Contents

Troubleshooting Zones and Zone Sets

This section describes how to identify and resolve problems that might occur while implementing zones and zone sets on switches in the Cisco MDS 9000 Family. It includes the following sections:

- Overview
- Troubleshooting Checklist

- Zone and Zone Set Issues
- Zone Merge Failure
- Enhanced Zoning Issues

Overview

Zoning enables access control between storage devices and user groups. Creating zones increases network security and prevents data loss or corruption.

Zone sets consist of one or more zones in a VSAN. A zone set can be activated or deactivated as a single entity across all switches in the fabric, but only one zone set can be activated at any time in a VSAN.

Zones can be members of more than one zone set. A zone consists of multiple zone members. Members in a zone can access each other; members in different zones cannot access each other.

Troubleshooting Checklist

The following criteria must be met for zoning to function properly:

Checklist	Check off
Verify that you have an active zone set.	
Verify that you have the correct hosts and storage devices in the same zone.	
Verify that the zone is part of the active zone set.	
Verify that the default zone policy is permit if you are not using zoning.	
Verify that you have only pWWN-based zoning if you have a Cisco MDS 9020 fabric switch in your fabric.	

For zone configuration problems, use the following helpful tools:

- Cisco Fabric Analyzer. (See the "Cisco Fabric Analyzer" section.)

- Cisco Fabric Manager and CLI system messages. (See the "System Messages" section.)

- Log messages (See the "Troubleshooting with Logs" section.)

Troubleshooting Zone Configuration Issues with Fabric Manager

Much of the information accessible through Fabric Manager can also be accessed using the CLI. (See the "Troubleshooting Zone Configuration Issues with the CLI" section.)

To verify which devices belong to the active zone set on a specific VSAN using Fabric Manager, follow these steps:

1. Choose **Tools > Edit Full Zone Database**. You see the Select VSAN dialog box.

2. Select a VSAN and click **OK**. You see the Edit Local Full Zone Database dialog box for the selected VSAN.

3. Click **Zones** in the left pane. The right pane lists the members for each zone.

Note: The active zone set appears in bold. If there is no zone set in bold, you have not activated a zone set for this VSAN.

Troubleshooting Zone Configuration Issues with the CLI

Much of the information accessed and summarized using Fabric Manager can also be found using CLI **show** commands.

Table 14-1 Zone Troubleshooting Commands in the CLI

Command	Command Description
show zone analysis [active] vsan *vsan-id*	Displays zone database information for a specific VSAN
show zone name *zonename*	Displays members of a specific zone.
show device-alias database| Displays any device aliases configured.	
show fcalias *vsan-id*	Displays if and how FC aliases are configured.
show zone member *pWWN-id, fcalias-id, or pWWN-id*	Displays all zones to which a member belongs using the FC ID, the FC alias, or the pWWN.
show zone statistics	Displays the number of control frames exchanged with other switches.
show zone internal *vsan-id*	Displays the internal state of the zone server for a specific VSAN.
show zoneset *zonesetname*	Displays information about the named zone set.
show zoneset active	Displays information about the active zone set.
show zone tech-support	Gathers relevant zoning information that may be requested by your customer support representative when troubleshooting zoning issues.

Note: To issue commands with the **internal** keyword, you must have a network-admin group account.

To better manage the zones and zone sets on your switch, you can display zone and zone set information using the **show zone analysis** command. (See Example 14-1 through Example 14-3.)

Example 14-1 Full Zoning Analysis

```
switch# show zone analysis vsan 1
Zoning database analysis vsan 1
 Full zoning database
   Last updated at: 15:57:10 IST Feb 20 2006
```

```
   Last updated by: Local [ CLI ]
   Num zonesets: 1
   Num zones: 1
   Num aliases: 0
   Num attribute groups: 0
   Formattted size: 36 bytes / 2048 Kb
 Unassigned Zones: 1
   zone name z1 vsan 1
```

Example 14-2 Active Zoning Database Analysis

```
switch# show zone analysis active vsan 1
Zoning database analysis vsan 1
  Active zoneset: zs1 [*]
    Activated at: 08:03:35 UTC Nov 17 2005
    Activated by: Local [ GS ]
    Default zone policy: Deny
    Number of devices zoned in vsan: 0/2 (Unzoned: 2)
    Number of zone members resolved: 0/2 (Unresolved: 2)
    Num zones: 1
    Number of IVR zones: 0
    Number of IPS zones: 0
    Formattted size: 38 bytes / 2048 Kb
```

Example 14-3 Zone Set Analysis

```
switch# show zone analysis zoneset zs1 vsan 1
Zoning database analysis vsan 1
  Zoneset analysis: zs1
    Num zonesets: 1
    Num zones: 0
    Num aliases: 0
    Num attribute groups: 0
    Formattted size: 20 bytes / 2048 Kb
```

See the *Cisco MDS 9000 Family Command Reference* for the description of the information displayed in the command output.

The **debug zone change** CLI command followed by the zone name in question can help you get started debugging zones for protocol errors, events, and packets.

Note: To enable debugging for zones, use the **debug zone** command in EXEC mode. To disable a debug command, use the **no** form of the command or use the **no debug** all command to turn off all debugging.

For protocol errors, use:

```
debug zone change errors vsan-id
```

For protocol events, use:

```
debug zone change events vsan-id
```

For protocol packets, use:

```
debug zone change packets vsan-id
```

Other useful **debug** commands include:

Troubleshooting Zone Configuration Issues with the CLI   4

```
debug zone {all |
 change {errors | events | packets} |
 database {detail | errors | events} |
 gs errors {errors | events | packets} |
 lun-zoning {errors | events | packets} |
 merge {errors | events | packets} |
 mts notifications |
 pss {errors | events} ||
 read-only-zoning {errors | events | packets} |
 tcam errors {errors | events | packets} |
 transit {errors | events}}} [vsan vsan-id]
```

Zone and Zone Set Issues

The section covers the following zone and zone set issues:

- Host Cannot Communicate with Storage
- Troubleshooting Zone Set Activation
- Troubleshooting Full Zone Database Synchronization Across Switches
- Mismatched Default Zone Policy
- Recovering from Link Isolation
- Mismatched Active Zone Sets Within the Same VSAN

Host Cannot Communicate with Storage

A host cannot see a storage device for the following reasons:

- The default zone policy does not allow the devices to communicate.
- Storage devices and host interfaces do not belong to the same zone or the zone is not part of the active zone set.

Symptom Host cannot communicate with storage.

Table 14-2 Host Cannot Communicate with Storage

Symptom	Possible Cause	Solution
Host cannot communicate with storage.	Host and storage are not in the same zone.	See the **"Resolving Host Not Communicating with Storage Issue Using Fabric Manager"** section or the **"Resolving Host Not Communicating with Storage Using the CLI"** section.
	Zone is not in active zone set.	
	No active zone set and default zone policy is deny.	
	The xE port connecting to the remote switch is isolated.	See the **"E Port Is Isolated in a VSAN"** section.
	Host and storage are not in the same VSAN.	Verify the VSAN membership. See the **"Verifying VSAN Membership Using Fabric Manager"** section or the **"Verifying VSAN Membership Using the CLI"** section.

Resolving Host Not Communicating with Storage Issue Using Fabric Manager

To verify that the host is not communicating with storage using Fabric Manager, follow these steps:

1. Verify that the host and storage device are in the same VSAN. See the "Verifying VSAN Membership Using Fabric Manager" section. 2. Configure zoning, if necessary, by choosing Fabric**xx > VSANxx > Default Zone** and selecting the **Policies** tab to determine if the default zone policy is set to **deny**.

> The default zone policy of **permit** means all nodes can see all other nodes. **Deny** means all nodes are isolated when not explicitly placed in a zone.

3. (Optional) Select **permit** from the Default Zone Behavior drop-down menu to set the default zone policy to permit if you are not using zoning. Got to Step 8 of the "Resolving Host Not Communicating with Storage Using the CLI" procedure.

4. Choose **Zone > Edit Local Full Zone Database** and select the VSAN you are interested in. Click on the zones folder and verify that the host and storage are both members of the same zone. If they are not in the same zone, see the "Resolving Host and Storage Not in the Same Zone Using Fabric Manager" section.

5. Choose **Zone > Edit Local Full Zone Database** and select the VSAN you are interested in. Click on the active zone folder and determine if the zone in Step 5 and the host and disk appear in the active zone set. If the zone is not in the active zone set, see the "Resolving Zone is Not in Active Zone Set Using Fabric Manager" section.

6. If there is no active zone set, right-click the zone set you want to activate in the Edit Local Full Zone Database dialog box and select **Activate** to activate the zone set.

7. Verify that the host and storage can now communicate.

Resolving Host and Storage Not in the Same Zone Using Fabric Manager

To move the host and storage device into the same zone using Fabric Manager, follow these steps:

1. Choose **Zone > Edit Local Full Zone Database** and select the VSAN you are interested in. Click on the zones folder and find the zones that the host and storage are members of.

2. Click on the zone that contains the host or storage that you want to move. Right-click the row that represents this zone member and select **Delete** from the pop-up menu to remove this end device from the zone.

3. Click the zone that you want to move the end device to. Click and drag the row that represents the end device in the bottom table and add it to the zone in the top table.

4. Verify that you have an active zone set for this VSAN by selecting the zone set name that appears in bold. If you do not have an active zone set, right-click the zone set you want to activate in the Edit Local Full Zone Database dialog box and select **Activate** to activate the zone set.

5. Expand the active zone set folder to verify that the zone in Step 3 is in the active zone set. If it is not, see the "Resolving Zone is Not in Active Zone Set Using Fabric Manager" section.

6. Click **Activate...** to activate the modified zone set.

7. Verify that the host and storage can now communicate.

Resolving Zone is Not in Active Zone Set Using Fabric Manager

To add a zone to the active zone set using Fabric Manager, follow these steps:

1. Choose **Zone > Edit Local Full Zone Database** and select the VSAN you are interested in. Right-click the active zone set, which is in bold, and select **Insert**.

2. Click the zone that you want to add to this zone set and click **Add**.

3. **Activate...** to activate the modified zone set.

4. Verify that the host and storage can now communicate.

Resolving Host Not Communicating with Storage Using the CLI

To verify that the host is not communicating with storage using the CLI, follow these steps:

1. Verify that the host and storage device are in the same VSAN. See the "Verifying VSAN Membership Using the CLI" section. 2. Configure zoning, if necessary, by using the **show zone status** *vsan-id* command to determine if the default zone policy is set to **deny**.

```
switch# show zone status vsan 1
VSAN: 1 default-zone: deny distribute: active only Interop: default
    mode: basic merge-control: allow session: none
    hard-zoning: enabled
Default zone:
    qos: low broadcast: disabled ronly: disabled
Full Zoning Database :
    Zonesets:0  Zones:0 Aliases: 0
Active Zoning Database :
    Name: Database Not Available
Status:
```

> The default zone policy of **permit** means all nodes can see all other nodes. **Deny** means all nodes are isolated when not explicitly placed in a zone.

3. (Optional) Use the **zone default-zone permit** command to set the default zone policy to permit if you are not using zoning. Go to Step 7.

4. Use the **show zone member** command for host and storage device to verify that they are both in the same zone. If they are not in the same zone, see the "Resolving Host and Storage Not in the Same Zone Using Fabric Manager" section.

5. Use the **show zoneset active** command to determine if the zone in Step 4 and the host and disk appear in the active zone set.

```
v_188# show zoneset active vsan 2
zoneset name ZoneSet3 vsan 2
  zone name Zone5 vsan 2
    pwwn 10:00:00:00:77:99:7a:1b [Hostalias]
    pwwn 21:21:21:21:21:21:21:21 [Diskalias]
```

6. If the zone is not in the active zone set, see the "Resolving Zone is Not in Active Zone Set Using Fabric Manager" section.

7. If there is no active zone set, use the **zoneset activate** command to activate the zone set.

```
 switch(config)# zoneset activate ZoneSet1 vsan 2.
```

8. Verify that the host and storage can now communicate.

Resolving Host and Storage Not in the Same Zone Using the CLI

To move the host and storage device into the same zone using the CLI, follow these steps:

1. Use the **zone name** *zonename vsan-id* command to create a zone in the VSAN if necessary, and add the host or storage into this zone.

```
ca-9506(config)# zone name NewZoneName vsan 2
ca-9506(config-zone)# member pwwn 22:35:00:0c:85:e9:d2:c2
ca-9506(config-zone)# member pwwn 10:00:00:00:c9:32:8b:a8
```

Note: The pWWNs for zone members can be obtained from the device or by issuing the **show flogi database** vsan-id command.

2. Use the **show zone** command to verify that host and storage are now in the same zone.

```
switchA# show zone
zone name NewZoneName vsan 2
  pwwn 22:35:00:0c:85:e9:d2:c2
  pwwn 10:00:00:00:c9:32:8b:a8
zone name Zone2 vsan 4
  pwwn 10:00:00:e0:02:21:df:ef
  pwwn 20:00:00:e0:69:a1:b9:fc
zone name zone-cc vsan 5
  pwwn 50:06:0e:80:03:50:5c:01
  pwwn 20:00:00:e0:69:41:a0:12
  pwwn 20:00:00:e0:69:41:98:93
```

3. Use the **show zoneset active** command to verify that you have an active zone set. If you do not have an active zone set, use the **zoneset activate** command to activate the zone set.

4. Use the **show zoneset active** command to verify that the zone in Step 2 is in the active zone set. If it is not, use the **zoneset name** command to enter the zone set configuration submode, and use the **member** command to add the zone to the active zone set.

```
 switch(config)# zoneset name zoneset1 vsan 2
 ca-9506(config-zoneset)# member NewZoneName
```

5. Use the **zoneset activate** command to activate the zone set.

```
 switch(config)# zoneset activate ZoneSet1 vsan 2
```

Verify that the host and storage can now communicate.

Resolving Zone is Not in Active Zone Set Using the CLI

To add a zone to the active zone set using the CLI, follow these steps:

1. Use the **show zoneset active** command to verify that you have an active zone set. If you do not have an active zone set, use the **zoneset activate** command to activate the zone set.

2. Use the **show zoneset active** command to verify that the zone in Step 1 is not in the active zone set.

3. Use the **zoneset name** command to enter the zone set configuration submode, and use the **member** command to add the zone to the active zone set.

```
switch(config)# zoneset name zoneset1 vsan 2
ca-9506(config-zoneset)# member NewZoneName
```

4. Use the **zoneset activate** command to activate the zone set.

```
 switch(config)# zoneset activate ZoneSet1 vsan 2
```

5. Verify that the host and storage can now communicate.

Troubleshooting Zone Set Activation

When you activate a zone set, a copy of the zone set from the full zone set is used to enforce zoning, and is called the *active zone set*. A zone that is part of an active zone set is called an *active zone*. Two main problems can occur with activating a zone set:

- No zone set is active.
- Zone set activation fails.

Zone activation can fail if a new switch joins the fabric. When a new switch joins the fabric, it acquires the existing zone sets. Also, large zone sets may experience timeout errors in Cisco MDS SAN-OS Release 1.3(4a) and earlier.

When a zone set activation fails, you may see the following system messages:

> **Error Message** ZONE-2-ZS_CHANGE_ACTIVATION_FAILED: Activation failed.

>> **Explanation** The zone server cannot activate the zone set.
>> **Recommended Action** Use the zoneset activate CLI command or similar Fabric Manager procedure to activate the zone set.

> **Error Message** ZONE-2-ZS_CHANGE_ACTIVATION_FAILED_RESN: Activation failed : reason chars].

>> **Explanation** The zone server cannot activate because of reason shown in the error message.
>> **Recommended Action** No action is required.

If this message has the reason "FC2 sequence size exceeded", then the zone database size has been exceeded. You must simplify the zone configuration, or, if full zone set distribution is enabled, then disable full zone

set distribution and activate the zone set.

Error Message ZONE-2-ZS_CHANGE_ACTIVATION_FAILED_RESN_DOM: Activation failed:
reason [chars] domain [dec].

Explanation The zone server cannot activate because of reason shown in the error message
on the domain.
Recommended Action No action is required.

Troubleshooting Zone Activation Using Fabric Manager

To verify the active zone set and active zones using Fabric Manager, follow these steps:

1. Choose **Zone > Edit Local Full Zone Database** and select the VSAN you are interested in. Click on the
active zone set, which is in bold.

2. Verify that the needed zones are active. If a zone is missing from the active zone set, see the "Resolving
Zone is Not in Active Zone Set Using Fabric Manager" section.

3. Click **Activate...** to activate the zone set.

4. If you are still experiencing zone set activation failure, use the **show zone internal change event-history
vsan** *vsan-id* CLI command to determine the source of zone set activation problem.

Troubleshooting Zone Activation Using the CLI

To verify the active zone set and active zones using the CLI, follow these steps:

1. Use the **show zone analysis active vsan** *vsan-id* command to analyze the active zone set database. Verify
that the formatted size does not exceed the 2048 KB limit shown. If it exceeds the limit, you must remove
some zones or devices within a zone.

```
switch# show zone analysis active vsan 1
Zoning database analysis vsan 1
  Active zoneset: zs1 [*]
    Activated at: 08:03:35 UTC Nov 17 2005
    Activated by: Local [ GS ]
    Default zone policy: Deny
    Number of devices zoned in vsan: 0/2 (Unzoned: 2)
    Number of zone members resolved: 0/2 (Unresolved: 2)
    Num zones: 1
    Number of IVR zones: 0
    Number of IPS zones: 0
    Formattted size: 38 bytes / 2048 Kb
```

2. Use the **show zone analysis vsan** *vsan-id* command to analyze the full zone set database. Verify that the
formatted size does not exceed the 2048 KB limit shown. If it exceeds the limit, you must remove some
zones or devices within a zone.

```
switch# show zone analysis vsan 1
Zoning database analysis vsan 1
 Full zoning database
   Last updated at: 15:57:10 IST Feb 20 2006
```

```
   Last updated by: Local [ CLI ]
   Num zonesets: 1
   Num zones: 1
   Num aliases: 0
   Num attribute groups: 0
   Formattted size: 36 bytes / 2048 Kb

 Unassigned Zones: 1
   zone name z1 vsan 1
```

3. Use the **show zoneset active** *vsan-id* command to display the active zones.

```
switchA# show zoneset active vsan 2
zoneset name ZoneSet1 vsan 2
  zone name NewZoneName vsan 2
    * pwwn 22:35:00:0c:85:e9:d2:c2
    * pwwn 10:00:00:00:c9:32:8b:a8
```

4. Verify that the needed zones are active.

5. (Optional) Use the **zoneset name** *ActiveZonesetName vsan-id* command and the **member** *NewZone* command to add the zone to the active zone set in the VSAN.

```
 switch(config)# zoneset name ZoneSet1 vsan 2
 switch(config-zoneset)# member NewZoneAdded
```

6. Use the **zoneset activate** command to activate the zone set.

```
 switch(config)# zoneset activate ZoneSet1 vsan 2
```

7. If you are still experiencing zone set activation failure, use the **show zone internal change event-history vsan** *vsan-id* command to determine the source of the zone set activation problem.

Troubleshooting Full Zone Database Synchronization Across Switches

All switches in the Cisco MDS 9000 Family distribute active zone sets when new E port links come up or when a new zone set is activated in a VSAN. The zone set distribution takes effect while sending merge requests to the adjacent switch or while activating a zone set.

Resolving Out of Sync Full Zone Database Using Fabric Manager

To verify if the full zone database is in sync across switches using Fabric Manager, follow these steps:

1. Choose **Fabric**xx **> VSAN**xx **>** *zonesetname* and select the **Policies** tab.

2. Verify that the Propagation field is set to **FullZoneSet**. If it is not, select **FullZoneSet** from the drop-down menu.

3. Click **Apply Changes** to save these changes.

Resolving an Out of Sync Full Zone Database Using the CLI

To verify if the full zone database is in sync across switches using the CLI, follow these steps:

1. Use the **show zone status** command to verify if the distribute flag is on.

Troubleshooting Zone Activation Using the CLI   11

```
switch# config t show zone status
VSAN: 1 default-zone: deny distribute: active only Interop: default
    mode: basic merge-control: allow session: none
    hard-zoning: enabled
Default zone:
    qos: low broadcast: disabled ronly: disabled
Full Zoning Database :
    Zonesets:3  Zones:7 Aliases: 9
Active Zoning Database :
    Name: ZoneSet1  Zonesets:1  Zones:2
Status:
```

This example shows that only the active zone set is distributed.

2. Verify that the distribute flag is on.

Mismatched Default Zone Policy

If you are using basic zoning, you must verify that the default zone policy is the same for all switches in the VSAN. If the default zone policy varies, then you may experience zoning problems. If all switches in the VSAN have Cisco SAN-OS Release 2.0(1b) or later, you can use enhanced zoning. Enhanced zoning synchronizes your zone configuration across all switches in the VSAN, eliminating the possibility of mismatched default zone policies.

Resolving Mismatched Default Zone Policies Using Fabric Manager

To resolve mismatched default zone policies using Fabric Manager, follow these steps:

1. Choose **Fabric*xx* > VSAN*xx* >** *zonesetname* and select the **Policies** tab.

2. View the Default Zone Behavior field for each switch in the VSAN to determine which switches have mismatched default zone policies.

3. Click **Apply Changes** to save these changes.

4. If you are using basic zoning, Select the same value from the Default Zone Behavior drop-down menu for each switch in the VSAN to set the same default zone policy.

5. If you are using enhanced zoning, follow these steps:

> a. Choose **Fabric*xx* > VSAN*xx*** and view the Release field to verify that all switches are capable of working in the enhanced mode.
> All switches must have Cisco MDS SAN-OS Release 2.0(1b) or later. If one or more switches are not capable of working in enhanced mode, then your request to move to enhanced mode is rejected.

> b. Choose **Fabric*xx* > VSAN*xx* >** *zonesetname* and select the **Policies** tab and set Default Zone Behavior field to set the default zone policy.

> c. Click **Apply Changes** to save these changes.

> d. Select the **Enhanced** tab and select **enhanced** from the Action drop-down menu.

> e. Click **Apply Changes** to save these changes.
> By doing so, you automatically start a session, acquire a fabric wide lock, distribute the active and

full zoning database using the enhanced zoning data structures, distribute zoning policies, and then release the lock. All switches in the VSAN then move to the enhanced zoning mode.

Note: After moving from basic zoning to enhanced zoning (or vice versa), we recommend that you save the running configuration.

Resolving Mismatched Default Zone Policies Using the CLI

To resolve mismatched default zone policies using the CLI, follow these steps:

1. Issue the **show zone status** command.

```
v_188# show zone status
VSAN: 1 default-zone: deny distribute: active only Interop: default
    mode: basic merge-control: allow session: none  <------------------
    hard-zoning: enabled
Default zone:
    qos: low broadcast: disabled ronly: disabled
Full Zoning Database :
    Zonesets:5  Zones:18 Aliases: 11
Active Zoning Database :
    Name: ZoneSet1  Zonesets:1  Zones:2
Status:
```

This example shows the default zone policy is deny, and the zone mode is basic.

2. If you are using basic zoning, follow these steps:

   a. Repeat **Step 1** for all switches in the VSAN to verify that they have the same zone mode. Use the **zone mode basic** command to change any switches that are not in basic mode.

   b. Use the **zone default-zone** command on each switch in the VSAN to set the same default zone policy.

3. If you are using enhanced zoning, follow these steps:

   a. Use the **show version** command on all switches in the VSAN to verify that all switches are capable of working in the enhanced mode.
   All switches must have Cisco MDS SAN-OS Release 2.0(1b) or later. If one or more switches are not capable of working in enhanced mode, then your request to move to enhanced mode is rejected.

   b. Use the **zone default-zone** command to set the default zone policy.

   c. Use the **zone mode enhanced** *vsan-id* command to set the operation mode to enhanced zoning mode.
   By doing so, you will automatically start a session, acquire a fabric wide lock, distribute the active and full zoning database using the enhanced zoning data structures, distribute zoning policies, and then release the lock. All switches in the VSAN then move to the enhanced zoning mode.

```
switch(config)# zone mode enhanced vsan 3000
```

Note: After moving from basic zoning to enhanced zoning (or vice versa), we recommend that you use the **copy running-config startup-config** command to save the running configuration.

Zone Merge Failure

A zone merge request may fail because of the following configuration issues:

- Too many zone sets
- Too many aliases
- Too many attribute groups
- Too many zones
- Too many LUN members
- Too many zone members

Use the **show zone internal merge event-history** CLI command to determine the cause of the zone merge failure.

You may see one or more of the following system messages after a zone merge failure:

> **Error Message** ZONE-2-ZS_MERGE_ADJ_NO_RESPONSE: Adjacent switch not responding, Isolating Interface [chars] (VSAN [dec]).
>
> > **Explanation** Interface on the VSAN was isolated because the adjacent switch is not responding to zone server requests.
> > **Recommended Action** Flap the interface.

Introduced Cisco MDS SAN-OS Release 1.2(2a).

> **Error Message** ZONE-2-ZS_MERGE_FAILED: Zone merge failure, Isolating interface [chars].
>
> > **Explanation** Interface isolated because of a zone merge failure.
> > **Recommended Action** Compare active zoneset with the adjacent switch or enter the zone merge interface CLI command or similar Fabric Manager/Device Manager command.

Introduced Cisco MDS SAN-OS Release 1.2(2a).

> **Error Message** ZONE-2-ZS_MERGE_FULL_DATABASE_MISMATCH: Zone merge full database mismatch on interface [chars].
>
> > **Explanation** Full zoning databases are inconsistent between two switches connected by the interface . Databases are not merged.
> > **Recommended Action** Compare full zoning database with the adjacent switch. Correct the difference and flap the link.

Introduced Cisco MDS SAN-OS Release 1.3(1).

> **Error Message** ZONE-2-ZS_MERGE_FULL_DATABASE_MISMATCH: Zone merge full database mismatch on interface [chars].

Explanation Full zoning databases are inconsistent between two switches connected by the interface. Databases are not merged.
Recommended Action Compare full zoning database with the adjacent switch, correct the difference and flap the link.

Introduced Cisco MDS SAN-OS Release 1.2(2a).

Error Message ZONE-2-ZS_MERGE_UNKNOWN_FORMAT: Unknown format, isolating interface [chars].

Explanation Interface isolated because of an unknown format in the merge request.
Recommended Action Set the interoperability mode to the same value on both switches.

Introduced Cisco MDS SAN-OS Release 2.0(1b).

Note: Zoning information exists on a per VSAN basis. Therefore, for a TE port, it may be necessary to verify that the zoning information does not conflict with any allowed VSAN.

Recovering from Link Isolation

When two switches in a fabric are merged using a TE or E port, the port may become isolated when the active zone set databases are different between the two switches or fabrics. When a TE port or an E port become isolated, you can recover that port from its isolated state using one of three options:

- Import the neighboring switch's active zone set database and replace the current active zone set.

- Export the current database to the neighboring switch.

- Manually resolve the conflict by editing the full zone set, activating the corrected zone set, and then bringing up the link.

If after verifying the Fibre Channel name server , you still experience FSPF problems (such as discovering remote switches and their attached resources), the fabric may have zone configuration problems. Examples of zone configuration problems are mismatched active zone sets and misconfigured zones within the active zone set.

Resolving a Link Isolation Because of a Failed Zone Merge Using Fabric Manager

Using the Zone Merge Analysis tool in Fabric Manager, the compatibility of two active zone sets in two switches can be checked before actually merging the two zone sets. Refer to the *Cisco MDS 9000 Fabric Manager Configuration Guide* for more information.

To perform a zone merge analysis using Fabric Manager, follow these steps:

1. Choose **Zone > Merge Analysis** from the Zone menu.

You see the Zone Merge Analysis dialog box.

2. Select the first switch to be analyzed from the Check Switch 1 drop-down list.

3. Select the second switch to be analyzed from the And Switch 2 drop-down list.

4. Enter the VSAN ID where the zone set merge failure occurred in the For Active Zoneset Merge Problems in VSAN Id field.

4. Click **Analyze** to analyze the zone merge. Click **Clear** to clear the analysis data from the Zone Merge Analysis dialog box.

Resolving a Link Isolation Because of a Failed Zone Merge Using the CLI

The following CLI commands are used to resolve a failed zone merge:

- **zoneset import** *vsan-id*

- **zoneset export** *vsan-id*

To resolve a link isolation because of a failed zone merge using the CLI, follow these steps:

1. Use the **show interface** command to confirm that the port is isolated because of a zone merge failure.

```
switch# show interface fc2/14
fc2/14 is down (Isolation due to zone merge failure)
   Hardware is Fibre Channel, WWN is 20:4e:00:05:30:00:63:9e
   vsan is 1
   Beacon is turned off
     40 frames input, 1056 bytes, 0 discards
     0 runts, 0 jabber, 0 too long, 0 too short
     0 input errors, 0 CRC, 3 invalid transmission words
     0 address id, 0 delimiter
     0 EOF abort, 0 fragmented, 0 unknown class
     79 frames output, 1234 bytes, 16777216 discards
     Received 23 OLS, 14 LRR, 13 NOS, 39 loop inits
     Transmitted 50 OLS, 16 LRR, 21 NOS, 25 loop inits
```

    An E port is segmented (isolation due to zone merge failure) if the following conditions are true:

◊ The active zone sets on the two switches differ from each other in terms of zone membership (provided there are zones at either side with identical names).
◊ The active zone set on both switches contain a zone with the same name but with different zone members.

2. Verify the zoning information, using the following commands on each switch:

◊ **show zone vsan** *vsan-id*

◊ **show zoneset vsan** *vsan-id*

3. You can use two different approaches to resolve a zone merge failure by overwriting the zoning configuration of one switch with the other switch's configuration. This can be done with either of the following commands:

◊ **zoneset import interface***interface-number* **vsan** *vsan-id*

◊ **zoneset export interface***interface-number* **vsan** *vsan-id*

The **import** option of the command overwrites the local switch's active zone set with that of the remote switch. The **export** option overwrites the remote switch's active zone set with the local switch's active zone set.

4. If the zoning databases between the two switches are overwritten, you cannot use the **import** option. To work around this, you can manually change the content of the zone database on either of the switches, and then issue a **shutdown/no shutdown** command sequence on the isolated port.

5. If the isolation is specific to one VSAN and not on an E port, the correct way to issue the cycle up/down, is to remove the VSAN from the list of allowed VSANs on that trunk port, and reinsert it.

Note: Do not issue a **shutdown** or **no shutdown** command sequence on the port. This affects all of the VSANs crossing the EISL instead of just the VSAN experiencing the isolation problem.

Mismatched Active Zone Sets Within the Same VSAN

When merging switch fabrics, you must ensure that the zones in both active zone sets have unique names, or that any zones with the same name have exactly the same members. If either of these conditions is violated the E port connecting the two fabrics will appear in an isolated state.

For example, two switches may have the same zone set name, and the same zone names, but different zone members. As a result, the VSAN is isolated on the TE port that connects the two switches.

This issue can be resolved by doing one of the following:

- Modify the zone members on both zone sets to match and eliminate the conflict.

- Deactivate the zone set on one of the switches and restart the zone merge process.

- Explicitly import or export a zone set between the switches to synchronize them.

Resolving Mismatched Active Zone Sets Within the Same VSAN Using Fabric Manager

Mismatched active zone sets within the same VSAN result in that VSAN being segmented in Fabric Manager. To verify a mismatched active zone set within the same VSAN using Fabric Manager, follow these steps:

1. Choose **Zone > Edit Local Full Zone Database** and select the segmented VSAN you are interested in. Click on the active zone set, which is in bold, to view the list of zones and zone members for this active zone set.

2. Repeat Step 1 for the other segmented VSAN.

A mismatched active zone set may include zones with the same name but different members, or a missing zone within the zone set.

3. Do one of the following to resolve the isolation problem:

◊ Change the membership of one of the zones to match the other zone of the same name. See the "Resolving Host and Storage Not in the Same Zone Using Fabric Manager" section.

◊ Discard one of the zone sets completely by deactivating it using the **no zoneset activate** command. If a VSAN does not have an active zone set, it automatically takes the active zone set of the other merging switch. See the "Deactivating a Zone Set and Restarting the Zone Merge Process Using Fabric Manager" section.

◊ Choose **Zone > Copy Full Zone Database** to overwrite the active zone set on one switch. This method is destructive to one of the active zone sets.

Resolving Mismatched Active Zone Sets Within the Same VSAN Using the CLI

To verify a mismatched active zone set within the same VSAN using the CLI, follow these steps:

1. Use the **show zoneset active** *vsan-id* command to display the active zone set configuration of the first switch.

```
Switch1# show zoneset active vsan 99
zoneset name ZoneSet1 vsan 99
  zone name VZ1 vsan 99
  * fcid 0x7800e2 [pwwn 22:00:00:20:37:04:ea:2b]
  * fcid 0x7800d9 [pwwn 22:00:00:20:37:04:f8:a1]
```

2. Use the **show zoneset active** *vsan-id* command to display the active zone set configuration of the second switch:

```
Switch2# show zoneset active vsan 99
zoneset name ZoneSet1 vsan 99
  zone name VZ1 vsan 99
    pwwn 22:00:00:20:37:04:f8:a1
    pwwn 22:00:00:20:37:0e:65:44
```

Even though the zones have the same name, their respective members are different.

3. Issue the **show interface** command to view information about the TE port and the interface.

```
Switch2# show interface fc1/8
fc1/8 is trunking
    Hardware is Fibre Channel
    Port WWN is 20:08:00:05:30:00:5f:1e
    Peer port WWN is 20:05:00:05:30:00:86:9e
    Admin port mode is E, trunk mode is auto
    Port mode is TE
    Port vsan is 1
    Speed is 2 Gbps
    Receive B2B Credit is 255
    Receive data field size is 2112
    Beacon is turned off
    Trunk vsans (admin allowed and active) (1,99)
    Trunk vsans (up)                       (1)
    Trunk vsans (isolated)                 (99)
    Trunk vsans (initializing)             ()
    5 minutes input rate 120 bits/sec, 15 bytes/sec, 0 frames/sec
    5 minutes output rate 88 bits/sec, 11 bytes/sec, 0 frames/sec
      10845 frames input, 620268 bytes, 0 discards
        0 CRC,  0 unknown class
        0 too long, 0 too short
      10842 frames output, 487544 bytes, 0 discards
      3 input OLS, 4 LRR, 3 NOS, 0 loop inits
      18 output OLS, 2 LRR, 14 NOS, 0 loop inits
```

From this output, you can see that VSAN 99 is isolated.

4. Use the **show port internal interface** *interface number* CLI command to get information about why the interface is isolated.

Note: To issue commands with the **internal** keyword, you must have an account that is a member of the network-admin group.

```
switch# show port internal info interface fc1/8
fc1/8 – if_index: 0x0109C000, phy_port_index: 0x3c
  Admin Config – state(up), mode(TE), speed(auto), trunk(on)
    beacon(off), snmp trap(on), tem(false)
    rx bb_credit(default), rx bb_credit multiplier(default)
    rxbufsize(2112), encap(default), user_cfg_flag(0x3)
    description()
    Hw Capabilities: 0xb
    trunk vsans (up) (1)
    .
    .
    .
    trunk vsans (isolated) (99)
  TE port per vsan information
  fc2/29, Vsan 1 – state(up), state reason(None), fcid(0x690202)
    port init flag(0x38000), current state [TE_FSM_ST_E_PORT_UP]
  fc2/29, Vsan 99 – state(down), state reason(Isolation due to zone merge failure),
fcid(0x000000)
    port init flag(0x0), current state [TE_FSM_ST_ISOLATED_VSAN_MISMATCH]
```

From this output, you can see the VSAN is isolated because of o a zone merge failure.

5. Do one of the following to resolve the isolation problem:

- ◊ Change the membership of one of the zones to match the other zone of the same name. See the "Resolving Host and Storage Not in the Same Zone Using Fabric Manager" section.

- ◊ Discard one of the zone sets completely by deactivating it using the **no zoneset activate** command. If a VSAN does not have an active zone set, it automatically takes the active zone set of the other merging switch. See the "Deactivating a Zone Set and Restarting the Zone Merge Process Using the CLI" section.

- ◊ Overwrite the active zone set on one switch using the **import** or **export** commands. This method is destructive to one of the active zone sets.
  - · **zoneset import interface** *interface-number* **vsan** *vsan-id*
  - · **zoneset export interface***interface-number* **vsan** *vsan-id*

6. Use the **show interface** *fcx/y* **trunk** *vsan-id* command to verify that VSAN 99 is no longer isolated:

```
Switch1# show interface fc1/5 trunk vsan 99
fc1/5 is trunking
    Vsan 99 is up, FCID is 0x780102
```

Deactivating a Zone Set and Restarting the Zone Merge Process Using Fabric Manager

To deactivate a zone set and restart the zone merge process using Fabric Manager, follow these steps:

Resolving Mismatched Active Zone Sets Within the Same VSAN Using the CLI 19

1. Choose **Zone > Deactivate** Zone Set to deactivate the zone set configuration.

Caution: This will disrupt traffic and cause the MDS 9000 switch to lose connectivity with the network.

2. Choose **Interfaces > FC Physica**l and select **down** from the Status Admin drop-down menu to shut down the connection to the zone to be merged. You may see the following system messages:

```
Nov 19 10:26:10 switch4 %LOG_PORT-5-IF_DOWN_CHANNEL_ADMIN_DOWN: Interface fc1/14 is down
(Channel admin down)
Nov 19 10:26:10 switch4 %LOG_PORT-5-IF_DOWN_CHANNEL_ADMIN_DOWN: Interface fc1/15 is down
(Channel admin down)
Nov 19 10:26:10 switch4 %LOG_PORT-5-IF_DOWN_CHANNEL_ADMIN_DOWN: Interface fc1/16 is down
(Channel admin down)
Nov 19 10:26:10 switch4 %LOG_PORT-5-IF_DOWN_PORT_CHANNEL_MEMBERS_DOWN: Interface
port-channel 1 is down (No operational members)
Nov 19 10:26:10 switch4 %LOG_PORT-5-IF_DOWN_ADMIN_DOWN: Interface port-channel 1 is down
(Administratively down)
Nov 19 10:26:10 switch4 %LOG_PORT_CHANNEL-5-FOP_CHANGED: port-channel 1: first operational
port changed from fc1/16 to none
```

3. Choose **Interfaces > FC Physica**l and select **up** from the Status Admin drop-down menu to enable the connection to the zone to be merged. You may see the following system messages:

```
Nov 19 10:28:11 switch4 %LOG_PORT_CHANNEL-5-FOP_CHAN
GED: port-channel 1: first operational port changed from none to fc1/15
Nov 19 10:28:21 switch4 %LOG_PORT-5-IF_UP: Interface port-channel 1 is up in mode TE
Nov 19 10:28:21 switch4 %LOG_PORT-5-IF_TRUNK_UP: Interface fc1/14, vsan 1 is up
Nov 19 10:28:21 switch4 %LOG_PORT-5-IF_TRUNK_UP: Interface fc1/15, vsan 1 is up
Nov 19 10:28:21 switch4 %LOG_PORT-5-IF_TRUNK_UP: Interface fc1/16, vsan 1 is up
Nov 19 10:28:21 switch4 %LOG_PORT-5-IF_TRUNK_UP: Interface fc1/14, vsan 1 is up
Nov 19 10:28:21 switch4 %LOG_PORT-5-IF_TRUNK_UP: Interface fc1/15, vsan 1 is up
Nov 19 10:28:21 switch4 %LOG_PORT-5-IF_TRUNK_UP: Interface fc1/16, vsan 1 is up
```

4. Choose **Zone > Edit Local Full Zone Database** to verify the active zone set configuration.

After deactivating the zone set onthe first switch and performing a shutdown followed by a no shutdown on the ISL that connects it to the second switch, the zone merge is processed again. Because the first switch has no active zone set, it learns the active zone set from the second switch during the zone merge process.

Deactivating a Zone Set and Restarting the Zone Merge Process Using the CLI

To deactivate a zone set and restart the zone merge process using the CLI, follow these steps:

1. Use the **no zoneset activate name** *zoneset-name vsan-id* command to deactivate the zone set configuration from the switch:

Caution: This will disrupt traffic and cause the MDS 9000 switch to lose connectivity with the network.

```
switch4(config)# no zoneset activate name excal2 vsan 1
Zoneset Deactivation initiated. check zone status
```

2. Use the **show zoneset active** command to confirm that the zone set has been removed.

3. Use the **shut down** command to shut down the connection to the zone to be merged.

```
switch4(config)# interface port-channel 1
```

Deactivating a Zone Set and Restarting the Zone Merge Process Using FabricManager   20

```
switch4(config-if)# shutdown
Nov 19 10:26:10 switch4 %LOG_PORT-5-IF_DOWN_CHANNEL_ADMIN_DOWN: Interface fc1/14 is down
(Channel admin down)
Nov 19 10:26:10 switch4 %LOG_PORT-5-IF_DOWN_CHANNEL_ADMIN_DOWN: Interface fc1/15 is down
(Channel admin down)
Nov 19 10:26:10 switch4 %LOG_PORT-5-IF_DOWN_CHANNEL_ADMIN_DOWN: Interface fc1/16 is down
(Channel admin down)
Nov 19 10:26:10 switch4 %LOG_PORT-5-IF_DOWN_PORT_CHANNEL_MEMBERS_DOWN: Interface
port-channel 1 is down (No operational members)
Nov 19 10:26:10 switch4 %LOG_PORT-5-IF_DOWN_ADMIN_DOWN: Interface port-channel 1 is down
(Administratively down)
Nov 19 10:26:10 switch4 %LOG_PORT_CHANNEL-5-FOP_CHANGED: port-channel 1: first operational
port changed from fc1/16 to none
```

4. Use the **no shutdown** command to reactivate the connection to the zone to be merged:

```
switch4(config-if)# no shutdown
Nov 19 10:28:11 switch4 %LOG_PORT_CHANNEL-5-FOP_CHAN
GED: port-channel 1: first operational port changed from none to fc1/15
Nov 19 10:28:21 switch4 %LOG_PORT-5-IF_UP: Interface port-channel 1 is up in mode TE
Nov 19 10:28:21 switch4 %LOG_PORT-5-IF_TRUNK_UP: Interface fc1/14, vsan 1 is up
Nov 19 10:28:21 switch4 %LOG_PORT-5-IF_TRUNK_UP: Interface fc1/15, vsan 1 is up
Nov 19 10:28:21 switch4 %LOG_PORT-5-IF_TRUNK_UP: Interface fc1/16, vsan 1 is up
Nov 19 10:28:21 switch4 %LOG_PORT-5-IF_TRUNK_UP: Interface fc1/14, vsan 1 is up
Nov 19 10:28:21 switch4 %LOG_PORT-5-IF_TRUNK_UP: Interface fc1/15, vsan 1 is up
Nov 19 10:28:21 switch4 %LOG_PORT-5-IF_TRUNK_UP: Interface fc1/16, vsan 1 is up
```

5. Use the **show zoneset active** *vsan-id* commands to exit configuration mode and check the active zone sets.

```
switch4# show zoneset active
zoneset name wall vsan 1
  zone name excal1 vsan 1
  * fcid 0x620200
    fcid 0x6200ca
zone name $default_zone$ vsan 1
  * fcid 0x6e00da
  * fcid 0x6e00d9
  * fcid 0x6e00d6
  * fcid 0x6e0100
```

After deactivating the zone set on switch 4 and performing a shutdown followed by a no shutdown on the ISL that connects it to switch 3, the zone merge is processed again. Because switch 3 has no active zone set, it learns the active zone set from switch 4 during the zone merge process.

Enhanced Zoning Issues

Enhanced zoning uses a session locking facility like CFS to prevent simultaneous zoning configuration changes by two users on the same or separate switches. When a user starts to make a zoning change on one switch for a VSAN, that switch will lock the fabric to prevent others from making zoning changes. The user must issue a commit to make the changes active and release the fabric wide lock.

Problems can occur when the lock is acquired, but not released. In this situation, you cannot configure zoning on that VSAN. If you are using the CLI, you see error messages when you attempt to enter the zoning configuration mode.

Troubleshooting CLI commands to use for enhanced zoning issues:

- **show zone internal change event-history**

- **show zone status vsan**
- **show zone pending-diff**
- **show zone pending vsan**

Symptom Cannot configure zoning.

Table 14-3 Cannot Configure Zoning

Symptom	Possible Causes	Solutions
Cannot configure zoning.	Another user on the same switch is holding the enhanced zoning configuration lock. If you are using the CLI, you see a message stating that another session is active.	See the "Resolving Enhanced Zoning Lock Issues with Fabric Manager" section or the "Resolving Enhanced Zoning Lock Issues with the CLI" section.
	Another user on a different switch is holding the enhanced zoning configuration lock. If you are using the CLI, you see a message stating that the lock is currently busy.	

Resolving Enhanced Zoning Lock Issues with Fabric Manager

To resolve a lock failure using Fabric Manager, follow these steps:

1. Choose **Fabric*xx* > VSAN*xx*** and select the zone set that you want to configure.

2. Select the **Enhanced** tab from the Information pane and view the Config DB Locked By column to determine which switch and which user holds the enhanced zoning lock for this VSAN.

3. Check the **Config DB Discard Changes** check box and click **Apply Changes** to clear the enhanced zoning lock.

Note: Verify that no valid configuration change is in progress before you clear a lock.

Resolving Enhanced Zoning Lock Issues with the CLI

To resolve a lock issue using the CLI, follow these steps:

1. Use the **show zone status vsan** command to determine the lock holder. If the lock holder is on this switch, the command output shows the user. If the lock holder is on a remote switch, the command output shows the domain ID of the remote switch.

```
switch#show zone status vsan 16


  VSAN: 16 default-zone: deny distribute: active only Interop: default
    mode: enhanced merge-control: allow session: cli [admin]  <---- user admin has lock
    hard-zoning: enabled
```

2. Use the **no zone commit vsan** command on the switch that holds the lock to release the lock if you are the holder of the lock.

3. Use the **no zone commit vsan** *vsan id* **force** command on the switch that holds the lock to release the lock if another user holds the lock.

Note: Verify that no valid configuration change is in progress before you clear a lock.

4. If problems persist, use the **clear zone lock** command to remove the lock from the switch. This should only be done on the switch that holds the lock.

Back to Main Page: Cisco MDS SAN-OS Troubleshooting Guide