CHAPTER 5

# SAN スイッチングの問題のトラブルシューティング

Storage Area Network（SAN; ストレージ エリア ネットワーク）は、サーバ用のデータ ストレージを提供するストレージ デバイスのネットワークです。

この章では、SAN と Cisco Nexus 5000 シリーズ スイッチで起こり得る問題を特定し、解決する方法について説明します。

この章で説明する内容は、次のとおりです。



## 概要

ストレージ ネットワークの問題で最もよく見られる症状は次の 2 つです。

- ホストから、ホストに割り当てられたストレージにアクセスできない。
- アプリケーションが、割り当てられたストレージにアクセスしようとした後、応答しない。

次の項目を確認することで、実施する手順と詳細な調査が必要なコンポーネントを特定できます。これらの項目はホスト、スイッチ、またはサブシステムのベンダーに依存しません。

次の項目を確認して、インストールのステータスを判別します。

- 新たにインストールしたシステムであるか、既存のシステムであるかを確認します（新しい SAN、ホスト、またはサブシステムであるか、既存のホストにエクスポートされた新しい LUN であるか）。
- これまでホストがそのストレージを認識していたかどうかを確認します。
- ホストがサブシステム内のいずれかの LUN を認識しているかどうかを確認します。
- 既存のアプリケーションの問題（遅い、遅延が長い、応答時間が極端に長い）を解決しようとしているのか、最近出現した問題であるかを確認します。
- アプリケーションで問題が発生する直前に、設定またはインフラストラクチャ全体にどのような変更を加えたかを確認します。

# 一般的な SAN のトラブルシューティング手順

**ステップ 1**　ファブリック内の問題に関する情報を収集します。

**ステップ 2**　スイッチとエンド デバイス間の物理接続を確認します。

**ステップ 3**　すべての SAN 要素についてファブリックへの登録を確認します。

**ステップ 4**　エンド デバイス（ストレージ サブシステムおよびサーバ）の設定を確認します。

**ステップ 5**　エンドツーエンドの接続とファブリックの設定を確認します。

# NPV

## NPV エッジ スイッチの NP アップリンク ポートが初期化ステートでスタックしている

コア NPIV スイッチに接続された NP アップリンク ポートがオンラインにならず、初期化ステートでスタックしています。

**考えられる原因**

コア スイッチで NPIV がイネーブルになっていない可能性があります。

例：

```
switch(config-if)# sh int fc2/2
fc2/2 is down (Initializing)
Hardware is Fibre Channel, SFP is short wave laser w/o OFC (SN)
Port WWN is 20:42:00:0d:ec:a4:3b:80
Admin port mode is NP, trunk mode is on
```

**解決方法**

- NPV 外部インターフェイスのステータスを確認します。
  コア スイッチで NPIV がイネーブルになっているかどうかを確認します。

  例：

  ```
  switch(config-if)# sh npv status
  npiv is disabled
  disruptive load balancing is disabled
  External Interfaces:
  ====================
  Interface: fc2/1, State: Failed(NPIV is not enabled in upstream switch)
  Interface: fc2/2, State: Failed(NPIV is not enabled in upstream switch)
  Interface: san-port-channel 200, State: Down
  ```

- NPIV がディセーブルの場合は、コア スイッチで NPIV をイネーブルにします。

  例：

  ```
  switch(config)# feature npiv
  ```

# サーバ インターフェイスがアップせず、「NPV upstream port not available」メッセージが表示される

NPV エッジ スイッチに接続されたサーバ ポートがオンラインにならず、show interface コマンドを実行すると「NPV upstream port not available」のステータスが表示されます。

考えられる原因

NPV エッジ スイッチ上のアップストリーム NP_Port とダウンストリーム サーバ F_Port が同じ VSAN に属していない可能性があります。

例：

```
switch# sh int fc2/7
fc2/7 is down (NPV upstream port not available)
Hardware is Fibre Channel, SFP is short wave laser w/o OFC (SN)
Port WWN is 20:47:00:0d:ec:a4:3b:80
Admin port mode is F, trunk mode is off
snmp link state traps are enabled
Port vsan is 99
Receive data field Size is 2112
```

解決方法

- アップストリーム ポートとサーバ ポートの VSAN メンバーシップを確認します。

  例：

  ```
  switch# show vsan membership
  vsan 1 interfaces:
  fc2/1 fc2/2 fc2/3 fc2/4
  fc2/5 fc2/6 san-port-channel 200
  vsan 99 interfaces:
  fc2/7 fc2/8
  ```

- 上の例では、アップストリーム ポート（fc2/1-2）は VSAN 1 に属し、サーバ ポート（fc2/7-8）は VSAN 99 に属しています。
  NPV エッジ上の NP ポートと NPIV コア上の F ポートをサーバ ポートと同じ VSAN に移動します。

  例：

  ```
  switch(config)# vsan database
  switch(config-vsan-db)# vsan 99 interface fc2/1-2
  switch(config-if)# vsan database
  switch(config-vsan-db)# vsan 99 interface fc1/17-18
  Traffic on fc1/17 may be impacted. Do you want to continue? (y/n) y
  Traffic on fc1/18 may be impacted. Do you want to continue? (y/n) y
  ```

（注）　あるいは、NPIV コア スイッチと NPV エッジ スイッチが F_Port トランキングに対応したスイッチである場合は、それが推奨されるコンフィギュレーションです。

# NPV NP ポート間の不均等なロード バランシング

同じ VSAN のメンバーである NP アップストリーム ポートを調べると、ロード バランシングが不均等になっています。

考えられる原因

これは通常の状態で、N5000 Dee Why 4.2(1)N1 リリースよりも前のリリースで提供されているデフォルトの SID/DID ロード バランシングの直接の結果である可能性があります。

解決方法

アップストリーム スイッチが 4.1(3) 以上のコードを実行している MDS スイッチであり、なおかつ NPV F_Port トランキングに対応したスイッチである場合、推奨されるコンフィギュレーションは F_Port トランキング ポート チャネリング機能を実行することです。

例（NPIV コア）：

```
pod3-9222i(config)# feature npiv
pod3-9222i(config)# feature fport-channel-trunk

pod3-9222i(config)# interface port-channel 1
pod3-9222i(config-if)# switchport mode f
pod3-9222i(config-if)# switchport trunk mode on
pod3-9222i(config-if)# channel mode active
pod3-9222i(config-if)# interface fc2/13, fc2/19
pod3-9222i(config-if)# switchport mode f
pod3-9222i(config-if)# switchport rate-mode dedicated
pod3-9222i(config-if)# switchport trunk mode on
pod3-9222i(config-if)# channel-group 1 force
```

この例では、fc2/13 と fc2/19 がポートチャネル 100 に追加され、ディセーブルになります。ポートチャネルの相手側のスイッチでも同じ操作を行い、両方で「no shutdown」を実行して両インターフェイスを起動します。

例：

```
pod3-9222i(config-if)# no shut
```

例（NPV エッジ）：

```
pod7-5020-51(config)# interface san-port-channel 1
pod7-5020-51(config-if)# switchport mode np
pod7-5020-51(config-if)# switchport trunk mode on
pod7-5020-51(config-if)# interface fc2/1-2
pod7-5020-51(config-if)# switchport mode np
pod7-5020-51(config-if)# switchport trunk mode on
pod7-5020-51(config-if)# channel-group 1
```

この例では、fc2/1 と fc2/2 がポートチャネル 1 に追加され、ディセーブルになります。ポートチャネルの相手側のスイッチでも同じ操作を行い、両方で「no shutdown」を実行して両インターフェイスを起動します。

例：

```
pod7-5020-51(config-if)# no shut
```

# ダウンストリーム NPV エッジ スイッチ上のサーバがファブリックにログインしない

ダウンストリーム NPV エッジ スイッチに接続されたサーバがファブリックにログインしません。

考えられる原因

ダウンストリーム NPV エッジ スイッチ上のサーバがファブリックにログインしないか、「waiting for FLOGI」メッセージが表示されます（両方が起こる場合もあります）。

例：

```
switch# show npv status
npiv is enabled
Server Interfaces:
==================
Interface: fc1/6, VSAN: 1, NPIV: No, State: Waiting for FLOGI
```

解決方法

- NPV エッジ スイッチとコア スイッチの両方の設定を確認します。F_Port トランキング機能を実行していない場合は、VSAN の不一致がないこと、およびサーバ ポート、NPV NP ポート、NPIV コア F_Port、ストレージ ポートがすべて同じ VSAN に属していてオンラインになっていることを確認します。
- 設定が正しい場合は、問題の所在を突き止めるために Ethanalyzer トレースを収集して、Fabric Login（FLOGI）フレームが受信されていること、Fabric Discovery（FDISC）コマンドとして NPIV コアに送信されていることを確認できます。

  Ethanalyzer トレースの例：

  ```
  switch# ethanalyzer local sniff-interface inbound-hi display-filter "!llc && !stp"
  limit-captured-frames 0 write bootflash:npv-trace
  Capturing on eth4
  ```

- NPV に接続されたサーバ ポートをフラップすることにより、問題を再現します。トレースがブートフラッシュに書き込まれるので、その内容を次のコマンドを使用してスイッチから別の場所にコピーします。

  ```
  copy bootflash: ftp:
  ```

- トレースをコピーしたら、Wireshark を使用してトレースを開き、フローを検証します。

  通常の NPV ログイン フローの例：

```
Server --------------------> FLOGI ----------> NPV Edge Switch  Fabric Login frame =
                                                                FLOGI

NPV Edge Switch ------> FDISC ----------> NPIV Core Switch      Fabric DISCovery
                                                                frame maps parameters
                                                                from Server FLOGI
```

```
NPV Core Switch ------> Accept ---------> NPV Edge Switch       NPIV Core assigns an
                                                                FCID with the Accept
                                                                to the FDISC from NPV
                                                                Edge Switch

NPV Edge Switch ------> Accept ---------> Server                Accept to original
                                                                Server FLOGI with FCID
                                                                assigned from NPIV
                                                                Core Switch
```

# サーバが物理的に接続されている正確なポートの特定

NPIV スイッチからは、ダウンストリーム NPV 接続サーバが接続されている物理ポートはわかりません。次の手順を使用して、その物理ポートを特定できます。

考えられる原因

NPIV コア スイッチに複数のダウンストリーム NPV エッジ スイッチが接続されている場合、サーバが物理的に接続されている正確なポートを特定するには、次の手順を実行します。

解決方法

- サーバの PWWN と、それに対応するサーバの接続先スイッチを特定します。

  例：

  ```
  NPIV-Core(config-if)# show flogi database

  fc1/16 100 0xee00e4 21:00:00:04:cf:17:66:b7 20:00:00:04:cf:17:66:b7
  fc1/16 100 0xee00e8 21:00:00:04:cf:17:66:0e 20:00:00:04:cf:17:66:0e
  fc1/25 100 0xee0100 20:41:00:0d:ec:a3:da:40 20:64:00:0d:ec:a3:da:41
  fc1/26 100 0xee0200 20:42:00:0d:ec:a3:da:40 20:64:00:0d:ec:a3:da:41
  fc1/26 100 0xee0201 21:00:00:c0:dd:12:04:f3 20:00:00:c0:dd:12:04:f3
  ```

  この例では、サーバは次の行によって特定されます。

  ```
  fc1/26 100 0xee0201 21:00:00:c0:dd:12:04:f3 20:00:00:c0:dd:12:04:f3
  ```

  スイッチは次の行によって特定されます。

  ```
  fc1/26 100 0xee0200 20:42:00:0d:ec:a3:da:40 20:64:00:0d:ec:a3:da:41
  ```

- NPV エッジ スイッチの IP アドレスを特定します。

  例：

  ```
  NPIV-Core(config-if)# sh fcns database npv
  VSAN 100:

  20:64:00:0d:ec:a3:da:41 172.18.217.51 fc2/1 20:00:00:0d:ec:51:0c:00 fc1/25
  20:64:00:0d:ec:a3:da:41 172.18.217.51 fc2/2 20:00:00:0d:ec:51:0c:00 fc1/26
  ```

- NPV エッジ スイッチに telnet します。

  例：

  ```
  NPIV-Core(config-if)# telnet 172.18.217.51
  ```

- サーバの PWWN を特定します。

  例：

```
switch-NPV-Edge# show npv flogi-table

vfc3 100 0xee0201 21:00:00:c0:dd:12:04:f3 20:00:00:c0:dd:12:04:f3 fc2/2
```

- 上の例に示すようにインターフェイスが FCoE（VFC）インターフェイスである場合は、show interface vfc3 コマンドを使用して、VFC の物理的な宛先ポートを確認します。

# 4.2(1)N1 F_Port トランキング機能を設定した後、VSAN が初期化ステートでスタックしている

F_Port トランキング ポート チャネル、またはポート チャネルのトランキング メンバーに対して show interface コマンドを実行すると、特定の VSAN が初期化ステートにあり、オンラインになっていません。

考えられる原因

4.2(1)N1 F_Port トランキング機能を設定した後、トランク ポート上の VSAN が初期化ステートでスタックしているように見えます。

例：

```
switch(config-if)# sh int fc2/1
fc2/1 is trunking
Hardware is Fibre Channel, SFP is short wave laser w/o OFC (SN)
Port WWN is 20:41:00:0d:ec:a4:3b:80
Admin port mode is NP, trunk mode is on
snmp link state traps are enabled
Port mode is TNP
Port vsan is 1
Speed is 4 Gbps
Transmit B2B Credit is 16
Receive B2B Credit is 16
Receive data field Size is 2112
Beacon is turned off
Belongs to san-port-channel 200
Trunk vsans (admin allowed and active) (1,99,200)
Trunk vsans (up) (1,99)
Trunk vsans (isolated) ()
Trunk vsans (initializing) (200)
```

Fabric Manager の [Trunk Failures] タブでも、トランク VSAN がリスト表示される場合があります。ただし、これは通常の状態である可能性があります。ある特定の VSAN にダウンストリーム デバイスが 1 つもログインしていない場合、その VSAN は初期化ステートにとどまります。

解決方法

次のコマンドを使用して、問題の VSAN にログインしているデバイスがあるかどうかを確認します。

例：

```
switch# show npv flogi-table

fc2/7 99 0xba0002 10:00:00:00:00:02:00:00 10:00:00:00:00:00:02:00 Spo200
fc2/8 99 0xba0003 10:00:00:00:00:01:00:00 10:00:00:00:00:00:01:00 Spo200
Total number of flogi = 2.
```

上の例では、VSAN 200 にログインしているデバイスはありません。

# ゾーン分割

## ゾーンセットをアクティブにできず、拡張ゾーン分割モードでゾーン分割を設定できない

ゾーンセットをアクティブにできず、拡張ゾーン分割モードでゾーン分割を設定できません。エラーメッセージ「Zoning database update in progress, command rejected」を受け取る場合があります。

考えられる原因

同じスイッチ上または別のスイッチ上の別のユーザが拡張ゾーン分割設定のロックを保持しています。

解決方法

一般的な方法は、ゾーン分割ロックを解放することです。

**ステップ 1**　ロックを保持しているスイッチ（ドメイン /IP アドレス）を特定します。

**ステップ 2**　そのスイッチ上のロックを保持しているユーザを特定します。

**ステップ 3**　そのスイッチ上のそのユーザのロックをクリアします。

- 同じスイッチで「show zone status vsan <vsan-id>」コマンドを実行して、ロックを保持しているユーザを特定します。

  例：

  ```
  switch1# show zone status vsan 200
  VSAN: 200 default-zone: deny distribute: active only Interop: default
  mode: enhanced merge-control: allow
  session: remote [dom: 121][ip: 171.165.98.20] <<==
  ```

  この例では、IP アドレスが 171.165.98.20 のリモート スイッチがロックを保持しています。

- リモート スイッチに接続し、コマンド「show zone status vsan」を実行します。

  例：

  ```
  switch2# show zone status vsan 200

  VSAN: 200 default-zone: deny distribute: active only Interop: default
  mode: enhanced merge-control: allow
  session: cli [remi] <<==
  ```

  この例では、ユーザ「Remi」が拡張ゾーン分割のロックを保持しています。

- リモート スイッチ（上の例では N5K2）で、コマンド「no zone commit vsan <vsan-id>」を使用してロックを解放します。
- ロックがクリアされたことを確認するには、コマンド「show zone status vsan <vsan-id>」を実行します。

  この時点で、session パラメータは「none」と表示されます。

- ロックがまだ残っている場合は、コマンド「clear zone lock」を使用して、ロックを保持しているスイッチからロックを解除します。
- それでもロックが残っている場合は、次のコマンドを使用して、詳細な分析に役立つ情報を収集します。

```
show zone internal vsan <vsan-id>
show zone status vsan <vsan-id>
show fcdomain domain-list vsan <vsan-id>
show users
show tech-support zone
show tech-support device-alias
show logging
```

# ホストがストレージと通信できない

SAN の初期導入時または SAN のトポロジ変更後に、一部のホストがストレージと通信できない場合があります。イニシエータが、ストレージ アレイ内のそれらのホスト用に割り当てられた LUN にアクセスできません。

考えられる原因

ホストとストレージが 2 つの異なるスイッチに接続している場合は、ISL リンク、つまり両方のスイッチに接続している xE ポートが分離されている可能性があります。

特定の VSAN 内で xE ポートが分離される原因としては、次が考えられます。

- ファブリック タイマーの設定ミス
- ポート パラメータの設定ミス
- ゾーン分割の不一致

解決方法

TE ポートでの VSAN 分離を解決する方法は次のとおりです。

- TE ポートで「show interface fc slot/port」コマンドを使用して、VSAN 番号を確認します。

  分離された VSAN の番号は、ホストおよびストレージが接続している VSAN の番号と一致している必要があります。

  コマンド出力で、「Trunk vsans (isolated) (Vsan <vsan-id>)」を確認します。
- 「show port internal info interface fc slot/port」コマンドを使用して、VSAN 分離の根本原因を突き止めます。

考えられる原因

ホストとストレージが同じ VSAN に属していません。

解決方法

- 「show vsan membership」コマンドを使用して、ホストとストレージの両方が同じ VSAN に属しているかどうかを確認します。
- ホストとストレージが異なる VSAN に属している場合は、コンフィギュレーション モードでコマンド「vsan database」と「vsan vsan-id interface fc slot/port」を使用して、ホストおよびストレージ デバイスに接続されたインターフェイスを同じ VSAN に移動します。

考えられる原因

ホストとストレージが同じゾーンに属していません。ゾーンがアクティブ ゾーンセットに含まれていません。アクティブ ゾーンセットが存在せず、デフォルトのゾーン ポリシーが拒否に設定されています。

解決方法

- コマンド「show zone status vsan-id」を使用して、デフォルトのゾーン ポリシーが拒否に設定されているかどうかを確認します。

例：

```
switch# show zone status
VSAN: 1 default-zone: deny distribute: active only Interop: default
mode: basic merge-control: allow
session: none
```

ステート「default zone policy permit」は、どのノードからも他のすべてのノードが見えることを意味します。deny は、明示的にゾーンに配置されていないノードはすべて分離されることを意味します。

ゾーン分割を使用していない場合は、「zone default-zone permit」を使用してデフォルトのゾーン ポリシーを変更できますが、これはベスト プラクティスではありません。

- ホストとストレージに対してコマンド「show zone member」を使用して、両者が同じゾーンに属しているかどうかを確認します。同じゾーンに属していない場合は、コマンド「zone name zonename vsan-id」を使用して、その VSAN 内にゾーンを作成します。

  例：

  ```
  switch(config)# zone name testzone vsan 100
  switch(config-zone)# member pwwn 21:00:00:20:37:9e:02:3e
  switch(config-zone)# member pwwn 21:00:00:c0:dd:12:04:ce
  ```

  コマンド「show zone vsan vsan-id」を使用して、ホストとストレージが同じゾーンに配置されたことを確認します。

- コマンド「show zoneset active vsan vsan-id」を使用して、アクティブ ゾーンセットの名前を確認します。

  ホストとストレージを含むゾーンがアクティブ ゾーンセットに含まれていない場合は、コンフィギュレーション モードでコマンド「zoneset name」を使用してゾーンセット サブ モードに入り、「member」コマンドを使用してゾーンをアクティブ ゾーンセットに追加します。

  例：

  ```
  switch(config)#zoneset name testzoneset vsan 100
  switch(config-zoneset)#member testzone
  ```

- 「zoneset activate」コマンドを使用して、ゾーンセットをアクティブにします。

  例：

  ```
  switch(config)# zoneset activate testzoneset vsan 100
  ```

# 2 つのスイッチが E または TE ポートを使用して接続しているときにゾーン結合が失敗する

2 つのスイッチが E または TE ポートを使用して接続しているとき、ゾーン結合が失敗する場合があります。

「show logging」ログに表示される場合があるログ メッセージの例を次に示します。

例：

```
%ZONE-2-ZS_MERGE_FAILED: %$VSAN 1%$ Zone merge failure, isolating interface fc2/1 error:
Received rjt from adjacent switch:[reason:0]
%ZONE-2-ZS_MERGE_FAILED: %$VSAN 1%$ Zone merge failure, isolating interface fc1/2 error:
Member mismatch
%ZONE-2-ZS_MERGE_ADJ_NO_RESPONSE: Adjacent switch not responding,isolating interface
%ZONE-2-ZS_MERGE_FULL_DATABASE_MISMATCH: Zone merge full database mismatch on interface
```

考えられる原因

2 つのスイッチが同じゾーンセット名とゾーン名を持っているにもかかわらず、それらのゾーン メンバーが異なっている可能性があります。

スイッチ ファブリックを結合するときは、両方のアクティブ ゾーン セットに含まれるゾーンの名前が重複していないか、同じ名前を持つゾーンが正確に同じメンバーを持つ必要があります。これらの条件がどちらも満たされない場合、2 つのファブリックを接続する E ポートは分離した状態になります。

スイッチ ファブリックを結合するプロセスは次のとおりです。

- ソフトウェアがプロトコル バージョンを比較します。プロトコル バージョンが異なる場合、ISL は分離されます。
- プロトコル バージョンが同じである場合、ゾーン ポリシーが比較されます。ゾーン ポリシーが異なる場合、ISL は分離されます。
- ゾーン結合オプションが同じである場合、結合制御設定に基づいて比較が行われます。
  - 設定が「制限」の場合、アクティブ ゾーン セットとフル ゾーン セットが同じである必要があります。これらが同じでない場合、リンクは分離されます。
  - 設定が「許可」の場合、結合ルールを使用して結合が行われます。ホストとストレージが同じゾーンに属していません。ゾーンがアクティブ ゾーンセットに含まれていません。アクティブ ゾーンセットが存在せず、デフォルトのゾーン ポリシーが「拒否」に設定されています。

解決方法

ゾーン結合が失敗した場合、この問題は次のいずれかの方法を使用して解決できます。

- 両方のゾーンセットのゾーン メンバーが一致するよう修正し、競合を解消します。
  - 両方のスイッチで「show zoneset active vsan vsan-id」コマンドを使用して、ゾーンと各ゾーンのメンバーを比較します。
  - いずれかのゾーンのメンバーシップを変更して、同じ名前を持つ他のゾーンに合わせます。
- いずれかのスイッチでゾーンセットを非アクティブにし、ゾーン結合プロセスをもう一度行います。
  - 「no zoneset activate name zonesetname vsan-id」コマンドを使用して、いずれかのスイッチのゾーンセット設定を非アクティブにします。
  - 「show zoneset active」コマンドを使用して、ゾーンセットが削除されたことを確認します。
  - 「shutdown」コマンドを使用して結合するゾーンへの接続をシャットダウンしてから、「no shutdown」コマンドを使用して結合するゾーンへの接続を再びアクティブにします。
  - 「show zoneset active vsan-id」を使用してすべてのメンバーが正しいことを確認し、「show interface fc slot/port」を使用して VSAN が分離されていないことを確認します。
- スイッチ間でゾーンセットを明示的にインポートまたはエクスポートして、両スイッチを同期します。
  - 「zoneset import interface interface-number vsan vsan-id」コマンドまたは「zoneset export interface interface-number vsan vsan-id」コマンドを使用して、いずれかのスイッチでアクティブ ゾーンセットを上書きします。
  - 「show interface fc slot/port」を使用して、この中断操作の後に VSAN が分離されていないことを確認します。

# ゾーンセットのアクティブ化の失敗

ゾーンセットのアクティブ化が失敗したとき、「show logging」ログに表示される場合があるログ メッセージの例を次に示します。

例：

```
ZONE-2-ZS_CHANGE_ACTIVATION_FAILED: Activation failed.
ZONE-2-ZS_CHANGE_ACTIVATION_FAILED_RESN: Activation failed : reason
```

**考えられる原因**

ゾーン データベースのサイズが 2048 KB を超えているときに新しいスイッチがファブリックに加入した場合、ゾーンセットのアクティブ化が失敗することがあります。

**解決方法**

- 「show zone analysis active vsan vsan-id」コマンドを使用して、アクティブ ゾーンセット データベースを分析します。フォーマット サイズが 2048 KB を超えていないかどうかを確認します。

  2048 KB の上限を超えている場合は、ゾーンまたはゾーン内のデバイスをいくつか削除する必要があります。

  例：

  ```
  switch# show zone analysis active vsan 100
  Zoning database analysis vsan 100
  Active zoneset: vsm_vem_v100_zs [-]
  Activated at: 13:13:44 UTC May 27 2010
  Activated by: Merge [ Interface san-port-channel 100 ]
  Default zone policy: Deny
  Number of devices zoned in vsan: 1/9 (Unzoned: 8)
  Number of zone members resolved: 1/3 (Unresolved: 2)
  Num zones: 1
  Number of IVR zones: 0
  Number of IPS zones: 0
  Formatted size: 92 bytes / 2048 Kb
  ```

- 「show zone internal change event-history vsan vsan-id」コマンドを使用して、ゾーンセット アクティブ化の問題があるかどうかを確認します。
- この問題をさらにトラブルシューティングするには、「show tech-support zone」コマンドと「show logging log」コマンドの出力をキャプチャします。

# 2 つのスイッチ間でのフル ゾーン データベース同期の失敗

2 つのスイッチが E または TE ポートを使用して接続していて、それらのスイッチが異なるゾーンセット配信ポリシーを持つとき、フル ゾーン データベース同期が失敗する場合があります。ファブリックの分離/結合の結果として、あるファブリックの実行コンフィギュレーションにフル ゾーンセット データベースが含まれないことがあります。

**考えられる原因**

ゾーンセットの配信は、隣接スイッチへの結合要求の送信時、またはゾーンセットのアクティブ化の際に行われます。

ゾーン配信ポリシーは 2 つのスイッチで異なるように設定できますが、そうすると同期が失敗する場合があります。

**解決方法**

「show zone status」コマンドを使用して、両方のスイッチの配信ポリシーを確認します。

例：

```
VSAN: 100 default-zone: deny distribute: active only Interop: default
mode: basic merge-control: allow
```

配信ポリシーが「active only」に設定されている場合は、アクティブ ゾーンセットが配信されます。また、配信ポリシーがフルに設定されていることも確認します。

コンフィギュレーション モードで VSAN ごとにすべてのスイッチへのフル ゾーン セットおよびアクティブ ゾーン セットの配信をイネーブルにするには、「zoneset distribute full vsan vsan-id」コマンドを使用します。

# VSAN 内のスイッチのデフォルト ゾーン ポリシーの不一致が原因で、ストレージへのアクセス時に予期しない結果が起こる

基本ゾーン モードで VSAN 内のすべてのスイッチのデフォルト ゾーン ポリシーが一致していない場合、ホストがストレージにアクセスするときに予期しない結果が起こる場合があります。

考えられる原因

デフォルト ゾーン ポリシーが「permit」に設定されていて、VSAN にアクティブ ゾーンセットがない場合は、その VSAN のどのメンバーからも他のすべてのノードが見えます。

解決方法

1 つの方法は、ゾーン運用モードを基本から拡張に移行することです。拡張ゾーン分割では、ゾーン設定が VSAN 内のすべてのスイッチ間で同期されます。これにより、デフォルト ゾーン ポリシーが一致しない可能性はなくなります。

- 「show zone status」コマンドを使用して、ゾーンのステータスを表示します。

  ```
  VSAN: 300 default-zone: deny distribute: active only Interop: default
  mode: basic merge-control: allow
  ```

- 「zone default-zone」コマンドを使用してデフォルト ゾーン ポリシーを設定し、「zone mode enhanced vsan-id」コマンドを使用して運用モードを拡張ゾーン分割モードに設定します。

解決方法

もう 1 つの方法を次に示します。

- VSAN 内のすべてのスイッチで「show zone status」を使用して、運用モードとデフォルトゾーン ポリシーを確認します。
- 「zone mode basic」コマンドを使用して、基本モードでないスイッチをすべて変更します。
- VSAN 内の各スイッチで「zone default-zone」コマンドを使用して、同じデフォルト ゾーン ポリシーを設定します。

# SAN PortChannel

## スイッチを SAN PortChannel 経由で接続しようとするとファイバ チャネル ポートがダウンする

スイッチを SAN PortChannel 経由で接続しようとすると、ファイバ チャネル ポートがダウンします。

「show interface brief」コマンドを実行すると、次のように出力されます。

```
fc slot/port is down (Error disabled - Possible port channel misconfiguration)
```

考えられる原因

コンフィギュレーションでいずれかの SAN ポートチャネル互換性パラメータの設定が間違っています。

互換性チェックでは、チャネルのすべての物理ポートで同一のパラメータ設定が確実に使用されるようにします。そうでない場合、ポートが PortChannel に所属できません。互換性チェックは、ポートを PortChannel に追加する前に実施します。

互換性チェックでは、PortChannel の両側で次のパラメータと設定が一致していることを確認します。

- 機能パラメータ
  (インターフェイスのタイプ、両側ともギガビット イーサネットまたは両側ともファイバ チャネル)。
- 管理互換性パラメータ
  (速度、モード、レート モード、ポート VSAN、許可 VSAN リスト、ポート セキュリティ)。
- 動作パラメータ
  (リモート スイッチ WWN とトランキング モード)。

解決方法

- 「show san-port-channel compatibility-parameters」を使用して、コンフィギュレーションでチェックするパラメータを確認します。

  一般に、コンフィギュレーションを修正して FC ポートを shut/no shut した場合、ポートは正常に回復します。

- 別のエラー メッセージが表示されて問題が解決しない場合は、次のいずれか、または複数のコマンドを実行してさらにデバッグします。

```
show port internal info interface fc slot/port
show port internal event-history interface fc slot/port
show san-port-channel internal event-history errors
show logging log | grep fc slot/port
show san-port-channel internal event-history all
show tech-support detail > bootflash:showtechdet
```

## 新しく追加したファイバチャネル インターフェイスが SAN PortChannel でオンラインにならない

新しいファイバチャネル インターフェイスを追加したとき、そのインターフェイスが SAN PortChannel でオンラインになりません。

設定操作時に次のエラー メッセージが表示される場合があります。

「`Command failed: port not compatible [reason]`」

考えられる原因

ポート チャネル モードが「on」に設定されています。

スイッチ間の不整合な状態を防ぐため、およびスイッチ間の整合性を維持するためにデフォルトの ON モードを使用した場合、ポートはシャットダウンします。

解決方法

「no shutdown」を使用して、ポートを再び明示的にイネーブルにします。

考えられる原因

インターフェイス パラメータが既存の SAN PortChannel と互換性がありません。

解決方法

force オプションを使用して、物理インターフェイスに SAN PortChannel のパラメータを受け入れるよう強制します。インターフェイス サブ コンフィギュレーション モードで、「channel-group <channel-group number> force」コマンドを使用します。

# トランキングを設定できない

インターフェイス コンフィギュレーション モードでトランキングを設定できません。

CLI 出力に次のエラー メッセージが表示される場合があります。

```
「error:invalid switchport config」
```

考えられる原因

トランキング プロトコルがディセーブルになっています。

解決方法

「trunk protocol enable CLI」コマンドを使用して、トランキングをイネーブルにします。

# VSAN トラフィックがトランクを通過しない

VSAN トラフィックがトランクを通過できません。

ホストから、同じ VSAN に属していて、なおかつ TE ポートを使用して 2 つの異なるスイッチに接続されたターゲットにアクセスできません。VSAN トラフィックがトランクを通過できません。ホストからターゲットへのパスによっては、パフォーマンスが低下する場合や、どのディスクにもアクセスできない場合があります。

考えられる原因

VSAN が allowed-active VSAN リストに登録されていません。

解決方法

「switchport trunk allowed vsan CLI」コマンドを使用して、VSAN を allowed-active リストに追加します。

# SAN PortChannel のインターフェイスの下にある特定の VSAN で xE ポートが分離される

SAN PortChannel のインターフェイスの下にある特定の VSAN で xE ポートが分離されます。

ロギング ログに次のエラー メッセージが表示される場合があります。

「%$VSAN <VSAN#>%$ Interface port-channel <channel #>, vsan <vsan #> is down (isolation due to [cause])」

考えられる原因

特定の VSAN 内で xE ポートが分離される原因としては、次が考えられます。

- ファブリック タイマーの設定ミス
- ポート パラメータの設定ミス
- ゾーン分割の不一致

解決方法

TE ポートでの VSAN 分離を解決するには、TE ポートで「show interface fc slot/port」コマンドを使用して VSAN 番号を確認します。分離された VSAN の番号は、ホストおよびストレージが接続している VSAN の番号と一致している必要があります。

コマンドの出力で、「Trunk vsans (isolated) (Vsan <number>)」のような情報を探します。

「show port internal info interface san-port-channel <number>」コマンドを使用して、VSAN 分離の原因を突き止めます。

# SAN ポートチャネル インターフェイスが作成できない

SAN ポートチャネル インターフェイスが作成できません。

コンフィギュレーション モード時に次のエラー メッセージが表示される場合があります。

「failed to create port-channel channel-id:」

考えられる原因

ユーザは次のメッセージを受け取ります。

failed to create port-channel channel-id: all port-channels have been created [max channel number reached]

（注）　SAN ポートチャネルは最大 4 つ作成できます（NX-OS 4.2(1)N1(1) を含む）。これはソフトウェアの制限です。

解決方法

特定の番号を持つ SAN ポートチャネルを作成する場合に、4 つの SAN ポートチャネルがすでに設定されているときは、使用頻度の低いいずれかの SAN ポートチャネルを削除する必要があります。「no interface san-port-channel x」コマンドを使用して、いずれかの SAN ポートチャネルを削除します。

考えられる原因

ユーザは次のメッセージを受け取ります。

Channel group X is already an Ethernet port channel

解決方法

SAN ポートチャネルを設定する際に 1 ～ 256 の範囲の別の番号を選択する必要があります。

「show port-channel usage」コマンドを使用して、既存のポートチャネルで使用されている番号を確認します。

例：

```
show port-channel usage
Total 3 port-channel numbers used
========================================
Used : 198 - 199 , 500
Unused: 1 - 197 , 200 - 499 , 501 - 4096
(some numbers may be in use by SAN port channels)
```

# FC サービス

ここでは、シスコ ファイバ チャネル サービスのトラブルシューティングの概要を示し、一般的な問題とその解決方法について説明します。

## 概要

ファイバ チャネル ファブリックは、そのクライアント（ファイバ チャネル ノード）に対して一連のサービスを提供します。各ノードはこれらのファイバ チャネル サービス（FC サービス）を使用してストレージ ネットワークとやり取りし、接続ステート、接続パラメータ、設定、トポロジ変更などの情報を交換します。

FC サービスには、Well Known Address（WKA; well-known アドレス）を持つポートへのログインを通じてアクセスできます。WKA は、ファブリックの内部使用（通常はファブリック サービス）のために予約されているポート FC ID です。

次の表に、well-known アドレスと各アドレスに関連するサービスを示します。
（出典：www.t11.org）

| well-known アドレス | 説明 |
|---|---|
| x'FF FC 01'<br>～ x'FF FC FE' | ドメイン コントローラのために予約済み |
| x'FF FF F0' | N_Port コントローラのために予約済み |
| x'FF FF F1'<br>～ x'FF FF F3' | 予備 |
| x'FF FF F4' | イベント サービス（FC-GS-5） |
| x'FF FF F5' | マルチキャスト サーバ（FC-PH3） |
| x'FF FF F6' | クロック同期サーバ（FC-PH3） |
| x'FF FF F7' | セキュリティ キー配信サービス（FC-PH3） |
| x'FF FF F8' | エイリアス サーバ（FC-PH2） |
| x'FF FF F9' | Quality of Service Facilitator-Class4（FC-PH2） |
| x'FF FF FA' | 管理サービス（FC-GS-5） |
| x'FF FF FB' | タイム サービス（FC-GS-5） |

| well-known アドレス | 説明 |
|---|---|
| x'FF FF FC' | ディレクトリ サービス（FC-GS-5） |
| x'FF FF FD' | ファブリック コントローラ |
| x'FF FF FE' | F_Port コントローラ |
| x'FF FF FF' | ブロードキャスト アドレス / サーバ |

# ファイバ チャネル ポートが初期化ステートにとどまる

ファイバ チャネル F タイプ ポートがオンラインにならず、初期化ステートでスタックしています。

「show interface fc slot/port」コマンドを実行すると、次のように出力されます。

```
fc slot/port is down (Initializing)
```

ファイバ チャネル ポートは、リンク レベル初期化が正常に完了した後、初期化ステートに入ります。F タイプ ポートでは、次のステップは FLOGI（ファブリック ログイン）プロセスを完了することです。ポートは FLOGI プロセスが完了するまで初期化ステートにとどまります。

**考えられる原因**

リンク パートナーがバイパス モードになったことが原因で、ポートがアップしています。

**解決方法**

「show hardware internal fc-mac <slot-number> port <port-number> statistics」コマンドを使用して、リンク初期化が正常に完了した後に Class-3 入力カウンタが増加しているかどうかを確認します。

例：

```
switch# show hardware internal fc-mac 2 port 1 statistics
 ADDRESS     STAT                                                  COUNT
_________ ________                                          ____________________
0x0000003c FCP_CNTR_MAC_RX_LOSS_OF_SYNC                                    0x1
0x0000003d FCP_CNTR_MAC_RX_BAD_WORDS_FROM_DECODER                         0x50
0x00000042 FCP_CNTR_MAC_CREDIT_IG_XG_MUX_SEND_RRDY_REQ                   0x152
0x00000043 FCP_CNTR_MAC_CREDIT_EG_DEC_RRDY                                0x7c
0x00000061 FCP_CNTR_MAC_DATA_RX_CLASS3_FRAMES                            0x130
0x00000062 FCP_CNTR_MAC_DATA_RX_CLASSF_FRAMES                             0x22
0x00000069 FCP_CNTR_MAC_DATA_RX_CLASS3_WORDS                           0x61c98
0x0000006a FCP_CNTR_MAC_DATA_RX_CLASSF_WORDS                             0xff0
0x00000065 FCP_CNTR_MAC_DATA_TX_CLASS3_FRAMES                             0x52
0x00000066 FCP_CNTR_MAC_DATA_TX_CLASSF_FRAMES                             0x2a
0x0000006d FCP_CNTR_MAC_DATA_TX_CLASS3_WORDS                           0x944c
0x0000006e FCP_CNTR_MAC_DATA_TX_CLASSF_WORDS                           0xec4
0xffffffff FCP_CNTR_LINK_RESET_IN                                          0x1
0xffffffff FCP_CNTR_OLS_IN                                                 0x1
0xffffffff FCP_CNTR_NOS_IN                                                 0x1
0xffffffff FCP_CNTR_LRR_IN                                                 0x2
0xffffffff FCP_CNTR_LINK_RESET_OUT                                         0x1
0xffffffff FCP_CNTR_OLS_OUT                                                0xa
0xffffffff FCP_CNTR_NOS_OUT                                                0x2
0xffffffff FCP_CNTR_LRR_OUT                                                0xb
0xffffffff FCP_CNTR_LINK_FAILURE                                           0x2
```

**考えられる原因**

FLOGI パケットが、FC-MAC から FLOGI サーバまでのデータ パス上のどこかでドロップされました。

**解決方法**

次の方法を検討します。

- 「show hardware internal fc-mac <slot-number> port <port-number> statistics」コマンドを使用して、Class-3 パケットのカウンタを確認します。
- 「show flogi internal all interface fc slot/port」コマンドの出力を分析し、パス上のどこで FLOGI パケットのドロップが起こり得るかを調べます。
- 「Fport server fault-injection」テーブルをチェックし、「Invalid」、「Drop」の FLOGI パケットがないかどうかを確認します。
- 「shut」CLI コマンド、「no shut」コマンドの順に入力して、FC スロット/ポートをいったんディセーブルにしてからイネーブルにします。
- これで問題が解決しない場合は、同じ FC モジュールの別のポートまたは他の FC モジュールのポートに接続を移動してみます。
- それでも問題が解決しない場合は、次のコマンドを使用して、詳細な分析に役立つ情報を収集します。

```
Show tech-support flogi
Show logging log | grep  fc slot/port
show port internal info interface fc slot/port
show port internal event-history interface fc slot/port
show tech-support detail > bootflash:showtechdet
show platform fwm info pif fc slot/port {find the gatos instance for the port}
show platform fwm info gatos-errors 13 {check for the non-zero counters for drops}
```

次のコマンドを使用して、debug flogi をキャプチャします。

```
switch# debug logfile flogi_debug
switch# debug flogi all
switch(config)# int fc slot/port
switch(config-if)# shut
switch(config-if)# no shut
switch(config-if)# undebug all
switch# dir log:  {check if you have the file in log: directory}
         31     Aug 03 13:45:13 2010  dmesg
      34941     Aug 06 07:21:15 2010  flogi_debug

switch# copy log:flogi_debug ftp://x.y.z.w {or use tftp/scp/sftp}
```

# 特定の VSAN トラフィックが SAN ファブリック経由でルーティングされない

VSAN の実装では、設定された各 VSAN がそれぞれ異なるファブリック サービスのセットをサポートできます。そのようなサービスの 1 つに FSPF ルーティング プロトコルがあります。このプロトコルは VSAN ごとに個別に設定できます。不適切なトラフィック エンジニアリング機能が使用されている場合、特定の VSAN トラフィックがルーティングされないことがあります。

考えられる原因

FSPF hello 間隔が適切に設定されていません。

「show logging」ログに表示される場合があるログ メッセージの例を次に示します。

例：

```
FSPF-3-HELLO_MISMATCH: %$VSAN <vsan-id>%$ Mismatch in Hello timer in the Hello packet on
interface san-port-channel <channel-id>
%FSPF-3-FC2_PROC_ERR: %$VSAN <vsan-id>%$ Error in processing HELLO  packet on interface
san-port-channel <channel-id>, Error  = Bad packet received
```

解決方法

NX-OS CLI を使用して ISL 上の不適切な hello 間隔を解決するには、次の手順を実行します。

**ステップ 1**　「debug fspf all」コマンドを使用して不適切な hello 間隔のメッセージを探すか、「show logging」ログの最後のメッセージをチェックしてエラー メッセージを探します。

デバッグ出力では、次のメッセージが生成されます。

```
fspf: Wrong hello interval for packet on interface 40000c7 in VSAN 200
fspf: Error in processing hello packet , error = Bad packet received
```

**ステップ 2**　「undebug all」コマンドを使用して、デバッグをオフにします。

**ヒント**　ヒント：いずれかのデバッグ コマンドを入力する前に、telnet または SSH セッションをもう 1 つ開きます。デバッグ出力で現在のセッションがあふれた場合は、2 番目のセッションを使用して「undebug all」コマンドを入力し、デバッグ メッセージの出力を停止します。

**ステップ 3**　「show fspf vsan <vsan-id> interface」コマンドを使用して、両方のスイッチで FSPF の設定を表示します。

例：

```
switch# show fspf vsan 200 interface port-channel 200
FSPF interface port-channel 200 in VSAN 200
FSPF routing administrative state is active
Interface cost is 125
Timer intervals configured, Hello 40 s, Dead 80 s, Retransmit 5 s
FSPF State is INIT
Statistics counters :
   Number of packets received : LSU  3  LSA  3  Hello 136  Error packets 3
   Number of packets transmitted : LSU  3  LSA  3  Hello 182  Retransmitted LSU  0
   Number of times inactivity timer expired for the interface = 0


switch# show fspf vsan 200 interface san-port-channel 200
FSPF interface san-port-channel 200 in VSAN 200
FSPF routing administrative state is active
Interface cost is 125
Timer intervals configured, Hello 20 s, Dead 80 s, Retransmit 5 s
FSPF State is INIT

Statistics counters :
   Number of packets received : LSU  3  LSA  3  Hello 185  Error packets 169
   Number of packets transmitted : LSU  3  LSA  3  Hello 139  Retransmitted LSU  0
   Number of times inactivity timer expired for the interface = 24
```

**（注）**　この例では、

- 最初のスイッチでは、Hello タイマーがデフォルト（20 秒）に設定されていません。ネイバー スイッチ（Nexus 5000）の設定を確認して設定値を合わせます。
- FSPF が FULL ステートではありません。これは問題があることを示します。

**ステップ 4**　インターフェイス コンフィギュレーション モードで、両方のスイッチの fspf hello-interval が同じ値になるように変更します。

例：

```
switch(config)# interface san-port-channel 200
switch(config-if)# fspf hello-interval 40 vsan 200
```

**ステップ 5**　変更後、FSPF が FULL ステートになったことを確認します。

```
switch(config-if)# show fspf vsan 200 interface san-port-channel 200
FSPF interface san-port-channel 200 in VSAN 200
FSPF routing administrative state is active
Interface cost is 125
Timer intervals configured, Hello 40 s, Dead 80 s, Retransmit 5 s
FSPF State is FULL
Neighbor Domain Id is 0x18(24)
Neighbor Interface is san-port-channel 200 (0x000400c7)

Statistics counters :
   Number of packets received : LSU  7  LSA  7  Hello 238  Error packets 218
   Number of packets transmitted : LSU  7  LSA  7  Hello 180  Retransmitted LSU  0
  Number of times inactivity timer expired for the interface = 32
```

### 考えられる原因

FSPF デッド間隔が適切に設定されていません。

「show logging」ログに表示される場合があるログ メッセージの例を次に示します。

例：

```
%FSPF-3-HELLO_MISMATCH: %$VSAN <vsan-id>%$ Mismatch in Dead timer in the Hello packet on
interface san-port-channel <channel-id>
N5K-2 %FSPF-3-FC2_PROC_ERR: %$VSAN <vsan-id>%$ Error in processing HELLO  packet on
interface san-port-channel <channel-id>, Error  = Bad packet received
```

### 解決方法

NX-OS CLI を使用して ISL 上のデッド間隔の不一致を特定するには、次の手順を実行します。

**ステップ 1**　「debug fspf all」コマンドを使用して不適切なデッド間隔のメッセージを探すか、「show logging」ログの最後のメッセージをチェックしてエラー メッセージを探します。

デバッグ出力では、次のメッセージが生成されます。

```
fspf: Wrong hello interval for packet on interface 40000c7 in VSAN 200
fspf: Error in processing hello packet , error = Bad packet received
```

**ステップ 2**　「undebug all」コマンドを使用して、デバッグをオフにします。

**ヒント**　ヒント：いずれかのデバッグ コマンドを入力する前に、telnet または SSH セッションをもう 1 つ開きます。デバッグ出力で現在のセッションがあふれた場合は、2 番目のセッションを使用して「undebug all」コマンドを入力し、デバッグ メッセージの出力を停止します。

**ステップ 3**　「show fspf vsan <vsan-id> interface」コマンドを使用して、両方のスイッチで FSPF の設定を表示します。

例：

```
switch# show fspf vsan 200 interface san-port-channel 200
FSPF interface san-port-channel 200 in VSAN 200
FSPF routing administrative state is active
Interface cost is 125
Timer intervals configured, Hello 20 s, Dead 120 s, Retransmit 5 s
FSPF State is INIT
```

```
Statistics counters :
   Number of packets received : LSU  4  LSA  4  Hello 27  Error packets 4
   Number of packets transmitted : LSU  4  LSA  4  Hello 38  Retransmitted LSU  0
   Number of times inactivity timer expired for the interface = 0

switch# show fspf vsan 200 interface port-channel 200
FSPF interface port-channel 200 in VSAN 200
FSPF routing administrative state is active
Interface cost is 125
Timer intervals configured, Hello 20 s, Dead 80 s, Retransmit 5 s
FSPF State is INIT

Statistics counters :
   Number of packets received : LSU  4  LSA  4  Hello 41  Error packets 35
   Number of packets transmitted : LSU  4  LSA  4  Hello 29  Retransmitted LSU  0
  Number of times inactivity timer expired for the interface = 4
```

**（注）** この例では、

- 最初のスイッチでは、デッド タイマーがデフォルト（80 秒）に設定されていません。ネイバー スイッチ（MDS）の設定を確認して設定値を合わせます。
- FSPF が FULL ステートではありません。これは問題があることを示します。

**ステップ 4**　インターフェイス コンフィギュレーション モードで、両方のスイッチの fspf dead-interval が同じ値になるように変更します。

```
switch(config)# interface san-port-channel 200
switch(config-if)# fspf dead-interval 80 vsan 200
```

**ステップ 5**　変更後、FSPF が FULL ステートになったことを確認します。「show fspf internal route vsan <vsan-id>」コマンドを使用して、VSAN トラフィックのルートがあることを確認します。

例：

```
switch# show fspf internal route vsan 200

FSPF Unicast Routes
---------------------------
 VSAN Number  Dest Domain   Route Cost    Next hops
-----------------------------------------------
         200     0x18(24)          125 san-port-channel 200

switch# show fspf vsan 200 interface san-port-channel 200
FSPF interface san-port-channel 200 in VSAN 200
FSPF routing administrative state is active
Interface cost is 125
Timer intervals configured, Hello 20 s, Dead 80 s, Retransmit 5 s
FSPF State is FULL
Neighbor Domain Id is 0x18(24)
Neighbor Interface is san-port-channel 200 (0x000400c7)

Statistics counters :
   Number of packets received : LSU  8  LSA  8  Hello 47  Error packets 4
   Number of packets transmitted : LSU  8  LSA  8  Hello 70  Retransmitted LSU  0
  Number of times inactivity timer expired for the interface = 0
```

考えられる原因

スイッチにリージョンの不一致があります。

「show logging」ログに表示される場合があるログ メッセージの例を次に示します。

例：

```
%FSPF-3-BAD_FC2_PKT: %$VSAN 200%$ Received bad FC2 packet on interface san-port-channel
<channel-id>  : Packet received for non existant region in VSAN
```

解決方法

NX-OS CLI を使用してスイッチ上のリージョン不一致の問題を特定するには、次の手順を実行します。

**ステップ 1**　「show fspf vsan <vsan-id>」コマンドを使用して、VSAN に現在設定されているリージョンを表示します。

例（リージョン値は 2。デフォルトのリージョン値は 0）：

```
switch# show fspf vsan 200
FSPF routing for VSAN 200
FSPF routing administration status is enabled
FSPF routing operational status is UP
It is an intra-domain router
Autonomous region is 2
SPF hold time is 0 msec
MinLsArrival = 1000 msec , MinLsInterval = 2000 msec
Local Domain is 0x22(34)
Number of LSRs = 1, Total Checksum = 0x00000c10

Protocol constants :
   LS_REFRESH_TIME = 30 minutes (1800 sec)
   MAX_AGE         = 60 minutes (3600 sec)

Statistics counters :
   Number of LSR that reached MaxAge = 0
   Number of SPF computations        = 0
   Number of Checksum Errors         = 0
   Number of Transmitted packets :  LSU 0 LSA 0 Hello 19 Retranmsitted LSU 0
   Number of received packets :  LSU 0 LSA 0 Hello 0 Error packets 18
```

**ステップ 2**　「debug fspf all」コマンドを使用して、存在しないリージョンに関するメッセージを探します。

例：

```
fspf: Hello timer reached for interface san-port-channel 200 in VSAN 200
fspf: FC2 packet received for non existant region 0 in VSAN 200
fspf: FC2 packet received for non existant region 0 in VSAN 200
```

ネイバー スイッチがアドバタイズしているリージョンは 0 です。FSPF は ISL ごとに INIT ステートにあります。

例：

```
switch# show fspf vsan 200 interface san-port-channel 200
FSPF interface san-port-channel 200 in VSAN 200
FSPF routing administrative state is active
Interface cost is 125
Timer intervals configured, Hello 20 s, Dead 80 s, Retransmit 5 s
FSPF State is INIT

Statistics counters :
   Number of packets received : LSU  0  LSA  0  Hello 0  Error packets 0
```

```
  Number of packets transmitted : LSU  0  LSA  0  Hello 49  Retransmitted LSU  0
Number of times inactivity timer expired for the interface = 9
```

**ステップ 3**　「undebug all」コマンドを使用して、デバッグをオフにします。

**ステップ 4**　「show fspf vsan <vsan-id>」コマンドを使用して FSPF の設定を表示し、自律リージョンを確認します。

例：

```
switch# show fspf vsan 200
FSPF routing for VSAN 200
FSPF routing administration status is enabled
FSPF routing operational status is UP
It is an intra-domain router
Autonomous region is 2
SPF hold time is 0 msec
MinLsArrival = 1000 msec , MinLsInterval = 2000 msec
Local Domain is 0x22(34)
Number of LSRs = 1, Total Checksum = 0x00000c10

switch# show fspf vsan 200
FSPF routing for VSAN 200
FSPF routing administration status is enabled
FSPF routing operational status is UP
It is an intra-domain router
Autonomous region is 0
SPF hold time is 0 msec
MinLsArrival = 1000 msec , MinLsInterval = 2000 msec
Local Domain is 0x18(24)
Number of LSRs = 2, Total Checksum = 0x00014f9f
```

**ステップ 5**　「fspf config vsan」コマンドを使用して FSPF コンフィギュレーション モードに入り、「region」コマンドを使用してリージョンを変更します。リージョンは、VSAN 内のすべてのスイッチで一致する必要があります。

例：

```
switch(config)# fspf config vsan 200
switch(config-(fspf-config))# region 0
```

# 無効な FLOGI が多すぎることが原因で、ファイバ チャネル ポートが一時停止する

NPV 機能がイネーブルになっている Cisco Nexus 5000、またはファブリック モードで動作している Cisco Nexus 5000 に接続されたファイバ チャネル ノードが、FLOGI 拒否が原因で SAN ファブリックにログインできません。

「show logging」ログに表示される場合があるログ メッセージの例を次に示します。

例：

```
%FLOGI-1-MSG_FLOGI_REJECT_FCID_ERROR: %$VSAN <vsan-id>%$ [VSAN <vsan-id>, Interface
fcslot/port/: mode[F]] FLOGI rejected - FCID allocation failed.
PORT-5-IF_DOWN_TOO_MANY_INVALID_FLOGIS: %$VSAN <vsan-id>%$ Interface fc slot/port is down
(Suspended due to too many invalid flogis
```

インターフェイスのステータスは「invalidFlogis」を示します。

```
show interface fc slot/port brief
fc slot/port      <vsan-id>      F      --      invalidFlogis
```

考えられる原因

その VSAN の FC ID 永続性テーブルがいっぱいになっている可能性があります。Nexus 5000 シリーズ スイッチが NPV エッジ スイッチとして設定されている場合は、NPV コア スイッチの FC ID 永続性テーブルがいっぱいになっている可能性があります。

**FC ID :**

Cisco Nexus 5000 シリーズ スイッチにログインした N ポートには、FC ID が割り当てられます。デフォルトでは、永続的 FC ID 機能はイネーブルです。この機能がディセーブルの場合は、次のようになります。

- N ポートが Cisco Nexus 5000 シリーズ スイッチにログインします。要求元 N ポートの WWN および割り当てられた FC ID が維持され、揮発性キャッシュに格納されます。揮発性キャッシュの内容は、再起動時に保存されません。
- スイッチは、FC ID と WWN のバインディングをベストエフォート方式で保持するように設計されています。たとえば、スイッチから 1 つの N ポートを切断したあとに、別のデバイスから FC ID が要求されると、この要求が許可されて、WWN と初期 FC ID の関連付けが解除されます。
- 揮発性キャッシュには、WWN と FC ID バインディング エントリを 4000 まで格納できます。このキャッシュが満杯になると、新しい（より最近の）エントリによって、キャッシュ内の最も古いエントリが上書きされます。この場合、最も古いエントリの対応する WWN と FC ID の関連付けが失われます。
- N ポートを取り外し、同じスイッチの任意のポートに接続すると、（このポートが同じ VSAN に属するかぎり）この N ポートには同じ FC ID が割り当てられます。

永続的 FC ID は、選択的に消去できます。現在使用中のスタティック エントリおよび FC ID は、削除できません。

解決方法

「show flogi internal」コマンドを使用して、FLOGI エラー メッセージを確認します。

例：

「show flogi internal event-history debugs」

```
222) Event:E_FLOGI_DEBUG, length:309, at 989582 usecs after Thu Jun 17
09:03:01 2010
fs_print_port_stats(10049): Port Stats for fc2/1, after cleanup:
   timestamp: Wed Jun 17 07:03:01 2010
   MSG_FLOGI: 52
   MSG_FC2_LS_RJT_OUT: 51
   EXCEPTION_CANNOT_ALLOCATE_FCID: 51
   EXCEPTION_TIMEOUT: 1
   EXCEPTION_FC2_INVALID_XCHG: 1
   tot_internal_exceptions: 51, since: Thu Dec 31 17:00:00 1969
```

「show flogi internal errors」

```
52) Event:E_DEBUG, length:119, at 977471 usecs after Thu Jun 17 09:03:01
2010
    [102] Interface fc2/1, nwwn 20:01:00:1b:32:af:d6:8c, pwwn
21:01:00:1b:32:af:d6:8c: flogi is valid; exchange is INVALID.
```

「show fcdomain address-allocation」コマンドを使用して FC ドメイン アドレス割り当てテーブルをチェックし、空き FC ID を確認します（NPV がイネーブルの場合は、NPV コア スイッチでこのコマンドを実行します）。

例：

「show fcdomain address-allocation」

```
VSAN 1
Free FCIDs: 0xe73f4f to 0xe73fff
            0xe7ff00 to 0xe7fffe

Assigned FCIDs: 0xe70000 to 0xe73f4e
                0xe74000 to 0xe7feff
                0xe7ffff

Reserved FCIDs: 0xe7ffff

Number free FCIDs: 432
Number assigned FCIDs: 65104
Number reserved FCIDs: 1
```

自動エリアリストおよび永続的 FCID を検索するには、「show flogi auto-area-list」コマンドと「show fcdomain fcid persistent」コマンドを使用します。

例：

```
「show flogi auto-area-list」
Fcid area allocation company id info:
<...>
   00:14:5E
   00:1B:32
   00:50:2E
   00:E0:69
   00:E0:8B
```

```
「show fcdomain fcid persistent」{OUI 00:E0:8B 用に予約されているエリア全体}

102    21:01:00:1b:32:2f:7f:63    0x020003    SINGLE FCID     YES    DYNAMIC
102    21:00:00:1b:32:0f:7f:63    0x020004    SINGLE FCID     YES    DYNAMIC

102    21:00:00:e0:8b:89:a7:07    0x021c00    ENTIRE AREA     YES    DYNAMIC
102    21:00:00:e0:8b:88:e9:22    0x024300    ENTIRE AREA     YES    DYNAMIC
```

FCID が十分にない場合は、「purge fcdomain」コマンドを使用して、指定した VSAN のダイナミック FC ID と未使用の FC ID を消去できます。

例：

```
switch#purge fcdomain fcid vsan <vsan-id>
```

ポートはすぐにアップします。

また、HBA が S_ID != 0x0 でログインしようとしている可能性もあります。

これが起こった場合に、永続性テーブルに HBA の WWN に対応するエントリがないときは、HBA で使用されている S_ID をその HBA 自体に割り当ててみます。

S_ID がすでに使用されているか、間違ったドメインに属する場合は、fcdomain によって要求が拒否されます。数回再試行した後、ポートが一時停止します。

このモードになった HBA は、FCID 空間にあるすべての FCID（0x00.00.01 から、最大ですべての 0xDD.AA.PP 番号まで）を使用してログインを試みます。

この動作は「show flogi internal event-history msgs」で確認できます。

「show flogi internal event-history msgs」（HBA がさまざまな FCID を使用してログインを試みています）

例：

```
841) Event:E_FLOGI_LRX, length:20, at 56079 usecs after Tue Jun 22 15:40:59 2010
    WWN: 21:01:00:1b:32:af:d6:8c  VSAN: 1  ifindex: fc2/1  FCID: 0x000032
```

```
886) Event:E_FLOGI_RX, length:20, at 897472 usecs after Tue Jun 22 15:40:58 2010
    WWN: 21:01:00:1b:32:af:d6:8c  VSAN: 1  ifindex: fc2/1  FCID: 0x000030

888) Event:E_FLOGI_FAIL, length:20, at 884758 usecs after Tue Jun 22 15:40:58 2010
    WWN: 21:01:00:1b:32:af:d6:8c  VSAN: 1  ifindex: fc2/1  ev_id: 21
    rjt reason: 7 OPC: MTS_OPC_DM_GET_FCIDS(275)

903) Event:E_FLOGI_RX, length:20, at 835015 usecs after Tue Jun 22 15:40:58 2010
    WWN: 21:01:00:1b:32:af:d6:8c  VSAN: 1  ifindex: fc2/1  FCID: 0x00002f
```

この場合の解決方法は、次の例に示すように、永続性テーブルに HBA の WWN に対応するエントリを手動で設定することです。その他に、デバイスの電源を再投入するという方法もあります。こうすると通常、HBA はまず S_ID=0x0 を使用した通常の FLOGI を実行します。

例：

```
switch# conf t
switch(config)# fcdomain fcid database
switch(config-fcid-db)# vsan <vsan-id> wwn 50:05:08:b2:00:71:c8:c2 fcid 0x6fee00 area
```

それでも問題が解決しない場合は、次のコマンドを使用して、詳細な分析に役立つ情報を収集します。

```
Show tech-support flogi
Show tech-support fcdomain
Show logging log
show port internal info interface fc slot/port
show port internal event-history interface fc slot/port
show tech-support detail > bootflash:showtechdet
Capture debug flogi & debug fcdomain via following below steps:
switch# debug logfile flogi_fcdomain
switch# debug flogi all
switch# debug fcdomain all

switch(config)# int fc slot/port
switch(config-if)# shut
switch(config-if)# no shut
switch(config-if)# undebug all
switch# dir log:  {check if you have the file in log: directory}
          31     Aug 03 13:45:13 2010  dmesg
       55941     Aug 05 07:21:15 2010  flogi_fcdomain

switch# copy log:flogi_fcdomain ftp://x.y.z.w {or use tftp/scp/sftp}
```

# ファイバ チャネル ノードの古い FCNS エントリがある

ファイバ チャネル ノードは SAN ファブリックにログイン（FLOGI）できますが、それらのノードの FCNS エントリが不完全です。サーバはそれらのターゲットに到達できません。

その結果、FCNS データベースで「fc4-types:fc4_features」が空になります。

考えられる原因

Nexus 5000 シリーズ スイッチが NPV コア（NPIV を装備）として設定され、レガシー ゲートウェイ スイッチに接続されたトポロジにおいて、ファイバ チャネル ノードが自身の FC4 タイプと FC4 機能を FCNS データベースに登録していない可能性があります。fc4-types:fc4_features を確認するには、次の例に示すように、「show fcns database detail」コマンドを使用します。

例：

```
switch# show fcns da fcid 0x621400 detail vsan 2
------------------------
```

```
VSAN:2     FCID:0x621400
------------------------
port-wwn (vendor)           :21:01:00:1b:32:a3:d7:2c
                             [z7095ib-1_T]
node-wwn                    :20:01:00:1b:32:a3:d7:2c
class                       :3
node-ip-addr                :0.0.0.0
ipa                         :ff ff ff ff ff ff ff ff
fc4-types:fc4_features      :
symbolic-port-name          :
symbolic-node-name          :
port-type                   :N
port-ip-addr                :0.0.0.0
fabric-port-wwn             :20:d9:00:0d:ec:e0:0e:80
hard-addr                   :0x000000
permanent-port-wwn (vendor) :20:11:00:05:1e:06:da:ea
Connected Interface         :fc2/2
Switch Name (IP address)    :N5K (10.200.220.13)
```

レガシー ゲートウェイ スイッチの中には、スイッチの FCID のエリア部分と、そのポートを通じてログインされたすべてのブレードの FCID のエリア部分が同じでなければならないものがあります。

しかし、Qlogic HBA に関する古い問題が原因で、Cisco Nexus 5000 ドメイン サーバは、デフォルトである特定の OUI と一致する Qlogic HBA に対してそれぞれ異なるエリアを割り当てます。したがって、レガシー ゲートウェイの要件とシスコのドメイン割り当て方式の間に競合が起こります。シスコは、現場で使用されている既存の古い Qlogic HBA をサポートするため、引き続きこの方式をサポートします。

**解決方法**

まず、使用しているすべての Qlogic OUI について「no fcid-allocation area company <oui>」を設定します（今後、フラットな FCID 割り当てが行われるようにします）。次に、影響を受けるすべてのブレードを強制的にファブリックからログアウトさせ、すでに作成された永続的 FCID エントリを Nexus 5000 スイッチ コンフィギュレーションから削除します。最後に、ブレードに再度ログインさせます。

次の「show flogi database」の出力例では、すべてのデバイスが一意のエリア ID（x01、x08、x0c）を取得しています。

例：

```
Fc2/1    2     0x620104  20:10:00:05:1e:5e:6a:85 10:00:00:05:1e:5e:6a:85
Fc2/1    2     0x620800  21:01:00:1b:32:a3:c0:2e 20:01:00:1b:32:a3:c0:2e
Fc2/1    2     0x620c00  21:01:00:1b:32:33:8b:8e 20:01:00:1b:32:33:8b:8e
```

レガシー スイッチに特有のエリア ID 要件のため、最後の 2 つのブレードもエリアを x01 にする必要があります。次の手順に従って、Qlogic アダプタを強制的に再ログインさせて 0x6201xx の範囲内の FCID が取得されるようにします。

**ステップ 1**　この状況にある OUI と一致するすべての WWN について、今後の FCID 割り当て方式がフラットになるよう設定（強制）します。

```
switch(configure)# no fcid-allocation area company 0x001B32
```

**ステップ 2**　再設定中の FCID を強制的にファブリックからログアウトさせます。

**（注）**　単に、そのサーバのプライマリ アップリンクとして機能している Nexus 5000 インターフェイスをシャットダウンするだけでは不十分です。そうすると、別のインターフェイスを通じてログインするだけです。適切な方法は、影響を受けるブレードをシャットダウンして、WWN の FLOGI を確実に消去することです。

**ステップ 3**　次の例に示すように、永続的 FCID 割り当てのために自動的に作成された設定エントリを削除します。

例：

```
switch(config)# fcdomain fcid database
switch(config-fcid-db)# no vsan 2 wwn 21:01:00:1b:32:a3:c0:2e fcid 0x620800 area dynamic
```

**ステップ 4**　ブレードを起動して、適切な FCID が取得されるようにします。

例：

```
Fc2/1    2     0x620104  20:10:00:05:1e:5e:6a:85 10:00:00:05:1e:5e:6a:85
Fc2/1    2     0x620123  21:01:00:1b:32:a3:c0:2e 20:01:00:1b:32:a3:c0:2e
```

# FC ドメイン ID の重複が原因でインターフェイスが分離される

xE ポート タイプを使用して FC スイッチに接続された（ファブリック モードの）Cisco Nexus 5000 のファイバ チャネル インターフェイスまたは SAN ポートチャネル インターフェイスが、ドメインの重複が原因で分離されます。「show logging」ログに表示される場合があるログ メッセージの例を次に示します。

例：

```
PORT-5-IF_DOWN_DOMAIN_OVERLAP_ISOLATION: Interface fc <slot/port> is down (Isolation due
to domain overlap).
%FCDOMAIN-2-EPORT_ISOLATED: %$VSAN <vsan-id>%$ Isolation of interface san-port-channel
<channel-id> (reason: domain ID assignment failure)
%FCDOMAIN-2-EPORT_ISOLATED: %$VSAN <vsan-id>%$ Isolation of interface san-port-channel
<channel-id> (reason: other side Eport indicates isolation)
```

考えられる原因

2 つのスイッチ ファブリックが結合できない可能性があります。2 台以上のスイッチを含む 2 つのファブリックが接続されている場合に、それらのファブリックが共通の割り当て済みドメイン ID を少なくとも 1 つ持ち、さらに自動再設定オプションがディセーブルになっているとき（このオプションはデフォルトでディセーブルになっています）、2 つのファブリックの接続に使用される E ポートは、ドメイン ID の重複が原因で分離されます。

ファイバ チャネル ネットワークでは、新しいスイッチが既存のファブリックに追加されると、主要スイッチによってドメイン ID が割り当てられます。ただし、2 つのファブリックが結合するときは、主要スイッチ選出プロセスによって、既存のいずれのスイッチが結合ファブリックの主要スイッチになるかが決定されます。

新しい主要スイッチの選出は次のルールに従います。

- 空でないドメイン ID リストを持つスイッチの方が、空のドメイン ID リストを持つスイッチよりも優先されます。主要スイッチは、空でないドメイン ID リストを持つファブリック内のスイッチになります。
- 両方のファブリックがドメイン ID リストを持つ場合、2 台の主要スイッチ間の優先順位はスイッチ プライオリティの設定値によって決まります。これはユーザが設定可能なパラメータです。パラメータの値が小さいほど優先順位が高くなります。
- 上記の 2 つの基準によって主要スイッチを決定できない場合は、2 台のスイッチの WWN によって主要スイッチが決定されます。WWN の値が小さいほどスイッチ プライオリティが高くなります。

解決方法

FC ドメイン ID の重複を解決するには、分離されたスイッチ用の新しいスタティック ドメイン ID を手動で設定して重複するスタティック ドメイン ID を変更するか、スタティックなドメイン割り当てをディセーブルにして、ファブリック再設定後にスイッチが新しいドメイン ID を要求するようにします。

### NX-OS CLI を使用してスタティック ドメイン ID を割り当てるには

VSAN 内のスイッチに接続されたデバイスはすべて、新しいドメイン ID が割り当てられるときに新しい FC ID を取得します。ホストまたはストレージ デバイスの FC ID が変更された場合、一部のホストまたはストレージ デバイスが期待どおりに機能しない可能性があります。

CLI を使用して FC ドメイン ID の重複を確認し、新しいドメイン ID を再割り当てするには、次の手順を実行します。

**ステップ 1**　「show interface fc <slot/port>」コマンドを実行して、E ポートの分離エラー メッセージを表示します。

例：

```
switch(config)# show int fc 2/2
fc2/2 is down (Isolation due to domain other side eport isolated)
    Hardware is Fibre Channel, SFP is short wave laser w/o OFC (SN)
    Port WWN is 20:42:00:0d:ec:d5:fe:00
    Admin port mode is E, trunk mode is off
    snmp link state traps are enabled
    Port vsan is 3
```

「show interface san-port-channel <channel-id>」コマンドを実行して、特定の VSAN の分離エラーを表示します。

例：

```
switch(config)# show interface san-port-channel 200
san-port-channel 200 is trunking (Not all VSANs UP on the trunk)
    Hardware is Fibre Channel
    Port WWN is 24:c8:00:0d:ec:d5:a3:80
    Admin port mode is auto, trunk mode is on
    snmp link state traps are enabled
    Port mode is TE
    Port vsan is 1
    Speed is 8 Gbps
    Trunk vsans (admin allowed and active) (1,200)
    Trunk vsans (up)                       (1)
    Trunk vsans (isolated)                 (200)
    Trunk vsans (initializing)             ()
```

**ステップ 2**　「show fcdomain domain-list vsan <vsan-id>」コマンドを使用して、現在ファブリック内にあるドメインを表示します。

例（ドメイン ID 44 の重複が原因でスイッチが分離されています）：

```
switch(config)# show fcdomain domain-list vsan 3

Number of domains: 1
Domain ID              WWN
---------    -----------------------
 0x2c(44)    20:03:00:0d:ec:3f:a5:81 [Local] [Principal]

switch(config)# show fcdomain domain-list vsan 3

Number of domains: 1
Domain ID              WWN
---------    -----------------------
```

```
 0x2c(44)    20:03:00:0d:ec:d5:fe:01 [Local] [Principal]
```

SAN ポートチャネル インターフェイスの下の特定の VSAN で分離が発生している場合は、次の例に示すように、「show port internal info interface san-port-channel <channel-id> vsan <vsan-id>」を使用してエラーを表示できます。

例：

```
switch(config)# show port internal info interface san-port-channel 200 vsan 200

  san-port-channel 200, Vsan 200 - state(down), state reason(Isolation due to domain other
side eport isolated), fcid(0x000000)
    port init flag(0x10000),  num_active_ports (2),
    Lock Info: resource [san-port-channel 200, vsan 200]
      type[0] p_gwrap[(nil)]
          FREE @ 159645 usecs after Thu Aug  5 13:35:00 2010
      type[1] p_gwrap[(nil)]
          FREE @ 159964 usecs after Thu Aug  5 13:35:00 2010
      type[2] p_gwrap[(nil)]
          FREE @ 450507 usecs after Tue Aug  3 14:14:08 2010
    0x50c8efc7
current state [TE_FSM_ST_ISOLATED_DM_ZS]
    RNID info not found.
    first time elp: 0
    Peer ELP Revision: 3
```

**ステップ 3**　「fcdomain domain domain-id [static | preferred] vsan vsan-id」コマンドを使用して、重複しているいずれかのドメイン ID のドメイン ID を変更します。

- static オプションを指定すると、スイッチはその特定のドメイン ID を要求します。その特定のアドレスを取得できない場合は、ファブリックから分離されます。
- preferred オプションを指定すると、スイッチは指定されたドメイン ID を要求します。その ID を取得できない場合は、別の ID を受け入れます。

**ステップ 4**　「fcdomain restart vsan」コマンドを使用して、Domain Manager を再起動します。

static オプションは、中断再起動または非中断再起動後の実行時に適用できますが、preferred オプションは中断再起動後の実行時にだけ適用できます。

**（注）**　ドメイン ID の再起動は中断的です。そのドメインにログインしていたファイバ チャネル ノードはいったんログアウトし、再びログインします。中断再設定が発生すると、データ トラフィックが影響を受けることがあります。

### ファブリック再設定後にダイナミック ドメイン ID を割り当てるには

ファブリック再設定を使用してドメイン ID を再割り当てし、ドメイン ID の重複を解決できます。ファブリックを接続する前に両方のスイッチで auto-reconfigure オプションをイネーブルにした場合、中断再設定（RCF）が発生します。RCF が発生すると、新しい主要スイッチ選出が自動的に強制実行され、新しいドメイン ID が異なるスイッチに割り当てられます。

NX-OS CLI でファブリック再設定を使用して特定の VSAN 用のドメイン ID を再割り当てするには、次の手順を実行します。

**ステップ 1**　「show fcdomain domain-list」コマンドを使用して、スイッチにドメイン ID がスタティックに割り当てられているかどうかを確認します。

**ステップ 2**　ドメイン ID がスタティックに割り当てられている場合は、「no fcdomain domain」コマンドを使用してスタティックな割り当てを解除します。

**ステップ 3**　「show fcdomain vsan <vsan-id>」コマンドを使用して、RCF 拒否オプションがイネーブルになっているかどうかを確認します。

例：

```
switch# show fcdomain vsan 3
The local switch is the Principal Switch.

Local switch run time information:
        State: Stable
        Local switch WWN:    20:03:00:0d:ec:d5:fe:01
        Running fabric name: 20:03:00:0d:ec:d5:fe:01
        Running priority: 128
        Current domain ID: 0x2c(44)

Local switch configuration information:
        State: Enabled
        FCID persistence: Enabled
        Auto-reconfiguration: Disabled
        Contiguous-allocation: Disabled
        Configured fabric name: 20:01:00:05:30:00:28:df
        Optimize Mode: Disabled
        Configured priority: 128
        Configured domain ID: 0x2c(44) (preferred)

Principal switch run time information:
        Running priority: 128
Interface               Role          RCF-reject
----------------    -------------    ------------
fc2/2               Isolated         Enabled
----------------    -------------    ------------
```

**ステップ 4**　rcf-reject オプションがイネーブルになっている場合は、interface コマンドを使用してから、インターフェイス モードで「no fcdomain rcf-reject vsan <vsan-id>」コマンドを使用します。

例：

```
switch(config)# interface fc 2/2
switch(config-if)# no fcdomain rcf-reject vsan 3
switch(config-if)#
```

**ステップ 5**　両方のスイッチで、EXEC モードで「fcdomain auto-reconfigure vsan <vsan-id>」コマンドを使用して、Domain Manager の再起動後に auto-reconfiguration がイネーブルになるようにします。

**ステップ 6**　「fcdomain restart vsan <vsan-id>」コマンドを使用して、Domain Manager を再起動します。

これは中断操作/中断再設定であり、データ トラフィックが影響を受けることがあります。

# シスコ ファブリック サービス

ここでは、Cisco Fabric Service（CFS; シスコ ファブリック サービス）のトラブルシューティングの概要を示し、一般的な問題とその解決方法について説明します。

# 概要

CFS の問題をトラブルシューティングする際は、まず次のことを確認します。

- 影響を受けるすべてのスイッチで、同じアプリケーションについて CFS がイネーブルになっていることを確認します。
- 影響を受けるすべてのスイッチで、同じアプリケーションについて CFS 配信がイネーブルになっていることを確認します。

  CFS リージョン機能を使用している場合は、影響を受けるすべてのスイッチでアプリケーションが同じリージョンにあることを確認します。
- アプリケーションの保留中の変更がないこと、および CFS がイネーブルになっているアプリケーションのすべての設定変更について CFS コミットが発行されたことを確認します。
- 予期しない CFS ロック済みセッションがないことを確認します。

  予期しないロック済みセッションがある場合はクリアします。

# CLI を使用した CFS の確認

CLI を使用して CFS を確認するには、次の手順を実行します。

**ステップ 1**　デフォルトでは、CFS 配信はイネーブルに設定されています。アプリケーションは、ファブリック内のアプリケーションが存在するすべての CFS 対応スイッチにデータと設定情報を配信できます。これが通常の動作モードです。スイッチでの CFS 配信のステートを確認するには、「show cfs status」コマンドを実行します。

例：

```
switch(config)# show cfs status
Distribution : Enabled
Distribution over IP : Enabled - mode IPv4
IPv4 multicast address : 239.255.70.83
IPv6 multicast address : ff15::efff:4653
Distribution over Ethernet : Disabled

switch(config)# show cfs merge status name rscn
```

**ステップ 2**　アプリケーションが一覧表示され、イネーブルになっていることを確認するには、すべてのスイッチで「show cfs application」コマンドを実行します。

例：

```
switch# show cfs application

----------------------------------------------
 Application    Enabled   Scope
----------------------------------------------
 fwm            Yes       Physical-eth
 ntp            No        Physical-fc-ip
 stp            Yes       Physical-eth
 fscm           Yes       Physical-fc
 role           No        Physical-fc-ip
 rscn           No        Logical
 radius         No        Physical-fc-ip
 fctimer        No        Physical-fc
 syslogd        No        Physical-fc-ip
 callhome       No        Physical-fc-ip
 fcdomain       No        Logical
```

```
 device-alias   Yes       Physical-fc

Total number of entries = 12
```

（注）　Physical スコープは、そのアプリケーションの設定がスイッチ全体に適用されることを意味します。Logical スコープは、そのアプリケーションの設定が特定の VSAN に適用されることを意味します。

**ステップ 3**　ある特定のアプリケーションが CFS に登録されているスイッチのセットを確認します。物理スコープ アプリケーションでは「show cfs peers name application-name」コマンドを使用し、論理スコープ アプリケーションでは「show cfs peers name application-name vsan vsan-id」コマンドを使用します。

例：

```
switch# show cf peers name device-alias

Scope      : Physical-fc
--------------------------------------------------------------------------
Switch WWN              IP Address
--------------------------------------------------------------------------
20:00:00:0d:ec:da:6e:00 172.25.183.124                          [Local]
20:00:00:0d:ec:24:5b:c0 172.25.183.123
20:00:00:0d:ec:50:09:00 172.25.183.42

Total number of entries = 3
```

（注）　論理アプリケーションに対して「show cfs peers name application-name」コマンドを実行すると、すべての VSAN のピアが表示されます。

例：

```
switch(config)# show cfs peers name rscn

Scope      : Logical [VSAN 1]
--------------------------------------------------------------------------------
 Domain Switch WWN              IP Address
--------------------------------------------------------------------------------
 106    20:00:00:0d:ec:da:6e:00 172.25.183.124                        [Local]
 98     20:00:00:0d:ec:24:5b:c0 172.25.183.123
 238    20:00:00:0d:ec:50:09:00 172.25.183.42

Total number of entries = 3


Scope      : Logical [VSAN 10]
--------------------------------------------------------------------------------
 Domain Switch WWN              IP Address
--------------------------------------------------------------------------------
 82     20:00:00:0d:ec:da:6e:00 172.25.183.124                        [Local]
 5      20:00:00:0d:ec:50:09:00 172.25.183.42
 83     20:00:00:0d:ec:24:5b:c0 172.25.183.123

Total number of entries = 3


Scope      : Logical [VSAN 50]
--------------------------------------------------------------------------------
 Domain Switch WWN              IP Address
--------------------------------------------------------------------------------
 66     20:00:00:0d:ec:da:6e:00 172.25.183.124                        [Local]
```

```
 28     20:00:00:0d:ec:24:5b:c0 172.25.183.123
 235    20:00:00:0d:ec:50:09:00 172.25.183.42

Total number of entries = 3


Scope      : Logical [VSAN 100]
--------------------------------------------------------------------------------
 Domain Switch WWN              IP Address
--------------------------------------------------------------------------------
 90     20:00:00:0d:ec:da:6e:00 172.25.183.124                          [Local]
 100    20:00:00:0d:ec:24:5b:c0 172.25.183.123
 111    20:00:00:0d:ec:50:09:00 172.25.183.42

Total number of entries = 3
```

**ステップ 4**　ファブリック内のすべてのスイッチが 1 つの CFS ファブリックを構成するか、または多数の分割された CFS ファブリックを構成するかを確認するには、「show cfs merge status name application-name」コマンドと「show cfs peers name application-name」コマンドを実行して出力を比較します。2 つの出力に示されるスイッチのリストが同じである場合は、スイッチのセット全体が 1 つの CFS ファブリックを構成しています。この場合、結合ステータスはすべてのスイッチで常に「成功」になります。

例：

```
switch(config)# show cfs merge status name rscn

Logical [VSAN 1] Merge Status: Success [ Thu Aug  5 11:33:50 2010 ]
 Local Fabric
--------------------------------------------------------------------------------
 Domain Switch WWN              IP Address
--------------------------------------------------------------------------------
 98     20:00:00:0d:ec:24:5b:c0 172.25.183.123                  [Merge Master]
 238    20:00:00:0d:ec:50:09:00 172.25.183.42
 106    20:00:00:0d:ec:da:6e:00 172.25.183.124
                                switch

Total number of switches = 3


Logical [VSAN 10] Merge Status: Success [ Thu Aug  5 11:36:43 2010 ]
 Local Fabric
--------------------------------------------------------------------------------
 Domain Switch WWN              IP Address
--------------------------------------------------------------------------------
 83     20:00:00:0d:ec:24:5b:c0 172.25.183.123                  [Merge Master]
 5      20:00:00:0d:ec:50:09:00 172.25.183.42
 82     20:00:00:0d:ec:da:6e:00 172.25.183.124
                                switch

Total number of switches = 3


Logical [VSAN 50] Merge Status: Success [ Thu Aug  5 11:36:23 2010 ]
 Local Fabric
--------------------------------------------------------------------------------
 Domain Switch WWN              IP Address
--------------------------------------------------------------------------------
 28     20:00:00:0d:ec:24:5b:c0 172.25.183.123                  [Merge Master]
 235    20:00:00:0d:ec:50:09:00 172.25.183.42
 66     20:00:00:0d:ec:da:6e:00 172.25.183.124
                                switch

Total number of switches = 3
```

```
Logical [VSAN 100] Merge Status: Success [ Thu Aug  5 11:33:50 2010 ]
 Local Fabric
--------------------------------------------------------------------------------
 Domain Switch WWN              IP Address
--------------------------------------------------------------------------------
 100    20:00:00:0d:ec:24:5b:c0 172.25.183.123                  [Merge Master]
 111    20:00:00:0d:ec:50:09:00 172.25.183.42
 90     20:00:00:0d:ec:da:6e:00 172.25.183.124
                                switch

Total number of switches = 3
```

「show cfs merge status name」コマンドの出力に示されるスイッチのリストが「show cfs peers name」コマンドの出力よりも短い場合、ファブリックは複数の CFS ファブリックに分割されていて、結合ステータスが「失敗」、「保留中」、「待機中」のいずれかになる場合があります。

# 結合の失敗のトラブルシューティング

結合時、結合するファブリック内の結合マネージャは相互にコンフィギュレーション データベースを交換します。いずれかのファブリックのアプリケーションが情報を結合し、結合が成功したかどうかを判断して、結合されたファブリック内のすべてのスイッチに結合ステータスを通知します。

結合が成功した場合、結合されたデータベースが結合ファブリック内のすべてのスイッチに配信され、新規ファブリック全体が一貫したステートになります。結合の失敗は、結合するファブリックに結合できない不整合データが含まれることを示します。

新しいスイッチをファブリックに追加した場合に、あるアプリケーションの結合ステータスが長時間「In Progress」を示すときは、いずれかのスイッチにそのアプリケーションのアクティブなセッションが存在する可能性があります。「show cfs lock」コマンドを使用して、すべてのスイッチでそのアプリケーションのロック ステータスを確認します。ロックが存在する場合、結合プロセスは進みません。変更をコミットするかセッションのロックをクリアして、結合プロセスを進めます。

**（注）** 結合の失敗は正しく分析する必要があります。ブランク コミットを行うスイッチを選ぶときは注意してください。小さいコンフィギュレーションによって大きいコンフィギュレーションが消去される場合があります。

## CLI を使用した結合の失敗からの回復

CLI を使用して結合の失敗から回復するには、次の手順を実行します。

**ステップ 1**　結合の失敗を示すスイッチを特定するには、「show cfs merge status name application-name」コマンドを実行します。

例：

```
switch(config)# show cfs merge status name ntp

Physical-fc-ip  Merge Status: Success [ Thu Aug  5 11:47:58 2010 ]
 Local Fabric
--------------------------------------------------------------------------------
 Switch WWN              IP Address
--------------------------------------------------------------------------------
 20:00:00:0d:ec:da:6e:00 172.25.183.124                  [Merge Master]
                         switch
```

```
Total number of switches = 1

switch(config)# show cfs merge status name ntp

Physical-fc-ip  Merge Status: Success [ Thu Aug  5 11:43:39 2010 ]
 Local Fabric
-------------------------------------------------------------------------------
 Switch WWN              IP Address
-------------------------------------------------------------------------------
 20:00:00:0d:ec:50:09:00 172.25.183.42                           [Merge Master]
                         MDS-9134
 20:00:00:0d:ec:da:6e:00 172.25.183.124

Total number of switches = 2
```

**ステップ 2**　結合の失敗の詳細な説明を表示するには、「show cfs internal session-history name application name detail」コマンドを実行します。

例：

```
switch(config)# show cfs internal session-history name ntp
-------------------------------------------------------------------------------
Time Stamp                Source WWN              Event
User Name                 Session ID
-------------------------------------------------------------------------------
Thu Aug  5 11:45:19 2010  20:00:00:0d:ec:da:6e:00  LOCK_ACQUIRED
admin                     34684
Thu Aug  5 11:45:19 2010  20:00:00:0d:ec:da:6e:00  COMMIT[2]
admin                     34689
Thu Aug  5 11:45:20 2010  20:00:00:0d:ec:da:6e:00  LOCK_RELEASED
admin                     34684

-------------------------------------------------------------------------------
```

**ステップ 3**　コンフィギュレーション モードに入り、「application-name commit command」コマンドを実行してファブリック内のすべてのピアを同じコンフィギュレーション データベースに戻します。

例：

```
switch(config)# ntp commit
switch(config)# show cfs merge status name ntp

Physical-fc-ip  Merge Status: Success [ Thu Aug  5 11:51:02 2010 ]
 Local Fabric
-------------------------------------------------------------------------------
 Switch WWN              IP Address
-------------------------------------------------------------------------------
 20:00:00:0d:ec:50:09:00 172.25.183.42                           [Merge Master]
 20:00:00:0d:ec:da:6e:00 172.25.183.124
                         switch

Total number of switches = 2

switch(config)# show cfs merge status name ntp

Physical-fc-ip  Merge Status: Success [ Thu Aug  5 11:51:02 2010 ]
 Local Fabric
-------------------------------------------------------------------------------
 Switch WWN              IP Address
-------------------------------------------------------------------------------
 20:00:00:0d:ec:50:09:00 172.25.183.42                           [Merge Master]
                         MDS-9134
```

```
 20:00:00:0d:ec:da:6e:00 172.25.183.124

Total number of switches = 2
```

# ロックの失敗のトラブルシューティング

ファブリック内で設定を配信するためには、まずファブリック内のすべてのスイッチでロックを取得する必要があります。ロックが取得されたら、コミットを実行してファブリック内のすべてのスイッチにデータを配信できます。その後でロックが解放されます。

別のアプリケーション ピアによってすでにロックが取得されている場合は、新しい設定変更をコミットできません。これは通常の状況であり、ロックが解放されるまでアプリケーションの変更を延期する必要があります。この項のトラブルシューティング手順を実行するのは、ロックが適切に解放されていないと確信される場合に限ります。

ロックは、管理者が CFS イネーブル アプリケーションの変更を設定するときに発生します。2 人の管理者が同じスイッチで同じアプリケーションを設定しようとした場合は、一方の管理者のみにロックが与えられます。もう一方の管理者は、最初の管理者が変更をコミットまたは廃棄するまで、そのアプリケーションに変更を加えることはできません。アプリケーションのロックを保持している管理者の名前を確認するには、「show cfs lock name」コマンドを使用します。ロックをクリアする前に、その管理者を確認してください。

ファブリック内の別のスイッチが CFS ロックを保持している場合もあります。「show cfs peers name」コマンドを使用して、アプリケーションの CFS 配信に参加しているすべてのスイッチを確認します。次に、各スイッチで「show cfs lock name」コマンドを使用して、そのアプリケーションの CFS ロックを所有している管理者を確認します。ロックをクリアする前に、その管理者を確認してください。CFS abort オプションを使用すると、データをファブリックに配信せずにロックが解放されます。

## CLI を使用したロックの失敗に関する問題の解決

CLI を使用してロックの失敗を解決するには、次の手順を実行します。

**ステップ 1**　「show cfs lock name」コマンドを使用して、ロック保持者を確認します。

例：

```
switch(config)# show cfs lock name ntp

Scope      : Physical-fc-ip
--------------------------------------------------------------------------------
 Switch WWN              IP Address                  User Name    User Type
--------------------------------------------------------------------------------
 20:00:00:0d:ec:50:09:00 172.25.183.42               admin        CLI/SNMP v3

Total number of entries = 1
```

**ステップ 2**　ロックの失敗の詳細な説明を表示するには、「show cfs internal session-history name application name detail」コマンドを実行します。

例：

```
switch(config)# show cfs internal session-history name ntp detail
--------------------------------------------------------------------------------
Time Stamp                Source WWN              Event
User Name                 Session ID
--------------------------------------------------------------------------------
Thu Aug  5 11:51:02 2010  20:00:00:0d:ec:da:6e:00  LOCK_REQUEST
```

```
admin                     35035
Thu Aug  5 11:51:02 2010  20:00:00:0d:ec:da:6e:00  LOCK_ACQUIRED
admin                     35035
Thu Aug  5 11:51:03 2010  20:00:00:0d:ec:da:6e:00  COMMIT[2]
admin                     35040
Thu Aug  5 11:51:03 2010  20:00:00:0d:ec:da:6e:00  LOCK_RELEASE_REQUEST
admin                     35035
Thu Aug  5 11:51:03 2010  20:00:00:0d:ec:da:6e:00  LOCK_RELEASED
admin                     35035
Thu Aug  5 12:03:18 2010  20:00:00:0d:ec:50:09:00  REMOTE_LOCK_REQUEST
admin                     284072
Thu Aug  5 12:03:18 2010  20:00:00:0d:ec:50:09:00  LOCK_OBTAINED
admin                     284072
```

**ステップ 3**　リモート ピアがロックを保持している場合は、そのスイッチで「application-name commit」コマンドまたは「application-name abort」コマンドを実行する必要があります。

例：

application-name commit コマンドの例を次に示します。

```
switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ntp commit
switch(config)#
```

例：

application-name abort コマンドの例を次に示します。

```
switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ntp abort
switch(config)#
```

# システム ステートが不整合で、ロックが保持されている

不整合なシステム ステートは次のいずれかの場合に起こります。

- ファブリック内のすべてのスイッチでロックが保持されていない場合。
- ファブリック内のすべてのスイッチでロックが保持されているが、スイッチを保持しているロックを持つセッションが存在しない場合。

どちらの場合でも、clear オプションを使用してロックを解放する必要があります。

## CLI を使用したロックのクリア

リモート ピアでロックが保持されていて、「application-name commit」コマンドまたは「application-name abort」コマンドを実行してもロックがクリアされないときは、「clear application-name session」コマンドを使用してファブリック内のすべてのロックをクリアします。すべてのロックがクリアされた後、ファブリック内のすべてのスイッチを同じステートに戻すために新しい配信を開始する必要があります。

例：

```
switch# clear ntp session
switch# config terminal
switch(config)# ntp commit
switch(config)#
```

# 配信ステータスの確認

アプリケーションを設定して変更をコミットした後、ファブリックまたは VSAN 全体に設定変更が配信されたかどうかを確認できます。

## CLI を使用した配信の確認

「show cfs lock name application-name」コマンドを使用して、ファブリックで配信が進行中であるかどうかを確認します。該当するアプリケーションが出力に表示されない場合、配信は完了しています。

例：

```
switch(config)# show cfs lock name ntp

Scope      : Physical-fc-ip
------------------------------------------------------------------------------
 Switch WWN              IP Address                  User Name    User Type
------------------------------------------------------------------------------
 20:00:00:0d:ec:50:09:00 172.25.183.42               admin        CLI/SNMP v3

Total number of entries = 1
```

# CFS リージョンのトラブルシューティング

CFS リージョンには次のルールが適用されます。

- CFS リージョンを使用しているとき、特定のスイッチ上のアプリケーションは同時に 1 つのリージョンにのみ属することができます。
- CFS リージョンは、物理スコープ内のアプリケーションにのみ適用できます。アプリケーションの論理スコープで CFS リージョンを作成することはできません。
- アプリケーションへのリージョンの割り当ては、配信においてその初期物理スコープよりも優先されます。
- CFS リージョンの設定は、登録解除されたアプリケーション（条件付きサービス）または現在ロックされている物理スコープ アプリケーションについてはサポートされません。
- ユーザ設定に使用できるリージョンの範囲は 1 ～ 200 です。201 ～ 255 のリージョンは予約されており、ユーザ設定には使用できません。

## 配信の失敗

ある CFS リージョンにおけるすべてのスイッチへの設定配信の失敗を解決するには、次の手順を実行します。

**ステップ 1**　アプリケーションの配信がイネーブルになっていることを確認します。詳細については、「概要」（P.33）を参照してください。

**ステップ 2**　すべてのスイッチで、アプリケーションが同じリージョンにあることを確認します。

各スイッチで CLI を使用して、「show cfs application name application-name」コマンドを実行します。

例（device-alias アプリケーションの場合）：

```
switch(config)# show cfs lock name ntp
```

```
Scope      : Physical-fc-ip
--------------------------------------------------------------------------------
 Switch WWN              IP Address                   User Name    User Type
--------------------------------------------------------------------------------
 20:00:00:0d:ec:50:09:00 172.25.183.42                admin        CLI/SNMP v3

Total number of entries = 1
```

例（アプリケーションが結合可能で、デフォルト リージョンにある場合）：

```
switch(config)# sho cfs application name device-alias

 Enabled        : Yes
 Timeout        : 20s
 Merge Capable  : Yes
 Scope          : Physical-fc
 Region         : Default
```

例（アプリケーションが結合可能で、リージョン 1 にある場合）：

```
switch# show cfs application name device-alias
Enabled : Yes
Timeout : 20s
Merge Capable : Yes
Scope : Physical-fc
Region : 1
```

## 条件付きサービスのリージョン

条件付きサービスがダウンすると（CFS から登録解除されると）、そのリージョン設定が失われます。同じ条件付きサービスが再起動されると、自動的にデフォルト リージョンに配置されます。この状況を回避するには、条件付きサービスを再起動する前に適切なリージョン情報を再設定します。

## リージョンの変更

アプリケーションをあるリージョンから別のリージョンに移動した場合、結合しようとしたときにデータベースの不一致が起こることがあります。この不一致を特定して解決するには、「結合の失敗のトラブルシューティング」（P.36）を参照してください。

（注）　アプリケーションをあるリージョンから別のリージョン（デフォルト リージョンを含む）に移動すると、そのアプリケーションのすべての履歴が失われます。

# VSAN

ここでは、VSAN のトラブルシューティングの概要を示し、一般的な問題とその解決方法について説明します。

# 概要

VSAN に関するほとんどの問題は、VSAN 実装のベスト プラクティスに従うことで回避できます。

ただし、必要であれば、Fabric Manager のファブリック分析ツールを使用して、VSAN、ゾーン分割、FCdomain、管理に関する問題、スイッチ固有の問題、ファブリック固有の問題などのさまざまなカテゴリの問題を確認できます。

Fabric Manager にはコンフィギュレーション整合性チェック ツールがあります。

[Fabric Configuration] オプションを使用してスイッチのコンフィギュレーションを分析するには、次の手順を実行します。

**ステップ 1**　Fabric Manager のツール メニューから、[Health] > [Fabric Configuration] をクリックします。

[Fabric Configuration Analysis] ダイアログボックスが表示されます。

**ステップ 2**　選択したスイッチを別のスイッチと比較するか、またはポリシー ファイルと比較するかを決定します。

- 選択したスイッチを別のスイッチと比較するには、[Policy Switch] を選択し、スイッチのドロップダウン リストからスイッチを選択します。
- ポリシー ファイルと比較するには、[Policy File] を選択し、右側のボタンをクリックしてファイル システム上のポリシー ファイル（*.XML）を選択します。

**ステップ 3**　[Rules] をクリックし、Fabric Configuration Analysis ツールの実行時に適用するルールを設定します。

[Rules] ウィンドウが表示されます。

**ステップ 4**　必要に応じて既存のルールを変更し、[OK] をクリックします。

**ステップ 5**　[Compare] をクリックし、コンフィギュレーションを比較します。

分析結果が表示されます。

**ステップ 6**　[Resolve] 列で、解決する問題をクリックします。

**ステップ 7**　[Resolve Issues] をクリックし、特定された問題を解決します。

**ステップ 8**　[Clear] をクリックし、ウィンドウの内容を消去します。

**ステップ 9**　[Close] をクリックし、操作を終了してウィンドウを閉じます。

コンフィギュレーション整合性チェック ツールの詳細については、『*Cisco MDS 9000 Family Fabric Manager Configuration Guide, Release 5.x*』を参照してください。

**（注）**　VSAN を一時停止または削除するときは、一度に 1 つの VSAN を一時停止および一時停止解除するよう注意してください。vsan suspend コマンドを実行した後、別のコンフィギュレーション コマンドを実行するときは、60 秒以上待ってください。60 秒以上待たないと、一部のファイバ チャネル インターフェイス、または PortChannel のメンバー ポートが一時停止または errdisable になる場合があります。

SAN の問題のトラブルシューティングでは、個々のデバイスの設定と接続、および SAN ファブリック全体のステータスに関する情報を収集する必要があります。

## VSAN のトラブルシューティング操作

### Fabric Manager でよく使うトラブルシューティング ツール

Fabric Manager で VSAN を確認するには、次の手順を実行します。

- [Information] ペインに VSAN の設定を表示するには、[Fabricxx] > [VSANxx] を選択します。
- VSAN のメンバーを表示するには、[Fabricxx] > [VSANxx] を選択してから、[Information] ペインの [Host] または [Storage] タブを選択します。
- [Information] ペインに FC ドメインの設定を表示するには、[Fabricxx] > [VSANxx] > [Domain Manager] を選択します。

### トラブルシューティングによく使う CLI コマンド

VSAN、FC ドメイン、および FSPF の情報を表示するには、次の CLI コマンドを使用します。

```
show vsan
show vsan vsan-id
show vsan membership
show interface fc slot/port trunk vsan-id
show vsan-id membership
show vsan membership interface fc slot/port
```

### チェックリスト

次のことを確認します。

- VSAN 内のスイッチのドメイン パラメータを確認します。
- 問題のあるポートまたは VSAN の物理接続を確認します。
- 両方のデバイスがネーム サーバにあることを確認します。
- 両方のエンド デバイスが同じ VSAN にあることを確認します。
- 両方のエンド デバイスが同じゾーンにあることを確認します。

# Nexus 5000 トランク ポートがアップストリーム SAN スイッチに接続しない

Nexus 5000 トランク ポートがアップストリーム SAN スイッチに接続しないことを示す状況は、次のとおりです。

- アップストリーム スイッチに接続されたトランク ポートのステータスが「isolated」になります。
- スイッチポート トランク モードは両側でイネーブルになっています。
- 物理的なケーブル配線には問題はありません。
- ポートは両方のスイッチでアップしています。

次の例に示すように、インターフェイスのステートを調べ、インターフェイスの状況を照会することで、この問題が明らかになります。

例：

```
switch(config-if)# sho interf brief
```

```
--------------------------------------------------------------------------------
Interface  Vsan   Admin  Admin   Status          SFP    Oper  Oper   Port
                  Mode   Trunk                         Mode  Speed  Channel
                         Mode                                (Gbps)

fc2/3      1      E      on      isolated         swl    --           --

switch(config-if)# show interface fc 2/3
fc2/3 is down (Isolation due to no common vsans with peer on trunk)
    Hardware is Fibre Channel, SFP is short wave laser w/o OFC (SN)
    Port WWN is 20:43:00:0d:ec:da:6e:00
    Admin port mode is E, trunk mode is on
```

**考えられる原因**

両方のインターフェイスの VSAN 許可リストが同じではありません。具体的には、両方のインターフェイスで許可されている共通の VSAN がありません。

これは次のことが原因で起こる場合があります。

- 両方のスイッチに共通の VSAN がない。
- トランクで許可されている VSAN のメンバーに共通のメンバーが含まれていない。

この例では、Nexus 5000 と MDS の FC インターフェイス上のトランク VSAN 許可リストが一致していません。

**解決方法**

接続されたポートを確認し、両方の FC インターフェイスについてトランクで許可される VSAN を解決します。

例：

```
switch(config-if)# show run interface fc 2/3

!Command: show running-config interface fc2/3
!Time: Wed Aug  4 16:06:04 2010

version 4.2(1)N1(1)

interface fc2/3
  switchport mode E
  switchport trunk allowed vsan 1
  no shutdown

switch(config-if)# show run interface fc 1/1

!Command: show running-config interface fc1/1
!Time: Wed Aug  4 16:20:07 2010

version 5.0(1a)

interface fc1/1
  switchport rate-mode dedicated
  switchport mode E
  switchport trunk allowed vsan 100
  no shutdown

switch(config-if)# interface fc 2/3
switch(config-if)# switchport trunk allowed vsan
add   all
switch(config-if)# switchport trunk allowed vsan add 100
switch(config-if)# show run interface fc 2/3
```

```
!Command: show running-config interface fc2/3
!Time: Wed Aug  4 16:07:25 2010

version 4.2(1)N1(1)

interface fc2/3
  switchport mode E
  switchport trunk allowed vsan 1
  switchport trunk allowed vsan add 100
  no shutdown

switch(config-if)# switchport trunk allowed vsan add 1
switch(config-if)# show run interface fc 1/1

!Command: show running-config interface fc1/1
!Time: Wed Aug  4 16:20:54 2010

version 5.0(1a)

interface fc1/1
  switchport rate-mode dedicated
  switchport mode E
  switchport trunk allowed vsan 1
  switchport trunk allowed vsan add 100
  no shutdown

fc2/3 is trunking
    Hardware is Fibre Channel, SFP is short wave laser w/o OFC (SN)
    Port WWN is 20:43:00:0d:ec:da:6e:00
    Peer port WWN is 20:01:00:0d:ec:24:5b:c0
    Admin port mode is E, trunk mode is on
    snmp link state traps are enabled
    Port mode is TE
    Port vsan is 1
    Speed is 4 Gbps
    Transmit B2B Credit is 250
    Receive B2B Credit is 16
    Receive data field Size is 2112
    Beacon is turned off
    Trunk vsans (admin allowed and active) (1,100)
    Trunk vsans (up)                       (1,100)
    Trunk vsans (isolated)                 ()
    Trunk vsans (initializing)             ()

switch(config-if)# show interface brief

--------------------------------------------------------------------------------
Interface  Vsan   Admin  Admin   Status          SFP    Oper  Oper   Port
                  Mode   Trunk                         Mode  Speed  Channel
                         Mode                                (Gbps)

fc2/3      1      E      on      trunking         swl    TE      4    --
```

# Nexus 5000 E ポート（非トランキング）がアップストリーム SAN スイッチに接続しない

Nexus 5000 E ポートがアップストリーム SAN スイッチに接続しないことを示す状況は、次のとおりです。

- 相互接続された非トランキング E ポートのステータスを調べると、ステータスはアップになっています。ただし、すべてのファイバ チャネル サービスがスイッチ間で機能していません。
- どちらのスイッチでも、同じ VSAN 内のデバイスが FCNS データベースに表示されません。
- show topology コマンドでピア スイッチ情報が表示されません。
- ゾーンでは、メンバーがログインしていないと表示されます。

例：

```
switch(config-vsan-db)# show interface brief

--------------------------------------------------------------------------------
Interface  Vsan   Admin  Admin   Status          SFP    Oper  Oper   Port
                  Mode   Trunk                         Mode  Speed  Channel
                         Mode                                (Gbps)
--------------------------------------------------------------------------------
fc2/4      50     E      off     up               swl    E       2    --

switch(config-if)# sho interface brief

--------------------------------------------------------------------------------
Interface  Vsan   Admin  Admin   Status          SFP    Oper  Oper   Port
                  Mode   Trunk                         Mode  Speed  Channel
                         Mode                                (Gbps)
--------------------------------------------------------------------------------
fc1fc1/2      100    E      off     up               swl    E       2    --
```

FC トポロジは有効なピア インターフェイスを示しません。

例：

```
switch(config-if)# show topo

FC Topology for VSAN 100 :
--------------------------------------------------------------------------------
       Interface  Peer Domain Peer Interface     Peer IP Address
--------------------------------------------------------------------------------
            fc1/2  0x42(66)      Port 65795   ::

The zoneset shows one member is not active

switch(config-vsan-db)# show zoneset active vsan 100
zoneset name ZoneSet_Host_Storage vsan 100
  zone name Zone_Host_Storage vsan 100
    pwwn 20:00:00:25:b5:00:20:0e [Host]
  * fcid 0x5a0000 [pwwn 50:0a:09:81:86:78:39:66] [Storage]

switch(config-if)# show zoneset active vsan 100
zoneset name ZoneSet_Host_Storage vsan 100
  zone name Zone_Host_Storage vsan 100
  * fcid 0x640114 [pwwn 20:00:00:25:b5:00:20:0e] [Host]
    pwwn 50:0a:09:81:86:78:39:66 [Storage]
```

ストレージとホストは正しい VSAN に属しています。

例：

```
switch(config-vsan-db)# show flogi database vsan 100
--------------------------------------------------------------------------------
INTERFACE        VSAN    FCID           PORT NAME               NODE NAME
--------------------------------------------------------------------------------
fc2/2            100   0x5a0000  50:0a:09:81:86:78:39:66 50:0a:09:80:86:78:39:66
                         [Storage]

switch(config-if)# show flogi database vsan 100
--------------------------------------------------------------------------------
INTERFACE        VSAN    FCID           PORT NAME               NODE NAME
--------------------------------------------------------------------------------
fc4/2            100   0x640114  20:00:00:25:b5:00:20:0e 20:00:00:25:b5:02:02:09
                         [Host]
```

**考えられる原因**

このエラーは、「show interface brief」コマンドと「show vsan membership」コマンドによって表示されます。これらのコマンドは、一方のスイッチの E ポートが間違った VSAN に属していることを示します。

一方のスイッチの非トランキング E ポートが間違った VSAN に属しています（VSAN 100 が正しい VSAN です）。

例：

```
switch(config-if)# sho interface brief

--------------------------------------------------------------------------------
Interface  Vsan   Admin  Admin   Status          SFP    Oper  Oper   Port
                 Mode   Trunk                          Mode  Speed  Channel
                        Mode                                 (Gbps)
--------------------------------------------------------------------------------
fc1fc1/2   100    E      off     up               swl    E       2    --
```

**解決方法**

非トランキング E ポートを VSAN 100 に移動します。

例：

```
switch(config-vsan-db)# vsan 100 interface fc 2/4
Traffic on fc2/4 may be impacted. Do you want to continue? (y/n) [n] y
```

これでゾーンセットがアクティブになり、FC トポロジが正しくなります。

例：

```
switch(config-if)# show zoneset active vsan 100
zoneset name ZoneSet_Host_Storage vsan 100
  zone name Zone_Host_Storage vsan 100
  * fcid 0x640114 [pwwn 20:00:00:25:b5:00:20:0e] [Host]
  * fcid 0x5a0000 [pwwn 50:0a:09:81:86:78:39:66] [Storage]
switch(config-if)# show topology

FC Topology for VSAN 100 :
--------------------------------------------------------------------------------
       Interface  Peer Domain Peer Interface     Peer IP Address
--------------------------------------------------------------------------------
            fc1/2  0x5a(90)            fc2/4  172.25.183.124
```

# ホストとストレージ デバイス間の通信の問題

ホストとストレージ デバイス間の通信の問題を示す状況は、次のとおりです。

- ゾーンはアクティブです。
- ホストとストレージの両方が SAN にログインしています。
- ストレージ ポートがアクティブ ゾーンセットにログインしていません。

例：

```
zoneset name ZoneSet_Host_Storage vsan 100
  zone name Zone_Host_Storage vsan 100
  * fcid 0x640114 [pwwn 20:00:00:25:b5:00:20:0e] [Host]
    pwwn 50:0a:09:81:86:78:39:66 [Storage]
```

**考えられる原因**

ホストまたはストレージ ポートが間違った VSAN に属しています。

例：

```
switch(config)# show fcns database

VSAN 50:
--------------------------------------------------------------------------
FCID        TYPE  PWWN                    (VENDOR)        FC4-TYPE:FEATURE
--------------------------------------------------------------------------
0x420000    N     50:0a:09:81:86:78:39:66 (NetApp)        scsi-fcp:target
                  [Storage]
```

**解決方法**

ストレージ ポートを正しい VSAN に移動します（この例では、VSAN 100 が正しい VSAN です）。

例：

```
switch(config)# show flogi database vsan 50
--------------------------------------------------------------------------------
INTERFACE        VSAN    FCID           PORT NAME               NODE NAME
--------------------------------------------------------------------------------
fc2/2            50    0x420000  50:0a:09:81:86:78:39:66 50:0a:09:80:86:78:39:66
                         [Storage]

Total number of flogi = 1.

switch(config)# vsan database
switch(config-vsan-db)# vsan 100 interface fc 2/2
Traffic on fc2/2 may be impacted. Do you want to continue? (y/n) [n] y
switch(config-vsan-db)# show zoneset active vsan 100
zoneset name ZoneSet_Host_Storage vsan 100
  zone name Zone_Host_Storage vsan 100
  * fcid 0x640114 [pwwn 20:00:00:25:b5:00:20:0e] [Host]
  * fcid 0x5a0000 [pwwn 50:0a:09:81:86:78:39:66] [Storage]
```

# スイッチ間の VSAN がダウンしている

スイッチ間の VSAN がダウンしている問題を示す状況は、次のとおりです。

- 両方のスイッチで VSAN が設定されています。
- トランク許可リストによってその VSAN が許可されています。

- VSAN がダウンしている（初期化ステート）と報告されます。
- ゾーンはアクティブです。
- ホストとストレージの両方が SAN にログインしています。

この障害では、ストレージ ポートがアクティブ ゾーンセットにログインしていません。

次の例に示すように、インターフェイスを調べるとエラーが表示されます。

例：

```
switch(config-if)# show interface fc 2/4 trunk vsan 10
fc2/4 is trunking
    Vsan 10 is down (Isolation due to domain id assignment failure)

switch(config-if)# show port internal info interface fc 2/4 | grep Isolation
  fc2/4, Vsan 10 - state(down), state reason(Isolation due to domain id assignment
failure), fcid(0x000000)
  fc2/4, Vsan 50 - state(down), state reason(Isolation due to vsan not configured on
peer), fcid(0x000000)
```

### 考えられる原因

複数の VSAN に同じスタティック DomainID が設定されている可能性があります。

例：

```
switch(config-if)# show fcdomain domain-list vsan 10

Number of domains: 1
Domain ID              WWN
---------    -----------------------
 0x53(83)    20:0a:00:0d:ec:da:6e:01 [Local] [Principal]

switch(config)# show fcdomain domain-list vsan 10

Number of domains: 1
Domain ID              WWN
---------    -----------------------
 0x53(83)    20:0a:00:0d:ec:24:5b:c1 [Local] [Principal]
```

### 解決方法

いずれかの VSAN の DomainID を変更します。

例：

```
switch(config)# vsan database
switch(config-vsan-db)# vsan 10 suspend
switch(config-vsan-db)# no vsan 10 suspend
switch(config-vsan-db)# show interface fc 2/4

Number of domains: 1
Domain ID              WWN
---------    -----------------------
 0x52(82)    20:0a:00:0d:ec:da:6e:01 [Local] [Principal]

switch(config-vsan-db)# sho interface fc 2/4  | begin Trunk
    Trunk vsans (admin allowed and active) (1,10,50,100)
    Trunk vsans (up)                       (1,10,50,100)
    Trunk vsans (isolated)                 ()
    Trunk vsans (initializing)             ()
```

# レジスタとカウンタ

## 物理層の問題の特定

ファイバ チャネル SFP 光ファイバに関する物理層の問題をトラブルシューティングするには、次のコマンドを使用します。

```
switch# show interface fc x/y transceiver details
```

次の例では、サポートされている速度、公称ビット レート、SFP でサポートされているリンク長などの有用な情報がコマンドの結果に含まれていることがわかります。

例：

```
switch# show interface fc 3/1 transceiver details
fc3/1 sfp is present
    name is CISCO-FINISAR
    part number is FTLF8524P2BNL-C2
    revision is 0000
    serial number is FNS0928K161
    fc-transmitter type is short wave laser w/o OFC (SN)
    fc-transmitter supports intermediate distance link length
    media type is multi-mode, 62.5m (M6)
    Supported speed is 400 MBytes/sec
    Nominal bit rate is 4300 MBits/sec
    Link length supported for 50/125mm fiber is 150 m(s)
    Link length supported for 62.5/125mm fiber is 70 m(s)
    cisco extended id is unknown (0x0)

    no tx fault, no rx loss, in sync state, Diag mon type 104
```

このコマンドは、詳細な SFP 診断情報と警告およびアラーム（存在する場合）も出力します。

例：

```
SFP Detail Diagnostics Information
  ------------------------------------------------------------------------------
                                    Alarms                  Warnings
                                 High        Low         High          Low
  ------------------------------------------------------------------------------
  Temperature  41.50 C         95.00 C    -25.00 C     90.00 C      -20.00 C
  Voltage       3.45 V          3.90 V      2.70 V      3.70 V        2.90 V
  Current       7.18 mA        17.00 mA     1.00 mA    14.00 mA       2.00 mA
  Tx Power     -4.41 dBm       -2.00 dBm  -11.74 dBm   -2.00 dBm    -11.02 dBm
  Rx Power     -4.40 dBm        1.00 dBm  -20.00 dBm   -1.00 dBm    -18.24 dBm
  Transmit Fault Count = 0
  ------------------------------------------------------------------------------
  Note: ++  high-alarm; +  high-warning; --  low-alarm; -  low-warning
```

次に、このコマンドの出力例を 2 つ示します。最初の例は、RX 電力の下限アラームを示します。2 番目の例は、TX、RX、および電流の下限アラームを示します。2 番目の例の問題となっているインターフェイスは、ビット エラー レートが高すぎることが原因で「Error Disabled」ステートになっていました。

### RX 電力の下限アラーム

```
--------------------------------------------------------------------------------
                                    Alarms                  Warnings
                                 High        Low         High          Low

--------------------------------------------------------------------------------
   Temperature  35.02 C         70.00 C      0.00 C     70.00 C        0.00 C
   Voltage       0.00 V          0.00 V      0.00 V      0.00 V        0.00 V
   Current       7.22 mA        16.00 mA     2.00 mA    14.00 mA       2.40 mA
   Tx Power     -0.57 dBm        1.00 dBm   -8.21 dBm    0.00 dBm     -7.21 dBm
   Rx Power    -18.86 dBm --     1.00 dBm  -16.58 dBm    0.00 dBm    -14.44 dBm

--------------------------------------------------------------------------------
   Note: ++  high-alarm; +  high-warning; --  low-alarm; -  low-warning
```

### 電流、TX 電力、および RX 電力の下限アラーム

```
--------------------------------------------------------------------------------
                                    Alarms                  Warnings
                                 High        Low         High          Low

--------------------------------------------------------------------------------
   Temperature  32.75 C         70.00 C      0.00 C     70.00 C        0.00 C
   Voltage       0.00 V          0.00 V      0.00 V      0.00 V        0.00 V
   Current       0.00 mA  --    16.00 mA     2.00 mA    14.00 mA       2.40 mA
   Tx Power       N/A     --     1.00 dBm   -8.21 dBm    0.00 dBm     -7.21 dBm
   Rx Power    -22.22 dBm --     1.00 dBm  -16.58 dBm    0.00 dBm    -14.44 dBm

--------------------------------------------------------------------------------
   Note: ++  high-alarm; +  high-warning; --  low-alarm; -  low-warning
```

次の例では、Twinax（銅）の詳細なトランシーバ情報は示されていないことに注意してください。

```
switch# sh interface ethernet 1/19 transceiver details
Ethernet1/19
    sfp is present
    name is Molex Inc.
    part number is 74752-1301
    revision is E
    serial number is 733010037
    nominal bitrate is 0 MBits/sec
    Link length supported for 50/125mm fiber is 0 m(s)
    Link length supported for 62.5/125mm fiber is 0 m(s)
    cisco id is --
    cisco extended id number is 4

    Invalid calibration
```

# FcoE にバインドされたイーサネット インターフェイスのカウンタの表示

「show interface ethernet」コマンドには簡易版と詳細版の 2 種類があります。それぞれの例を次に示します。

### 簡易版

例：

（注）　ジャンボ フレームが増えていることと、RX または TX ポーズ フレーム カウンタ（存在する場合）を確認してください。後者は輻輳の問題を示す場合があります。

```
switch# show interface ethernet 1/4
Ethernet1/4 is up
  Hardware: 1000/10000 Ethernet, address: 000d.ecd5.a38b (bia 000d.ecd5.a38b)
  MTU 1500 bytes, BW 10000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA
  Port mode is trunk
  full-duplex, 10 Gb/s, media type is 10g

  [省略]

  RX
    9507 unicast packets  918874 multicast packets  3473 broadcast packets
    931854 input packets  76225281 bytes
    7121 jumbo packets  0 storm suppression packets
    0 runts  0 giants  0 CRC  0 no buffer
    0 input error  0 short frame  0 overrun   0 underrun  0 ignored
    0 watchdog  0 bad etype drop  0 bad proto drop  0 if down drop
    0 input with dribble  0 input discard
    0 Rx pause
  TX
    3986 unicast packets  294583 multicast packets  36307 broadcast packets
    334876 output packets  46873259 bytes
    1227 jumbo packets
    0 output errors  0 collision  0 deferred  0 late collision
    0 lost carrier  0 no carrier  0 babble
    2266 Tx pause
  24 interface resets
```

### 詳細版

次の例では、「show interface ethernet」コマンドの詳細版の出力を分けて示しています。これには、通常トラフィックのカウンタと物理層およびプロトコル エラーのカウンタがどちらも含まれます。接続やパフォーマンスの問題があるときは常にこれらのカウンタをモニタしてください。

例：

```
switch# sh interface ethernet 1/4 counters detailed all Ethernet1/4

  64 bit counters:
   0.                      rxHCTotalPkts = 931881
   1.                       txHCTotalPks = 335522
   2.                    rxHCUnicastPkts = 9507
   3.                    txHCUnicastPkts = 3986
   4.                  rxHCMulticastPkts = 918901
   5.                  txHCMulticastPkts = 295229
   6.                  rxHCBroadcastPkts = 3473
   7.                  txHCBroadcastPkts = 36307
```

```
   8.                          rxHCOctets = 76228116
   9.                          txHCOctets = 46926647
  10.                 rxTxHCPkts64Octets = 1065359
  11.              rxTxHCpkts65to127Octets = 105246
  12.             rxTxHCpkts128to255Octets = 43798
  13.             rxTxHCpkts256to511Octets = 13822
  14.            rxTxHCpkts512to1023Octets = 30742
  15.           rxTxHCpkts1024to1518Octets = 88
  16.           rxTxHCpkts1519to1548Octets = 0
  17.                      rxHCTrunkFrames = 895722
  18.                      txHCTrunkFrames = 69387
  19.                       rxHCDropEvents = 0

All Port Counters:
   0.                            InPackets = 931881
   1.                             InOctets = 76228116
   2.                          InUcastPkts = 9507
   3.                          InMcastPkts = 918901
   4.                          InBcastPkts = 3473
   5.                          InJumboPkts = 7121
   6.                    StormSuppressPkts = 0
   7.                           OutPackets = 335522
   8.                            OutOctets = 46926647
   9.                          OutUcastPkts = 3986
  10.                          OutMcastPkts = 295229
  11.                          OutBcastPkts = 36307
  12.                          OutJumboPkts = 1227
  13.                    rxHCPkts64Octets = 889975
  14.                 rxHCPkts65to127Octets = 26702
  15.                rxHCPkts128to255Octets = 6072
  16.                rxHCPkts256to511Octets = 1913
  17.               rxHCpkts512to1023Octets = 11
  18.              rxHCpkts1024to1518Octets = 87
  19.              rxHCpkts1519to1548Octets = 0
  20.                    txHCPkts64Octets = 175384
  21.                 txHCPkts65to127Octets = 78544
  22.                txHCPkts128to255Octets = 37726
  23.                txHCPkts256to511Octets = 11909
  24.               txHCpkts512to1023Octets = 30731
  25.              txHCpkts1024to1518Octets = 1
  26.              txHCpkts1519to1548Octets = 0
  27.                           ShortFrames = 0
  28.                            Collisions = 0
  29.                             SingleCol = 0
  30.                              MultiCol = 0
  31.                               LateCol = 0
  32.                          ExcessiveCol = 0
  33.                           LostCarrier = 0
  34.                             NoCarrier = 0
  35.                                 Runts = 0
  36.                                Giants = 0
  37.                              InErrors = 0
  38.                             OutErrors = 0
  39.                          InputDiscards = 0
  40.                          BadEtypeDrops = 0
  41.                            IfDownDrops = 0
  42.                         InUnknownProtos = 0
  43.                               txErrors = 0
  44.                                  rxCRC = 0
  45.                                 Symbol = 0
  46.                              txDropped = 0
  47.                          TrunkFramesTx = 69387
  48.                          TrunkFramesRx = 895722
  49.                             WrongEncap = 0
```

```
50.                          Babbles = 0
51.                        Watchdogs = 0
52.                              ECC = 0
53.                         Overruns = 0
54.                        Underruns = 0
55.                          Dribbles = 0
56.                          Deferred = 0
57.                           Jabbers = 0
58.                          NoBuffer = 0
59.                           Ignored = 0
60.                       bpduOutLost = 0
61.                       cos0OutLost = 0
62.                       cos1OutLost = 0
63.                       cos2OutLost = 0
64.                       cos3OutLost = 0
65.                       cos4OutLost = 0
66.                       cos5OutLost = 0
67.                       cos6OutLost = 0
68.                       cos7OutLost = 0
69.                           RxPause = 0
70.                           TxPause = 2266
71.                            Resets = 0
72.                           SQETest = 0
73.                    InLayer3Routed = 0
74.               InLayer3RoutedOctets = 0
75.                   OutLayer3Routed = 0
76.              OutLayer3RoutedOctets = 0
77.                   OutLayer3Unicast = 0
78.             OutLayer3UnicastOctets = 0
79.                 OutLayer3Multicast = 0
80.           OutLayer3MulticastOctets = 0
81.                    InLayer3Unicast = 0
82.               InLayer3UnicastOctets = 0
83.                   InLayer3Multicast = 0
84.              InLayer3MulticastOctets = 0
85.                InLayer3AverageOctets = 0
86.              InLayer3AveragePackets = 0
87.               OutLayer3AverageOctets = 0
88.             OutLayer3AveragePackets = 0
```

# ファイバ チャネル インターフェイスのカウンタについて

「show interface」コマンドは、ファイバ チャネル インターフェイスに関する物理層またはパフォーマンスの問題をトラブルシューティングするときに非常に便利です。

このコマンドの出力では、入力/出力カウンタと入力/出力の廃棄またはエラーに注意します。

入力廃棄が増えるときは、Forwarding Information Base（FIB; 転送情報ベース）内にその FC パケットの有効なルートがありません。ルートを持たないパケットはすべて廃棄と見なされ、スーパーバイザに送信されます。これらのパケットはドロップされないことに注意してください。ただし、スーパーバイザに送信される前にポリシングされます。また、MAC ASIC にエラーがないかチェックする必要があります。

出力廃棄が増えるときは、出力が遅すぎるためにパケットが出力でタイムアウトしています。接続先のデバイスが、バッファ クレジットに応答しない、またはバッファ クレジットを補充しない低速ドレイン レシーバである可能性があるため、接続先のデバイスを確認します。この場合は、Nexus 5000 FC インターフェイスでバック プレッシャが起こります。

例：

```
switch# show interface fc2/1
fc2/1 is trunking
```

```
    Hardware is Fibre Channel, SFP is short wave laser w/o OFC (SN)
    Port WWN is 20:41:00:0d:ec:a4:02:80

[省略]

    1 minute input rate 5048 bits/sec, 631 bytes/sec, 9 frames/sec
    1 minute output rate 6752 bits/sec, 844 bytes/sec, 9 frames/sec
      36398816 frames input, 2422447564 bytes
        0 discards, 0 errors
        0 CRC,  0 unknown class
        0 too long, 0 too short
      36368010 frames output, 3213593392 bytes
        0 discards, 0 errors
      1 input OLS, 1 LRR, 0 NOS, 0 loop inits
      1 output OLS, 2 LRR, 0 NOS, 0 loop inits
      16 receive B2B credit remaining
      250 transmit B2B credit remaining
      0 low priority transmit B2B credit remaining
    Interface last changed at Thu Jan 28 18:26:30 2010
```

# ファイバ チャネルの MAC に関する問題のトラブルシューティング

「show hardware」コマンドは、FC の物理層の問題をトラブルシューティングするときに非常に便利です。

```
Show hardware internal fc-mac x port y statistics
```

このコマンドの出力には、次の有用な情報が含まれます。

- 物理層の情報

  ```
  FCP_CNTR_MAC_RX_LOSS_OF_SYNC - Loss of Sync received counter
  ```

- パフォーマンスの情報

  ```
  FCP_CNTR_MAC_CREDIT_IG_XG_MUX_SEND_RRDY_REQ - Receiver Ready's Sent
  FCP_CNTR_MAC_CREDIT_EG_DEC_RRDY - Receiver Ready's Received
  ```

- クラス 3 通常トラフィックのカウンタ

  ```
  FCP_CNTR_MAC_DATA_RX_CLASS3_FRAMES
  FCP_CNTR_MAC_DATA_RX_CLASSF_FRAMES
  FCP_CNTR_MAC_DATA_RX_CLASS3_WORDS
  FCP_CNTR_MAC_DATA_RX_CLASSF_WORDS
  FCP_CNTR_MAC_DATA_TX_CLASS3_FRAMES
  FCP_CNTR_MAC_DATA_TX_CLASSF_FRAMES
  FCP_CNTR_MAC_DATA_TX_CLASS3_WORDS
  FCP_CNTR_MAC_DATA_TX_CLASSF_WORDS
  ```

- ファイバ チャネルのプリミティブ シーケンス

  ```
  FCP_CNTR_LINK_RESET_IN - Link Resets Received
  FCP_CNTR_OLS_OUT- Offline Sequences Sent
  FCP_CNTR_NOS_OUT - Not Operational Sequence Sent
  FCP_CNTR_LRR_OUT - Link Reset Responses Sent
  FCP_CNTR_LINK_FAILURE
  ```

例：

```
switch# show hardware internal fc-mac 2 port 1 statistics
 ADDRESS     STAT                                                  COUNT
__________ ________                                          ____________________
0x0000003c FCP_CNTR_MAC_RX_LOSS_OF_SYNC                                       0x5
0x0000003d FCP_CNTR_MAC_RX_BAD_WORDS_FROM_DECODER                            0xec
```

```
0x00000042 FCP_CNTR_MAC_CREDIT_IG_XG_MUX_SEND_RRDY_REQ                  0x5ec
0x00000043 FCP_CNTR_MAC_CREDIT_EG_DEC_RRDY                              0xc41
0x00000061 FCP_CNTR_MAC_DATA_RX_CLASS3_FRAMES                           0x5d2
0x00000062 FCP_CNTR_MAC_DATA_RX_CLASSF_FRAMES                            0x1a
0x00000069 FCP_CNTR_MAC_DATA_RX_CLASS3_WORDS                         0x140b14
0x0000006a FCP_CNTR_MAC_DATA_RX_CLASSF_WORDS                            0xdcc
0x00000065 FCP_CNTR_MAC_DATA_TX_CLASS3_FRAMES                           0xc24
0x00000066 FCP_CNTR_MAC_DATA_TX_CLASSF_FRAMES                            0x1d
0x0000006d FCP_CNTR_MAC_DATA_TX_CLASS3_WORDS                         0x4b9538
0x0000006e FCP_CNTR_MAC_DATA_TX_CLASSF_WORDS                            0xabc
0xffffffff FCP_CNTR_LINK_RESET_IN                                        0x2
0xffffffff FCP_CNTR_OLS_OUT                                              0x5
0xffffffff FCP_CNTR_NOS_OUT                                              0x2
0xffffffff FCP_CNTR_LRR_OUT                                              0x7
0xffffffff FCP_CNTR_LINK_FAILURE                                         0x2
```

FC のパフォーマンスの問題をトラブルシューティングするときは、R_RDY、Link Reset、Link Reset Response の各カウンタを調べます。これらのカウンタは、パフォーマンスの問題を引き起こす可能性があるバッファ ツー バッファ クレジットの問題を判別するのに役立ちます。

# ファイバ チャネルの転送に関する問題のトラブルシューティング

ファイバ チャネルの転送に関する問題をトラブルシューティングするには、N5K に GATOS という MAC/転送 ASIC が搭載されていることを知っておくことが重要です。ここでは、この ASIC 専用のコマンドについて説明します。

各ファイバ チャネル インターフェイスには GATOS 番号が割り当てられるので、転送の問題を理解するには、問題になっている FC インターフェイスの GATOS 番号を特定する必要があります。

次の例について考えます。

```
switch# sh platform fwm info pif fc2/1
dump pif info: ifindex 0x1080000 dump_all 0 verbose 1
fc2/1: slot 1 port 0 state 0x0 pi_if 0x88bbb74 fwimpd ctx 0x889d4ec
fc2/1: oper_mode 0x1 rcvd_rbind: No
fc2/1: iftype 0x1  encap 0x5  bound_if? N #lifs 1 fwimpd ctx 0x88bd74c
fc2/1: lif_blk(pi) 0x8523da4 vif_id_alloc_bmp 0x887360c
fc2/1: cfg_lif_blk_size 0 lif_blk_base(pi) 1922 lif_blk_size(pi) 1
fc2/1: cfg_lif_blk_size(pi) 0
fc2/1: if_flags 0x0 num_sub_lif_tbls 0 Num HIFs pinned 0
fc2/1 pd: lif_entries 1  if_map_idx 49  if_lid 33 if_fcoe_lid 34
fc2/1 pd: reverse ifmap lookup 'same' ifmap_idx 49
fc2/1: SAT_HIF Port?: No
```

この例の次の部分で、gatos_num 13 がファイバ チャネル インターフェイス 2/1 の GATOS インスタンスであることがわかります。

```
fc2/1 pd: slot 1  logical port num 4  gatos_num 13  fwm_inst 0  fc 0
fc2/1 pd: pif_type 'data fc'(2) hw_present 1  port map idx 49
fc2/1 pd: fabric a info: voq 0-1  port_id 29 connected 1 up 1
fc2/1 pd: fabric b info: voq 0-1  port_id 29 connected 1 up 1
fc2/1 pd: subported 1 primary 1 atherton 0
fc2/1 pd: sup_src_dst_if 17  lif_blk 0-0
fc2/1 pd: policer info: uc (sel 2) mc (sel 1) bc (sel 0)
fc2/1 pd: mac-addr 000d.eca4.02b4
```

この例の次の部分で、転送のドロップおよび廃棄情報も出力されていることがわかります。

```
fc2/1 pd: tx stats: bytes 4958178736 frames 36360131 discard 0 drop 0
fc2/1 pd: rx stats: bytes 2421909296 frames 36390924 discard 0 drop 0
```

また、問題の FC インターフェイスに対応する GATOS インスタンスの GATOS エラーを表示することもできます。この例の次の部分で、このコマンドではゼロでないカウンタのみが表示されることがわかります。

```
switch# show platform fwm info gatos-errors 13
Printing non zero Gatos error registers:
DROP_FCF_SW_VSAN_IDX_MISS: res0 = 60 res1 = 0
DROP_FCF_SW_DOMAIN_IDX_MISS: res0 = 489036 res1 = 0
DROP_FCF_SW_TBL_MISS: res0 = 489036 res1 = 0
DROP_NO_FABRIC_SELECTED: res0 = 489036 res1 = 0
DROP_VLAN_MASK_TO_NULL: res0 = 489036 res1 = 0
```

上の 2 つの部分の最初の方に、ドロップと廃棄が示されています。vethernet および VFC インターフェイスではドロップ カウンタと廃棄カウンタは分かれていることに注意してください。2 番目の例の出力を見ると、ドロップの理由を関連付けるのに役立ちます。

```
switch# show platform fwm info pif ethernet 1/4
dump pif info: ifindex 0x1a003000 dump_all 0 verbose 1
Eth1/4: slot 0 port 3 state 0x0 pi_if 0x876acb4 fwimpd ctx 0x876171c
Eth1/4: oper_mode 0x100000 rcvd_rbind: No
Eth1/4: iftype 0x1  encap 0x1  bound_if? Y #lifs 1 fwimpd ctx 0x879f70c
Eth1/4: lif_blk(pi) 0x87cc9a4 foo vif_id_alloc_bmp 0x88313f4
Eth1/4:    0
Eth1/4: cfg_lif_blk_size 0 lif_blk_base(pi) 512 lif_blk_size(pi) 128
Eth1/4: cfg_lif_blk_size(pi) 0
Eth1/4: if_flags 0x0 num_sub_lif_tbls 0 Num HIFs pinned 0
Eth1/4: max_hifpc_mbrs 0, max_hif_ports 0
Eth1/4 pd: lif_entries 1  if_map_idx 8  if_lid 35 if_fcoe_lid 36
Eth1/4 pd: reverse ifmap lookup 'same' ifmap_idx 8
Eth1/4: SAT_HIF Port?: No
Eth1/4 pd: slot 0  logical port num 3  gatos_num 0  fwm_inst 0  fc 0
Eth1/4 pd: pif_type 'data eth'(1) hw_present 1  port map idx 8
Eth1/4 pd: fabric a info: voq 0-7  port_id 55 connected 1 up 1
Eth1/4 pd: fabric b info: voq 0-7  port_id 55 connected 1 up 1
Eth1/4 pd: subported 0 primary 1 atherton 0
Eth1/4 pd: sup_src_dst_if 6  lif_blk 384-511
Eth1/4 pd: policer info: uc (sel 2) mc (sel 1) bc (sel 0)
Eth1/4 pd: mac-addr 000d.ecd5.a38b
```

この例の次の部分の 2 行目にドロップが示されています。

```
Eth1/4 pd: tx stats: bytes 50256531 frames 336488 discard 0 drop 0
Eth1/4 pd: rx stats: bytes 6718252 frames 77220 discard 0 drop 845482
```

この例の次の部分で、FcoE カウンタが分かれていることがわかります。

```
Eth1/4 pd fcoe: tx stats: bytes 2927716 frames 3919 discard 0 drop 0
Eth1/4 pd fcoe: rx stats: bytes 15307492 frames 9470 discard 0 drop 0
```

この例の次の部分で、このコマンドがドロップの原因の特定に役立つことがわかります。

```
switch# show platform fwm info gatos-errors 0
Printing non zero Gatos error registers:
DROP_INGRESS_FW_PARSING_ERROR: res0 = 93 res1 = 0
DROP_SRC_VLAN_MBR: res0 = 2567226 res1 = 0
DROP_FCF_SW_DOMAIN_IDX_MISS: res0 = 2445 res1 = 0
DROP_FCF_SW_TBL_MISS: res0 = 2445 res1 = 0
DROP_NO_FABRIC_SELECTED: res0 = 2556 res1 = 0
DROP_VLAN_MASK_TO_NULL: res0 = 2556 res1 = 0
DROP_SRC_MASK_TO_NULL: res0 = 522 res1 = 0
```