィンドウが表示されます。



(注) ホストに複数の HCA が搭載されている場合には、個々の HCA をイニシエータとして設定する必要があります。ホストの 1 つの HCA を設定しても、ホストの他の HCA は自動的に設定されません。

- ステップ 7** Define New SRP Host ウィンドウの GUID プルダウン メニューから、GUID を選択します。メニューには、接続されていて、まだイニシエータとして設定されていないすべてのホストの GUID が表示されます。
- ステップ 8** (任意) Define New SRP Host ウィンドウの Description フィールドに説明を入力します。
- ステップ 9** **Next >** ボタンをクリックします。Define New SRP Host ウィンドウに、ホストの推奨 WWNN と、既存および潜在的なファイバチャネルゲートウェイポート上でホストを識別するための推奨 WWPN が表示されます。



(注) WWNN または WWPN は手動でも設定できますが、対立を避けるためにデフォルト値を使用することを強く推奨します。

- ステップ 10** **Finish** ボタンをクリックします。SRP Hosts ディスプレイに新規のホストが表示されます。
- ステップ 11** Storage ナビゲーション ツリーで **SRP Hosts** フォルダを展開し、作成したホストをクリックします。インターフェイスの右側フレームに、ホストディスプレイが表示されます。
- ステップ 12** (任意) ホストディスプレイで **LUN Access** タブをクリックし、さらに **Discover LUNs** ボタンをクリックします。Accessible LUNs フィールドに、ファイバチャネルゲートウェイが認識しているターゲットおよび関連 LUN が表示されます。
- ステップ 13** Topspin Storage Manager ウィンドウの **Refresh** ボタンをクリックします。

Element Manager による ITL の設定（グローバル ポリシーの制限を適用した場合）

ITL を設定する前に、SRP ホストをすべてのストレージからログアウトする必要があります。設定が終了したら、再びログインします。ここで説明する手順は、Linux ホストの例です。ホストの種類に応じて、ステップ 1 およびステップ 2 の内容を調整してください。

この手順は、ポートマスク ポリシーおよび LUN マスキング ポリシーの両方の制限を適用している環境で使用します。ポリシー制限が適用されているかどうかを確認するには、CLI で **show fc srp-global** コマンドを入力します。**default-gateway-portmask-policy** および **default-lun-policy** のフィールドを確認してください。いずれかのフィールドに制限が適用されている場合、フィールド出力に **restricted** と表示されます。

ポート マスキングおよび LUN マスキングのポリシーが制限されている場合、Linux SRP ホストで ITL を設定する手順は、次のとおりです。

ステップ 1 ホストにログインします。

ステップ 2 ホスト GUID の CLI に **/usr/local/topspin/bin/vstat --verbose|grep -i guid** コマンドを入力して、ホストの GUID を表示します。



(注) GUID の値を書き留めておいてください。以降で、この値を繰り返し入力します。

ステップ 3 次の手順で、サーバスイッチのファイバチャネル ゲートウェイを起動します。

- a. Element Manager を開始します。
- b. 起動したいファイバチャネルゲートウェイ カードをダブルクリックします。Fibre Channel Card ウィンドウが開きます。
- c. Enable/Disable Card フィールドで、**up** オプション ボタンをクリックし、**Apply** ボタンをクリックします。
- d. (任意) 追加のゲートウェイについて、この手順を繰り返します。

ファイバチャネルゲートウェイが、接続されているすべてのストレージを自動的に検出します。



(注) 検出された LU は、SRP ホストがこれらの LU に接続するまでは、グレー表示（非アクティブ）のままです。ホストが LU に接続すると、アイコンがブルー（アクティブ）に変わります。

ステップ 4 FibreChannel メニューで、**Storage Manager** を選択します。

ステップ 5 インターフェイスの左側フレームにある **Storage** ナビゲーション ツリーで、**SRP Hosts** フォルダをクリックします。インターフェイスの右側フレームに、SRP Hosts のディスプレイが表示されます。

ステップ 6 SRP Hosts ディスプレイの **Define New** ボタンをクリックします。Define New SRP Host ウィンドウが表示されます。



(注) ホストに複数の HCA が搭載されている場合には、個々の HCA をイニシエータとして設定する必要があります。ホストの 1 つの HCA を設定しても、ホストの他の HCA は自動的に設定されません。

- ステップ 7** Define New SRP Host ウィンドウの GUID プルダウン メニューから、GUID を選択します。メニューには、まだイニシエータとして設定されていない、使用可能なすべてのホストの GUID が表示されます。
- ステップ 8** (任意) Define New SRP Host ウィンドウの Description フィールドに説明を入力します。説明を入力しない場合、デバイスによって説明が割り当てられます。
- ステップ 9** **Next >** ボタンをクリックします。Define New SRP Host ウィンドウに、ホストの推奨 WWNN と、既存および潜在的なファイバチャネルゲートウェイポート上でホストを識別するための推奨 WWPN が表示されます。



(注) WWNN または WWPN は手動でも設定できますが、対立を避けるためにデフォルト値を使用することを強く推奨します。

- ステップ 10** **Finish** ボタンをクリックします。SRP Hosts ディスプレイに新規のホストが表示されます。
- ステップ 11** Storage ナビゲーションツリーで **SRP Hosts** フォルダを展開し、作成したホストをクリックします。インターフェイスの右側フレームに、ホストディスプレイが表示されます。
- ステップ 12** ホストディスプレイで **Targets** タブをクリックします。ホストにアクセスを許可するターゲットの WWPN をダブルクリックします。IT Properties ウィンドウが開きます。
- ステップ 13** Port Mask フィールドの横にある 3 つのドット ... 付きのボタンをクリックします。Select Port(s) ウィンドウが開き、シャーシの各スロットについて 2 つのポート番号が表示されます。「押されていない」ポート番号は、制限されているポートを意味します。「押されている」ポート番号は、アクセス可能なポートを意味します。
- ステップ 14** SAN が接続するポートをクリックして「押されている」状態にし、イニシエータにこれらのポートを使用したターゲットへのアクセスを許可します。**OK** ボタンをクリックします。
- ステップ 15** IT Properties ウィンドウの **Apply** ボタンをクリックして、ウィンドウを閉じます。
- ステップ 16** ホストディスプレイで **LUN Access** タブをクリックし、さらに **Discover LUNs** ボタンをクリックします。Available LUNs フィールドに、ファイバチャネルゲートウェイが認識しているターゲットおよび関連 LUN が表示されます。
- ステップ 17** **LUN Access** タブをクリックし、ステップ 12 で設定したターゲットをクリックして、**Add >** ボタンをクリックします。Inactive ITL フォルダの Accessible LUNs フィールドに、ターゲットおよびその LUN が表示されます。
- ステップ 18** ホストからアクセスする LUN をクリックし、**Edit ITL Properties** ボタンをクリックします。ITL Properties ウィンドウが開きます。
- ステップ 19** Port Mask フィールドの横にある 3 つのドット ... 付きのボタンをクリックします。Select Port(s) ウィンドウが開き、シャーシの各スロットの 2 つのポート番号が表示されます。「押されていない」ポート番号は、制限されているポートを意味します。「押されている」ポート番号は、アクセス可能なポートを意味します。
- ステップ 20** SAN が接続するポートをクリックして「押されている」状態にし、イニシエータにこれらのポートを使用したターゲットへのアクセスを許可します。**OK** ボタンをクリックします。

ステップ 21 Topspin Storage Manager ウィンドウの **Refresh** ボタンをクリックします。

CLI による ITL の設定 (グローバル ポリシーによる制限を適用した場合)、オプション 1

Element Manager の GUI を使用しないで ITL を設定する手順は、次のとおりです。

ステップ 1 ホストにログインします。

ステップ 2 ホストの CLI に `/usr/local/topspin/bin/vstat --verbose|grep -i guid` コマンドを入力して、ホストの GUID を表示します。



(注) GUID の値を書き留めておいてください。以降で、この値を繰り返し入力します。

ステップ 3 サーバスイッチの CLI に `no shutdown` コマンドを入力して、デバイスとファイバチャネルストレージを接続するすべてのファイバチャネルゲートウェイを起動します。ゲートウェイにより、すべてのストレージが自動的に検出されます。

```
SFS-3012R# configure terminal
SFS-3012R(config)# card 6
SFS-3012R(config-card-6)# no shutdown
```

ステップ 4 (任意) `show fc srp target` コマンドを入力して、ゲートウェイによって検出されたストレージを表示します。

```
SFS-3012R# show fc srp target

=====
SRP Targets
=====
          wwpn: 21:00:00:04:cf:f6:c2:ab
          wwnn: 20:00:00:04:cf:f6:c2:ab
description: SRP.T10:21000004CFF6C2AB
          ioc-guid: 00:05:ad:00:00:00:15:1a
service-name: SRP.T10:21000004CFF6C2AB
protocol-ids: 04:00:00:00:00:00:00:00:00:00:00
          fc-address: 00:00:ef
              mtu: 0
connection-type: nl-port
physical-access: 6/1
Total: 1 targets.

SFS-3012R#
```

ステップ 5 `fc srp initiator` コマンドを入力して、次の内容を指定します。

- ホストの GUID (ステップ 2 を参照)
- GUID の拡張名 (常に `00:00:00:00:00:00:00:00`)
- `auto-bind` キーワード

ホストが設定されます。



(注) イニシエータをストレージに正常に接続させるには、各物理ファイバチャネルゲートウェイポートに、イニシエータを示す固有の WWPN を持つ仮想ポートが必要です。また、イニシエータには固有の WWNN が必要です。これらの値は手動で設定することもできますが、CLI オプションの利点を活用して、これらの値を動的に割り当てることを強く推奨します。この手順では、WWNN および WWPN を動的に割り当てます。

auto-bind キーワードを指定すると、次の処理が実行されます。

- イニシエータに固有の WWNN が割り当てられます。
- (実ポートおよび潜在ポートになり得る) 各物理ファイバチャネルゲートウェイポートに (イニシエータにマップされる) 仮想ポートが作成され、各仮想ポートに WWPN が割り当てられます。

```
SFS-3012R# configure terminal
SFS-3012R(config)# fc srp initiator 00:05:ad:00:00:01:29:5c 00:00:00:00:00:00:00:00
auto-bind
```



(注) ホストに複数の HCA が搭載されている場合には、個々の HCA をイニシエータとして設定する必要があります。ホストの1つの HCA を設定しても、ホストの他の HCA は自動的に設定されません。

ステップ 6 (任意) **fc srp initiator** コマンドを入力して、次の内容を指定します。

- ホストの GUID
- GUID の拡張名
- **description** キーワード

イニシエータに、簡単に認識できる識別名が割り当てられます。

```
SFS-3012R(config)# fc srp initiator 00:05:ad:00:00:01:29:c5 00:00:00:00:00:00:00:00
description Bender
```

ステップ7 (任意) `show fc srp initiator` コマンドを入力して、新規イニシエータを確認します。

```
SFS-3012R# show fc srp initiator

=====
SRP Initiators
=====
      guid: 00:05:ad:00:00:01:29:c5
      extension: 00:00:00:00:00:00:00:00
      description: Bender
      wwnn: 20:01:00:05:ad:00:40:00
      credit: 0
      active-ports: none
      pkeys:
      action: auto-bind
      result: success
      wwpns: port      wwpn      fc-addr
              2/1      20:01:00:05:ad:20:40:00  00:00:00
              2/2      20:01:00:05:ad:24:40:00  00:00:00
              3/1      20:01:00:05:ad:30:40:00  00:00:00
              3/2      20:01:00:05:ad:34:40:00  00:00:00
              4/1      20:01:00:05:ad:40:40:00  00:00:00
              4/2      20:01:00:05:ad:44:40:00  00:00:00
              5/1      20:01:00:05:ad:50:40:00  00:00:00
              5/2      20:01:00:05:ad:54:40:00  00:00:00
              6/1      20:01:00:05:ad:60:40:00  00:00:02
              6/2      20:01:00:05:ad:64:40:00  00:00:00
              7/1      20:01:00:05:ad:70:40:00  00:00:00
              7/2      20:01:00:05:ad:74:40:00  00:00:00
              8/1      20:01:00:05:ad:80:40:00  00:00:00
              8/2      20:01:00:05:ad:84:40:00  00:00:00
              9/1      20:01:00:05:ad:90:40:00  00:00:00
              9/2      20:01:00:05:ad:94:40:00  00:00:00
              10/1     20:01:00:05:ad:a0:40:00  00:00:00
              10/2     20:01:00:05:ad:a4:40:00  00:00:00
              11/1     20:01:00:05:ad:b0:40:00  00:00:00
              11/2     20:01:00:05:ad:b4:40:00  00:00:00
              12/1     20:01:00:05:ad:c0:40:00  00:00:00
              12/2     20:01:00:05:ad:c4:40:00  00:00:00
              13/1     20:01:00:05:ad:d0:40:00  00:00:00
              13/2     20:01:00:05:ad:d4:40:00  00:00:00
              14/1     20:01:00:05:ad:e0:40:00  00:00:00
              14/2     20:01:00:05:ad:e4:40:00  00:00:00

Total: 1 initiators.

SFS-3012R#
```

ステップ8 `fc srp initiator` コマンドを入力して、次の内容を指定します。

- ホストの GUID
- ホストの GUID 拡張名
- `discover-itl` キーワード

デバイスにより、イニシエータが作成できる潜在的な ITL が検出されます。



(注) このコマンドの実行には時間を要することがあります。

```
SFS-3012R(config)# fc srp initiator 00:05:ad:00:00:01:29:c5 00:00:00:00:00:00:00:00
discover-itl
```


ステップ 9 `show fc srp itl` コマンドを入力して、潜在的な ITL を表示し、`target-wwpn` および `fc-lunid` の値を書き留めます。

```
SFS-3012R(config)# exit
SFS-3012R# show fc srp itl

=====
SRP ITL
=====
                                guid: 00:05:ad:00:00:01:29:c5
                                extension: 00:00:00:00:00:00:00:00
                                target-wwpn: 21:00:00:04:cf:f6:c2:ab
                                fc-lunid: 00:00:00:00:00:00:00:00
                                srp-lunid: 00:00:00:00:00:00:00:00
                                logical-id (raw 64 bytes):
01:03:00:08:20:00:00:04:cf:f6:c2:ab:00:00:00:00
                                :
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
                                :
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
                                :
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
                                logical-id (formatted display): 2000000000000000
                                description: itl
                                device-category: random
                                lun-policy: restricted
                                non-restricted-ports: none
                                active-ports: none
                                physical-access: 6/1
                                hi-mark: 16
                                max-retry: 5
                                min-io-timeout: 10
                                dynamic-path-affinity: false
                                dynamic-gateway-port-loadbalancing: true
                                dynamic-storage-port-loadbalancing:
                                dynamic-gateway-port-failover: false
                                dynamic-storage-port-failover:
                                active-slots: none

Total: 1 itls.

SFS-3012R#
```



(注) `fc-lunid` フィールドには、設定する ITL の LUN ID が表示されます。

ステップ 10 `no fc srp itl` コマンドを入力して、次の内容を指定します。

- ホストの GUID
- ホストの GUID 拡張名
- ターゲットの WWPN (ステップ 9 を参照)
- ストレージディスクの LUN ID (ステップ 9 を参照)
- `lun-policy` キーワード
- `restricted` キーワード

LUN マスキングにより ITL が設定されます。

```
SFS-3012R(config)# no fc srp itl 00:05:ad:00:00:01:29:c5 00:00:00:00:00:00:00:00
21:00:00:04:cf:f6:c2:ab 00:00:00:00:00:00:00:00 lun-policy restricted
```

ステップ 11 `no fc srp it` コマンドを入力して、次の内容を指定します。

- ホストの GUID
- ホストの GUID 拡張名
- ターゲットの WWPN
- **gateway-portmask-policy** キーワード
- **restricted** キーワード
- **all** キーワードまたはマスクを適用しないポート

イニシエータに、ターゲットへのポートマスクポリシー アクセスが許可されます。

```
SFS-3012R(config)# no fc srp it 00:05:ad:00:00:01:29:c5 00:00:00:00:00:00:00:00
21:00:00:04:cf:f6:c2:ab gateway-portmask-policy restricted all
```

ステップ 12 `no fc srp itl` コマンドを入力して、次の内容を指定します。

- ホストの GUID
- ホストの GUID 拡張名
- ターゲットの WWPN
- ストレージディスクの LUN ID
- **gateway-portmask-policy** キーワード
- **restricted** キーワード
- **all** キーワードまたはマスクを適用しないポート

イニシエータに、LUN へのポートマスク ポリシー アクセスが許可されます。

```
SFS-3012R(config)# no fc srp itl 00:05:ad:00:00:01:29:c5 00:00:00:00:00:00:00:00:
21:00:00:04:cf:f6:c2:ab 00:00:00:00:00:00:00:00 gateway-portmask-policy restricted all
```

ステップ 13 ユーザ EXEC モードまたは特権 EXEC モードに戻り、`show fc srp itl` コマンドを入力して、ITL がアクティブであることを確認します。physical-access フィールドおよび active-ports フィールドに、ITL がアクティブであることを示すポート番号が表示されます。

CLI による ITL の設定 (グローバル ポリシーによる制限を適用した場合)、オプション 2

Element Manager の GUI を使用しないで ITL を設定する手順は、次のとおりです。

ステップ 1 ホストにログインします。

ステップ 2 ホストの CLI に `/usr/local/topspin/bin/vstat --verbose|grep -i guid` コマンドを入力して、ホストの GUID を表示します。



(注) GUID の値を書き留めておいてください。以降で、この値を繰り返し入力します。

ステップ 3 サーバスイッチの CLI に **no shutdown** コマンドを入力して、デバイスとファイバチャネルストレージを接続するすべてのファイバチャネルゲートウェイを起動します。ゲートウェイにより、すべてのストレージが自動的に検出されます。

```
SFS-3012R# configure terminal
SFS-3012R(config)# card 6
SFS-3012R(config-card-6)# no shutdown
```

ステップ 4 (任意) **show fc srp target** コマンドを入力して、ゲートウェイによって検出されたストレージを表示します。

```
SFS-3012R# show fc srp target

=====
                        SRP Targets
=====
      wwpn: 21:00:00:04:cf:f6:c2:ab
      wwnn: 20:00:00:04:cf:f6:c2:ab
description: SRP.T10:21000004CFF6C2AB
      ioc-guid: 00:05:ad:00:00:00:15:1a
service-name: SRP.T10:21000004CFF6C2AB
protocol-ids: 04:00:00:00:00:00:00:00
      fc-address: 00:00:ef
              mtu: 0
connection-type: nl-port
physical-access: 6/1
Total: 1 targets.

SFS-3012R#
```

ステップ 5 **fc srp initiator** コマンドを入力して、次の内容を指定します。

- ホストの GUID (ステップ 2 を参照)
- GUID の拡張名 (常に **00:00:00:00:00:00:00**)
- **auto-bind** キーワード

ホストが設定されます。



(注) イニシエータをストレージに正常に接続させるには、各物理ファイバチャネルゲートウェイポートに、イニシエータを示す固有の WWPN を持つ仮想ポートが必要です。また、イニシエータには固有の WWNN が必要です。これらの値は手動で設定することもできますが、CLI オプションの利点を活用して、これらの値を動的に割り当てることを強く推奨します。この手順では、WWNN および WWPN を動的に割り当てます。

auto-bind キーワードを指定すると、次の処理が実行されます。

- イニシエータに固有の WWNN が割り当てられます。
- (実ポートおよび潜在ポートになり得る) 各物理ファイバチャネルゲートウェイポートに (イニシエータにマップされる) 仮想ポートが作成され、各仮想ポートに WWPN が割り当てられます。

```
SFS-3012R# configure terminal
SFS-3012R(config)# fc srp initiator 00:05:ad:00:00:01:29:5c 00:00:00:00:00:00:00
auto-bind
```



(注) ホストに複数の HCA が搭載されている場合には、個々の HCA をイニシエータとして設定する必要があります。ホストの1つの HCA を設定しても、ホストの他の HCA は自動的に設定されません。

ステップ6 (任意) `fc srp initiator` コマンドを入力して、次の内容を指定します。

- ホストの GUID
- GUID の拡張名
- **description** キーワード

イニシエータに、簡単に認識できる識別名が割り当てられます。

```
SFS-3012R(config)# fc srp initiator 00:05:ad:00:00:01:29:c5 00:00:00:00:00:00:00:00
description Bender
```

ステップ7 (任意) `show fc srp initiator` コマンドを入力して、新規イニシエータを確認します。

```
SFS-3012R# show fc srp initiator

=====
SRP Initiators
=====
      guid: 00:05:ad:00:00:01:29:c5
      extension: 00:00:00:00:00:00:00:00
      description: Bender
      wwnn: 20:01:00:05:ad:00:40:00
      credit: 0
      active-ports: none
      pkeys:
      action: auto-bind
      result: success
      wwpns: port      wwpn              fc-addr
              2/1      20:01:00:05:ad:20:40:00  00:00:00
              2/2      20:01:00:05:ad:24:40:00  00:00:00
              3/1      20:01:00:05:ad:30:40:00  00:00:00
              3/2      20:01:00:05:ad:34:40:00  00:00:00
              4/1      20:01:00:05:ad:40:40:00  00:00:00
              4/2      20:01:00:05:ad:44:40:00  00:00:00
              5/1      20:01:00:05:ad:50:40:00  00:00:00
              5/2      20:01:00:05:ad:54:40:00  00:00:00
              6/1      20:01:00:05:ad:60:40:00  00:00:02
              6/2      20:01:00:05:ad:64:40:00  00:00:00
              7/1      20:01:00:05:ad:70:40:00  00:00:00
              7/2      20:01:00:05:ad:74:40:00  00:00:00
              8/1      20:01:00:05:ad:80:40:00  00:00:00
              8/2      20:01:00:05:ad:84:40:00  00:00:00
              9/1      20:01:00:05:ad:90:40:00  00:00:00
              9/2      20:01:00:05:ad:94:40:00  00:00:00
              10/1     20:01:00:05:ad:a0:40:00  00:00:00
              10/2     20:01:00:05:ad:a4:40:00  00:00:00
              11/1     20:01:00:05:ad:b0:40:00  00:00:00
              11/2     20:01:00:05:ad:b4:40:00  00:00:00
              12/1     20:01:00:05:ad:c0:40:00  00:00:00
              12/2     20:01:00:05:ad:c4:40:00  00:00:00
              13/1     20:01:00:05:ad:d0:40:00  00:00:00
              13/2     20:01:00:05:ad:d4:40:00  00:00:00
              14/1     20:01:00:05:ad:e0:40:00  00:00:00
              14/2     20:01:00:05:ad:e4:40:00  00:00:00

Total: 1 initiators.

SFS-3012R#
```

ステップ 8 `no fc srp it` コマンドを入力して、次の内容を指定します。

- ホストの GUID
- ホストの GUID 拡張名
- ターゲットの WWPN
- **gateway-portmask-policy** キーワード
- **restricted** キーワード
- **all** キーワードまたはマスクを適用しないポート

イニシエータに、ターゲットへのポートマスクポリシー アクセスが許可されます。



(注) 次のステップ 9 で検出される ITL は、IT のアトリビュートを継承します。

```
SFS-3012R(config)# no fc srp it 00:05:ad:00:00:01:29:c5 00:00:00:00:00:00:00  
21:00:00:04:cf:f6:c2:ab gateway-portmask-policy restricted all
```

ステップ 9 `fc srp initiator` コマンドを入力して、次の内容を指定します。

- ホストの GUID
- ホストの GUID 拡張名
- **discover-itl** キーワード

デバイスにより、イニシエータが作成できる潜在的な ITL が検出されます。



(注) このコマンドの実行には時間を要することがあります。

```
SFS-3012R(config)# fc srp initiator 00:05:ad:00:00:01:29:c5 00:00:00:00:00:00:00  
discover-itl
```

ステップ 10 `show fc srp itl` コマンドを入力して、潜在的な ITL を表示し、`target-wwpn` および `fc-lunid` の値を書き留めます。

```
SFS-3012R(config)# exit
SFS-3012R# show fc srp itl

=====
SRP ITL
=====
      guid: 00:05:ad:00:00:01:29:c5
      extension: 00:00:00:00:00:00:00:00
      target-wwpn: 21:00:00:04:cf:f6:c2:ab
      fc-lunid: 00:00:00:00:00:00:00:00
      srp-lunid: 00:00:00:00:00:00:00:00
      logical-id (raw 64 bytes):
01:03:00:08:20:00:00:04:cf:f6:c2:ab:00:00:00:00
      :
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
      :
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
      :
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
      logical-id (formatted display): 2000000000000000
      description: itl
      device-category: random
      lun-policy: restricted
      non-restricted-ports: none
      active-ports: none
      physical-access: 6/1
      hi-mark: 16
      max-retry: 5
      min-io-timeout: 10
      dynamic-path-affinity: false
      dynamic-gateway-port-loadbalancing: true
      dynamic-storage-port-loadbalancing:
      dynamic-gateway-port-failover: false
      dynamic-storage-port-failover:
      active-slots: none

Total: 1 itls.

SFS-3012R#
```



(注) `fc-lunid` フィールドには、設定する ITL の LUN ID が表示されます。非シーケンシャル LUN の場合、この値は常に `00:00:00:00:00:00:00:00` として表示されます。シーケンシャル LUN の場合、ターゲットデバイスの各 LUN について 1 回ずつ、値が反復されます。

ステップ 11 `no fc srp itl` コマンドを入力して、次の内容を指定します。

- ホストの GUID
- ホストの GUID 拡張名
- ターゲットの WWPN (ステップ 9 を参照)
- ストレージディスクの LUN ID (ステップ 9 を参照)
- `lun-policy` キーワード
- `restricted` キーワード

LUN マスキングにより ITL が設定されます。

```
SFS-3012R(config)# no fc srp itl 00:05:ad:00:00:01:29:c5 00:00:00:00:00:00:00:00
21:00:00:04:cf:f6:c2:ab 00:00:00:00:00:00:00:00 lun-policy restricted
```

ステップ 12 ユーザ EXEC モードまたは特権 EXEC モードに戻り、**show fc srp itl** コマンドを入力して、ITL がアクティブであることを確認します。physical-access フィールドおよび active-ports フィールドに、ITL がアクティブであることを示すポート番号が表示されます。

カスタム WWNN および WWPN を使用する ITL の設定

SAN に特定の WWNN および WWPN 方式を使用していて、IB ファブリック上のデバイスをこの方式と一致させる場合には、IB ファブリック上のイニシエータの WWNN および WWPN を手動で設定できます。



(注) できるだけ、イニシエータの作成時にオートバインド機能を使用することを強く推奨します。

Element Manager を使用する

Element Manager を使用してカスタム WWNN および WWPN の ITL を設定する手順は、次のとおりです。

ステップ 1 ホストにログインします。

ステップ 2 次の手順で、サーバスイッチのファイバチャネルゲートウェイを起動します。

- a. Element Manager を開始します。
- b. 起動したいファイバチャネルゲートウェイカードをダブルクリックします。Fibre Channel Card ウィンドウが開きます。
- c. **Enable/Disable Card** フィールドで、**up** オプション ボタンをクリックし、**Apply** ボタンをクリックします。
- d. (任意) 追加のゲートウェイについて、この手順を繰り返します。

ファイバチャネルゲートウェイが、接続されているすべてのストレージを自動的に検出します。



(注) 検出された LU は、SRP ホストがこれらの LU に接続するまでは、グレー表示 (非アクティブ) のままです。ホストが LU に接続すると、アイコンがブルー (アクティブ) に変わります。

ステップ 3 FibreChannel メニューで、**Storage Manager** を選択します。Topspin Storage Manager ウィンドウが開きます。

ステップ 4 **SRP Hosts** フォルダをクリックします。ウィンドウに SRP Hosts のディスプレイが表示されます。

ステップ 5 **Define New** ボタンをクリックします。Define New SRP Host ウィンドウが表示されます。



(注) ホストに複数の HCA が搭載されている場合には、個々の HCA をイニシエータとして設定する必要があります。ホストの 1 つの HCA を設定しても、ホストの他の HCA は自動的に設定されません。

- ステップ 6** Host GUID プルダウン メニューからホストの GUID を選択するか、対応するフィールドにホストの GUID を入力します。
- ステップ 7** (任意) Description フィールドにイニシエータの説明を入力します。
- ステップ 8** **Next**> ボタンをクリックします。Define New SRP Host ウィンドウに、推奨 WWNN および推奨 WWPN が表示されます。
- ステップ 9** Host WWNN フィールド内のダイナミックに生成された WWNN を、カスタム WWNN に書き換えます。

**注意**

他のデバイスが同じ WWNN を使用していないことを確認してください。

- ステップ 10** (任意) カスタマイズしたいすべての WWPN を手動で書き換えます。
- ステップ 11** **Finish** ボタンをクリックします。
- ステップ 12** 「Element Manager による ITL の設定 (グローバル ポリシーの制限を適用していない場合)」(p.5-10) または「Element Manager による ITL の設定 (グローバル ポリシーの制限を適用した場合)」(p.5-12) を参照して、この手順を完了します。

CLI を使用する

CLI を使用してカスタム WWNN および WWPN の ITL を設定する手順は、次のとおりです。

- ステップ 1** ホストにログインします。
- ステップ 2** ホストの CLI に `/usr/local/topspin/bin/vstat --verbose|grep -i guid` コマンドを入力して、ホストの GUID を表示します。



(注) GUID の値を書き留めておいてください。以降で、この値を繰り返し入力します。

- ステップ 3** サーバスイッチの CLI に `no shutdown` コマンドを入力して、デバイスとファイバチャネルストレージを接続するすべてのファイバチャネルゲートウェイを起動します。ゲートウェイにより、すべてのストレージが自動的に検出されます。

```
SFS-3012R# configure terminal
SFS-3012R(config)# card 6
SFS-3012R(config-card-6)# no shutdown
```


ステップ4 (任意) `show fc srp target` コマンドを入力して、ゲートウェイによって検出されたストレージを表示します。

```
SFS-3012R# show fc srp target

=====
                        SRP Targets
=====
      wwpn: 21:00:00:04:cf:f6:c2:ab
      wwnn: 20:00:00:04:cf:f6:c2:ab
      description: SRP.T10:21000004CFF6C2AB
      ioc-guid: 00:05:ad:00:00:00:15:1a
      service-name: SRP.T10:21000004CFF6C2AB
      protocol-ids: 04:00:00:00:00:00:00:00:00
      fc-address: 00:00:ef
      mtu: 0
      connection-type: nl-port
      physical-access: 6/1
Total: 1 targets.

SFS-3012R#
```

ステップ5 `fc srp initiator` コマンドを入力して、次の内容を指定します。

- ホストの GUID (ステップ2を参照)
- GUID の拡張名 (常に `00:00:00:00:00:00:00`)
- `wwnn` キーワード
- イニシエータに割り当てたい WWNN

ホストが設定されます。

ステップ6 `fc srp initiator-wwpn` コマンドを入力して、次の内容を指定します。

- ホストの GUID (ステップ2を参照)
- GUID の拡張名 (常に `00:00:00:00:00:00:00`)
- WWPN を追加する物理ファイバチャネルゲートウェイポート (スロット番号/ポート番号形式)
- ポートに追加する WWPN

ファイバチャネルトラフィックを SRP ホストに転送する物理ファイバチャネルゲートウェイポートに WWPN が割り当てられます。

ステップ7 「CLIによるITLの設定(グローバルポリシーによる制限を適用した場合)、オプション1」(p.5-14)を参照して、この手順を完了します。

既存の IT および ITL へのポート アクセスの設定

イニシエータと LUN 間でトラフィックを正常に転送するには、IT および ITL の両方にポート アクセスを設定する必要があります。



(注) IT にポート アクセスを設定しても、関連する ITL には、そのアクセス設定は反映されません。

Element Manager によるポート アクセスの許可

イニシエータに、ファイバチャネル ゲートウェイ ポート経由でのターゲットおよび LUN へのアクセスを許可する手順は、次のとおりです。

- ステップ 1** ホストにログインします。
- ステップ 2** Element Manager を起動して、サーバスイッチに接続します。
- ステップ 3** FibreChannel メニューで、**Storage Manager** を選択します。Storage Manager ウィンドウが開きます。
- ステップ 4** Storage ナビゲーション ツリーで **SRP Hosts** フォルダを展開し、デバイス上のイニシエータを表示します。
- ステップ 5** アクセスを許可または拒否したいホストをクリックします。インターフェイスの右側フレームに、ホスト ディスプレイが表示されます。
- ステップ 6** ホスト ディスプレイで **Targets** タブをクリックします。
- ステップ 7** Targets visible to this host テーブルで、イニシエータにアクセスを許可するターゲットを検索し、テーブル内の対応する行をダブルクリックします。IT Properties ウィンドウが開きます。
- ステップ 8** Port Mask フィールドの横にある「...」ボタンをクリックします。Select Port(s) ウィンドウが開き、シャーシの各スロットのポート番号が表示されます。「押されていない」ポート番号は、制限されているポートを意味します。「押されている」ポート番号は、アクセス可能なポートを意味します。
- ステップ 9** 1 つ以上の「押されていない」ポートをクリックし、イニシエータに、これらのポート経由でのターゲットへのアクセスを許可します。
- ステップ 10** Select Port(s) ウィンドウの **OK** ボタンをクリックし、IT Properties ウィンドウの **Apply** ボタンをクリックして、ウィンドウを閉じます。
- ステップ 11** **LUN Access** タブをクリックします。
- ステップ 12** Accessible LUN フィールドで、ゲートウェイのアイコンと適切なターゲットのアイコンを展開し、イニシエータにアクセスを許可する LUN の LUN アイコンをクリックします。



(注) 現時点でアクセス不能な LUN へのポートマスク アクセスを許可するには、Available LUNs フィールドを使用します。



(注) SRP ホストが接続されていない場合、LUN アイコンはグレー表示されます。

- ステップ 13** **Edit ITL Properties** ボタンをクリックします。ITL Properties ウィンドウが開きます。
- ステップ 14** **Port Mask** フィールドの横にある「...」ボタンをクリックします。**Select Port(s)** ウィンドウが開き、シャーシの各スロットの 2 つのポート番号が表示されます。「押されていない」ポート番号は、制限されているポートを意味します。「押されている」ポート番号は、アクセス可能なポートを意味します。
- ステップ 15** 1 つ以上の「押されていない」ポートをクリックし、イニシエータに、これらのポート経由での LUN へのアクセスを許可します。
- ステップ 16** **Select Port(s)** ウィンドウの **OK** ボタンをクリックし、ITL Properties ウィンドウの **Apply** ボタンをクリックします。

Element Manager によるポート アクセスの拒否

イニシエータに、ファイバチャネル ゲートウェイ ポート経由でのターゲットおよび LUN へのアクセスを拒否する手順は、次のとおりです。

- ステップ 1** ホストにログインします。
- ステップ 2** **Element Manager** を起動して、サーバスイッチに接続します。
- ステップ 3** **FibreChannel** メニューで、**Storage Manager** を選択します。**Storage Manager** ウィンドウが開きます。
- ステップ 4** **Storage** ナビゲーション ツリーで **SRP Hosts** フォルダを展開し、デバイス上のイニシエータを表示します。
- ステップ 5** アクセスを許可または拒否したいホストをクリックします。インターフェイスの右側フレームに、ホスト ディスプレイが表示されます。
- ステップ 6** ホスト ディスプレイで **Targets** タブをクリックします。
- ステップ 7** **Targets visible to this host** テーブルで、イニシエータにアクセスを許可するターゲットを検索し、テーブル内の対応する行をダブルクリックします。**IT Properties** ウィンドウが開きます。
- ステップ 8** **Port Mask** フィールドの横にある 3 つのドット ... 付きのボタンをクリックします。**Select Port(s)** ウィンドウが開き、シャーシの各スロットのポート番号が表示されます。「押されていない」ポート番号は、制限されているポートを意味します。「押されている」ポート番号は、アクセス可能なポートを意味します。
- ステップ 9** 1 つ以上の「押されている」ポートをクリックし、イニシエータに、これらのポート経由でのターゲットへのアクセスを拒否します。

ステップ 10 Select Port(s) ウィンドウの **OK** ボタンをクリックし、IT Properties ウィンドウの **Apply** ボタンをクリックして、ウィンドウを閉じます。

ステップ 11 LUN Access タブをクリックします。

ステップ 12 Accessible LUN フィールドで、ゲートウェイのアイコンと適切なターゲットのアイコンを展開し、イニシエータにアクセスを許可する LUN の LUN アイコンをクリックします。



(注) 現時点でアクセス不能な LUN へのアクセスを許可するには、Available LUNs フィールドを使用します。



(注) SRP ホストが接続されていない場合、LUN アイコンはグレー表示されます。

ステップ 13 Edit ITL Properties ボタンをクリックします。ITL Properties ウィンドウが開きます。

ステップ 14 Port Mask フィールドの横にある 3 つのドット ... 付きのボタンをクリックします。Select Port(s) ウィンドウが開き、シャーシの各スロットの 2 つのポート番号が表示されます。「押されていない」ポート番号は、制限されているポートを意味します。「押されている」ポート番号は、アクセス可能なポートを意味します。

ステップ 15 1 つ以上の「押されている」ポートをクリックし、イニシエータに、これらのポート経由での LUN へのアクセスを拒否します。

ステップ 16 Select Port(s) ウィンドウの **OK** ボタンをクリックし、ITL Properties ウィンドウの **Apply** ボタンをクリックします。

CLI によるポート アクセスの許可

イニシエータに、ターゲット ポート経由での LUN へのファイバチャネル ゲートウェイポート アクセスを許可する手順は、次のとおりです。

ステップ 1 ホストにログインします。

ステップ 2 CLI セッションを開き、ファイバチャネル読み書き権限のあるユーザとしてログインします。権限の詳細については、『Cisco SFS Product Family Command Reference』を参照してください。

```
Login: super
Password: xxxxxx
```

ステップ 3 enable コマンドを入力して、特権 EXEC モードを開始します。

```
SFS-3012R> enable
SFS-3012R#
```

ステップ 4 `configure terminal` コマンドを入力して、グローバル コンフィギュレーション モードを開始します。

```
SFS-3012R# configure terminal
SFS-3012R(config)#
```

ステップ 5 `no fc srp it` コマンドを入力して、次の内容を指定します。

- ホストの GUID
- ホストの GUID 拡張名
- ターゲットの WWPN
- `gateway-portmask-policy` キーワード
- `restricted` キーワード
- `all` キーワードまたはマスクを適用しないポート

イニシエータに、入力したポート経由でのターゲットへのポートマスク ポリシー アクセスが許可されます。

```
SFS-3012R(config)# no fc srp it 00:05:ad:00:00:01:29:c5 00:00:00:00:00:00:00:00
21:00:00:04:cf:f6:c2:ab gateway-portmask-policy restricted all
```

ステップ 6 `no fc srp itl` コマンドを入力して、次の内容を指定します。

- ホストの GUID
- ホストの GUID 拡張名
- ターゲットの WWPN
- ストレージ ディスクの LUN ID
- `gateway-portmask-policy` キーワード
- `restricted` キーワード
- `all` キーワードまたはマスクを適用しないポート

イニシエータに、入力したポート経由での LUN へのポートマスク ポリシー アクセスが許可されます。

```
SFS-3012R(config)# no fc srp itl 00:05:ad:00:00:01:29:c5 00:00:00:00:00:00:00:00:
21:00:00:04:cf:f6:c2:ab 00:00:00:00:00:00:00:00 gateway-portmask-policy restricted all
```

CLI でのポート アクセスの拒否

イニシエータに、ターゲット ポート経由での LUN へのファイバチャネルゲートウェイ ポートアクセスを拒否する手順は、次のとおりです。

ステップ 1 ホストにログインします。

ステップ 2 CLI セッションを開き、ファイバチャネル読み書き権限のあるユーザとしてログインします。権限の詳細については、『*Cisco SFS Product Family Command Reference*』を参照してください。

```
Login: super
Password: xxxxxx
```

ステップ 3 `enable` コマンドを入力して、特権 EXEC モードを開始します。

```
SFS-3012R> enable
SFS-3012R#
```

ステップ 4 `configure terminal` コマンドを入力して、グローバル コンフィギュレーション モードを開始します。

```
SFS-3012R# configure terminal
SFS-3012R(config)#
```

ステップ 5 `fc srp it` コマンドを入力して、次の内容を指定します。

- ホストの GUID
- ホストの GUID 拡張名
- ターゲットの WWPN
- `gateway-portmask-policy` キーワード
- `restricted` キーワード
- `all` キーワードまたはマスクを適用するポート

イニシエータに、入力したポート経由でのターゲットへのポートマスク ポリシー アクセスが拒否されます。

```
SFS-3012R(config)# no fc srp it 00:05:ad:00:00:01:29:c5 00:00:00:00:00:00:00:00:00:00:00:00:04:cf:f6:c2:ab gateway-portmask-policy restricted all
```

ステップ 6 `fc srp itl` コマンドを入力して、次の内容を指定します。

- ホストの GUID
- ホストの GUID 拡張名
- ターゲットの WWPN
- ストレージ ディスクの LUN ID
- `gateway-portmask-policy` キーワード
- `restricted` キーワード
- `all` キーワードまたはマスクを適用するポート

イニシエータに、入力したポート経由での LUN へのポートマスク ポリシー アクセスが拒否されます。

```
SFS-3012R(config)# fc srp itl 00:05:ad:00:00:01:29:c5 00:00:00:00:00:00:00:00:00:00:00:00:04:cf:f6:c2:ab 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00 gateway-portmask-policy restricted all
```

ポートアクセス設定の表示

変更を確認したり、接続の問題のトラブルシューティングを行ったりするには、LUN アクセス設定を表示します。ポートアクセス設定の表示では、イニシエータに LUN へのアクセスを許可するために設定した、サーバスイッチ上のポートが表示されます。

Element Manager でのポートマスク設定の表示

ポートマスク アクセス設定を表示する手順は、次のとおりです。

-
- ステップ 1** Element Manager を起動して、サーバスイッチに接続します。
 - ステップ 2** FibreChannel メニューで、SRP を選択します。SRP ウィンドウが開きます。
 - ステップ 3** ITL タブをクリックします。*GatewayPortMaskPolicy* カラムに、イニシエータが LUN にアクセスできるポートがリストされます。
-

CLI でのポートマスク設定の表示

ポートマスク アクセス設定を表示する手順は、次のとおりです。

-
- ステップ 1** CLI セッションを開いて、ログインします。

```
Login: super
Password: xxxxxx
```

- ステップ 2** `show fc srp itl` コマンドを入力して、次の内容を指定します。

- ポートアクセスを確認するイニシエータの GUID
- イニシエータの GUID の拡張名（常に 00:00:00:00:00:00:00:00）
- LUN を含むターゲットの WWPN
- LUN のファイバチャネル LU ID

■ ポート アクセス設定の表示

イニシエータが LUN にアクセスできるポートが表示されます。イニシエータが LUN に接続できるポートは、**non-restricted-ports** フィールドに表示されます。

```
SFS-3012R# show fc srp itl 00:05:ad:00:00:01:29:c5 00:00:00:00:00:00:00:00
21:00:00:04:cf:f6:c2:ab 00:00:00:00:00:00:00:00
```

```
=====
                                SRP ITL
=====
                                guid: 00:05:ad:00:00:01:29:c5
                                extension: 00:00:00:00:00:00:00:00
                                target-wwpn: 21:00:00:04:cf:f6:c2:ab
                                fc-lunid: 00:00:00:00:00:00:00:00
                                srp-lunid: 00:00:00:00:00:00:00:00
                                logical-id (raw 64 bytes):
01:03:00:08:20:00:00:04:cf:f6:c2:ab:00:00:00:00:00:00
                                :
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
                                :
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
                                :
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
                                logical-id (formatted display): 2000000000000000
                                description: itl
                                device-category: random
                                lun-policy: non restricted
                                non-restricted-ports: 2/1-2/2,3/1-3/2,4/1-4/2,5/1-5/2,
                                                        : 6/1-6/2,7/1-7/2,8/1-8/2,9/1-9/2,
                                                        : 10/1-10/2,11/1-11/2,12/1-12/2,
                                                        : 13/1-13/2,14/1-14/2
                                active-ports: 6/1
                                physical-access: 6/1
                                hi-mark: 16
                                max-retry: 5
                                min-io-timeout: 10
                                dynamic-path-affinity: false
                                dynamic-gateway-port-loadbalancing: true
                                dynamic-storage-port-loadbalancing:
                                dynamic-gateway-port-failover: false
                                dynamic-storage-port-failover:
                                active-slots: none

SFS-3012R#
```


既存 ITL への LUN アクセスの設定

グローバル LUN アクセスを制限した場合、新規 ITL は、その ITL に LUN アクセスを許可するまで、どのストレージにもアクセスできません。グローバル LUN アクセスを許可した場合、イニシエータにすべてのストレージへのアクセスを許可しないのであれば、LUN アクセスを個別に制限する必要があります。

Element Manager による ITL への LUN アクセスの許可

イニシエータに LUN へのアクセスを許可する手順は、次のとおりです。

- ステップ 1** ホストにログインします。
- ステップ 2** Element Manager を起動して、サーバスイッチに接続します。
- ステップ 3** FibreChannel メニューで、**Storage Manager** を選択します。Storage Manager ウィンドウが開きます。
- ステップ 4** Storage ナビゲーション ツリーで **SRP Hosts** フォルダを展開し、デバイス上のイニシエータを表示します。
- ステップ 5** アクセスを許可または拒否したいホストをクリックします。インターフェイスの右側フレームに、ホスト ディスプレイが表示されます。
- ステップ 6** ホスト ディスプレイで **LUN Access** タブをクリックします。
- ステップ 7** Available LUNs フィールドおよび Accessible LUNs フィールドで、展開可能なすべてのアイコンを展開します。
 - サーバ スイッチはイニシエータに対して、Available LUNs フィールドに表示されている LUN へのアクセスを拒否します。
 - サーバ スイッチはイニシエータに対して、Accessible LUNs フィールドに表示されている LUN へのアクセスを許可します。
- ステップ 8** (任意) Available LUNs フィールドの LUN をクリックし、**Add >** ボタンをクリックして、その LUN へのアクセスをイニシエータに許可します。



(注) ターゲット内のすべての LUN へのアクセスをイニシエータに許可するには、ターゲットアイコンをクリックして、**Add >** ボタンをクリックします。**Ctrl** ボタンを押しながら複数のアイコンをクリックし、**Add >** ボタンをクリックすると、選択したすべての項目へのアクセスがイニシエータに許可されます。すべての使用可能な LUN へのアクセスをイニシエータに許可するには、**Add All >>** ボタンをクリックします。

- ステップ 9** **Apply** ボタンをクリックします。

ステップ 10 Topspin Storage Manager ウィンドウの **Refresh** ボタンをクリックします。

Element Manager による ITL への LUN アクセスの拒否

イニシエータに LUN へのアクセスを拒否する手順は、次のとおりです。

ステップ 1 ホストにログインします。

ステップ 2 Element Manager を起動して、サーバスイッチに接続します。

ステップ 3 FibreChannel メニューで、**Storage Manager** を選択します。Storage Manager ウィンドウが開きます。

ステップ 4 Storage ナビゲーション ツリーで **SRP Hosts** フォルダを展開し、デバイス上のイニシエータを表示します。

ステップ 5 アクセスを許可または拒否したいホストをクリックします。インターフェイスの右側フレームに、ホスト ディスプレイが表示されます。

ステップ 6 ホスト ディスプレイで **LUN Access** タブをクリックします。

ステップ 7 Available LUNs フィールドおよび Accessible LUNs フィールドで、展開可能なすべてのアイコンを展開します。

- サーバ スイッチはイニシエータに対して、Available LUNs フィールドに表示されている LUN へのアクセスを拒否します。
- サーバ スイッチはイニシエータに対して、Accessible LUNs フィールドに表示されている LUN へのアクセスを許可します。

Available LUNs フィールドで Inactive ITL フォルダを展開すると、ターゲットのアイコンが表示されます。さらに、ターゲットのアイコンを展開すると、非アクティブ LUN のアイコンが表示されます。**Accessible LUNs** フィールドでゲートウェイのアイコンを展開すると、ターゲットのアイコンが表示されます。さらに、ターゲットのアイコンを展開すると、アクティブ LUN のアイコンと非アクティブ LUN のアイコンが表示されます。

ステップ 8 (任意) Available LUNs フィールドの LUN をクリックし、**Remove >** ボタンをクリックして、イニシエータに、その LUN へのアクセスを拒否します。



(注) イニシエータに、ターゲット内のすべての LUN へのアクセスを拒否するには、ターゲットアイコンをクリックして、**Remove >** ボタンをクリックします。**Ctrl** ボタンを押しながら複数のアイコンをクリックし、**Remove >** ボタンをクリックすると、選択したすべての項目へのアクセスがイニシエータに拒否されます。すべての使用可能な LUN へのアクセスをイニシエータに拒否するには、**Remove All >>** ボタンをクリックします。

ステップ 9 Apply ボタンをクリックします。

ステップ 10 Topspin Storage Manager ウィンドウの **Refresh** ボタンをクリックします。

CLI による ITL への LUN アクセスの許可

イニシエータに LUN へのアクセスを許可する手順は、次のとおりです。

ステップ 1 ホストにログインします。

ステップ 2 CLI セッションを開き、ファイバチャネル読み書き権限のあるユーザとしてログインします。権限の詳細については、『*Cisco SFS Product Family Command Reference*』を参照してください。

```
Login: super
Password: xxxxxx
```

ステップ 3 `enable` コマンドを入力して、特権 EXEC モードを開始します。

```
SFS-3012R> enable
SFS-3012R#
```

ステップ 4 (任意) `show fc srp itl` コマンドを入力して、アクティブおよび非アクティブの ITL を表示し、次の情報を記録します。

- アクセスを許可または拒否するイニシエータの GUID
- イニシエータのアクセスを許可または拒否するターゲットの WWPN
- イニシエータのアクセスを許可または拒否する LUN の fc-lunid

```
SFS-3012R# show fc srp itl
```

```
=====
                               SRP ITL
=====
                               guid: 00:05:ad:00:00:01:29:c5
                               extension: 00:00:00:00:00:00:00:00
                               target-wwpn: 21:00:00:04:cf:f6:c2:ab
                               fc-lunid: 00:00:00:00:00:00:00:00
                               srp-lunid: 00:00:00:00:00:00:00:00
                               logical-id (raw 64 bytes):
01:03:00:08:20:00:00:04:cf:f6:c2:ab:00:00:00:00
                               :
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
                               :
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
                               :
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
                               logical-id (formatted display): 2000000000000000
                               description: itl
                               device-category: random
                               lun-policy: restricted
                               non-restricted-ports: none
                               active-ports: none
                               physical-access: 6/1
                               hi-mark: 16
                               max-retry: 5
                               min-io-timeout: 10
                               dynamic-path-affinity: false
                               dynamic-gateway-port-loadbalancing: true
                               dynamic-storage-port-loadbalancing:
                               dynamic-gateway-port-failover: false
                               dynamic-storage-port-failover:
                               active-slots: none

Total: 1 itls.

SFS-3012R#
```

ステップ 5 `configure terminal` コマンドを入力して、グローバル コンフィギュレーション モードを開始します。

```
SFS-3012R# configure terminal
SFS-3012R(config)#
```

ステップ 6 (任意) `no fc srp itl` コマンドを入力して、次の内容を指定します。

- ホストの GUID
- ホストの GUID の拡張名 (常に `00:00:00:00:00:00:00`)
- ターゲットの WWPN (ステップ 4 を参照)
- ストレージ ディスクの LUN ID (ステップ 4 を参照)
- `lun-policy` キーワード
- `restricted` キーワード

イニシエータに、LUN へのアクセスが許可されます。

```
SFS-3012R(config)# no fc srp itl 00:05:ad:00:00:01:29:c5 00:00:00:00:00:00:00
21:00:00:04:cf:f6:c2:ab 00:00:00:00:00:00:00:00 lun-policy restricted
```

CLI による ITL への LUN アクセスの拒否

イニシエータに LUN へのアクセスを拒否する手順は、次のとおりです。

ステップ 1 ホストにログインします。

CLI セッションを開き、ファイバチャネル読み書き権限のあるユーザとしてログインします。権限の詳細については、『*Cisco SFS Product Family Command Reference*』を参照してください。

```
Login: super
Password: xxxxxx
```

ステップ 2 `enable` コマンドを入力して、特権 EXEC モードを開始します。

```
SFS-3012R> enable
SFS-3012R#
```

ステップ 3 (任意) `show fc srp itl` コマンドを入力して、アクティブおよび非アクティブの ITL を表示し、次の情報を記録します。

- アクセスを許可または拒否するイニシエータの GUID
- イニシエータのアクセスを許可または拒否するターゲットの WWPN
- イニシエータのアクセスを許可または拒否する LUN の fc-lunid

```

SFS-3012R# show fc srp itl

=====
                        SRP ITL
=====
                        guid: 00:05:ad:00:00:01:29:c5
                        extension: 00:00:00:00:00:00:00:00
                        target-wwpn: 21:00:00:04:cf:f6:c2:ab
                        fc-lunid: 00:00:00:00:00:00:00:00
                        srp-lunid: 00:00:00:00:00:00:00:00
                        logical-id (raw 64 bytes):
01:03:00:08:20:00:00:04:cf:f6:c2:ab:00:00:00:00:00:00
                        :
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
                        :
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
                        :
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
                        logical-id (formatted display): 200000000000000000
                        description: itl
                        device-category: random
                        lun-policy: restricted
                        non-restricted-ports: none
                        active-ports: none
                        physical-access: 6/1
                        hi-mark: 16
                        max-retry: 5
                        min-io-timeout: 10
                        dynamic-path-affinity: false
                        dynamic-gateway-port-loadbalancing: true
                        dynamic-storage-port-loadbalancing:
                        dynamic-gateway-port-failover: false
                        dynamic-storage-port-failover:
                        active-slots: none

Total: 1 itls.

SFS-3012R#

```

ステップ 4 `configure terminal` コマンドを入力して、グローバル コンフィギュレーション モードを開始します。

```

SFS-3012R# configure terminal
SFS-3012R(config)#

```

ステップ 5 (任意) `fc srp itl` コマンドを入力して、次の内容を指定します。

- ホストの GUID
- ホストの GUID の拡張名 (常に `00:00:00:00:00:00:00:00`)
- ターゲットの WWPN (ステップ 4 を参照)
- ストレージ ディスクの LUN ID (ステップ 4 を参照)
- `lun-policy` キーワード
- `restricted` キーワード

イニシエータに、LUN へのアクセスが拒否されます。

```

SFS-3012R(config)# fc srp itl 00:05:ad:00:00:01:29:c5 00:00:00:00:00:00:00:00
21:00:00:04:cf:f6:c2:ab 00:00:00:00:00:00:00:00 lun-policy restricted

```

LUN アクセス設定の表示

変更を確認したり、接続の問題のトラブルシューティングを行ったりするには、LUN アクセス設定を表示します。LUN アクセス設定の表示では、LUN へのアクセスがイニシエータに許可されているかどうかが表示されます。

Element Manager による LUN アクセスの表示

LUN アクセス設定を表示する手順は、次のとおりです。

-
- ステップ 1** Element Manager を起動して、サーバスイッチに接続します。
 - ステップ 2** FibreChannel メニューで、**Storage Manager** を選択します。Storage Manager ウィンドウが開きます。
 - ステップ 3** Storage ナビゲーション ツリーで **SRP Hosts** フォルダを展開し、デバイス上のイニシエータを表示します。
 - ステップ 4** LUN アクセスを表示したいホストをクリックします。インターフェイスの右側フレームに、ホストディスプレイが表示されます。
 - ステップ 5** **LUN Access** タブをクリックし、**Accessible LUNs** フィールド内のアイコンを展開します。イニシエータは、**Accessible LUNs** フィールド内の LUN にアクセスできます。イニシエータは、**Available LUNs** フィールド内の LUN にはアクセスできません。
-

CLI による LUN アクセスの表示

LUN アクセス設定を表示する手順は、次のとおりです。

-
- ステップ 1** CLI セッションを開いて、ログインします。

```
Login: super
Password: xxxxxx
```

- ステップ 2** `show fc srp itl` コマンドを入力して、次の内容を指定します。

- LUN アクセスを確認するイニシエータの GUID
- イニシエータの GUID の拡張名（常に 00:00:00:00:00:00:00:00）
- LUN を含むターゲットの WWPN
- LUN のファイバチャネル LU ID

イニシエータと LUN 間のアクセスが表示されます。イニシエータがアクセス可能な LUN は、**lun-policy** フィールドに表示されます。

```
SFS-3012R# show fc srp itl 00:05:ad:00:00:01:29:c5 00:00:00:00:00:00:00:00
21:00:00:04:cf:f6:c2:ab 00:00:00:00:00:00:00:00
```

```
=====
                        SRP ITL
=====
                        guid: 00:05:ad:00:00:01:29:c5
                        extension: 00:00:00:00:00:00:00:00
                        target-wwpn: 21:00:00:04:cf:f6:c2:ab
                        fc-lunid: 00:00:00:00:00:00:00:00
                        srp-lunid: 00:00:00:00:00:00:00:00
                        logical-id (raw 64 bytes):
01:03:00:08:20:00:00:04:cf:f6:c2:ab:00:00:00:00:00
:
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
:
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
:
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
                        logical-id (formatted display): 2000000000000000
                        description: itl
                        device-category: random
                        lun-policy: non restricted
                        non-restricted-ports: 2/1-2/2,3/1-3/2,4/1-4/2,5/1-5/2,
: 6/1-6/2,7/1-7/2,8/1-8/2,9/1-9/2,
: 10/1-10/2,11/1-11/2,12/1-12/2,
: 13/1-13/2,14/1-14/2
                        active-ports: 6/1
                        physical-access: 6/1
                        hi-mark: 16
                        max-retry: 5
                        min-io-timeout: 10
                        dynamic-path-affinity: false
                        dynamic-gateway-port-loadbalancing: true
                        dynamic-storage-port-loadbalancing:
                        dynamic-gateway-port-failover: false
                        dynamic-storage-port-failover:
                        active-slots: none

SFS-3012R#
```

個々の ITL アトリビュートの設定

グローバルに設定できる ITL アトリビュート（「[グローバルアトリビュートの設定](#)」 [p.3-2] を参照）はすべて、ITL の作成後に個別に設定して、ITL をカスタマイズすることができます。

ITL I/O ハイ マークの設定

ストレージ デバイスのパフォーマンスに応じて、ITL I/O ハイ マークを設定します。

Element Manager を使用する

このアトリビュートを設定する手順は、次のとおりです。

-
- ステップ 1** Element Manager を起動して、サーバ スイッチに接続します。
 - ステップ 2** FibreChannel メニューで、**Storage Manager** を選択します。Storage Manager ウィンドウが開きます。
 - ステップ 3** **Logical Units** フォルダを展開し、設定する LUN をクリックします。
 - ステップ 4** High Mark フィールドに、1 ~ 256 の整数値を入力し、**Apply** ボタンをクリックします。
-

CLI を使用する

このアトリビュートを設定する手順は、次のとおりです。

-
- ステップ 1** CLI セッションを開き、ファイバチャネル読み書き権限のあるユーザとしてログインします。権限の詳細については、『*Cisco SFS Product Family Command Reference*』を参照してください。

```
Login: super
Password: xxxxxx
```

- ステップ 2** **enable** コマンドを入力して、特権 EXEC モードを開始します。

```
SFS-3012R> enable
SFS-3012R#
```

- ステップ 3** **configure terminal** コマンドを入力して、グローバル コンフィギュレーション モードを開始します。

```
SFS-3012R# configure terminal
SFS-3012R(config)#
```

- ステップ 4** **fc srp lu** コマンドを入力して、次の内容を指定します。

- 設定する LU の論理 ID
- **io-hi-mark** キーワード
- 適用する値

ステップ 3 **configure terminal** コマンドを入力して、グローバル コンフィギュレーションモードを開始します。

```
SFS-3012R# configure terminal
SFS-3012R(config)#
```

ステップ 4 **fc srp lu** コマンドを入力して、次の内容を指定します。

- 設定する LUN の論理 ID
- **dynamic-gateway-port-loadbalancing** キーワード

ダイナミック ロード バランシングがイネーブルに設定され、フェールオーバーとパス アフィニティがディセーブルになります。

```
SFS-3012R(config)# fc srp lu
0103000820000004cf86a01f0000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000 dynamic-gateway-port-loadbalancing
```

ダイナミック フェールオーバーの設定

ダイナミック フェールオーバーを設定すると、ゲートウェイ上の一方のポートを休止し、他方のポートに障害が発生したときにトラフィックを引き継がせることができます。

Element Manager を使用する

このアトリビュートを設定する手順は、次のとおりです。

ステップ 1 Element Manager を起動して、サーバスイッチに接続します。

ステップ 2 FibreChannel メニューで、**Storage Manager** を選択します。Storage Manager ウィンドウが開きます。

ステップ 3 **Logical Units** フォルダを展開し、設定する LUN をクリックします。

ステップ 4 Dynamic Pathing フィールドで、**Gateway Port Failover** オプション ボタンをクリックし、**Apply** ボタンをクリックします。

CLI を使用する

このアトリビュートを設定する手順は、次のとおりです。

ステップ 1 CLI セッションを開き、ファイバチャネル読み書き権限のあるユーザとしてログインします。権限の詳細については、『*Cisco SFS Product Family Command Reference*』を参照してください。

```
Login: super
Password: xxxxxx
```


CLI を使用する

このアトリビュートを設定する手順は、次のとおりです。

- ステップ 1** CLI セッションを開き、ファイバチャネル読み書き権限のあるユーザとしてログインします。権限の詳細については、『*Cisco SFS Product Family Command Reference*』を参照してください。

```
Login: super
Password: xxxxxx
```

- ステップ 2** `enable` コマンドを入力して、特権 EXEC モードを開始します。

```
SFS-3012R> enable
SFS-3012R#
```

- ステップ 3** `configure terminal` コマンドを入力して、グローバル コンフィギュレーション モードを開始します。

```
SFS-3012R# configure terminal
SFS-3012R(config)#
```

- ステップ 4** `fc srp itl` コマンドを入力して、次の内容を指定します。

- 設定する ITL のイニシエータの GUID
- GUID の拡張名 (常に `00:00:00:00:00:00:00:00`)
- 設定する ITL のターゲットの WWPN
- 設定する ITL のファイバチャネル LU ID (LUN)
- `description` キーワード
- 引用符で囲んだ ASCII テキストによる説明

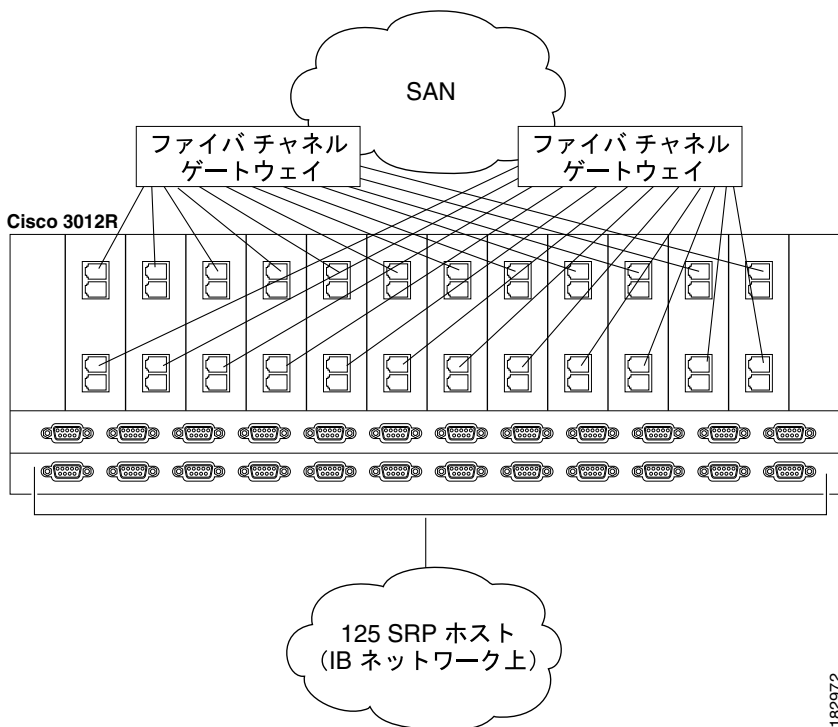
ITL にテキスト識別名が割り当てられます。

```
SFS-3012R(config)# fc srp itl 00:05:ad:00:00:01:29:c5 00:00:00:00:00:00:00:00
21:00:00:04:cf:f6:c2:ab 00:00:00:00:00:00:00:00 description "my-ITL"
SFS-3012R(config)#
```

ゲートウェイ グルーピング

ゲートウェイ グルーピングにより、SRP ホストおよびファイバチャネル ゲートウェイのログインによるファイバチャネル スイッチの過負荷を防止できます。特定のファイバチャネル スイッチでは、SAN に接続させたい SRP ホスト数を処理できないことがあります。

図 5-1 ハイ ノードカウント システム



この例では、1 台の Cisco SFS 3012R サーバスイッチにより、125 の InfiniBand SRP ホストがファイバチャネル SAN に接続します。ゲートウェイ グルーピングを使用しない場合、各 SRP ホストが、各ファイバチャネルゲートウェイ ポートを経由して SAN にログインします。この場合、Cisco SFS 3012R サーバスイッチが接続する各ファイバチャネル エッジスイッチは、1500 の同時ファイバチャネル ログインを受信する可能性があります。SAN 全体では、最大 3000 の同時ログインを受信することになります。

潜在的な同時ログイン数をファイバチャネル スイッチがサポートできる値に制限するには、ゲートウェイ グルーピングを開始する必要があります。ゲートウェイをグルーピングするには、イニシエータに WWPN を手動で設定してオートバインドを回避し、イニシエータを SAN にアクセスさせるゲートウェイだけに WWPN を設定する必要があります。以降のセクションで、オートバインドとゲートウェイ グルーピングを比較します。

オートバインドによる WWPN の過負荷

推奨する **auto-bind** キーワードを使用してイニシエータを設定した場合、ファイバチャネル ゲートウェイは、SRP ホストからストレージまでのすべての可能な物理ルートに対して、WWPN をダイナミックに作成します。その結果、複数のファイバチャネル ゲートウェイが SAN に接続している場合、SRP ホストにすべてのゲートウェイへのアクセスを許可するかどうかに関係なく、各 SRP ホストはゲートウェイのポートごとに WWPN を受信します。

ゲートウェイ グルーピングによる WWPN の制限

WWPN を手動で設定する (**auto-bind** キーワードを使用しない) 場合には、各 SRP ホストに、使用したいファイバチャネルゲートウェイに対応する WWPN だけを設定します。その結果、特定の SRP ホストは、設定されたファイバチャネルゲートウェイだけを使用してログインするので、フェブリック全体のログイン数を制限できます。

CLI による手動設定



(注) Element Manager では、WWPN を手動で割り当てることはできません。

WWPN を手動で設定する手順は、次のとおりです。

ステップ 1 「ITL の設定」(p.5-10) に記載されている ITL の設定を開始し、**auto-bind** キーワードを使用した **fc srp initiator** コマンドの手前までを実行します。

ステップ 2 **fc srp initiator** コマンドを入力して、次の内容を指定します。

- ホストの GUID
- ホストの GUID 拡張名
- **wwnn** キーワード
- SRP ホストに割り当てる WWNN

SRP ホストに WWNN が割り当てられます。

```
SFS-3012R(config)# fc srp initiator 00:05:ad:00:00:00:17:17 00:00:00:00:00:00:00:00
wwnn 20:03:00:05:ad:01:1a:5c
```

ステップ 3 **fc srp initiator-wwpn** コマンドを入力して、次の内容を指定します。

- WWPN を割り当てる SRP ホストの GUID
- SRP ホストの GUID 拡張名
- この WWPN を割り当てるゲートウェイ ポートのスロット番号 / ポート番号
- ポートに割り当てる WWPN

ファイバチャネルゲートウェイ ポートにより、仮想ポートに WWPN が割り当てられます。

```
SFS-3012R(config)# fc srp initiator-wwpn 00:05:ad:00:00:00:17:17
00:00:00:00:00:00:00:00 5/1 20:04:00:05:ad:51:1a:5c
SFS-3012R(config)# fc srp initiator-wwpn 00:05:ad:00:00:00:17:17
00:00:00:00:00:00:00:00 5/2 20:04:00:05:ad:55:1a:5c
```

ステップ 4 「ITL の設定」(p.5-10) に記載されている ITL 設定を続行します。

■ ゲートウェイ グループ