CHAPTER 2

Troubleshooting SANTap

This chapter describes how to identify and resolve problems that might occur when implementing SANTap. This chapter includes the following sections:

Note SANTap is not supported in SAN-OS Release 3.3(1).

SANTap Architecture Troubleshooting Best Practices

The Cisco SANTap service provides a level of availability that cannot be achieved with an appliance in the data path between a host and storage. By removing that appliance from the data path, the SANTap service enables a significantly more reliable solution than an appliance could offer because the primary data path between host and storage is independent of the appliance.

Enhanced Availability

If a SANTap-enabled appliance fails, data continues to flow between host and storage. This level of availability may be suitable for data migration, which is generally not mission critical, but not for continuous data protection. Redundant components can be used when deploying the SANTap service in the same way they are used with building fabrics.

Best Practices

The following hardware may be added to enhance the availability of SANTap-enabled applications:

- Redundant SANTap-connected partner appliances to the same fabric. The SANTap service can provide functionality to redundant SANTap connected appliances.
- Redundant SSMs within the same director.
- Redundant switches or directors which have multi-homed SANTap appliances.
- Multiple links between hosts and storage devices.

Multipathing Drivers and Software

The SANTap service enables hosts to see storage through the service as if the service were transparent. For instance, if a particular storage subsystem is attached and being serviced by SANTap, the same communication between host and storage device is uninhibited by the SANTap service. This transparency allows multipathing software to use multiple paths through separate fabrics, even when the SANTap service is enabled on that storage path. A configuration with multipathing software can even be nondisrputively migrated to use the SANTap service by failing over to a single fabric, adding the service to the fabric, failing back to the SANTap enabled fabric, and upgrading the other fabric.

Scaling SANTap

The SANTap service scales linearly by adding additional Service Nodes to the fabric. There is no limit to the number of Service Nodes that can be added to a fabric. Additional SANTap appliances may need to be added. Check with the SANTap partner for specifications on how many devices their appliances can support.

LUN Mapping and LUN Masking Considerations

LUN masking is an access control method that a storage device uses to restrict or permit access to volumes of data, or LUNs (logical unit numbers). The device has a list of hosts, typically identified by worldwide names (WWN), which are allowed to access particular LUNs on the storage device. LUN mapping generally incorporates the LUN masking function, but also adds a reference to a volume that is specific to the host accessing the data. For instance, host A and host B connect to the same port on a storage device. If both of these hosts want to access a volume identified as LUN 0 on the storage device, LUN masking either permits or denies the hosts access to this same volume.

LUN mapping provides an additional layer to actually associate a request from host A for LUN 0 to a different internal volume than a request from host B for LUN 0. Some vendors may have brand names for LUN mapping such as LUN Security or AccessLogix.

The SANTap service was designed in such a way that LUN masking and LUN mapping on a storage device never needs to be changed when SANTap is introduced into the fabric. The SANTap-enabled appliance can send and receive traffic through the virtual initiator, using the virtual initiator's WWN, which eliminates changes required on the storage device. Some SANTap vendors have not implemented this feature and may require changes to LUN masking and LUN mapping to overcome these limitations. Consult the SANTap vendor's documentation regarding any configuration changes that may be required on the storage device.

Best Practices

A common problem when configuring the SANTap service is that a host may be unable to see a LUN that is being serviced by SANTap.

This problem is most likely caused by zoning issues. The best way to configure SANTap is using an incremental process, whereby zoning is checked after the completion of each configuration step. In some instances, it may be practical to enable the default zone set policy in a VSAN to be set to permit to see if the problem is related to zoning. However, never use this method to troubleshoot zoning problems if any critical data resides on storage that is attached to that fabric. Doing so could cause data corruption.

Securing SANTap Using VSANs and Zoning

SANTap entities are presented as virtual devices into the SAN. They are placed into VSANs and send and receive SCSI commands over Fibre Channel, just as any other target or host. Because of these common characteristics that virtual devices share with real devices, they are managed in the same way as real devices. Namely, they are placed into VSANs, which provides fabric isolation, and placed into zones, which isolates communication between the devices.

Best Practices

The most effective way to ensure the security of the fabric is to follow the general best practices of security for both the fabric and management interfaces. Treat SANTap virtual devices as any other devices and incrementally zone the devices as they are added to the fabric. An incremental zoning approach aids in determining which devices are actually the virtual devices that were just added to the fabric. Never rely on a default zone permit communication between devices because this provides no access control when additional devices are added to the fabric.

Treat appliances and virtual devices just as any other device and zone these devices as they are added. Although some SANTap vendors may encourage short-cutting these processes, the additional care ensures the integrity of the fabric in case of error or misconfiguration.

HP-UX for Persistent FCID Limitations in SANTap

With HP-UX 11i v2 and earlier, when you map to an SCSI device, you can use the controller ID, target ID and the LUN ID to build the device filename. For example, if controller is 5, target is 1 and LUN is 0, and the device filename will be /dev/dsk/c5t1d0.

If there is a change in the FC ID and the controller or the target ID, then the device filename changes. This change will cause HP-UX to not to be able to see the target device that was used before the change.

A possible cause of the FC ID change is reloading the switch. By default, the switch assigns the same FC ID to a device. However, if the switch is rebooted, the pWWN/FC ID mapping database is not maintained.

Solution

By enabling persistent FC IDs, this database will be persistent across reboots, and the device name will not change if the switch reloads.

Figure 2-1 shows another case of FC ID change.

Figure 2-1 HP-UX for Persistent FCID Limitations

Figure 2-1 shows one path from the host to access the two target devices from two different switches in a same fabric.

If both switches have an MSM-18/4 line card, then you can maintain the same FC ID between the virtual target and the real target.

For HP-UX to see the same target devices, follow these steps:

1. Create a DVT VSAN from each switch by using the same domain ID.
2. Create a persistent FC ID that matches the target's FC ID in the VSAN where the physical target resides.
3. Move the host connection to DVT VSAN to see the same target devices.

If there is only one MSM-18/4 in Switch1, then the persistent FC ID for Target 2 cannot be used because the domain ID of Switch 1 is different from the domain ID of Target 2. When moving the host to DVT VSAN, the DVT2 FC ID is different from the Target 2 FC ID, and the HP-UX host does not see the target device anymore.

Solution

HP-UX 11i v3 introduces the Agile Addressing feature which replaces the device file named /dev/dsk/c5t1d0 with /dev/dsk/disk1 to its hardware path. The changes in the hardware path do not affect the device name.

Design Considerations

Devices connected to legacy switches leverage intelligent applications on the Cisco MDS 9000 Family without requiring the storage and hosts to be directly connected to the Cisco MDS 9000 Director. Some limitations of legacy switches must be considered when adding them to a SANTap design.

Transparent mode is the simpler of the two modes to use for connecting legacy fabrics. The same design considerations apply when using modern directors and switches as well as using legacy switches, namely that either the hosts or disks must be connected directly to the SSM running the SANTap service.

Limitations

The SANTap feature has the following limitations:

- An appliance cluster can have only one target VSAN.
- In the SANTap setup, the real host and real target cannot be in an IVR zone. An IVR zone can only be created between the real host and a SANTap DVT (SANTap virtual target for the real target).

Basic Troubleshooting

This section describes the basic troubleshooting tasks that you can perform, and includes the following topics:

Troubleshooting Checklist

Troubleshooting a SANTap problem involves gathering information about the configuration and connectivity of the various SANTap components. To begin your troubleshooting activity, use the following checklist:

Checklist	Check
Verify licensing requirements. See *Fabric Configuration Guide, Cisco DCNM for SAN*.	❑
Verify that SANTap is enabled on the SSM module of the selected switch.	❑
Verify the VSAN configuration and zones for the appliance, using the configuration and verification tools for the specific appliance.	❑
Verify the physical connectivity for any problem ports or VSANs.	❑
Verify the ports connected to the RPA are operationally up.	❑

Using DCNM-SAN for Troubleshooting

Use the following DCNM-SAN procedures to verify the VSAN configuration for the SANTap components:

- Choose **Fabric*xx* > VSAN*xx*** to view the VSAN configuration in the Information pane.
- Choose **Fabric*xx* > VSAN*xx*** and select the **Host** or **Storage** tab in the Information pane to view the VSAN members.

Using the CLI for Troubleshooting

Use the **show santap module** command to display information about SANTap.

The following examples show the kind of information you can collect with the **show santap module** command.

Example 2-1 Display SANTap CVT Information

```
switch# show santap module 2 cvt

CVT Information :
        cvt pwwn      = 23:4f:00:0d:ec:09:3c:02
        cvt nwwn      = 23:9d:00:0d:ec:09:3c:02
        cvt id        = 135895180
        cvt xmap_id   = 135895212
        cvt vsan      = 8
        cvt name      = MYCVT
```

Example 2-2 Display SANTap DVT Information

```
switch# show santap module 2 dvt

DVT Information :
       dvt pwwn        = 50:06:0e:80:03:81:32:36
       dvt nwwn        = 50:06:0e:80:03:81:32:36
       dvt id          = 136773180
       dvt mode        = 3
       dvt vsan        = 12
       dvt if_index    = 0x1080000
       dvt fp_port     = 1
       dvt name        = MYDVT
       dvt tgt-vsan    = 9
       dvt io timeout                 = 10 secs
       dvt lun size handling          = 0
       dvt app iofail behaviour       = 1
       dvt quiesce behavior           = 1
       dvt tgt iofail behavior        = 0
       dvt appio failover time        = 50 secs
       dvt inq data behavior          = 0
```

Example 2-3 Display SANTap DVT LUN Information

```
switch# show santap module 2 dvtlun

DVT LUN Information :

       dvt pwwn       = 22:00:00:20:37:88:20:ef
       dvt lun        = 0x0
       xmap id        = 8
       dvt id         = 3
       dvt mode       = 0
       dvt vsan       = 3
       tgt pwwn       = 22:00:00:20:37:88:20:ef
       tgt lun        = 0x0
       tgt vsan       = 1
```

Example 2-4 Display SANTap Session Information

```
switch# show santap module 2 session

Session Information :

    session id    = 1
    host pwwn     = 21:00:00:e0:8b:12:8b:7a
    dvt pwwn      = 50:06:0e:80:03:81:32:36
    dvt lun       = 0x0
    tgt pwwn      = 50:06:0e:80:03:81:32:36
    tgt lun       = 0x0
    adt pwwn      = 33:33:33:33:33:33:33:00
    adt lun       = 0x0
    aci pwwn      = 22:22:22:22:22:22:22:22
    cvt pwwn      = 23:4f:00:0d:ec:09:3c:02
    num ranges    = 0
    session state = 5
    redirect mode = 0
    mrl requested 1
    MRL : vsan 8 RegionSize 4806720, DiskPWWN 0x234f000dec093c02, DiskLun 0x 1, startLBA 1

    pwl requested 1
    PWL : type 2, UpdatePol 2, RetirePolicy 4, pwl_start 1

    iol requested 0
```

Example 2-5 Display SANTap AVT Information

```
switch# show santap module 2 avt

AVT Information :
      avt pwwn       = 2a:4b:00:05:30:00:22:25
      avt nwwn       = 2a:60:00:05:30:00:22:25
      avt id         = 12
      avt vsan       = 4
      avt if_index   = 0x1080000
      hi pwwn        = 21:00:00:e0:8b:07:61:aa
      tgt pwwn       = 22:00:00:20:37:88:20:ef
      tgt vsan       = 1
```

Example 2-6 Display SANTap AVT LUN Information

```
switch# show santap module 2 avtlun

AVT LUN Information :
      avt pwwn       = 2a:4b:00:05:30:00:22:25
      avt lun        = 0x0
      xmap id        = 16
      avt id         = 12
      tgt lun        = 0x0
```

Use the following commands to display more advanced troubleshooting information for SANTap:

- **show tech-support**
- **show santap module 2 tech-support**
- **show isapi tech-support**
- **show santap vttbl dvt** *dvt-pwwn*

Using Messages, Logs, and Databases

The following log files and databases can provide helpful information when troubleshooting SANTap problems:

- Look for SSM_CRIT in Supervisor syslog messages.
- Obtain the SANTap logs by using the **show isapi tech-support** CLI command. Search for the strings "Error" and "failed" or "failure."
- Review the FCNS and FLOGI databases by using the **show fcns** and **show flogi** CLI commands.

SANTap Technical Support

To collect SANTap technical support information, first attach to the module by entering the **attach module** command, and then enter the **show isapi tech-support santap file cisco** command:

```
switch# attach module 13
Attaching to module 13 ...
To exit type 'exit', to abort type '$.'
Bad terminal type: "ansi". Will assume vt100.
module-13# show isapi tech-support santap file cisco
Re-directing tech support information to file: cisco
```

SANTap technical support logs collected through this command are stored in the module's modflash modflash://modnumber-1. It includes iSAPI technical support and the outputs of the **show debug santap event-history** and **show santap tech-support** commands. The two outputs are not present in ISAPI technical support, and are not collected after a DPP crash.

The size of the modflash is limited to approximately 60 MB in NX-OS 4.1(x). If the size of the output file is greater than the space that remains on modflash, an unusable truncated file is created. To ensure that the SANTap technical support file is created in the modflash correctly, at least 20 MB of free space should be available before issuing the CLI command. Ensure that you copy the technical support file after collecting the technical support logs, and then delete the file from the modflash.

ISAPI technical support logs collected using the **show isapi tech-support file** *filename* command are stored in the line card log directory log://*modnumber* on the line card.

The size of the log directory is also limited to 180 MB. At least 20 MB free space should be available in the log directory before collecting the iSAPI technical support logs, and the file should be copied and deleted from the log directory once the process is complete.

To copy and delete files from the modflash and log directories on the line card, use the following commands:

- **copy log**://*module>/file name target fs*

(Issued on the supervisor module) Copies the iSAPI technical support file from /var/log/external.

- **copy modflash**://*module>-1/file name target fs*

(Issued on supervisor module) Copies the SANTap iSAPI technical support file from /mnt/cf/partner.

- **clear debug-logfile** *filename*

(Issued on module) Deletes the log files in /var/log/external.

- **delete modflash**://*module-1/filename*

(Issued on supervisor module) Deletes the log files in /mnt/cf/partner.

SANTap Issues

This section describes SANTap issues and includes the following topics:

Host Login Problems

Host login problems can be caused by DVT limitations, connectivity, or other issues.

To diagnose host login problems, follow these steps:

Step 1 Use the **show santap vttbl dvt** *dvt-pwwn* command to display SANTap information for the DVT.

Step 2 Use the **show santap vttbl dvt** *dvt-pwwn* **host** *host-pwwn* command to display SANTap information for the DVT and the host.

Step 3 Enable logging on the appropriate SSM module.

Step 4 Enter the following debug commands:

- **debug vsd vfc-felogin**
- **debug partner 0x92810000 d1**
- **debug partner 0x92810000 d2**
- **no debug partner 0x92810000 d3**

To turn off debug logs, enter the following command:

- **no debug all**

Note The debug logs need to be turned on only when necessary or as part of troubleshooting with Cisco TAC.

Step 5 Review the logs to determine the problem, and then take the appropriate corrective action.

Enabling ISAPI Log Collection and Debug Information

To collect logs, use these commands:

```
show tech-support details
show santap module X tech-support
show ssm-nvram santap module X
attach module x
     show isapi tech-support
```

```
show isapi dpp all queue
```

To obtain iSAPI debug information, use these commands:

```
attach mod x
debug dpp logfile debugdpp
debug dpp instance all
debug dpp level 7
debug dpp control
debug dpp exception
```

To turn off debug information, use this command:

```
no debug dpp all
```

To clear the debug DPP log files, use these commands:

```
attach mod x
clear debug-logfile debugdpp.1
clear debug-logfile debugdpp.2
clear debug-logfile debugdpp.3
clear debug-logfile debugdpp.4
clear debug-logfile debugdpp.5
clear debug-logfile debugdpp.6
clear debug-logfile debugdpp.7
clear debug-logfile debugdpp.8
```

Note The debug logs need to be turned on only when necessary or as part of troubleshooting with Cisco TAC.

ITL Problems

An initiator target LUN (ITL) problem may occur if the number of ITLs exceeds the limitations for the release of Cisco SAN-OS or NX-OS and SSI in use. For specific ITL limitations, see the "Scaling SANTap" section on page 2-2.

To diagnose and resolve ITL problems, follow these steps:

Step 1 Use the show **isapi dpp 4 queue** command to display DPP queue information.

Step 2 Verify that the number of ITLs on a DPP is within the limitations for the release of Cisco SAN-OS or NX-OS and SSI in use. Use the **show isapi dpp 4 queue | incl LUN** and **show isapi dpp 4 queue | count** commands.

Step 3 Verify that the number of ITLs on an SSM is within the limitations for the release of Cisco SAN-OS or NX-OS and SSI in use. Enter the **show isapi dpp all queue** command, using the **incl LUN** and **count** parameters.

Common Mismatch Problems

Problems are often caused by mismatching component versions, or using devices that are not supported by the interoperability matrix.

Table 2-1 lists the common mismatch situations.

Table 2-1 Common SANTap Mismatch Problems

Problem	Description
Version mismatch between the SSM and the RPA.	The version of SSM and the version of the replication appliance are not compatible.
Version mismatch between the supervisor and the SSI image.	The version of the supervisor and the SSI image are not compatible.
Hosts, targets, HBAs, or switches are not supported by the interoperability matrix.	Review the Cisco SANTap interoperability matrix at http://www.cisco.com/en/US/products/ps5989/products_device_support_tables_list.html.
CVT is in the host VSAN.	The CVT is the portal through which the appliance communicates with SANTap, and cannot be in the host VSAN.
IVR and SANTap are being used together.	In the SANTap setup, the real host and real target cannot be in IVR zone. IVR zone can only be created between real host and SANTap DVT (SANTap virtual target for the real target)
VIs in a DVT VSAN (CVT and DVT in the same VSAN).	This results in the creation of one CPP VI and eight DPP VIs in the DVT VSAN. The VIs attempt to log in to DVT, resulting in nondeterministic behavior.

Table 2-1 Common SANTap Mismatch Problems (continued)

Problem	Description
Overprovisioning, including: • Too many ITLs per SSM • Too many hosts per DVT • Too many ITLs per DPP	When replication is enabled, AVT LUNs are created, and that can increase the ITL count over the limit. (See "Scaling SANTap" section on page 2-2.) If Reservation Support is not enabled on the Recovery Point Application (RPA): • 26 AVT LUNs are created at a time. • The appliance completes recovery of these LUNs, and then deletes them before creating more. • This behavior does not significantly increase the ITL count. If Reservation Support is enabled on the RPA: • All AVT and AVT LUNs are permanently created. • In RPA 2.3, only half the appliance posts are zoned with AVTs. This does not increase the ITL count significantly. • In RPA 2.4, all appliance ports are zoned with AVTs. This behavior **can** increase the ITL count significantly.
Same pWWN occurs more than once in the same VSAN.	Misconfiguration can result in two DVTs (or two VIs) with the same WWN in the same VSAN. For example, assume that two DVTs are created on different SSMs or on different DPPs. Both of these DVTs have the same back-end VSAN. When a host HBA logs into both DVTs, an attempt is made to create two VIs with the same WWN in the same back-end VSAN. This results in nondeterministic behavior.
A host is moved from the front-end VSAN to the back-end VSAN.	There is a VI in the back-end VSAN with the same pWWN as the host. Before you can move the host: • Shut the host port. • Purge to remove VI from the back-end VSAN. The host can now be safely moved.

Table 2-1 Common SANTap Mismatch Problems (continued)

Problem	Description
Inaccurate zoning.	Zoning solutions differ based on the Cisco SAN-OS or NX-OS and SSI versions in use. • With SSI 3.0(2j), you must have default zoning in the back-end VSAN, or zone the target and VIs together in the back-end VSAN. • With SSI 3.1(2), only the host VI and target need to be zoned together in the back-end VSAN.
Adding and removing hosts without performing a purge.	If you have 16 hosts and you remove one and add another, the new host will not see the LUNs. In this situation, perform a purge to clear one of the 16 entries after removing the host. Then you can add the new host to the DVT.

Troubleshooting General Issues

This section describes some general SANTap troubleshooting issues.

SSM_CRIT in the Supervisor syslog Messages

You might see SSM_CRIT errors, which indicate the following problems:

- ITL count per DPP exceeded

```
 %ISAPI-SLOT2-2-SSM_CRIT: Error: Commit failed, number of ITLs exceeded limit for the DPP.
token = 3
```

- Too many LUNs for an IT pair

```
 %ISAPI-SLOT2-2-SSM_CRIT: Error : SCAN_FSM_0x83f978c_0 : hi_wwn[210000e08b926292]
vt_wwn[50060e8003813236] : Too many LUNs
 %ISAPI-SLOT2-2-SSM_CRIT: Error : 16 LUNS installed
```

- Too many hosts logging into DVT

```
 %ISAPI-SLOT2-2-SSM_CRIT: Error : 16 hosts are already logged in the DVT.
 %ISAPI-SLOT2-2-SSM_CRIT: Error : New [host=0x10000000c93f9021] trying to log in to
[dvt=0x50060e8003813236]
```

iSAPI Technical Support has SANTap Logs

You can examine the SANTap Logs in iSAPI Technical Support and do the following actions:

- Search for errors.
- Search for failed and failure.
- Check FCNS database.
- Check FLOGI database.

Host Login Problems

In case of host login problems, use the following commands:

```
module-2# show santap vttbl dvt dvt_pwwn

module-2# show santap vttbl dvt dvt_pwwn host host_pwwn
```

To enable the log, use the following commands:

```
module-2# debug vsd vfc-felogin
module-2# debug partner 0x92810000 d1
module-2# debug partner 0x92810000 d2
```

To turn off debug log, use the following commands:

```
module-2# no debug vsd vfc-felogin
module-2# no debug partner 0x92810000 d1
module-2# no debug partner 0x92810000 d2
module-2# debug vsd vfc-felogin
module-2# debug partner 0x92810000 d1
module-2# no debug all
```

ITL Problems

To check the ITLs, use this command:

```
module-2# show isapi dpp 4 queue
```

To check the number of ITLs on a DPP, use this command:

```
module-2# show isapi dpp 4 queue | incl LUN | count
```

To check the number of ITLs on an SSM, use this command:

```
module-2# show isapi dpp all queue | incl LUN | count
```

Configuration Errors

The following are some of the common configuration errors:

- Version mismatch between the SSM and appliance
- Version mismatch between the supervisor and SSI image
- Overprovisioning
- Too many ITLs per SSM
- Too many hosts per DVT
- Too many ITLs per DPP
- Not supported by interoperability matrix
- CVT in host VSAN
- Using IVR and SANTap together
- Same pWWN occurs twice in one VSAN
- Moving the host from front-end VSAN to back-end VSAN
- VIs in DVT VSAN
- Inaccurate zoning

CVT and DVT in the Same VSAN

When a CVT and DVT are in the same VSAN, the result is that one CPP VI and eight DPP VIs get created in a DVT VSAN. The VIs attempt to log in to DVT, which results in nondeterministic behavior.

Duplicate WWNs in the Same VSAN

Configuration errors can lead to duplicate WWNs in the same VSAN. This can lead to either of the two scenarios:

- Two DVTs with the same WWN in the same VSAN
- Two VIs with the same WWN in the same VSAN

Duplicate VIs

Duplicate VIs are created due to these configuration errors:

- Two DVTs are created on different SSMs or on different DPPs.
- The DVTs have the same back-end VSAN.

- A host HBA logs in to both DVTs.
- An attempt is made to create two VIs with same WWN in the same back-end VSAN.

This results in nondeterministic behavior.

Moving the Host

Moving the host from a front-end VSAN to a back-end VSAN creates the following problems:

- A VI is in the back-end VSAN.
- VI pWWN is the same as host pWWN.
- After shutting the host port, a purge has to be done to remove the VI in the back-end VSAN.

Now the host can be moved to the back-end VSAN.

Adding and Removing Hosts

Note If you remove a host and add another host, the new host will not see the LUNs.

After removing the host, a purge has to be done. One of the entries created is cleared, which enables the new host to log in to the DVT.

Interoperability Matrix

- Always make sure that the hosts, targets, HBAs and switches have been certified by Cisco.
- Cisco publishes a SANTap Interoperability Matrix, which is different from the Layer 2 Interoperability Matrix.