IBM System Storage SAN Volume Controller

Software Installation and Configuration Guide - Errata

Version 4.2.0
August 15, 2007

SC23-6628-00-Errata.

Contents

About this guide

This guide provides errata information that pertains to release 4.2.0 of the *IBM System Storage SAN Volume Controller Software Installation and Configuration Guide.*

This guide contains the corrections and additions on a per chapter basis. The chapter numbers in this guide correspond directly with the chapter numbers in the *Software Installation and Configuration Guide* supplied with your SAN Volume Controller.

Who should use this guide

Before using the IBM System Storage SAN Volume Controller, you should review the errata contained within this guide and note the details with respect to the copy of the *Software Installation and Configuration Guide* supplied with you SAN Volume Controller.

Last Update

This document was last updated: August 15, 2007

Change History

The following revisions have been made to this document:

Revision Date	Sections Modified
August 15, 2007	New document

Table 1: Change History

Chapter 1: SAN Volume Controller overview

Sending notifications

Page 30, The second paragraph of ***Call Home e-mail*** *should be replaced with:*

You must configure an SMTP server to be able to send e-mails outside of your local area network. The SMTP server must allow relaying of e-mails from the SAN Volume Controller cluster IP address. Then use the SAN Volume Controller Console or the SAN Volume Controller command-line interface to configure the e-mail settings (including contact information and e-mail recipients). For compatibility with different SMTP servers ensure you set the reply address to a valid e-mail address. You should send a test e-mail to check that all connections and infrastructure are set-up correctly. You can disable the Call Home function at any time using the SAN Volume Controller Console or the SAN Volume Controller command-line interface.

Page 31, The contact information bullet of ***Inventory information e-mail*** *should be replaced with:*

- Contact information, including name and phone number. This is the contact information that was set for the Call Home e-mail function. However, you can change the contact information specifically for inventory e-mail using the SAN Volume Controller Console or the **mkemailuser** or **chemailuser** CLI commands.

Chapter 4: Configuring the master console

Page 85, Replace the introduction with (strike through text indicates the removed sections):

You can configure the master console to access the SAN Volume Controller Console and the SAN Volume Controller command-line interface (CLI). If you installed the master console on your own hardware, you have already performed some of these steps during the installation process.

Perform the following process to configure the master console:

1. Log on as a local administrator (for example, as the Administrator user) to the system where the master console software is installed.

   Note: If you purchased the software master console, skip to step 3 because you already performed the tasks described in step 2 before or during the installation of the master console software.

2. If you purchased a hardware master console, perform the following configuration steps:

   a. Optionally, reconfigure the master console host name. When you receive the hardware master console, the host name is preconfigured as mannode. If you choose to change this name see "Changing the master console host name" for more information.

   b. Configure the internal IP network connection (Local Area Network). "Configuring the internal IP network connection" on page 86 provides more details for this step.

   c. Configure the browser. "Configuring the Web browser" on page 86 provides more details for this step.

   d. Generate an SSH key pair using the PuTTYgen. "Generating an SSH key pair using PuTTY" on page 87 provides more details for this step.

3. For a software master console or a hardware master console, perform the following configuration steps:

   a. Configure a default PuTTY session for command-line interface (CLI) access. "Configuring the PuTTY session for the CLI" on page 89 provides more details for this step.

   b. Store keys in the SAN Volume Controller Console software. "Storing the private SSH key in the SAN Volume Controller Console software" on page 88 provides more details for this step.

   ~~c. Set up e-mail notification and the call home feature for the SAN Volume Controller.~~

   d. Install your chosen antivirus software on the master console system.

Chapter 6: Using the SAN Volume Controller Console

Shutting down a cluster

Page 114. This section is modified as follows (strike through text indicates the removed sections):

You can shut down a SAN Volume Controller cluster from the Shutting Down cluster panel.

If you want to remove all input power to a cluster (for example, the machine room power must be shutdown for maintenance), you must shut down the cluster before the power is removed. If you do not shut down the cluster before turning off input power to the uninterruptible power supply (UPS), the SAN Volume Controller nodes detect the loss of power and continue to run on battery power until all data that is held in memory is saved to the internal disk drive. This increases the time that is required to make the cluster operational when input power is restored and severely increases the time that is required to recover from an unexpected loss of power that might occur before the UPS batteries have fully recharged.

When input power is restored to the UPSs, they start to recharge. However, the SAN Volume Controller nodes do not permit any I/O activity to be performed to the virtual disks (VDisks) until the UPS is charged enough to enable all the data on the SAN Volume Controller nodes to be saved in the event of an unexpected power loss. This might take as long as three hours. Shutting down the cluster prior to removing input power to the UPS units prevents the battery power from being drained and makes it possible for I/O activity to resume as soon as input power is restored.

Before shutting down a cluster, quiesce all I/O operations that are destined for this cluster. Failure to do so can result in failed I/O operations being reported to your host operating systems.

Attention:

- If you are shutting down the entire cluster, you lose access to all VDisks that are provided by this cluster. Shutting down the cluster also shuts down all SAN Volume Controller nodes. This shutdown causes the hardened data to be dumped to the internal hard drive.
- ~~Ensure that you have stopped all FlashCopy, Metro Mirror, Global Mirror, and data migration operations before you attempt a cluster shutdown. Also ensure that all asynchronous deletion operations have completed prior to a shutdown operation.~~

Begin the following process of quiescing all I/O to the cluster by stopping the applications on your hosts that are using the VDisks that are provided by the cluster.

1. Determine which hosts are using the VDisks that are provided by the cluster.
2. Repeat the previous step for all VDisks.

Perform the following steps to shut down a cluster:

1. Click Manage Clusters. Shut down Cluster in the portfolio. The Shutting Down cluster panel is displayed.
2. Click Yes.

When input power is restored, you must press the power button on the UPS units before you press the power buttons on the SAN Volume Controller nodes.

Shutting down a node

Page 115. This section is modified as follows (strike through text indicates the removed sections):

You can shut down a SAN Volume Controller node from the Shutting Down Node panel.

If you are shutting down the last SAN Volume Controller node in an I/O group, quiesce all I/O operations that are destined for this SAN Volume Controller node. Failure to do so can result in failed I/O operations being reported to your host operating systems.

~~**Attention:** Ensure that you have stopped all FlashCopy, Metro Mirror, Global Mirror, and data migration operations before you attempt a SAN Volume Controller node shutdown. Also ensure that all asynchronous deletion operations have completed prior to a shutdown operation.~~

This task assumes that you have already launched the SAN Volume Controller Console.

Perform the following steps to use the shutdown command to shut down a SAN Volume Controller node:

1. Click **Work with Nodes -> Nodes** in the portfolio. The Viewing Nodes panel is displayed.
2. Select the node that you want to shut down.
3. Select **Shut Down a Node** from the task list and click **Go**. The Shutting Down Node panel is displayed.
4. Click **Yes**.

When input power is restored, you must press the power button on the uninterruptible power supply units before you press the power button on the SAN Volume Controller node.

Chapter 7: Using the CLI

Setting up error notifications using the CLI

Page 198. Rename this section:

Setting up SNMP error notifications using the CLI

Chapter 10: Configuring and servicing storage subsystems

Discovering logical units

Page 230. This section has the following addition:

Guidelines for exporting LUs

- It is important that new LUs are only presented to SVC after the array initialisation/format has completed. Failure to follow these instructions may result in the customer attempting to add a LUN to an mdiskgrp whilst the underlying array or logical unit is still formatting/initialising - which would result in the mdiskgrp going offline (i.e. a loss of access to the vdisks in that mdisk group).

Manual discovery

Page 241. This section should be replaced with the following:

When you create or remove LUNs on a storage subsystem, the managed disk (MDisk) view is not always automatically updated.

You must issue the **svctask detectmdisk** command-line interface (CLI) command or use the **Discover MDisks** function from the SAN Volume Controller Console to have the cluster rescan the fibre-channel network. The rescan discovers any new MDisks that might have been added to the cluster and rebalances MDisk access across the available controller device ports.

Using **svctask detectmdisk** informs SVC that the current fabric configuration is as intended. The **svctask detectmdisk** command must be issued when previously used target ports are removed from SVC.

Note: You should only issue the **svctask detectmdisk** command when you are sure all disk controller ports are working, and correctly configured in the controller and the SAN zoning. Failure to do this may result in errors not being reported.

Configuring the Fujitsu ETERNUS subsystems

Configuring the Fujitsu ETERNUS to use with the SAN Volume Controller

Host response pattern

Page 261. This section is replaced by the following: (change bars show the differences in this errata)

The SAN Volume Controller requires that a new host response pattern is created. If the Host Affinity/Host Table Settings Mode is used, this host response pattern must be associated with each WWN. If the Host Affinity/Host Table Settings Mode is not used, this host response pattern must be associated with the target port.

The following table lists the settings that are required. See the documentation that is provided with your Fujitsu ETERNUS subsystem for more information because some options are only available on certain models.

Option	Fujitsu ETERNUS default setting	SAN Volume Controller required setting
Command timeout interval	Depends on the Fujitsu ETERNUS model	Default
Response status in overload	Unit Attention	Unit Attention
Byte 0 of Inquiry response/Response to inquiry commands	Default	Default
Inquiry Standard Data NACA Function	Disable	Disable
Inquiry Standard Data Version	Depends on the Fujitsu ETERNUS model	Default
Inquiry Command Page 83/Inquiry VPD ID Type	Depends on the Fujitsu ETERNUS model	Type 01 (see note 1 below)
Reservation Conflict Response to Test Unit Ready Commands	Disable/Normal Response	Enable/Conflict Response
Target Port Group Access Support	Disable	Enable (see note 2 below)
Host Specific Mode	Normal Mode	Normal Mode
Response Sense at Firmware Hot Switching	Enable	Enable
Change LUN Mapping	No Report	Report
LUN Capacity Expansion	No Report	Report
Asymmetric / Symmetric Logical Unit Access	Active/Active	Active/Active
Pattern of Sense Code Conversion	No Conversion	No Conversion

Note: 1. Setting Inquiry VPD ID Type to "Type 3" on E4000/E8000 range will cause mdisks to go offline.

Note: 2. Setting "Target Port Group Access Support" to Disabled on E3000 range will cause 1370 error in error log

Configuring NEC iStorage subsystems

Page 317. This section has the following additions:

Additional settings via Service Menus

The following additional settings are available via the service menus, these can be accessed via a web browser or via a direct attached maintenance PC.(reference NEC manuals Appendix "Maintenance PC")

Configuration: System Configuration

Tick Box	Description
✓	Patrol media Read On
✓	Patrol media Write On
✓	Automatic Rebuild Function On
✓	Automatic Hot Spare Function On
	Direct Transfer Mode On
	Verify On
✓	Buffer Mode Enable
	ACOS ALIVE Disable
	iSM ALIVE Disable
	RV Response Data Protect Enable
	Write FUA Enable
	Read FUA Enable
	Hot Spare Mode On
	Reduce Reassign Control Disable
	Reassign Count (Dec.) [value box contains 0]
	Prevent Maintenance Disable
	Prevent Maintenance Level (0-7) [value box contains 0]
	Patrol Coherency Check Enable
	PD Write Check Enable
✓	Auto Hot Copy Enable
	SFP Alarm Disable

Configuration: Cache Configuration

The following table gives examples of the Cache settings, these may vary from one model to another, its not recommended to change them from the default values unless directed to do so by NEC or IBM service personnel.

Tick Box	Description
✓	Read Cache Enable
✓	Write Cache Enable
✓	Fast Write Disable Without Backup Page
✓	Sequential Full Stripe Write Enable
✓	Sequential Prefetch Enable
✓	Semisequential Prefetch Enable
	Write Cache Ratio(%) [value box contains 60]
	Dirty High Water Ratio(%) [value box contains 80]
	Dirty Low Water Ratio(%) [value box contains 20]
	Write Back High Speed(dec.) [value box contains 60]
	Write Back Middle Speed(dec.) [value box contains 50]
	Write Back Low Speed(dec.) [value box contains 40]
	Minimum Prefetch Length(KB)(dec.) [value box contains 16]
	Max Prefetch Length(KB)(dec.) [value box contains 10000]
	Sequential Judge Count(dec.) [value box contains 3]
	Multi Number(dec.) [value box contains 10]

Configuration: Port Configuration

All ports should be set to Host Type AX (AIX).

Configuration: FC Port Configuration, Link Attach

The Link Attach mode of all ports must be set to "Fabric Only" via the service menus, see NEC documentation. Other settings should remain at defaults.

Configuring Bull FDA subsystems

Page 242. This section has the following additions:

Additional settings via Service Menus

The following additional settings are available via the service menus, these can be accessed via a web browser or via a direct attached maintenance PC.(reference Bull FDA manuals Appendix "Maintenance PC")

Configuration: System Configuration

Tick Box	Description
✓	Patrol media Read On
✓	Patrol media Write On
✓	Automatic Rebuild Function On
✓	Automatic Hot Spare Function On
	Direct Transfer Mode On
	Verify On
✓	Buffer Mode Enable
	ACOS ALIVE Disable
	iSM ALIVE Disable
	RV Response Data Protect Enable
	Write FUA Enable
	Read FUA Enable
	Hot Spare Mode On
	Reduce Reassign Control Disable
	Reassign Count (Dec.) [value box contains 0]
	Prevent Maintenance Disable
	Prevent Maintenance Level (0-7) [value box contains 0]
	Patrol Coherency Check Enable
	PD Write Check Enable
✓	Auto Hot Copy Enable
	SFP Alarm Disable

Configuration: Cache Configuration

The following table gives examples of the Cache settings, these may vary from one model to another, its not recommended to change them from the default values unless directed to do so by Bull or IBM service personnel.

Tick Box	Description
✓	Read Cache Enable
✓	Write Cache Enable
✓	Fast Write Disable Without Backup Page
✓	Sequential Full Stripe Write Enable
✓	Sequential Prefetch Enable
✓	Semisequential Prefetch Enable
	Write Cache Ratio(%) [value box contains 60]
	Dirty High Water Ratio(%) [value box contains 80]
	Dirty Low Water Ratio(%) [value box contains 20]
	Write Back High Speed(dec.) [value box contains 60]
	Write Back Middle Speed(dec.) [value box contains 50]
	Write Back Low Speed(dec.) [value box contains 40]
	Minimum Prefetch Length(KB)(dec.) [value box contains 16]
	Max Prefetch Length(KB)(dec.) [value box contains 10000]
	Sequential Judge Count(dec.) [value box contains 3]
	Multi Number(dec.) [value box contains 10]

Configuration: Port Configuration

All ports should be set to Host Type AX (AIX).

Configuration: FC Port Configuration, Link Attach

The Link Attach mode of all ports must be set to "Fabric Only" via the service menus, see Bull documentation. Other settings should remain at defaults.

Configuring NetApp FAS subsystems

Page 318. This section has the following additions:

Creating Logical Units

Creating a Logical Unit(LU) involves identifying a volume to create the LU from, and how much space to use. The following steps provide a description for successful LUN creation:

- Log onto the NetApp FAS.
- Go to 'Filer View' and authenticate.
- Identify a Volume to create an LU from; Click 'Volumes' on the left panel.
- A list of Volumes appears on the central panel.
- Be careful creating LUs from the root volume as it doesn't always preserve the 'Space Reserved' setting (see below).
- Identify a volume which has sufficient free space for the desired LUN size, and note its volume number (e.g. vol2).
- Click LUNs on the left hand panel.
- Click 'Add' from the list.
- Enter the following:
- Path: This should be /vol/volx/lun_name - where volx is the name of the volume identified above, and lun_name is a generic lun_name.
- LUN Type: Leave this as **Image**
- Description: Can leave this blank
- Size: Desired LUN Size
- Units: Desired LUN Size in units...
- Space Reserved: Ensure this is ticked
  - If this is not ticked then if the filer should decide that the file system is full, it will offline the LUN. This will cause your mdisk group to go offline and loss off access to the vdisks in that group.
- Click 'Add'

Note: To check the LUN settings going to the 'Manage LUNs' section, and click on the LUN of interest. Check that the 'Space Reserved' setting is set.

Deleting Logical Units

To Delete a Logical Unit:

- Log onto the NetApp FAS.
- Go to 'Filer View' and authenticate.
- Click 'LUNs' from the list on the left.
- Click Manage. This brings up a list of LUNs.
- Click on the LUN you wish to delete.
- Click Delete. A confirmation box is presented, confirm your choice.

Creating a Host Object

To Create a Host Object:

- Log onto the NetApp FAS.
- Go to 'Filer View' and authenticate
- Click 'LUNs' from the list on the left.
- Click 'Initiator Groups' from the list on the left (this opens up under the LUN option)
- Click 'Add'. The central panel displays several fields which need to be filled out:
  - Group Name: The name of the Initiator Group / Host.
  - Type: set to FCP
  - Operating System: set to Default
  - Initiators: A list of wwpns that are associated with this host type.
  - A list of WWPN candidates is displayed.

Note: It is recommended to delete all of the WWPNs in this list, and manually insert a list of WWPNs you know are your SVC ports. This list can be all the WWPNs of all the ports of the SVC nodes in the SVC cluster.

- Now click 'Add'

Presenting a LUN to a Host

To Map a Logical Unit:

- Log onto the NetApp FAS.
- Go to 'Filer View' and authenticate
- Click 'LUNs' from the list on the left.
- Click Manage. This brings up a list of LUNs.
- Click on the LUN you wish to Map.
- Click 'Map LUN'

Note: This window also lists Initiator Groups that this LUN is already mapped to.

- Click 'Add Groups to Map'
- Select your Host Name/Initiator Group from the list and click 'Add'

Note: The LUN ID section can be left blank; The FAS will allocate a LUN ID based off what both controllers are currently presenting or the user can specifiy the LUN ID.

Note: If you are re-mapping the LUN from one host to another, you can also at this stage tick the Unmap tickbox.

- Finally, click 'Apply'

Appendix F. Error Codes

Page 371. Replace the introduction of this appendix with:

Error codes provide a unique entry to service procedures. Each error code has an error ID that uniquely identifies the condition that caused the error.

Error IDs are recorded in the error log. When the number of error IDs of a specific type for a specific resource exceeds a pre-determined threshold, an SNMP trap is raised and an e-mail is sent. When the SNMP traps are received, the SNMP type is used by the management tools to control how the trap is processed. The SNMP type is used by the Call Home e-mail service to decide the recipients of the e-mail and the title and contents of the e-mail. The following SNMP types are possible:

Error This type identifies unexpected conditions that may be caused by a machine failure. If configured, an event of this type will cause an SNMP trap to be sent to the monitoring application and / or an e-mail to be sent to the IBM support center and the system administrator.

Warning
This type identifies unexpected conditions that might be experienced during user operations. These conditions can result from device errors or incorrect user actions. If configured, an event of this type will cause an SNMP trap to be sent to the monitoring application and / or an e-mail to be sent to the system administrator.

Information
This type identifies conditions where a user might want to be notified of the completion of an operation. If configured, an event of this type will cause an SNMP trap to be sent to the monitoring application and / or an e-mail to be sent to the system administrator.

Pages 371 to 377. Table 58. Error Codes, replace the column titles with the following:

	SNMP		**Error**
Error ID	**Type**	**Condition**	**Code**

Appendix G. Event Codes

Information event codes

Page 379. Replace the introduction to this section with:

The information event codes provide information on the status of an operation.

Information event codes are recorded in the error log and, if configured, an SNMP trap is raised and an e-mail is sent.

Information event codes can be either SNMP trap type I (information) or type W (warning). You can use the SNMP trap type, which is included in the e-mail, to determine if the information event resulted from an expected or unexpected condition. An information event report of type W might require user attention.

Page 379. Table 59, replace the column headings with:

Event code	SNMP Type	Description

Configuration event codes

Page 380. Replace the first two paragraphs of this section with:

Configuration event codes are generated when configuration parameters are set. Configuration event codes are recorded in a separate log and neither SNMP traps are raised nor e-mails sent. Their error fixed flags are ignored.