



## Troubleshooting IVR

---

This chapter describes how to troubleshoot and resolve inter-VSAN routing (IVR) configuration issues in the Cisco MDS 9000 Family of multilayer directors and fabric switches. It includes the following sections:

- [Overview, page 8-1](#)
- [Best Practices, page 8-1](#)
- [Initial Troubleshooting Checklist, page 8-3](#)
- [Common IVR Problems, page 8-6](#)
- [Troubleshooting the IVR Wizard, page 8-14](#)

### Overview

Troubleshooting IVR involves checking the configuration of domain IDs, VSANs, border switches, and zone sets. Configuration problems with IVR can prevent devices from communicating properly.

Prior to Cisco MDS SAN-OS Release 2.1(1a), IVR required unique domain IDs for all switches in the fabric. As of Cisco MDS SAN-OS Release 2.1(1a), you can enable IVR Network Address Translation (NAT) to allow non-unique domain IDs. This feature simplifies the deployment of IVR in an existing fabric where non-unique domain IDs might be present.



**Note**

---

By default, IVR-NAT is not enabled.

---

### Best Practices

This section provides the best practices for implementing IVR:

- Use Fabric Manager to configure IVR.  
Using Fabric Manager to configure IVR can help avoid errors and will ensure that the same IVR configuration is applied to all IVR enabled switches.
- Use IVR-NAT. If you do not use IVR-NAT, you must use non-overlapping domains across VSANs associated with IVR.



**Note**

---

If you are using IVR-NAT, you are not required to use non-overlapping domains across VSANs.

---

## Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

- For large installations, do not spread IVR zone members across many switches.  
The VSAN rewrite table is limited to 4096 entries, and the entries are per-domain, not per-end device, so it is best to minimize the number of switches that contain IVR zone members in very large implementations.
- Use static domain IDs. This prevents changes in domain IDs that may conflict with virtual domain ID assignments.
- Allow for multiple paths between the IVR zone members. Implement redundant path designs whenever possible.
- Set the default zone policy to deny and avoid using the **force** option when activating the IVR zone set.

In normal Fibre Channel environments, it is generally considered a best practice to set the default zone policy to deny. Because members of IVR zones cannot exist in the default zone, activation of an IVR zone set using the **force** option may lead to traffic disruption if IVR zone members previously existed in a default zone policy of permit.

- Use IVR auto-topology. If you do not use IVR auto-topology, use CFS distribution to ensure that the same IVR topology is applied to all IVR-enabled switches.
- Configure IVR only in the relevant border switches.
- Configure IVR-enabled VSANs in no interop (default) mode or interop 1 mode.
- Turn RDI mode on. This ensures that the switch will not assign used domain IDs and is compatible with third-party switches. In Cisco SAN-OS Release 2.0(x) and earlier, existing domain IDs are reserved in a local database. In Cisco SAN-OS Release 2.1(1a) and later, domain IDs are dynamically reserved using RDI.



### Note

---

Contact your customer support representative for more information regarding this feature (specifically for CSCei88345 and Field Notice 62187).

---

## Transit VSANs

Follow these guidelines when configuring transit VSANs:

- Besides defining the IVR zone membership, you can choose to specify a set of transit VSANs to provide connectivity between two edge VSANs:
  - If two edge VSANs in an IVR zone overlap, then a transit VSAN is not required (though not prohibited) to provide connectivity.
  - If two edge VSANs in an IVR zone do not overlap, you may need one or more transit VSANs to provide connectivity. Two edge VSANs in an IVR zone will not overlap if IVR is not enabled on a switch that is a member of both the source and destination edge VSANs.
- Traffic between the edge VSANs traverses only the shortest IVR path.
- Transit VSAN information is common to all IVR zones. Sometimes a transit VSAN can also be an edge VSAN in another IVR zone.

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)***

## Border switches

Always follow these guidelines when configuring border switches:

- Border switches require Cisco SAN-OS Release 1.3(1) or higher.
- A border switch must be a member of two or more VSANs.
- A border switch that facilitates IVR communications must be IVR enabled.
- For redundant paths between active IVR zone members, IVR can (optionally) be enabled on additional border switches.
- The VSAN topology configuration must be updated before a border switch is added or removed.

## Initial Troubleshooting Checklist

Begin troubleshooting IVR issues by checking the following issues first:

Checklist	Checkoff
Verify that IVR is enabled on all border switches involved in IVR.	<input type="checkbox"/>
Verify that you have the correct license installed (SAN_EXTENSION for IVR over FCIP or ENTERPRISE_PKG for IVR over Fibre Channel).	<input type="checkbox"/>
Verify that the IVR configuration is the same on all IVR-enabled switches.	<input type="checkbox"/>
Verify that the IVR zone is part of the active IVR zone set.	<input type="checkbox"/>
Verify that you have an active zone set or that you activate the IVR zone set using the <b>force</b> option.	<input type="checkbox"/>
Verify that you have added IVR virtual domains to the allowed domain ID list if you have a Cisco SN5428 storage router or a Cisco MDS 9020 switch in your fabric.	<input type="checkbox"/>

If you change any FSPF link cost, ensure that the FSPF path cost (that is, the sum of the link costs on the path) of any IVR path is less than 30,000.

This section includes the following topics:

- [Verifying IVR Configuration Using Fabric Manager, page 8-3](#)
- [Verifying IVR Configuration Using the CLI, page 8-4](#)
- [Limitations and Restrictions, page 8-5](#)
- [IVR Enhancements by Cisco SAN-OS Release, page 8-6](#)

## Verifying IVR Configuration Using Fabric Manager

To verify your IVR configuration using Fabric Manager, follow these steps:

- 
- Step 1** Choose **Fabricxx > All VSANs > IVR** to verify your IVR configuration.
- Step 2** Select the **CFS** tab to verify that the Oper column is enabled and the Global column is enabled for CFS distribution. Check the LastResult column for the status of the last CFS action.
- Step 3** Select the **Action** tab to determine if auto topology and IVR NAT are enabled.

## Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

- Step 4** Select the **Local Topology** and **Active Topology** tabs to verify your IVR VSAN topology.
- Step 5** Choose **Fabricxx > All VSANs > Domain Manager** to verify unique domain IDs if IVR NAT is not enabled.
- Step 6** Choose **Zone > IVR > Edit Local Full Zone Database** to verify your IVR zones and zone sets and to verify that you have activated your IVR zone set. The active IVR zone set name appears in bold.

## Verifying IVR Configuration Using the CLI

Several commands involving multiple configuration tasks can be used to verify the IVR configuration.

**Table 8-1** CLI Commands for Verification of IVR

CLI Command	Description
<b>show fcdomain domain-list</b>	Verifies unique domain ID assignment. If a domain overlap exists, edit and verify the allowed-domains list or manually configure static, non-overlapping domains for each participating switch and VSAN.
<b>show interface brief</b>	Verifies if the ports are operational, VSAN membership, and other configuration settings covered previously.
<b>show fcns database</b>	Verifies the name server registration for all devices participating in the IVR.
<b>show zoneset active</b>	Displays zones in the active zone set. This should include configured IVR zones.
<b>show ivr fcdomain</b>	Displays the IVR persistent fcdomain database.
<b>show ivr internal</b>	Shows the IVR internal troubleshooting information.
<b>show ivr pending-diff</b>	Shows the IVR pending configuration.
<b>show ivr service-group</b>	Shows the difference between the IVR pending and configured databases.
<b>show ivr tech-support</b>	shows information that is used by your customer support representative to troubleshoot IVR issues.
<b>show ivr virtual-domains</b>	Shows IVR virtual domains for all local VSANs.
<b>show ivr virtual-fcdomain-add-status</b>	Shows IVR virtual fcdomain status.
<b>show ivr vsan-topology</b>	Verifies the configured IVR topology.
<b>show ivr zoneset</b>	Verifies the IVR zone set configuration.
<b>show ivr zone</b>	Verifies the IVR zone configuration.
<b>clear ivr zone database</b>	Clears all configured IVR zone information. <b>Note</b> Clearing a zone set erases only the configured zone database, not the active zone database.

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)***

The following **show internal** commands can be useful for troubleshooting IVR issues.

add-rw	Show ivr fcid rewrite fsm internals
adv_vsans	Show IVR advertise VSANs for a native VSAN and domain
area-port-allocation	Show IVR area-port allocation
capability-fsm	Show IVR capability fsm internal debug information
commit-rw	Show ivr fcid rewrite fsm internals
debug-log-buffer1	Show IVR debug-log buffer
del-rw	Show ivr fcid rewrite fsm internals
dep	Show ivr dep internals
device-list	Show ivr device list
distribution	Show ivr distribution internals
domain-capture-list	Show ivr domain controller capture list
drav-fsm	Show DRAV FSM details
event-history	Show ivr internal event history
fcid-rewrite-fsm	Show ivr fcid rewrite fsm internals
fcid-rewrite-list	Show ivr fcid rewrite entries
fsmtca	Show IVR FSM transition statistics
global-data	Show ivr global data
mem-stats	Show memory statistics
nhvsan-change	Show ivr fcid rewrite fsm internals
plogi-captured-list	Show ivr PLOGI captured
pnat	Show IVR payload NAT internal information
pvm	Show IVR PV Master internal information
tu-fsm	Show TU FSM internal debug information
vdri-fsm	Show VDRI FSM internal debug information
virtual-domains	Show IVR capability fsm internal debug information
vsan-rewrite-list	Show ivr vsan rewrite list
vsan-topology	Show internal information on IVR VSAN topology
vsan-topology-graph	Show IVR VSAN Topology graph internal debug information
zone-fsm	Show ivr zone fsm internals

## Limitations and Restrictions

Limit the use of IVR NAT with write acceleration. Enabling IVR NAT on the same switch where write acceleration is enabled over a Port Channel of multiple FCIP links might result in frames from the source to the destination not transferring.

Design your SAN to properly use IVR and IVR zones. Design IVR zones to enable communications between devices that require it. Do not group all devices into one IVR zone if you do not require all those devices to communicate with each other.

**Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)**

Table 8-1 shows the limitations to the IVR configuration based on the Cisco SAN-OS release.

**Table 8-1** *IVR Configuration Limitations*

Parameter per Fabric	Cisco SAN-OS 2.0(1b)	Cisco SAN-OS 2.1(1a) or later
IVR zone members	2000	10000
IVR zones	200	2000
IVR zone sets	32	32
VSANs	64	128
IVR-enabled switches	128	128



**Note**

Two VSANS with the same VSAN ID combined with a unique AFID count as two VSANs in the total number of allowed VSANs per fabric.

## IVR Enhancements by Cisco SAN-OS Release

Table 8-2 lists the IVR enhancements by Cisco SAN-OS release.

**Table 8-2** *IVR Enhancements by Cisco SAN-OS Release*

Cisco SAN-OS Release	IVR Enhancement
Release 2.1(2)	Persistent FC IDs and domains for IVR
Release 2.1(1a)	<ul style="list-style-type: none"> <li>• IVR NAT</li> <li>• AFIDs</li> <li>• Auto-topology</li> <li>• Virtual domains added to remote domain lists</li> <li>• IVR LUN zoning</li> <li>• IVR QoS zoning</li> <li>• Service group</li> </ul>
Release 2.0(1)	IVR with CFS support
Release 1.3(4a)	Virtual domains added to remote domain lists.
Release 1.3(1)	IVR introduced.

## Common IVR Problems

This section describes the problems associated with IVR. This section includes the following topics:

- [IVR Licensing Issues, page 8-7](#)
- [Cannot Enable IVR, page 8-8](#)
- [IVR Network Address Translation Fails, page 8-8](#)

## Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

- [IVR Zone Set Activation Fails](#), page 8-9
- [Border Switch Fails](#), page 8-10
- [Traffic Does Not Traverse IVR Path](#), page 8-11
- [Link Isolated](#), page 8-12
- [Persistent FC ID for IVR Failed](#), page 8-12
- [LUN Configuration Failure in IVR Zoning](#), page 8-13
- [Host Does Not Have Write Access to Storage](#), page 8-13
- [Locked IVR CFS Session](#), page 8-13
- [CFS Merge Failed](#), page 8-14

IVR allows device discovery across VSANs. IVR also supports FC ping and FC traceroute across VSANs using the following criteria:

- Either FC ID or pWWN can be used.
- Must be initiated from a switch with an active IVR zone member.

## IVR Licensing Issues

To use IVR, you must obtain the correct licenses for the IVR features you are using and install those licenses on every IVR-enabled switch in your fabric. [Table 8-3](#) shows which license to purchase, based on the IVR feature you are using and the module or chassis you have enabled IVR on.

**Table 8-3 License Requirements for IVR**

IVR Feature	Chassis or Module Type	License Required	Number of Licenses
IVR over Fibre Channel	All	ENTERPRISE_PKG	One per IVR-enabled chassis
IVR over FCIP	MDS 9216i <sup>1</sup>	None	None
	MPS-14/2	SAN_EXTN_OVER_IPS2	One per module running IVR Over FCIP
	IPS-8	SAN_EXTN_OVER_IP	
	IPS-4	SAN_EXTN_OVER_IPS4	

1. Cisco MDS 9216i enables the SAN\_EXTENSION features without a license for the two Gigabit Ethernet ports on the integrated supervisor card.



### Note

If you are using IVR over FCIP and Fibre Channel, you need the ENTERPRISE\_PKG as well as the appropriate SAN extension license as shown in [Table 8-3](#).



### Tip

Be sure to enter the correct chassis serial number when purchasing your license packages. Choose **Switches > Hardware** and check the SerialNo Primary for the switch chassis in Fabric Manager or use the **show license host-id** CLI command to obtain the chassis serial number for each switch that requires a license. Your license will not operate if the serial number used does not match the serial number of the chassis you are installing the license on.

See [Chapter 4, “Troubleshooting Licensing,”](#) for complete details on troubleshooting licensing issues.

**Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)**

## Cannot Enable IVR

**Symptom** Cannot enable IVR.

**Table 8-4** Cannot Enable IVR

Symptom	Possible Cause	Solution
Cannot enable IVR.	License not installed and grace period has expired.	Purchase and install the appropriate licenses. See the “ <a href="#">IVR Licensing Issues</a> ” section on page 8-7.
	Switch not running Cisco SAN-OS Release 1.3(1) or later.	Upgrade to the Cisco SAN-OS release required for the IVR features you want to use. See <a href="#">Table 8-1</a> and <a href="#">Chapter 2</a> , “ <a href="#">Troubleshooting Installs, Upgrades, and Reboots.</a> ”
	Using IVR auto topology but CFS distribution is not enabled.	Choose <b>Fabricxx &gt; All VSANs &gt; IVR</b> and set the Global drop-down menu to <b>enable</b> . Click <b>Apply Changes</b> . Or use the <b>ivr distribute</b> CLI command before enabling IVR.

## IVR Network Address Translation Fails

**Symptom** IVR NAT fails.

**Table 8-5** IVR NAT Fails

Symptom	Possible Cause	Solution
IVR NAT fails.	Internal message payload uses destination ID.	IVR NAT modifies the destination ID in the Fibre Channel header. If this same destination ID appears inside the message payload, Cisco SAN-OS may not detect it and IVR NAT fails. Disable IVR NAT and ensure that all domain IDs are unique. Refer to the <i>Cisco MDS 9000 Family Configuration Guide</i> at the following website for a list of payloads that work with IVR NAT when the payload includes the destination ID: <a href="http://www.cisco.com/univercd/cc/td/doc/product/sn5000/mds9000/2_0/cliguide/part_4/ivr.htm#wp1176738">http://www.cisco.com/univercd/cc/td/doc/product/sn5000/mds9000/2_0/cliguide/part_4/ivr.htm#wp1176738</a>
	Some switches are running IVR without NAT.	You cannot combine IVR and IVR NAT in the same VSAN. Use the same IVR configuration on all switches. Deactivate the active zone set before converting to IVR or IVR NAT.

*Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)*

## IVR Zone Set Activation Fails

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

**Error Message** IVR-2-IVZS\_ACTIVATION\_FAILED\_RETRYING: Inter-VSAN zoneset activation failed in VSAN [dec] : [chars]. retrying after [dec] seconds.

**Explanation** Inter-VSAN zone set activation failed in the listed VSAN. This could be an intermittent, regular zone set activation error. The activation will be retried after the number of seconds listed in the message.

**Recommended Action** No action is required.

**Introduced** Cisco MDS SAN-OS Release 2.1(2).

**Error Message** IVR-3-IVZ\_ACTIVATION\_FAILED: Inter-VSAN zoneset [chars] activation failed.

**Explanation** Inter-VSAN zone set activation failed.

**Recommended Action** No action is required.

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

**Error Message** IVR-3-IVZ\_ACTIVATION\_FAILED\_VSAN: Inter-VSAN zoneset [chars] activation failed in VSAN [dec].

**Explanation** Inter-VSAN zone set activation failed in the VSAN.

**Recommended Action** No action is required.

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

**Error Message** IVR-5-IVZS\_ACTIVATION\_RETRYING: Inter-VSAN zoneset activation failed with error [hex] in VSAN [dec]. retrying after [dec] seconds.

**Explanation** Inter-VSAN zone set activation failed with VSAN shown in the error message. This could be an intermittent regular zone set activation error. The activation retried in the number of seconds shown in the error message.

**Recommended Action** No action is required.

**Introduced** Cisco MDS SAN-OS Release 1.3(3).

## Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

**Error Message** IVR-5-IVZS\_WAITING\_FOR\_LOWEST\_SWWN: Waiting for lowest switch WWN Inter-VSAN enabled switch in VSAN [dec].

**Explanation** This switch does not have the lowest switch world wide name (sWWN) in the VSAN. Only the inter-VSAN (IVR) enabled switch with the lowest sWWN can add the IVR zones to the regular active zone set in a VSAN. This switch is waiting until the IVR switch with the lowest sWWN adds the IVR zone and reactivates the zone set.

**Recommended Action** No action is required.

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

**Symptom** IVR zone set activation fails.

**Table 8-6** IVR Activation Fails

Symptom	Possible Cause	Solution
IVR zone set activation fails.	Overlapping domain IDs.	Use static domain IDs to assign unique domain IDs to each switch in the VSAN or use IVR NAT. Choose <b>Fabricxx &gt; All VSANs &gt; Domain Manager</b> in Fabric Manager or use the <b>fdomain domain domain-id [static   preferred] vsan vsan-id</b> CLI command
	Default zone policy is permit.	Choose <b>Zone &gt; IVR &gt; Edit Local Full Zone Database</b> in Fabric Manager. Right-click the IVR zone set that you want to activate and select <b>Activate</b> . Check the <b>Create Active Zone Set if none Present</b> check box or use the <b>force</b> option with the <b>ivr zoneset activate</b> CLI command.
	Default zone policy is deny and no active zone set present.	
	No active zone set.	No zone set has been activated. See the <a href="#">“Troubleshooting Zone Set Activation” section on page 9-9</a> to activate a zone set on an IVR-enabled switch, or use the <b>force</b> option when activating the IVR zone set.

## Border Switch Fails

If an IVR-enabled switch fails, you must update the IVR topology to reflect this change if you are not using auto topology.

**Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)**

**Symptom** Border switch fails.

**Table 8-7** *Border Switch Fails*

Symptom	Possible Causes	Solutions
Border switch fails.	IVR topology incorrect.	<p>Choose <b>Fabricxx &gt; All VSANs &gt; IVR</b> and select the <b>Action</b> tab in Fabric Manager. Check the <b>Auto Discover Topology</b> check box and click <b>Apply Changes</b>. Select the <b>CFS</b> tab and set ConfigAction to <b>commit</b> and click <b>Apply Changes</b>.</p> <p>Or use the <b>ivr vsan topology auto</b> CLI command to automatically reconfigure the IVR topology, or use the <b>ivr vsan topology database</b> CLI command to manually reconfigure the IVR topology.</p>

## Traffic Does Not Traverse IVR Path

**Symptom** Traffic does not traverse the IVR path.

**Table 8-8** *Traffic Does Not Traverse IVR Path*

Symptom	Possible Cause	Solution
Traffic does not traverse the IVR path.	Fabric includes an SN5428 or MDS 9020 switch and you have not added the IVR virtual domains to the remote VSAN domain lists.	<p>Choose <b>Fabricxx &gt; All VSANs &gt; IVR</b> and select the <b>Action</b> tab in Fabric Manager. Fill in the Create Virtual Domains for VSAN field and click <b>Apply Changes</b>. Select the <b>CFS</b> tab and set ConfigAction to <b>commit</b> and click <b>Apply Changes</b>.</p> <p>Or use the <b>ivr virtual-fcdomain-add vsan-ranges</b> CLI command to add existing and future virtual domains to the domain list for the selected VSANs.</p> <p>Repeat this on all edge VSANs.</p>
	Internal message payload uses destination ID.	See the <a href="#">“IVR Network Address Translation Fails”</a> section on page 8-8.

**Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)**

## Link Isolated

**Symptom** Link isolated.

**Table 8-9** *Link Isolated*

Symptom	Possible Cause	Solution
Link isolated.	Virtual domain overlap.	<p>Choose <b>Fabricxx &gt; All VSANs &gt; Domain Manager</b> in Fabric Manager to verify a domain overlap.</p> <p>Choose <b>Fabricxx &gt; All VSANs &gt; IVR</b> and select the <b>Action</b> tab in Fabric Manager. Fill in the Create Virtual Domains for VSAN field and click <b>Apply Changes</b>. Select the <b>CFS</b> tab and set ConfigAction to <b>commit</b> and click <b>Apply Changes</b>.</p> <p>Or use the <b>show fcdomain domain-list</b> CLI command to verify a domain overlap. Use the <b>ivr withdraw domain</b> CLI command to remove the overlapped domain. Use persistent FC IDs to reassign the overlapped domain. Use the <b>ivr virtual-fcdomain-add vsan-ranges</b> CLI command to add existing and future virtual domains to the domain list for the selected VSANs.</p> <p>Repeat this on all edge VSANs.</p>
	Internal message payload uses destination ID.	See the “ <a href="#">IVR Network Address Translation Fails</a> ” section on <a href="#">page 8-8</a> .

## Persistent FC ID for IVR Failed

**Symptom** Persistent FC ID for IVR failed.

**Table 8-10** *Persistent FC ID for IVR Failed*

Symptom	Possible Cause	Solution
Persistent FC ID for IVR failed.	Selected virtual FC ID does not match the assigned virtual domain.	<p>Use the <b>show ivr fcdomain database</b> CLI command to verify the virtual domain ID. Use the <b>native-autonomous-fabric-num</b> CLI command to assign the virtual domain and then use the <b>pwwn</b> CLI command to map the pWWN to an appropriate FC ID that matches the virtual domain ID.</p> <p>Refer to the <i>Cisco MDS 9000 Family Configuration Guide</i> for the related procedure to configure Persistent FC IDs for IVR.</p>

**Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)**

## LUN Configuration Failure in IVR Zoning

**Symptom** LUN configuration failed in IVR zoning.

**Table 8-11** LUN Configuration Failure in IVR Zoning

Symptom	Possible Cause	Solution
LUN configuration failed in IVR zoning.	One or more switches in the VSAN are not running Cisco MDS SAN-OS Release 2.1(1a) or later.	Upgrade to the Cisco SAN-OS release required for the IVR features you want to use. See <a href="#">Table 8-1</a> and <a href="#">Chapter 2</a> , “Troubleshooting Installs, Upgrades, and Reboots.”

## Host Does Not Have Write Access to Storage

**Symptom** Host does not have write access to storage.

**Table 8-12** Host Does Not Have Write Access to Storage

Symptom	Possible Cause	Solution
Host does not have write access to storage.	Host is a member of a read-only zone.	If a host is a member of a read-only zone, the host has no write access to any IVR zone it may be a member of. Remove the host from the read-only zone.

## Locked IVR CFS Session

IVR uses CFS to distribute the IVR configuration. If you enable IVR auto topology, it also uses CFS to distribute and update the IVR VSAN topology on all switches. In rare cases, you may encounter problems where CFS locks IVR so that you cannot modify the configuration.

**Symptom** Locked IVR CFS session.

**Table 8-13** Locked IVR CFS Session

Symptom	Possible Cause	Solution
Locked IVR CFS session.	CFS did not give up the session lock for IVR after the last commit or an IVR configuration change is pending and has not been committed.	Choose <b>Fabricxx &gt; All VSANS &gt; IVR</b> and select the <b>CFS</b> tab. Set the ConfigView As drop-down menu to <b>pending</b> and verify the pending configuration changes. Set the ConfigAction drop-down menu to <b>commit</b> to save these changes, <b>abort</b> to discard the changes, or <b>clear</b> to clear the session lock. Click <b>Apply Changes</b> .  Or use the <b>show ivr pending-diff</b> CLI command to determine if you have a pending configuration change. Use <b>ivr commit</b> to commit this change or <b>ivr abort</b> to discard the changes and free up the session lock. If you do not have pending configuration changes, use the <b>clear ivr session</b> CLI command to free the session lock.

**[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)**

## CFS Merge Failed

**Symptom** CFS merge failed.

**Table 8-14** CFS Merge Failed

Symptom	Possible Cause	Solution
CFS merge failed.	IVR topology incorrect.	Choose <b>Fabricxx &gt; All VSANs &gt; IVR</b> and select the <b>Action</b> tab in Fabric Manager. Check the <b>Auto Discover Topology</b> check box and click <b>Apply Changes</b> . Select the <b>CFS</b> tab and set ConfigAction to <b>commit</b> and click <b>Apply Changes</b> .  Or use either the <b>ivr vsan topology auto</b> CLI command to automatically reconfigure the IVR topology, or the <b>ivr vsan topology database</b> CLI command to manually reconfigure the IVR topology.
	Maximum number of VSANs or IVR VSAN topology entries reached.	Reconfigure your fabric before merging to reduce the number of VSANs or topology entries . See <a href="#">Table 8-1</a> .
	Conflicting entries in the AF ID database.	Modify the conflicting entries in the AFID database.
	Conflicting user-configured IVR VSAN topology database entries.	Enable IVR auto topology on both fabrics before the merge and remove any user-configured IVR VSAN topology database entries.

## Troubleshooting the IVR Wizard

The IVR Wizard in Fabric Manager simplifies the process of configuring IVR across your fabric. The IVR Wizard automatically checks for the appropriate Cisco SAN-OS version across the switches in the VSAN and determines which IVR features the switches are capable of. (See [Table 8-1](#).)

This section describes the following warning or error dialog boxes that display when you configure IVR using the Fabric Manager IVR wizard:

- [Warning: Not All Switches Are IVR NAT Capable or Are Unmanageable, page 8-15](#)
- [Error: The Following Switches Do Not Have Unique Domain IDs, page 8-15](#)
- [Error: Pending Action/ Pending Commits, page 8-16](#)
- [Error: Fabric Is Changing. Please Retry the Request Later, page 8-16](#)

**Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)**

## Warning: Not All Switches Are IVR NAT Capable or Are Unmanageable

**Symptom** Warning: Not all switches are IVR NAT capable or are unmanageable.

**Table 8-15** *Not All Switches Are IVR NAT Capable or Are Unmanageable*

Symptom	Possible Cause	Solution
Warning: Not all switches are IVR NAT capable or are unmanageable.	One or more switches in the fabric are not running Cisco MDS SAN-OS Release 2.1(1a) or later.	Upgrade to the Cisco SAN-OS release required for the IVR features you want to use. See <a href="#">Table 8-1</a> and <a href="#">Chapter 2, “Troubleshooting Installs, Upgrades, and Reboots.”</a>
	One or more switches in the fabric cannot communicate with Fabric Manager or are not Cisco SAN-OS switches.	Determine if any of the problem switches are required in the IVR topology. If not, ignore this message and proceed with the IVR configuration. If they are required, choose <b>Switches</b> and check the Status column to determine the cause and address the problem.

## Error: The Following Switches Do Not Have Unique Domain IDs

**Symptom** The following switches do not have unique domain IDs.

**Table 8-16** *The Following Switches Do Not Have Unique Domain IDs*

Symptom	Possible Cause	Solution
The following switches do not have unique domain IDs.	The listed switches have duplicate domain IDs in two or more VSANS in your proposed IVR configuration.	Choose <b>Fabricxx &gt; All VSANS &gt; Domain Manager</b> and set the ConfigDomainId to a unique number and set the Config Type drop-down menu to <b>static</b> . Set the Restart drop-down menu to <b>disruptive</b> and Click <b>Apply Changes</b> . This triggers a disruptive restart to make the running domain ID match the configured domain ID.
		Use IVR NAT. This may require upgrading to Cisco MDS SAN-OS Release 2.1(1a) or later.

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)***

## Error: Pending Action/ Pending Commits

**Symptom** Pending action on pending commit error displays.

**Table 8-17** Pending Action/Pending Commits

Symptom	Possible Cause	Solution
Pending action on pending commit error displays.	A separate IVR configuration change that was not committed.	IVR has pending changes that were not committed. Choose <b>Fabricxx &gt; All VSANS &gt; IVR</b> and select the <b>CFS</b> tab. Set the View Config As drop-down menu to <b>pending</b> and verify the pending configuration changes. Set the ConfigAction drop-down menu to <b>commit</b> to save these changes or <b>abort</b> to discard the changes. Click <b>Apply Changes</b> .
	The IVR CFS session was not unlocked after the last commit.	Choose <b>Fabricxx &gt; All VSANS &gt; IVR</b> and select the <b>CFS</b> tab. Set the ConfigAction drop-down menu to <b>clear</b> to remove the session lock. Click <b>Apply Changes</b> .

## Error: Fabric Is Changing. Please Retry the Request Later

This error may occur where there are different versions of Cisco SAN-OS on the IVR-enabled switches. You should upgrade all IVR-enabled switches to the same version of Cisco SAN-OS.