HP 9000 Virtual Library System User Guide
For VLS Firmware 6.1.0

Abstract

This document describes the HP VLS9000–series systems to facilitate their installation, operation, and maintenance. This document is intended for system administrators who are experienced with setting up and managing large storage systems.

HP Part Number: AG306-96034
Published: December 2012
Edition: Tenth

Acknowledgments

Warranty

WARRANTY STATEMENT: To obtain a copy of the warranty for this product, see the warranty information website:

http://www.hp.com/go/storagewarranty

Revision History

Revision AG306-96034 release of firmware version 6.1.0	December 2012
Revision AG306-96029 release of firmware version 3.4.0	September 2010
Revision AG306-96027 release of firmware version 3.3.1	March 2010
Revision AG306-96022 release of firmware version 3.2.1	September 2009

Contents

1 Introduction

The HP Virtual Library System (VLS) family consists of RAID disk-based SAN backup devices that emulate physical tape libraries, allowing you to perform disk-to-virtual tape (disk-to-disk) backups using your existing backup applications. The VLS family includes different series of models that vary in storage capacity and performance. Firmware version 6.0.0 marked the change to a 64–bit operating system on the nodes.

The VLS emulates a variety of physical tape libraries, including the tape drives and cartridges inside the libraries. You determine the number and types of tape libraries a VLS emulates, and the number and types of tape drives and cartridges included in each tape library to meet the needs of your environment. You configure the size of the virtual cartridges in your VLS, which provides even more flexibility.

The VLS offers many features such as:

- deduplication — storing only a single copy of a data block
- replication — transferring data from virtual cartridges on disk to a remote physical tape library across the LAN/WAN
- automigration — transferring data from virtual cartridges on disk to a physical tape library across the SAN
- Secure Erasure — overwriting data on cartridges to ensure that no data can be retrieved

The VLS accommodates mixed IT platform and backup application environments, allowing all your servers and backup applications to access the virtual media simultaneously. You can specify which servers are allowed to access each virtual library and tape drive you configure.

Data stored on a VLS is easily cloned to physical tape for off-site disaster protection or long-term archival using a backup application.

VLS9000 Components

A typical VLS system consists of the following components:

- VLS9000 nodes (at least one)
- VLS9000 disk array enclosures (at least one per node)

  You can add capacity by adding full arrays (one base enclosure and three capacity enclosures) or individual capacity enclosures. The enclosures come with the option of 1 TB or 2 TB drives.
- One VLS9000 20–port or 32–port connectivity kit

  (The VLS9000 7.5 TB and 10 TB systems omit the connectivity kit.)

  The 20-port connectivity kit includes two 10-port Fibre Channel switches and two Ethernet switches. The 32-port connectivity kit includes two 16-port Fibre Channel switches and two Ethernet switches. The 40-port connectivity kit includes two 20-port Fibre Channel switches and two Ethernet switches. By connecting two 40-port connectivity kits using an HP 9000 Virtual Library System Interswitch Link Kit, you can expand the capacity of the VLS system beyond 12 arrays to a maximum of 16 arrays. The two cabled connectivity kits function as one logical set of switches.

The VLS9000 7.5 TB and 10 TB systems consist of one node, one Ethernet switch, one base disk array enclosure, and up to three expansion disk array enclosures.

VLS9000 system scalability considerations:

- Two Fibre Channel ports (one Fibre Channel port on each Fibre Channel switch) are required for each VLS node.
- Two Fibre Channel ports (one Fibre Channel port on each Fibre Channel switch) are required for each VLS base enclosure.
- Up to two VLS arrays may be installed for every VLS node.
- For maximum capacity, install two arrays for every VLS node installed.
- For maximum performance, install one VLS array for every VLS node installed.
- A VLS system can support a maximum of eight 1U or 2U high performance nodes on non-deduplication systems and six nodes on deduplication-enabled systems.
- A VLS system can support a maximum of 12 arrays of 1 TB or 2 TB drives. To expand beyond 12 arrays, you must purchase and install a second connectivity kit.
- Install a maximum of four arrays per rack. Depending on the configuration, a VLS system requires one to four racks. If possible, install multiple racks next to each other.

See the *HP VLS9000 Virtual Library System Quickspec* on the HP web site (http://www.hp.com/go/vls) for performance data.

NOTE: HP recommends ordering a factory-configured rack to eliminate complicated cabling on-site.

The VLS uses 10.153.0.0/16 on its backend private network and requires its own subnet. Having another network interface (such as your public network) running on the same network will significantly interfere with the operation of the VLS.

2 Hardware Installation

This section details the steps to install the VLS hardware from installation preparation to final cabling.

Minimum Hardware Requirements

VLS9000 systems upgrading to firmware 6.1 have the following hardware requirements:

- Minimum system disk size is 120 GB, so systems with 60 GB drives must upgrade the drives
- Minimum memory is 16 GB of RAM, so systems with 4 GB of RAM must upgrade the memory

Preparing for the Installation

Tools for Installation

- Two people
- #1 and #2 Phillips screwdriver
- Standard screwdriver
- Allen wrench (provided; used with 6-mm screws and #12-24 x 3/8-inch sockethead screws)
- #3 Pozidrive screwdriver
- 7/16 inch wrench
- Box cutting knife

△ **CAUTION:** Do not use any power tools. They could strip or damage connections.

Taking ESD Precautions

To prevent damaging the system, be aware of the precautions you need to follow when setting up the system or handling parts. A discharge of static electricity from a finger or other conductor may damage system boards or other static-sensitive devices. This type of damage may reduce the life expectancy of the device.

To prevent electrostatic damage:

- Avoid hand contact by transporting and storing products in static-safe containers.
- Keep electrostatic-sensitive parts in their containers until they arrive at static-free workstations.
- Place parts on a grounded surface before removing them from their containers.
- Avoid touching pins, leads, or circuitry.
- Always be properly grounded when touching a static-sensitive component or assembly.

Grounding Methods to Prevent Electrostatic Discharge

Several methods are used for grounding. Use one or more of the following methods when handling or installing electrostatic-sensitive parts:

- Use a wrist strap connected by a ground cord to a grounded workstation or computer chassis. Wrist straps are flexible straps with a minimum of 1 megaohm ±10 percent resistance in the ground cords. To provide proper ground, wear the strap snug against the skin.
- Use heel straps, toe straps, or boot straps at standing workstations.

  Wear the straps on both feet when standing on conductive floors or dissipating floor mats.

- Use conductive field service tools.
- Use a portable field service kit with a folding static-dissipating work mat.

If you do not have any of the suggested equipment for proper grounding, have an authorized reseller install the part.

For more information on static electricity or assistance with product installation, contact your authorized reseller.

Unpacking

Place the shipping carton as close to the installation site as possible. Before unpacking the VLS, inspect the shipping carton for damage that may have occurred during shipment. If you detect any damage, notify the carrier and HP before unpacking the unit.

Removing the Packing Materials

To unpack the VLS:

1. Open the top of the shipping cartons.
2. Carefully lift the units out of the boxes and remove the packing materials.
3. Place the units on a stable work surface.

   NOTE: Inspect the units for any damage that may have occurred during shipment. If damage is detected, contact your authorized service representative.

4. Remove the accessory kits and documentation from the shipping cartons. Set them aside for later use.
5. Place shipping materials back into the shipping cartons.
6. Set the shipping cartons aside for later use.

Rack Planning Resources

The rack resource kit ships with all HP or Compaq branded 9000, 10000, and H9 series racks. A summary of the content of each resource follows:

- Custom Builder is a web-based service for configuring one or many racks. Rack configurations can be created using:
  - A simple, guided interface
  - Build-it-yourself model
- The Installing Rack Products video provides a visual overview of operations required for configuring a rack with rack-mountable components. It also provides the following important configuration steps:
  - Planning the site
  - Installing rack servers and rack options
  - Cabling servers in a rack
  - Coupling multiple racks
- The Rack Products Documentation CD enables you to view, search, and print documentation for HP and Compaq branded racks and rack options. It also helps you set up and optimize a rack in a manner that best fits your environment.

Rack Requirements

HP supports the HP System E racks and the HP 10000 Series racks for use with VLS systems. Other racks might also be suitable, but have not been tested with the VLS.

Rack Warnings

⚠ **WARNING!** To reduce the risk of personal injury or damage to the equipment, before installing equipment be sure that:

- The leveling jacks are extended to the floor.
- The full weight of the rack rests on the leveling jacks.
- The stabilizing feet are attached to the rack if it is a single-rack installation.
- The racks are coupled together in multiple-rack installations.
- Only one component is extended at a time. A rack may become unstable if more than one component is extended for any reason.

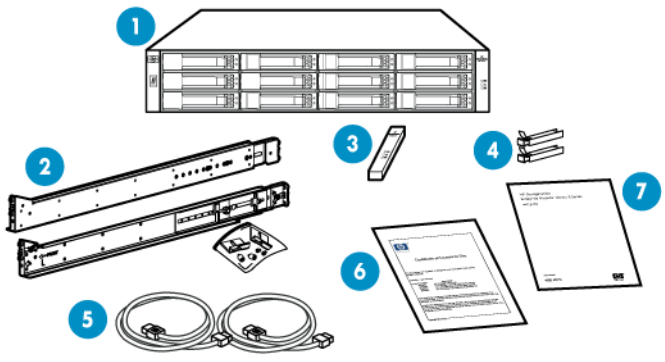
WARNING! To reduce the risk of personal injury or equipment damage when unloading a rack:

- At least two people are needed to safely unload a rack from a pallet. An empty 42U rack can weigh as much as 115 kg (253 lb), can stand more than 2.1 m (7 ft) tall, and may become unstable when being moved on its casters.
- Never stand in front of a rack when it is rolling down the ramp from the pallet. Always handle a rack from both sides.

Identifying the VLS Shipping Carton Contents

Unpack the VLS shipping cartons and locate the materials and documentation necessary for installing the VLS. All the rack mounting hardware and documentation necessary for installing a VLS node into a rack is included in the node shipping carton. All the rack mounting hardware and documentation necessary for installing a VLS disk array into a rack is included in the disk array shipping carton. All the rack mounting hardware and documentation necessary for installing a VLS connectivity kit into a rack is included in the connectivity kit shipping carton. All the documentation necessary for installing a VLS interswitch link kit into a rack is included in the interswitch link kit shipping carton.

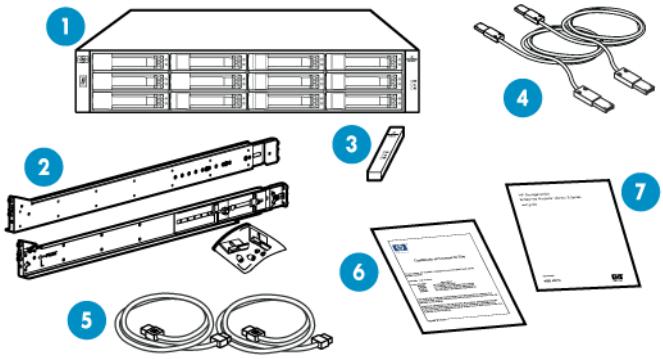
VLS9200 Base Enclosure Shipping Cartons



Item	Description
1	VLS9200 base enclosure, 10 TB or 20 TB (1)
2	1U rack mounting hardware kit (1)

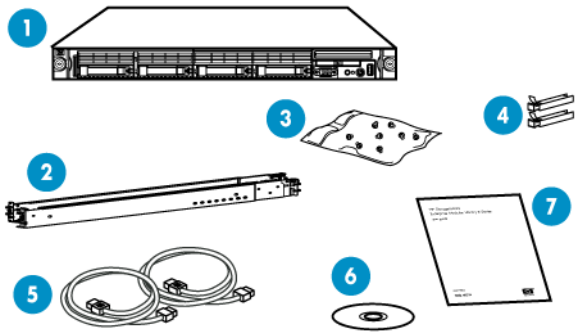
Item	Description
3	VLS badge (1)
4	8 Gb FC transceivers (2)
5	Power cords (2)
6	LTU (1 for 10 TB, 2 for 20 TB)
7	Printed VLS array installation poster (1)
	Ethernet cables (2) and FC cables (2), not shown (shipped separately)

VLS9200 Capacity Enclosure Shipping Cartons



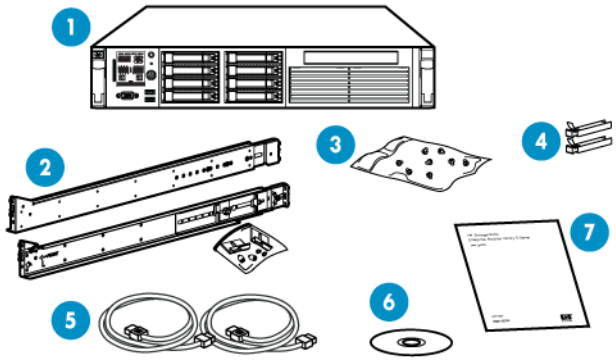
Item	Description
1	VLS9200 capacity enclosure, 10 TB or 20 TB (1)
2	1U rack mounting hardware kit (1)
3	VLS badge (1)
4	SAS cables (2)
5	Power cords (2)
6	LTU (1 for 10 TB, 2 for 20 TB)
7	Printed VLS array installation poster (1)

VLS9200 Node Shipping Carton



Item	Description
1	VLS9200 node (1)
2	1U rack mounting hardware kit (1) and documentation
3	Loopback plugs for FC ports (2)
4	8 Gb FC transceivers (2)
5	Power cords (2)
6	Quick Restore CD (1)
7	Printed VLS node installation poster (1)
	Ethernet cables (2) and Fibre Channel cables (2), not shown (shipped separately)

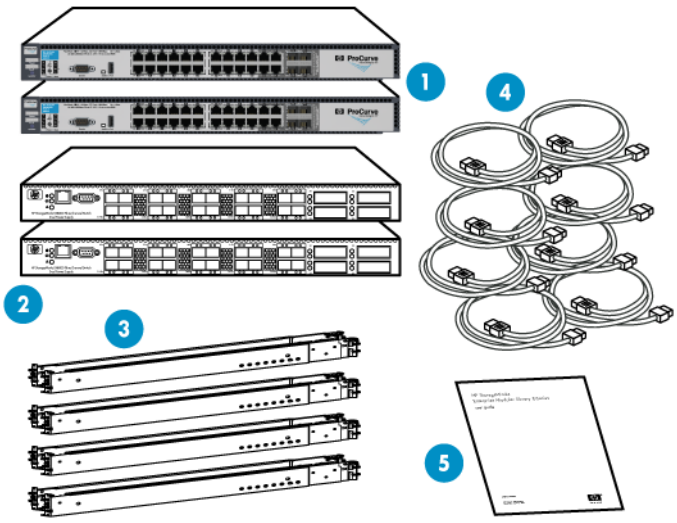
VLS9200 High Performance Node Shipping Carton



Item	Description
1	VLS9200 high performance node (1)
2	2U rack mounting hardware kit (1) and documentation
3	Loopback plugs for FC ports (4)
4	8 Gb Fibre Channel transceivers (2)
5	Power cords (2)
6	Quick Restore CD (1)

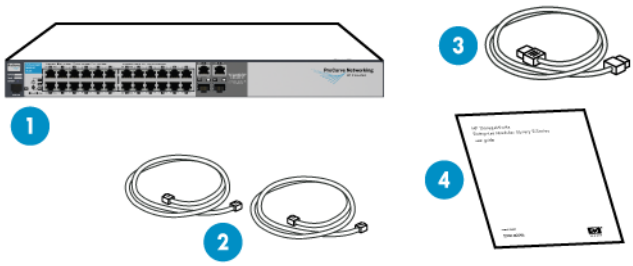
Item	Description
7	Printed VLS node installation poster (1)
	Ethernet cables (2) and Fibre Channel cables (2), not shown (shipped separately)

VLS9000 40-port Connectivity Kit Shipping Carton



Item	Description
1	Ethernet switches (2)
2	20–port FC switches (2)
3	1U rack mount kits (4) and documentation
4	Power cords (8)
5	Printed VLS connectivity kit installation poster (1)
	Air plenums for the Ethernet switches (2), not shown
	Ethernet cables (3), not shown (shipped separately)

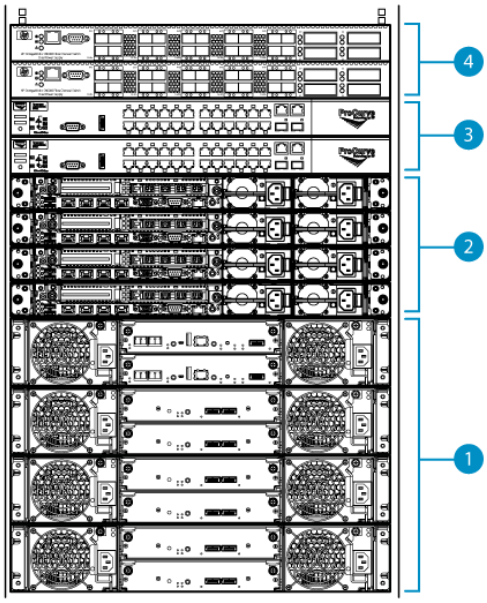
VLS9000 Entry-level Connectivity Kit Shipping Carton



Item	Description
1	Ethernet switch 2510–24 (1)
2	Ethernet cables (2)
3	Power cord (1)
4	Printed VLS connectivity kit installation poster (1)

VLS Assembly Overview

HP recommends you install the VLS9000 and VLS9200 components in the following order:



1. Install base and capacity disk array enclosures using *HP 9200 Virtual Library System 10 TB and 20 TB SAS Base Enclosure Installation Instructions* and *HP 9200 Virtual Library System 10 TB and 20 TB SAS Capacity Enclosure Installation Instructions*.
2. Install nodes using *HP 9200 Virtual Library System 4 Gb Node Installation Instructions* (shown) or *HP 9200 Virtual Library System 4 Gb High Performance Node Installation Instructions*.
3. Install Ethernet switches using *HP 9000 Virtual Library System 40-port Fibre Channel Connectivity Kit Installation Instructions* (shown) or *HP 9000 Virtual Library System Entry-level Connectivity Kit Installation Instructions*.
4. Install Fibre Channel switches using *HP 9000 Virtual Library System 40-port Fibre Channel Connectivity Kit Installation Instructions*.
5. Cable all components using the installation instructions provided with each component.
6. Install and cable XPAK transponders, if applicable, using *HP 9000 Virtual Library System Interswitch Link Kit Installation Instructions*.

NOTE: Not all systems use all of the components listed above.

Installing PDUs

If the rack you are using already has PDUs (power distribution units) installed, skip this procedure.

NOTE: This procedure is for racks using single phase PDUs. If your rack uses 3-phase PDUs, see the instructions that came with the PDUs.

1. Determine the number of PDUs to install.
   - The number of PDUs you install is based on the number of arrays to install.
   - Install up to four arrays in one rack.
   - Install up to a maximum of four additional arrays in racks two through four.

   Use the following table to determine how many PDUs to install:

Arrays	PDUs		PDMs	
	North America	Europe	North America	Europe
1	2	2	6	6
2	2	2	6	6
3	4	4	10	8
4	4	4	10	8

   NOTE: PDUs are installed in pairs.

   PDMs (power distribution modules) are the power outlet strips that connect to the PDUs.

   NOTE: Steps 2 through 6 correspond to the PDUs and PDMs called out in Figure 1 (page 22).

2. Install the first two PDUs in the front rack positions 1 and 2.

   If installing four PDUs, install the second pair in the rear rack positions 1 and 2.

   NOTE: To ensure high availability, HP recommends connecting half of the PDMs to one power source, and the other half to a second power source.

3. Install PDMs from the front PDU in rack position 1 to the lower left rack doorway.
4. Install PDMs from the front PDU in rack position 2 to the lower right rack doorway.
5. If you installed four PDUs:

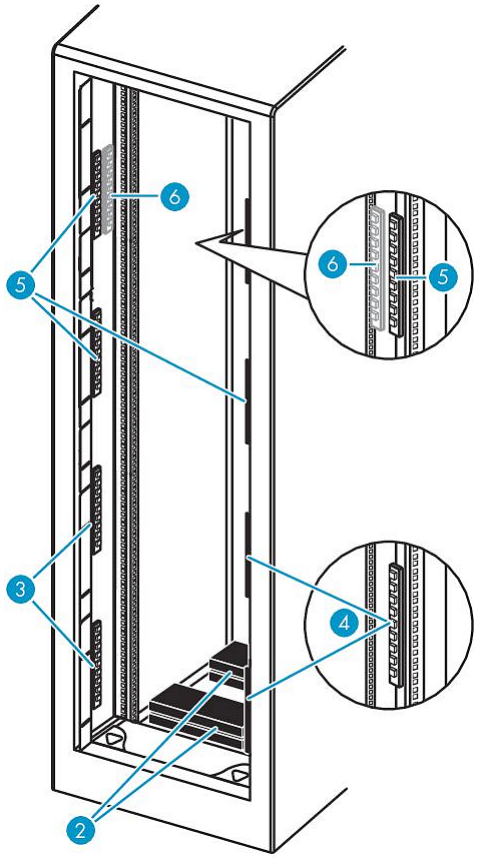
   Install PDMs from the rear PDU in rack position 1 to the upper left rack doorway.

   Install PDMs from the rear PDU in rack position 2 to the upper right rack doorway.
6. If needed, you may install a fifth PDM on the upper left and right rack doorway beside the top PDM for sites in North America, but do not exceed five PDMs per side. Do not exceed four PDMs per side for sites in Europe.

⚠ **WARNING!**

- In North America – Do not plug more than three PDMs into a PDU.
- In Europe – Do not plug more than two PDMs into a PDU.

Figure 1 PDU and PDM locations

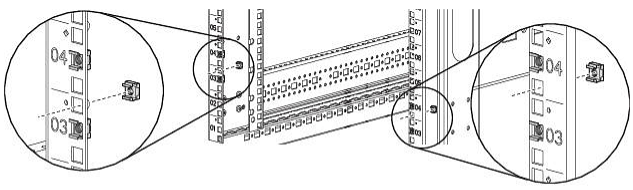


Installing the Disk Array Enclosures into a Rack

This section describes how to install the disk array enclosures into a rack.

Installing Cage Nuts

1. Locate the cage nuts from the rack mounting hardware kit contents.
2. Start at rack positions 3 and 4 when installing full arrays. Leave rack space for future expansion for any partial array being installed. See"Mounting the Disk Array Enclosures into the Rack" (page 25) for the placement of the enclosures.
3. Install a cage nut in the middle hole of each position on the front vertical posts for a total of two on each side.
4. On the left front post, between the two cage nuts just installed, install a cage nut in the bottom hole.
5. On the right front post, between the two cage nuts just installed, install a cage nut in the top hole.



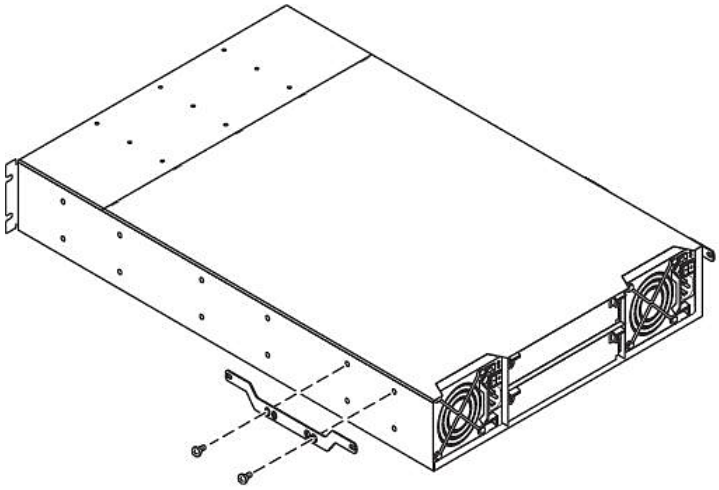
6. Repeat this procedure on the front vertical posts for each 2U enclosure to be installed.

7. On the rear vertical posts, starting at the same rack positions as in the front, install a cage nut in the middle hole of each position for each 2U enclosure to be installed.

Attaching Side Brackets to Enclosures

NOTE: The right and left enclosure side brackets are identical. Install the brackets with the beveled slots facing away from the disk array enclosures.

To attach enclosure side brackets to each side of a disk array enclosure, use two #8-32 x 3/16-inch flathead screws on each side.



11852

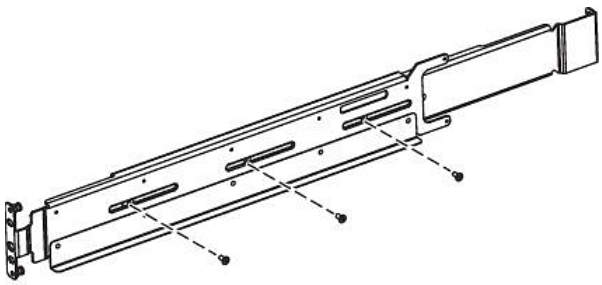
1. Locate the enclosure side brackets and screws from the rack mounting hardware kit contents.
2. Position the enclosure side bracket with the long edge down and the arms flush with the top of the enclosure.
3. Line up the outermost beveled slots of the enclosure side bracket with the rear holes in the enclosure. The rear arm extends slightly past the back of the enclosure.
4. Install two #8-32 x 3/16-inch flathead screws into the slots. Tighten both screws.

   NOTE: Using screws longer than #8-32 x 3/16-inch may result in interference with the power supply.

5. Repeat this procedure for the other side bracket, and for each enclosure to be added.

Attaching the Front to the Rear Rail Pieces

To attach the front and rear rail pieces, use three #8-32 x 3/8-inch flathead screws for each complete rail.

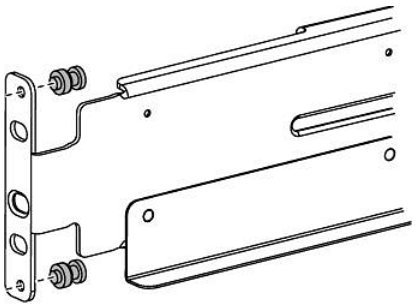


11855

1. Locate the front and rear rail pieces and screws from the rack mounting hardware kit contents.

   NOTE: The front rail piece has three long, beveled slots. The rear rail piece has holes.

2. Slide the rear rail piece behind the front rail piece so the brackets are at opposite ends and bend away from you.
3. Line up the center of the beveled slots on the front rail piece with the first, third, and fifth holes in the rear rail piece, counting from the unbent end.
4. Install but do not completely tighten three #8-32 x 3/8-inch flathead screws into the slots. Tighten them when instructed to do so.
5. Install rail hangers in the top and bottom holes of the front bracket and in the center hole of the rear bracket.



6. Repeat this procedure for the other side rail, and for each enclosure to be added.

Installing Enclosure Rails into the Rack

1. Locate the VLS badge that came with the enclosure. On the enclosure's right side, pop off the MSA badge and replace it with the VLS badge.
2. Locate the #10–32 5/8–inch flathead and #10–32 3/4 trusshead screws from the rack mounting hardware kit contents.
3. Start at rack positions 3 and 4 when installing full arrays. Leave rack space for future expansion for any partial array being installed.
4. On one front vertical post, insert the rail hangers of the front rail bracket into the top and bottom holes of the 2U section of post.

   NOTE: Install the rails with the three beveled slots to the front of the rack and the ledge at the bottom of the rail.

5. Install one #10–32 5/8–inch flathead screw into the bracket slot that is slightly offset from center. Do not tighten the screw completely.
6. In the rear of the rack, keeping the rail level, insert the rail hanger into the rear vertical post.
7. Push the bracket to the outside of the rack until snug.
8. Install two #10–32 3/4–inch trusshead screws into the top and bottom positions of the rear rail bracket. Tighten the screws.
9. In the front of the rack, push the bracket to the outside of the rack until snug. Tighten the screw in the front rail bracket.
10. Tighten the flathead screws connecting the front and rear rail pieces.
11. Repeat this procedure on the other side of the rack, and to install a set of rails for each enclosure to be added.

Mounting the Enclosures into the Rack

WARNING! The enclosure weighs 33.6 kg (74 lb) full. At least two people are required to lift, move, and install the enclosure.

If only one person is to perform the installation, remove the power modules and hard drives from an enclosure before installing it, and if possible position it on top of another device or shelf in the rack to hold it as you attach all the brackets.

CAUTION: When positioning an enclosure in the rack, ensure the air vents at the front and back of the enclosure are not blocked.

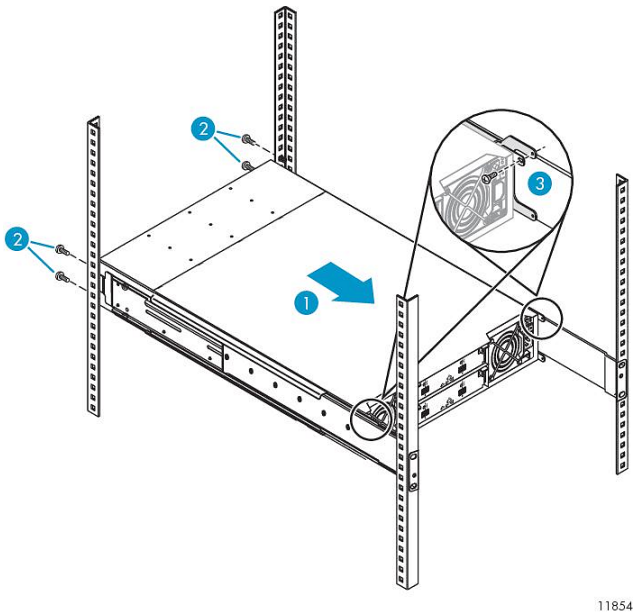
NOTE: The enclosures placements in this procedure are for racks using single phase PDUs. If your rack uses 3–phase PDUs, install all enclosures two rack positions lower than indicated here. (Single phase PDUs take up the bottom two rack positions while 3–phase PDUs do not.)

This procedure is for racks using singe phase PDUs. If your rack uses 3-phase PDUs, see the instructions that came with the PDUs.

1. If your system contains four full arrays (one base enclosure and three capacity enclosures) per rack, install the first capacity enclosure at rack positions 3 and 4.

   If your system contains fewer than four full arrays, start at rack position 9. Count down two rack positions for each available capacity enclosure and install the first capacity enclosure at the lowest point.

   NOTE: Install full arrays whenever possible. A partial array (one base enclosure and 1–2 capacity enclosures) should be installed above the full arrays.



   Lift the enclosure and slide it onto the rail ledges you previously installed.

2. Attach the front of the enclosure to the front vertical posts using two #10–32 x 3/4–inch trusshead screws on each side. Do not tighten the screws.
3. In the rear of the rack, align the enclosure side bracket arm holes with the holes in the rail. Install two #6-32 x 1/4 panhead screws.

   NOTE: You may need to remove the power supplies to install these screws.

4. Tighten all four screws.
5. Repeat this procedure to install up to two more capacity enclosure above the previous one.
6. At the top of the capacity enclosures, install the base enclosure.
7. Install the remaining base and capacity enclosures:
   - If you are installing four full arrays, continue installing three capacity enclosures beneath each base enclosure working up the rack.
   - If you are installing fewer than four full arrays, begin at rack position 17. Count down two rack positions for each available capacity enclosure and begin installing them at the lowest point. Then install the base enclosure at positions 17 and 18.

     Repeat this to add a third base enclosure, if available, at rack positions 25 and 26, and for a fourth base enclosure, if available, at positions 33 and 34.

     When you have completed the installation, you will have all full arrays at the bottom. A partial array will be at the top of the enclosures with empty space for the "missing" enclosures. This allows room to add capacity enclosures without needing to reinstall the existing enclosures.

Installing the Enclosure Power Cables

NOTE: When powering up (connecting the power cords) on a new array, power up the capacity enclosures before the base enclosure.

To connect enclosure power cables:

1. Locate the AC power cords.
2. Connect a black power cable to the left power supply of each enclosure, route the cables through the left side of the rack, and plug them into a PDM mounted on the left vertical post.
3. Connect a gray power cable to the right power supply of each enclosure, route the cables through the right side of the rack, and plug them into a PDM mounted on the right vertical post.

IMPORTANT: Equally distribute the current between the PDMs.

Cabling Base and Capacity Enclosures

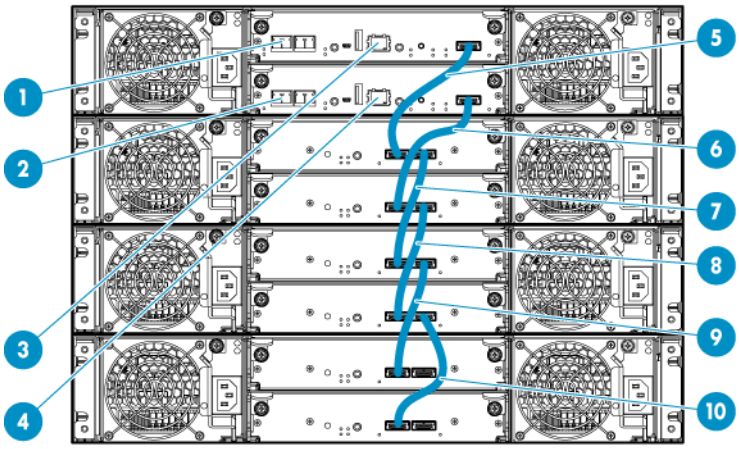


Table 1 Cabling the Base Enclosure

Item	Description	Connects to
1	FC port 1	Array 1 base enclosure: connects to port 9 of Fibre Channel switch #1 (FC SW1) via FC cable.
		Additional base enclosures: connects to the next available port on Fibre Channel switch #1 (FC SW1) via FC cable. Cable additional base enclosures to the switch ports in this order: 19, 8, 18, 7, 17, 6, 16.
2	FC port 1	Array 1 base enclosure: connects to port 9 of Fibre Channel switch #2 (FC SW2) via FC cable.
		Additional base enclosures: connects to the next available port on Fibre Channel switch #2 (FC SW2) via FC cable. Cable additional base enclosures to the switch ports in this order: 19, 8, 18, 7, 17, 6, 16.
3	Ethernet port	Array 1 base enclosure: connects to port 19 of Ethernet switch #2 (SW2).
		Additional base enclosures: connects to the next available port on Ethernet switch #2 (SW2) via Ethernet cable. Cable additional base enclosures to the switch ports in this order: 20, 17, 18, 15, 16, 13, 14.
4	Ethernet port	Array 1 base enclosure: connects to port 19 of Ethernet switch #1 (SW1).
		Additional base enclosures: connects to the next available port on Ethernet switch #1 (SW1) via Ethernet cable. Cable additional base enclosures to the switch ports in this order: 20, 17, 18, 15, 16, 13, 14.

If you are installing a single base enclosure, cable it to the Fibre Channel and Ethernet switches as indicated in Table 1 (page 27) and the installation is complete. Otherwise, continue to Table 2 (page 27) and the procedure that follows it.

Table 2 Cabling Capacity Enclosures

Item	Description	Connects to
5	SAS cable connected to SAS port 0 of RAID controller 1 of base enclosure	SAS port 0, input port, of capacity controller 1 of capacity enclosure 0
6	SAS cable connected to SAS port 0 of RAID controller 2 of base enclosure	SAS port 0, input port, of capacity controller 2 of capacity enclosure 0
7	SAS cable connected to SAS port 1, output port, of capacity controller 1 of capacity enclosure 0	SAS port 0, input port, of capacity controller 1 of capacity enclosure 1 (if available)
8	SAS cable connected to SAS port 1, output port, of capacity controller 2 of capacity enclosure 0	SAS port 0, input port, of capacity controller 2 of capacity enclosure 1 (if available)
9	SAS cable connected to SAS port 1, output port, of capacity controller 1 of capacity enclosure 1	SAS port 0, input port, of capacity controller 1 of capacity enclosure 2 (if available)
10	SAS cable connected to SAS port 1, output port, of capacity controller 2 of capacity enclosure 1	SAS port 0, input port, of capacity controller 2 of capacity enclosure 2 (if available)

NOTE: The base enclosure is on the top of the stack of capacity enclosures. From the top to the bottom they are: base enclosure, capacity enclosure 0, capacity enclosure 1, capacity enclosure 2. One base enclosure and three capacity enclosures make up an array.

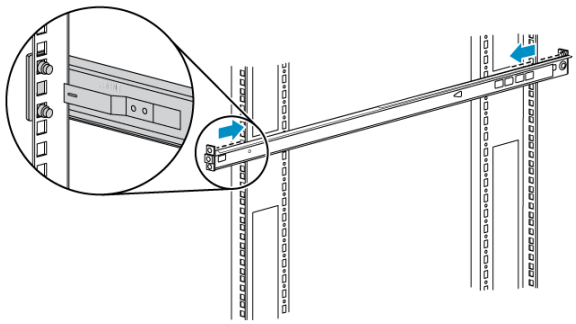
1. Locate the SAS cables included in the capacity enclosure kit contents.
2. Remove the tape and end caps from the SAS cables before installing.
3. Verify that both power cords are unplugged on each enclosure in the rack.
4. For each base enclosure, using the figure and table above, work downward to connect the base enclosure to up to three capacity enclosures.
5. Secure the SAS cables of the enclosures together with a Velcro® tie.

Installing the VLS Node into a Rack

NOTE: If you are installing the node into a telco rack, order the appropriate option kit at the RackSolutions.com web site: http://www.racksolutions.com/hp. Follow the instructions on the web site to install the rack brackets.

1. Locate the rail kit, part number 360332–003.
2. Install the two outer slide rails to the rack. The outer rails are marked "FRONT" and "REAR."

   On both sides of the rack, align the rail holes with the holes in the rack and secure with thumbscrews.

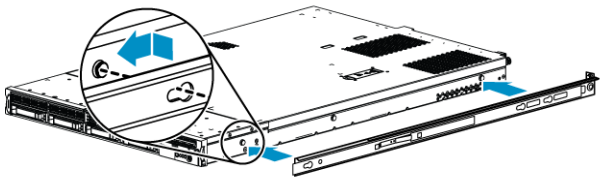


3. Attach the inner rails to the sides of the node.

   Align the holes in the rail with the round tabs on the side of the node and secure with thumbscrews.

   NOTE: The inner rails are identical.

   The word "FRONT" should face away from the node, but will appear upside-down on one side.



4. Align the rails on the node with the rails in the rack and slide the node fully into the rack.

   If your rack contains single phase PDUs, you will install the node in rack position 35. If your rack contains 3–phase PDUs, you will install the node in rack position 33.
5. Tighten the thumbscrews.
6. Repeat this procedure to install all of the nodes in the rack. See "NOTE" below for details.

NOTE: If your rack contains single phase PDUs:

- Install up to four nodes in the first rack starting in position 35 working up the rack.
- Install up to four nodes in the second rack starting in position 35 working up the rack.

If your rack contains 3–phase PDUs:

- Install up to six nodes in the first rack starting in position 33 working up the rack.
- Install up to two nodes in the second rack starting in position 33 working up the rack.

Cabling the Node

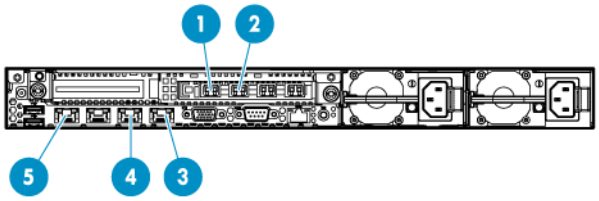


Table 3 Cabling the Node

Item	Description	Connects to
1	FC port 4	Primary node: connects to port 0 of Fibre Channel switch #2 in rack 1 (FC SW2) via FC cable.
		Secondary nodes: connects to the next available port on Fibre Channel switch #2 (FC SW2) via FC cable. Cable secondary nodes to the switch ports in this order: 10, 1, 11, 2, 12, 3, 13.
2	FC port 3	Primary node: connects to port 0 of Fibre Channel switch #1 in rack 1 (FC SW1) via FC cable.
		Secondary nodes: connects to the next available port on Fibre Channel switch #1 (FC SW1) via FC cable. Cable secondary nodes to the switch ports in this order: 10, 1, 11, 2, 12, 3, 13.
3	NIC 4	Primary node: connects to port 1 of Ethernet switch #2 (SW2) via Ethernet cable.
		Secondary nodes: connects to the next available port on Ethernet switch #2 (SW2) via Ethernet cable. Cable secondary nodes to the switch ports 2 through 8 in sequential order.
4	NIC 3	Primary node: connects to port 1 of Ethernet switch #1 (SW1) via Ethernet cable.
		Secondary nodes: connects to the next available port on Ethernet switch #1 (SW1) via Ethernet cable. Cable secondary nodes to the switch ports 2 through 8 in sequential order.
5	NIC 1	Primary node: connects to your system's external network via Ethernet cable.
		Secondary nodes: connects to your system's external network when using replication via Ethernet cable.

NOTE: Not all systems use all of the components listed in Table 3 (page 29).

The primary node, node 0, is on the bottom of the stack of nodes. From the bottom to the top they are: node 0, node 1, node 2, node 3. (The number of nodes will vary from system to system.)

1. Cable the primary node using Table 3 (page 29).
2. If you are installing more than one node, cable the nodes using Table 3 (page 29). Start at node 1 just above the primary node (node 0) and work your way up the rack.
3. Using Velcro®, secure the cables to the left side of the rack.
4. Install loopback plugs on the nodes in all unused Fibre Channel ports.

IMPORTANT: Do not touch the Fibre Channel cable tips.

Do not secure Fibre Channel cable with cable ties.

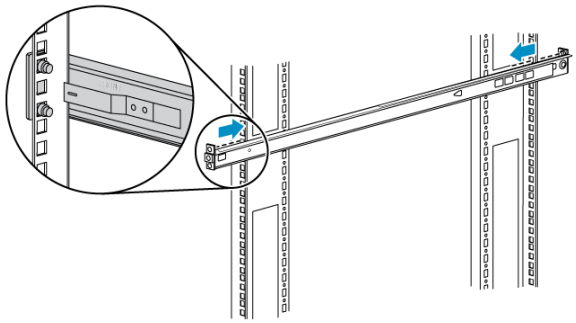
Installing the VLS High Performance Node into a Rack

NOTE: If you are installing the node into a telco rack, order the appropriate option kit at the RackSolutions.com web site: http://www.racksolutions.com/hp. Follow the instructions on the web site to install the rack brackets.

1. Locate the rail kit.
2. Install the two outer slide rails to the rack.

   If your rack contains single phase PDUs, you will install the node in rack positions 35 and 36. If your rack contains 3–phase PDUs, you will install the node in rack positions 33 and 34.

   On both sides of the rack, align the rail holes with the holes in the rack and secure with thumbscrews.



3. Attach the inner rails to the sides of the node.

   Align the holes in the rail with the round tabs on the side of the node and secure with thumbscrews.
4. Align the rails on the node with the rails in the rack and slide the node fully into the rack.
5. Tighten the thumbscrews.
6. Repeat this procedure to install all of the nodes in the rack. See "NOTE" (page 30) for details.

NOTE: If your rack contains single phase PDUs:

- Install up to two nodes in the first rack starting in positions 35 and 36 working up the rack.
- Install up to four nodes in the second rack starting in positions 35 and 36 working up the rack.
- Install up to two nodes in the third rack starting in positions 35 and 36 working up the rack.

If your rack contains 3–phase PDUs:

- Install up to three nodes in the first rack starting in positions 33 and 34 working up the rack.
- Install up to five nodes in the second rack starting in positions 33 and 34 working up the rack.

Cabling External Connections

NOTE: Ethernet port 1 (NIC 1), and Fibre Channel ports 1 and 2 on the nodes are only to be used for external connections.

On the nodes:

1. Connect one end of a Fibre Channel cable to Fibre Channel port 1 on the node. Connect the other end to your system's SAN.
2. Connect one end of a Fibre Channel cable to Fibre Channel port 2 on the node. Connect the other end to your system's SAN.

3. Connect one end of an Ethernet cable to NIC 1 on the primary node. Connect the other end to the external network.

If your configuration contains one connectivity kit, the VLS9200 hardware installation is complete. Continue installation by configuring the identities of each node and array. See the *HP 9200 Virtual Library System User Guide*.

If your configuration contains two connectivity kits, see the *HP 9000 Virtual Library System Interswitch Link Kit Installation Instructions* to install the XPAK transponders and cable the switches in racks 1 and 3.

Installing the Ethernet Switches 6600 into a Rack

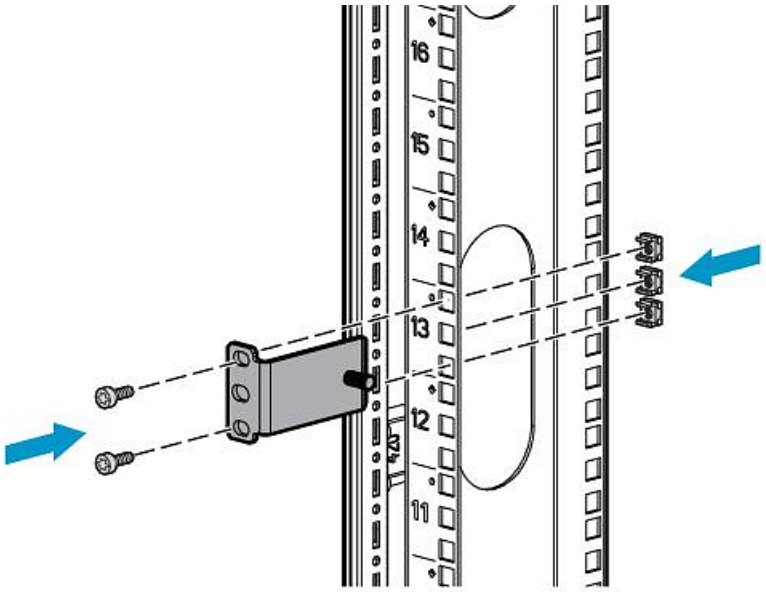
Installing the switch into the rack involves installing the rails in the rack, attaching the mounting brackets to the switch, and installing the switch into the rack. Install the switches immediately above the Fibre Channel switches previously installed.

1. Locate the following items and set them aside on a stable work surface:
   - Two Ethernet switches and two AC power cords
   - 1U rails, mounting brackets, and hardware to secure the rails to the rack
   - Screws to secure mounting brackets to the switch
2. Align the mounting holes at each end of a rail with the holes on the front and back rack posts so that they are at the same height.
3. For a square-hole rack, leave the pre-installed square-hole pin in each rail. Unscrew and re-install the 10-32 screw on each rail to secure it to the rack.

   For a round-hole rack, install the alternate round-hole pins that are shipped with the kit to set the rails in the rack. Install the alternate roundhole screws to secure the rails. (The round-hole screws have a different shoulder than the square-hole screws.)
4. Place a mounting bracket against one side of the switch. The bracket should be flush with the front (port side) of the switch.
5. Secure the bracket to the switch with four M4 8mm screws.
6. Perform these steps again to install the other mounting bracket on the other side of the switch.
7. Slide the switch onto the rails until the switch is fully inserted and the mounting hole in each bracket lines up with the mounting holes in the rack.
8. Connect each power cord to a power supply and secure the cord with a Velcro® strap. Route each cord through the rack.

Installing Cage Nuts and Rail Flanges

1. On the rack vertical posts, mark the holes (three on each front vertical post and two on each rear vertical post) that will be used by the rail flanges. Then, from the inside of each vertical post, insert a cage-nut into each marked hole.

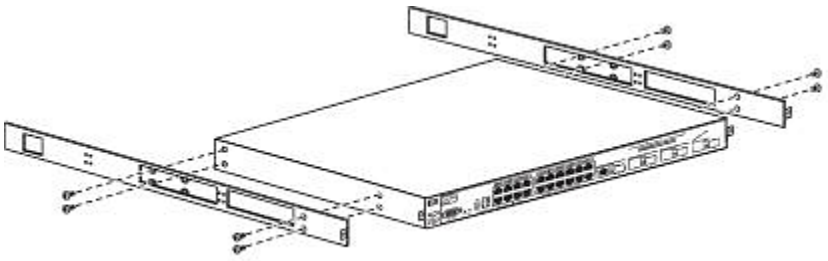


11749

2. From the front of the rack, secure the mounting flanges to the marked holes, using screws shipped with the rails.
3. Attach a washer and nut to the posts at the end of each mounting flange. Leave them loose and towards the open edge of the post.

Attaching Rails to the Ethernet Switch 6600-24G

1. Align the rail with the switch. The two holes at the front of the rail must align with the two holes at the front of the switch. The bracket end of the rail is towards the front of the switch.

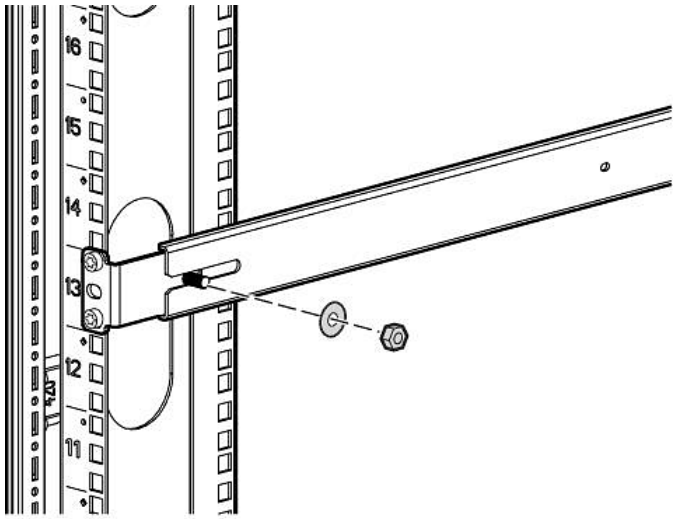


11193

2. Insert two of the pan-head screws through the rail and into the switch at the front of the switch. Tighten the screws.
3. Insert two of the pan-head screws through the appropriate holes in the rail and into the switch at the back of the switch. Tighten the screws.
4. Perform these steps again to install the other rail on the other side of the switch.

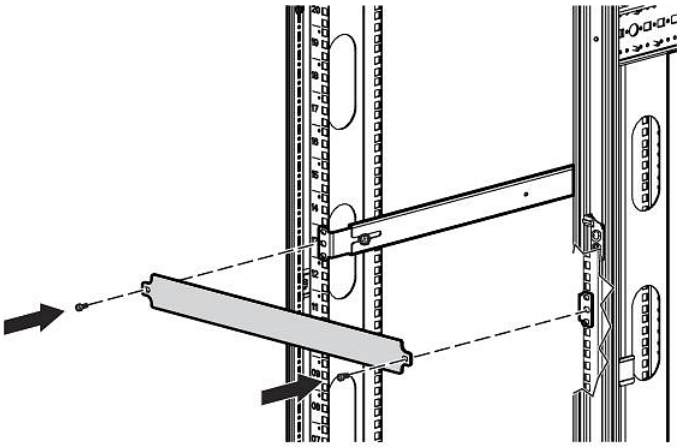
Mounting Ethernet Switch 6600-24G into the Rack

1. At rack position 39, from the back of the rack align the grooved ends of the switch rails with the posts on the mounting flanges. Placing the grooved ends between the mounting flange and the loose washer and nut provides guidance.



11756

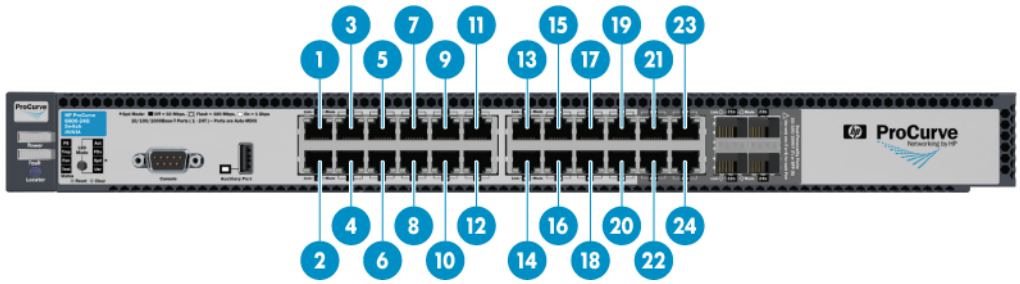
2. Slide the switch fully into the rack.
3. Tighten the washer and nut on both sides of the rack to secure the switch rails to the mounting flanges.
4. From the back of the rack, on each side of the switch, insert an M5 screw through the holes in the rail and into the holes in the rack.
5. Tighten the M5 screws to secure the switch to the rack.
6. Attach a power cable to the switch's power supply.
7. Plug the power cable into an AC power source.
8. Route the power cable through the left side of the rack and plug it into a PDM.
9. Attach a 1U cover plate to the front of the rack.



11752

10. Install the second Ethernet switch in rack position 40.

Cabling Ethernet Switches



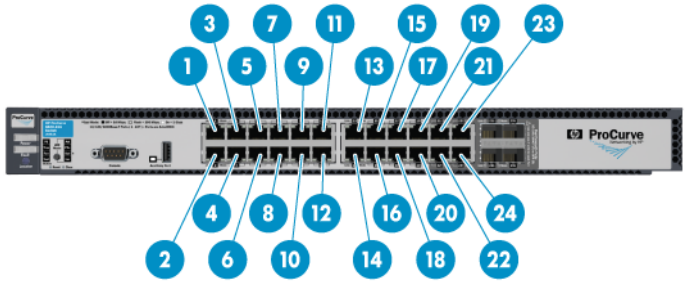


Table 4 Cabling Ethernet Switch #1 (SW1)

Item	Description	Connects to
1	Port 1	NIC 3 of primary node via Ethernet cable
2–8	Ports 2–8	NIC 3 of secondary nodes (if present) via Ethernet cable
9–18, 20	Ports 9–18, 20	Ethernet port of RAID controller 2 of additional base array enclosures (if present) via Ethernet cable
19	Port 19	Ethernet port of RAID controller 2 of first base array enclosures via Ethernet cable
21	Port 21	Port 21 of Ethernet switch #2 (SW2) in a second connectivity kit (if present) via Ethernet cable
22	Port 22	Port 22 of Ethernet switch #1 (SW1) in a second connectivity kit (if present) via Ethernet cable
23	Port 23	Ethernet port of FC switch #1 (FC SW1) via Ethernet cable
24	Port 24	Port 24 of Ethernet switch #2 via Ethernet cable

Table 5 Cabling Ethernet Switch #2 (SW2)

Item	Description	Connects to
1	Port 1	NIC 4 of primary node via Ethernet cable
2–8	Ports 2–8	NIC 4 of secondary nodes (if present) via Ethernet cable
9–18, 20	Ports 9–18, 20	Ethernet port of RAID controller 1 of additional base array enclosures (if present) via Ethernet cable
19	Port 19	Ethernet port of RAID controller 1 of first base array enclosures via Ethernet cable
21	Port 21	Port 21 of Ethernet switch #1 (SW1) in a second connectivity kit (if present) via Ethernet cable
22	Port 22	Port 22 of Ethernet switch #2 (SW2) in a second connectivity kit (if present) via Ethernet cable

Table 5 Cabling Ethernet Switch #2 (SW2) *(continued)*

Item	Description	Connects to
23	Port 23	Ethernet port of FC switch #2 (FC SW2) via Ethernet cable
24	Port 24	Port 24 of Ethernet switch #1 (SW1) via Ethernet cable

Table 6 Cabling Ethernet Switch #3, if present (SW1 of a second kit)

Item	Description	Connects to
17–20	Ports 17–20	Ethernet port of RAID Controller 2 of additional base array enclosures via Ethernet cable

Table 7 Cabling Ethernet Switch #4, if present (SW2 of a second kit)

Item	Description	Connects to
17–20	Ports 17–20	Ethernet port of RAID Controller 1 of additional base array enclosures via Ethernet cable

NOTE: Ethernet switch #1 is on the bottom and switch #2 is on the top. If present, Ethernet switch #3 is on the bottom and switch #4 is on the top.

1. Connect the Ethernet switches to each other and to the Fibre Channel switches using Table 4 (page 34) and Table 5 (page 34).
2. Connect the Ethernet switches to the nodes and base array enclosures if not already connected.

   If installing multiple arrays:

   a. Connect an Ethernet cable from Ethernet switch #1 to RAID controller 2 of additional arrays in order (array 1, array 2, etc.). Use the switch #1 ports in this order: 20, 17, 18, 15, 16, 13, 14.

   b. Connect an Ethernet cable from Ethernet switch #2 to RAID controller 1 of additional arrays in order (array 1, array 2, etc.). Use the switch #2 ports in this order: 20, 17, 18, 15, 16, 13, 14.

   NOTE: Each rack supports up to four arrays.

3. If installing a second connectivity kit in rack 4:

   a. Connect an Ethernet cable from Ethernet switch #3 to RAID controller 2 of additional arrays in order (array 13, array 14, etc.). Use the switch #3 ports in this order: 19, 20, 17, 18.

   b. Connect an Ethernet cable from Ethernet switch #4 to RAID controller 1 of additional arrays in order (array 13, array 14, etc.). Use the switch #4 ports in this order: 19, 20, 17, 18.

⚠ **WARNING!** Do not connect cables to unused ports on Ethernet switch #1 or #2. Doing so could result in data loss.

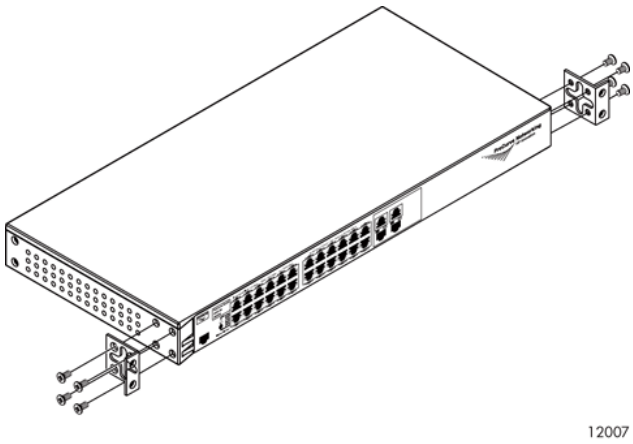
NOTE: Do not secure the Ethernet cables at this time. You will secure them with the Fibre Channel cables.

Installing the Ethernet Switch 2510–24 into a Rack

VLS9200 Entry-level systems use the Ethernet Switch 2510–24. No other switches are required.

NOTE: There are no rails associated with this switch.

1. If the metal mounting brackets are not attached to the switch, attach them as follows:
   a. Align the brackets so that the four screw holes are against the side of the switch. The side of the bracket with two screw holes extends from the switch and aligns with the front of the bezel.



   b. Adjust alignment so that the holes in the side of the mounting bracket line up with the holes in the switch.
   c. Use a Phillips (cross-head) screwdriver and the eight M4 screws (included) to attach the mounting brackets to the switch.
   d. Attach cap nuts to the vertical posts where the mounting brackets attach to the rack.
2. Immediately above the node, on each side of the switch secure the mounting bracket to the vertical posts with a Phillips screw.
3. Attach a power cable to the switch's power supply.
4. Plug the power cable into an AC power source.
5. Route the power cable through the right side of the rack and plug it into a PDM.
6. Attach a power cable to the switch's power supply.

Cabling Ethernet Switch 2510–24

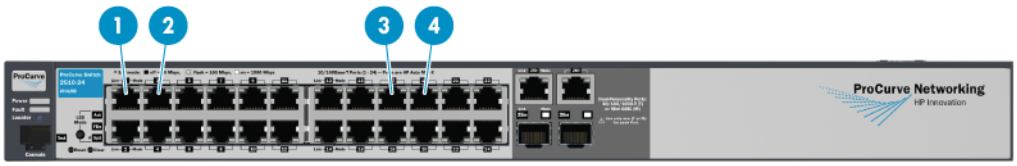


Table 8 Cabling the Ethernet Switch

Item	Description	Connects to
1	Port 1	NIC 3 of node via Ethernet cable
2	Port 2	NIC 4 of node via Ethernet cable
3	Port 15	Ethernet port of RAID controller 2 of base array enclosure via Ethernet cable
4	Port 16	Ethernet port of RAID controller 1 of base array enclosure via Ethernet cable

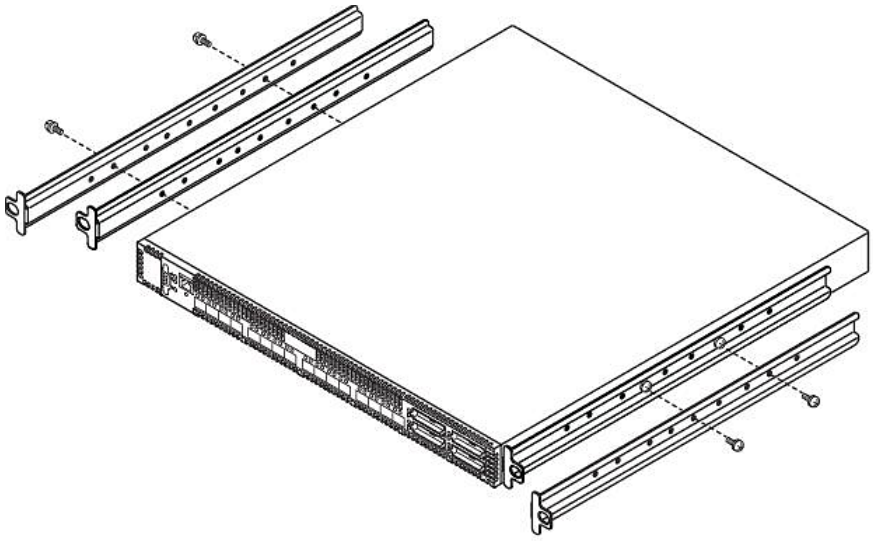
1. Connect the Ethernet switch to the node using Table 8 (page 36).
2. Connect the Ethernet switch to the base array enclosure working backwards from port 16 on the Ethernet switch.

3. Secure Ethernet cables with a Velcro® tie to the right side of the rack.

Installing the Fibre Channel Switches into a Rack

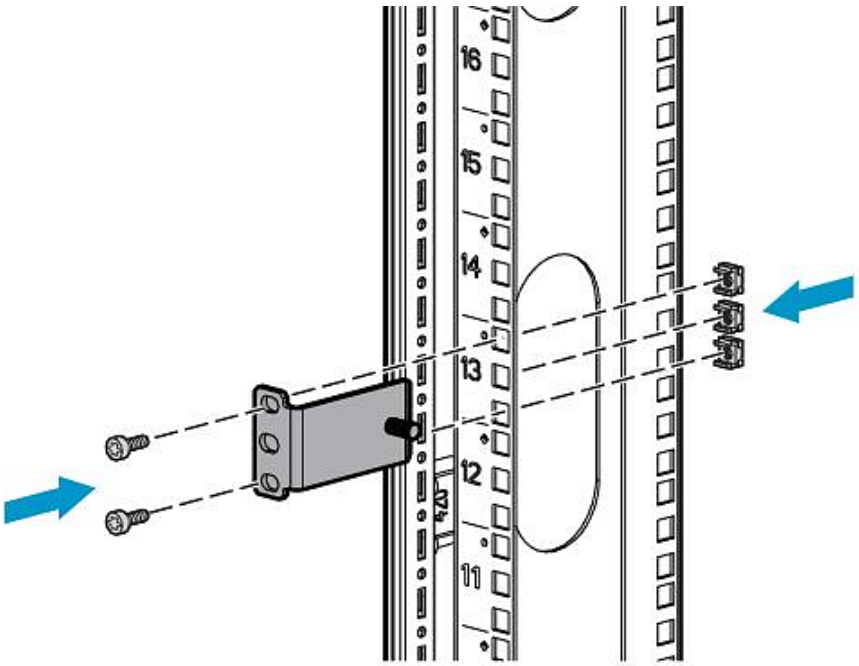
Installing the switches into the rack involves attaching rails to the Fibre Channel switches and then mounting them into the rack. Install the switches immediately above the nodes previously installed.

1. Locate the following items and set them aside on a stable work surface:
   - Two Fibre Channel switches and two AC power cords
   - 1U rails, adjustable mounting flanges, two 1U cover plates, and hardware to secure the rails to the rack
   - Screws to secure rails to the switch
2. Connect the two AC power cords to the two power supplies on the rear of both Fibre Channel switches.
3. Attach the rails to the sides of the switches, using screws provided.



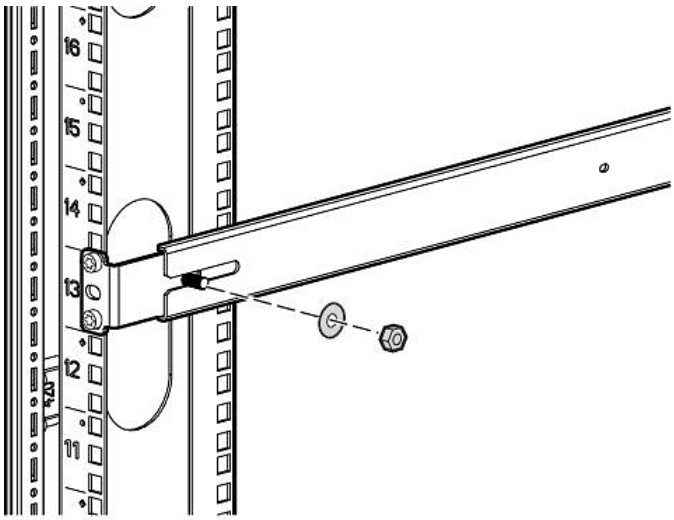
11753

4. On the rack vertical posts, mark the holes that will be used by the rail flanges (three on each front vertical post and two on each rear vertical post); the switch will be installed at rack position 41. Then, from the inside of each vertical post, insert a cage-nut into each marked hole.



11749

5. From the front of the rack, secure the adjustable mounting flanges to the marked holes, using screws shipped with the rails.
6. From the rear of the rack, slide the racking shelf assembly with Fibre Channel switch into the rack, sliding the rail ends onto the adjustable mounting flanges already installed in the front rack vertical posts.
7. When the rail flanges are flush with the rack vertical posts, secure them to the rack.



11756

8. Attach two 1U cover plates to the front of the rack.

   Attach one 1U cover plate in front of each Fibre Channel switch.
9. Plug the AC power cords into an AC power source.

   Route one cord to a PDM mounted on the right vertical post, and the other to a PDM on the left vertical post.
10. Repeat this procedure to install the second Fibre Channel switch in rack position 42.

Cabling Fibre Channel Switches

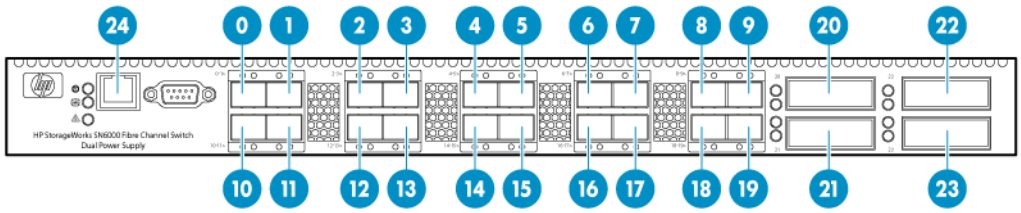


Table 9 Cabling Fibre Channel Switch #1 (FC SW1)

Item	Description	Connects to
0	Port 0	FC Port 3 of primary node via FC cable
1–3	Ports 1–3	FC Port 3 of secondary nodes (if present) via FC cable
4–8	Ports 4–8	Port 0 of RAID controller 1 of additional arrays (if present) via FC cable
9	Port 9	Port 0 of RAID controller 1 of first array via FC cable
10–13	Port 10–13	FC Port 3 of secondary nodes (if present) via FC cable
14–19	Ports 14–19	Port 0 of RAID controller 1 of additional arrays (if present) via FC cable
20–23	Ports 20–23	XPAK transponders from the interswitch link kit (if present)
24	Ethernet port	Port 23 of Ethernet Switch 1 (SW1) via Ethernet cable

Table 10 Cabling Fibre Channel Switch #2 (FC SW2)

Item	Description	Connects to
0	Port 0	FC Port 4 of primary node via FC cable
1–3	Ports 1–3	FC Port 3 of secondary nodes (if present) via FC cable
4–8	Ports 4–8	Port 0 of RAID controller 2 of additional arrays (if present) via FC cable
9	Port 9	Port 0 of RAID controller 2 of first array via FC cable
10–13	Ports 10–13	FC Port 4 of secondary nodes (if present) via FC cable
14–19	Ports 14–19	Port 0 of RAID controller 2 of additional arrays (if present) via FC cable
20–23	Ports 20–23	XPAK transponders from the interswitch link kit (if present)
24	Ethernet port	Port 23 of Ethernet Switch 2 (SW2) via Ethernet cable

Table 11 Cabling Fibre Channel Switch #3, if present (FC SW1 of a second kit)

Item	Description	Connects to
8–9	Ports 8–9	Port 0 of RAID controller 1 of additional arrays via FC cable
18–19	Ports 18–19	Port 0 of RAID controller 1 of additional arrays via FC cable

Table 12 Cabling Fibre Channel Switch #4, if present (FC SW2 of a second kit)

Item	Description	Connects to
8–9	Ports 8–9	Port 0 of RAID controller 2 of additional arrays via FC cable
18–19	Ports 18–19	Port 0 of RAID controller 2 of additional arrays via FC cable

NOTE: Fibre Channel switch #1 is on the bottom and switch #2 is on the top. If present, Fibre Channel switch #3 is on the bottom and switch #4 is on the top.

1. Connect the Fibre Channel switches to the nodes, base array enclosures, and Ethernet switches if not already connected using Table 9 (page 39) and Table 10 (page 39).
2. If you are installing more than one array:
   a. Connect a Fibre Channel cable from Fibre Channel switch #1 to port 0 of each additional RAID controller 1 (array 1, array 2, etc.) Use the switch #1 ports in this order: 19, 8, 18, 7, 17, 6, 16.
   b. Connect a Fibre Channel cable from Fibre Channel switch #2 to port 0 of each additional RAID controller 2 (array 1, array 2, etc.). Use the switch #2 ports in this order: 19, 8, 18, 7, 17, 6, 16.
3. If installing a second connectivity kit in rack 4:
   a. Connect a Fibre Channel cable from Fibre Channel switch #3 to port 0 of each additional RAID controller 1 (array 13, array 14, etc.) Use the switch #3 ports in this order: 9, 19, 8, 18.
   b. Connect a Fibre Channel cable from Fibre Channel switch #4 to port 0 of each additional RAID controller 2 (array 13, array 14, etc.). Use the switch #4 ports in this order: 9, 19, 8, 18.
4. Secure together the Fibre Channel cables installed in this procedure and the Ethernet cables installed previously with Velcro® ties. Route them to the right side of the rack.

Installing the VLS9000 Interswitch Link Kit

The following sections describe the procedures for configuring the Ethernet switches and installing the interswitch link kit.

Reconfiguring Ethernet Switches

Before cabling the interswitch kit, establish a CLI session with each Ethernet switch to ensure that Rapid Spanning Tree Protocol (RSTP) is enabled.

1. Locate a null-modem (serial) cable provided with the VLS.
2. Connect one end of the serial cable to a PC or workstation and the other to the serial port on the rear of an Ethernet switch in rack 1.
3. Establish a CLI session using a terminal emulation program, such as Windows Hyperterminal™.
4. At the prompt, select a baud rate between 9600 and 115200 with 8 data bits and no parity.
5. Press **Enter** twice to reach the command line, which reads `HP ProCurve Switch 6600-24G`.
6. Enter `show spanning-tree`. The screen displays the status of the spanning-tree protocol and the options set.

   This optional step serves as a check of the initial status before you make the change. If the status of the protocol is `Yes`, you may skip this procedure.
7. Enter `config`. The command line now reads `HP ProCurve Switch 6600-24G (config)#`.
8. Enter `spanning-tree force-version rstp-operation`.
9. Enter `spanning-tree`. This turns on the spanning-tree protocol as configured.
10. Enter `write memory`. This writes the changes to non-volatile flash memory.
11. Enter `show config`. Verify that the commands in Step 9 and Step 10 are present.
12. Enter `exit`.
13. Enter `exit`.
14. Enter `exit`.

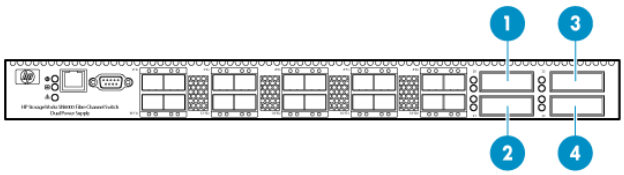
15. A prompt asks if you want to log out. Enter `y`.

    The switch logs off, and the spanning tree is now reconfigured to include the new switch.
16. Repeat this procedure for the remaining Ethernet switches in racks 1 and 3.

NOTE: After reconfiguring the Ethernet switches, power down the entire VLS system. See Powering Off the System for instructions.

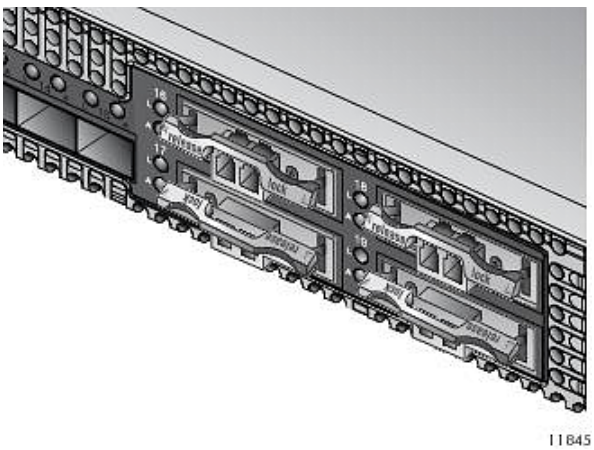
Installing XPAK Transponders

The XPAK transponders (XPAKs) plug into the 10 Gb Fibre Channel ports in the front of the 20–port Fibre Channel switches. The 20–port Fibre Channel switches are included in the 40–port connectivity kits.



Item	Description
1	Fibre Channel port 20
2	Fibre Channel port 21
3	Fibre Channel port 22
4	Fibre Channel port 23

1. Locate four XPAKs supplied in the interswitch link kit contents.
2. Remove the port covers from ports 16 through 19 on the 20–port Fibre Channel switches.
3. With the latch in the center position, slide the XPAK into the port until it clicks into place.



NOTE: Install XPAKs into ports 20 and 22 with the heat sink facing up. Install XPAKs into ports 21 and 23 with the heat sink facing down.

4. Move the latch to the locked position, as indicated on the latch.
5. Repeat steps 2 through 4 for each Fibre Channel switch with the remaining XPAKs.

Applying ISL Kit Labels

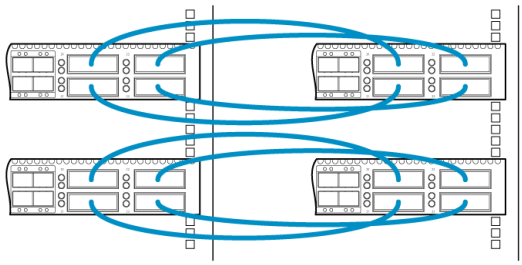
Locate the labels supplied in the interswitch link kit contents.

As you install each cable in the following sections, apply the appropriate label to each cable end.

NOTE: The labels for interlinking the switches use "A" to indicate rack 1 and "B" to indicate rack 3. For example, an Ethernet cable label will read, "SW6600–24A port 22 TO SW6600–24B port 22."

Installing Interswitch Fibre Channel Cables

1. Locate the Fibre Channel cables included in the interswitch link kit contents.
2. Remove the black cover from each XPAK.
3. Connect the Fibre Channel cables from the switches in rack 1 to the switches in rack 4.

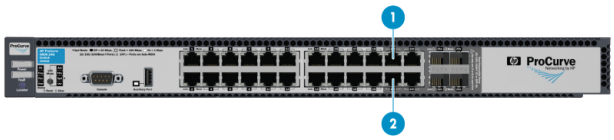


To identify individual ports in the image above, see Installing XPAK Transponders (page 41).

From Rack 1	To Rack 4
Switch 1 port 20	Switch 1 port 20
Switch 1 port 21	Switch 1 port 21
Switch 1 port 22	Switch 1 port 22
Switch 1 port 23	Switch 1 port 23
Switch 2 port 20	Switch 2 port 20
Switch 2 port 21	Switch 2 port 21
Switch 2 port 22	Switch 2 port 22
Switch 2 ort 23	Switch 2 port 23

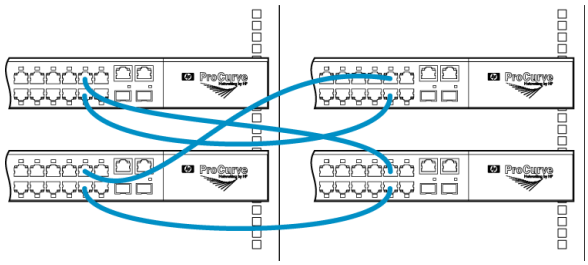
4. Secure Fibre Channel cables to one side of the rack with a Velcro® tie.

Installing Interswitch Ethernet Cables



Item	Description
1	Port 21
2	Port 22

1. Locate the Ethernet cables included in the interswitch link kit contents.
2. Connect the Ethernet cables from the switches in rack 1 to the switches in rack 4 as shown in the figure and table below.



From Rack 1	To Rack 4
Switch 0 port 22	Switch 0 port 22
Switch 1 port 22	Switch 1 port 22
Switch 0 port 21	Switch 1 port 21
Switch 1 port 21	Switch 0 port 21

3. Secure Ethernet cables to the right side of the rack using a Velcro® tie.

3 Multi-node Setup

This section explains how to configure the identities of each node after the nodes and other components of the system are installed and cabled.

NOTE: The Fibre Channel and Ethernet switches should be powered on before configuring the nodes.

NOTE: The VLS system can be configured remotely using iLO with virtual terminal or virtual media; see the iLO user guide for details.

Configuring the Primary Node 0

To configure the primary node:

1. Power on array 0. All other arrays should be powered off.
2. On the primary node, connect to the serial port or use the keyboard and mouse ports to connect to a console.
3. Power on the primary node. The node will now run cable checks and configuration checks.

   After several minutes, a menu will appear on your monitor asking whether the node is a primary (master, m) or secondary (slave, s) node.
4. Enter `m`. The node will then run cable checks and configuration checks.
5. After the checks are complete the node will reboot automatically. Wait for the primary node to fully boot.

   Rebooting is complete when you receive the "Initializing node#" and then "Initializing for node# completed." messages in the systems notifications (if you have DHCP enabled) of Command View VLS or when you see the login prompt on the terminal.
6. Set the IP address and other public network configurations on the VLS. Refer to Setting the Network Settings for instructions.

Configuring the Secondary Nodes

To configure each secondary node (nodes 1 through 5 or 7, depending on whether deduplication is enabled):

1. On the secondary node, connect to the serial port or use the keyboard and mouse ports to connect to a console.
2. Power on the primary node and all previously installed secondary nodes of the VLS.
3. Power on the secondary node being added to the VLS.

   The node will then run cable checks and configuration checks.

   After several minutes, a menu will appear on your monitor asking whether the node is a primary (master, m) or secondary (slave, s) node.
4. Enter `s`.
5. At the prompt, enter the node number (next sequential node number), and the node will then automatically reboot.

   NOTE: Node numbering must be sequential with no gaps. Gaps in ID numbering will prevent the VLS from recognizing any nodes with an ID after the gap. For example, if node numbering is 0, 1, 2, 4, the VLS will not recognize node 4.

   After the reboot, the VLS will automatically recognize and add the node.
6. Repeat this procedure for each secondary node in the system.

4 Storage Configuration

This section describes how to configure the storage pool policy and add or remove storage as needed after the nodes have been configured.

Managing VLS Capacity

There are several ways to manage the capacity of your system:

- Increase the number of VLS nodes
- Increase the number of VLS capacity enclosures. See Adding VLS Capacity.
- Reduce the number of VLS disk array enclosures. See Removing VLS Capacity.
- Create storage pools. See Configuring the Storage Pool Policy.

Adding VLS Capacity

Add capacity by increasing the number of VLS9200 capacity enclosures in your VLS system. New to the VLS family is the ability to purchase individual capacity enclosures instead of purchasing a capacity kit containing an array. (An array contains one base enclosure and three capacity enclosures.)

Each base enclosure can support three capacity enclosures so purchase accordingly. For example, if you have a base enclosure and one capacity enclosure, purchase 1–2 capacity enclosures. If you have a base enclosure and two capacity enclosures, purchase one additional capacity enclosure; for more capacity, purchase another base enclosure and up to three more capacity enclosures.

Each VLS9200 node can support up to two arrays. If you intend to add base and capacity enclosures that exceed that limit, purchase an additional node.

NOTE: The VLS sequentially numbers arrays as they are added, starting with Array 1. (Array numbering previously began at 0. Starting at array 1 is new to VLS firmware 6.1.0.) Only add one VLS array at a time so you can control the number assigned to each array.

NOTE: The Fibre Channel and Ethernet switches should be powered on before adding storage capacity.

To add a VLS9200 disk array enclosure:

1. Install the capacity licenses. See "Installing Additional Licenses" (page 48).

   Each base and capacity enclosure comes with its own capacity licenses (10 TB enclosures require one license while 20 TB enclosures require two).

   CAUTION: If a base or capacity enclosure is added to a VLS system without sufficient capacity licenses installed, a capacity license violation will occur.

   If the capacity license violation is detected during boot, this will disable the VLS storage capacity, so that the VLS is unable to perform for read/write operations. VLS storage capacity is re-enabled once the capacity license is installed on the VLS (without needing to reboot).

   If the capacity license violation is detected when Discover Unconfigured Storage is selected, this will prevent the new disk array enclosure from being added to the VLS. However, the VLS will remain operational. When the capacity license is then installed, the new disk array enclosure is automatically added to the VLS (without needing to reboot).

2. Install the base or capacity enclosure into the rack. See "Installing the Disk Array Enclosures into a Rack" (page 22).
3. Cable the enclosure to the VLS. See "Cabling Disk Array Enclosures" (page 26).

4. Power on the enclosure. See Powering on VLS Arrays (page 91).
5. Add the new disk array storage to the VLS using Command View VLS:
   a. Select the **System** tab.
   b. In the navigation tree, select **Storage LUNs**.
   c. Select **Discover Unconfigured Storage** from the task bar.

      The VLS locates the new array or capacity enclosure and the screen displays the LUN capacity that will be added to the storage pools, based on the storage pool policy, as a result of the new enclosure.

      NOTE: If the screen displays "0 storage LUN(s) discovered," check the notifications. You may have a problem that prevented the array from being configured or a license violation that prevented the array from being added.

   d. Click **Run Pool Policy**. The VLS adds the new LUNs to the storage pools.

      If you opt to cancel instead, you can return later and add the new storage to the storage pools using the Run Pool Policy task (see "Adding New Arrays to the Storage Pool" (page 48)).
   e. Click **Return** to return to the Storage LUNs screen.

Removing VLS Capacity

Remove capacity by decreasing the number of VLS disk array enclosures installed in your VLS system. At a minimum, one disk array enclosure must be installed for every node.

Removing disk array enclosures from the system destroys all current virtual tapes in the system. Once disk array enclosures are added to the VLS, the only way they can be removed from the a VLS storage pool is using the following procedure:

1. Power off the nodes.
2. Remove the disk array enclosures.
3. Power on the nodes.
4. Run the Rebuild All Storage Pools operation (see Rebuilding all Storage Pools).

This deletes the disk array enclosures from the configuration and reformats the remaining disk array enclosures into working capacity.

Configuring the Storage Pool Policy

VLS automatically creates storage pools on the VLS arrays in the system based on your storage pool policy. Storage pools are defined in terms of whole arrays (one base enclosure and three capacity enclosures). Use the Storage Pool Policy Wizard to set the storage pool width across the arrays in the system.

To set the storage pool policy from Command View VLS:

1. Select the **System** tab.
2. Select **Storage Pools** in the navigation tree.
3. From the task bar, select **Edit Policy**. The **Storage Pool Policy Wizard** screen is displayed.
4. Select the number of arrays wide in the Number of Arrays Wide field. You can select "All" for one storage pool across all arrays, or select 1–8 for that many arrays per storage pool.

   Only the Number of Arrays Wide default value can be changed.
5. Click **Next**.
6. Click **Next** to confirm.

   If the existing storage pools do not fit into the new storage pool policy selected, a dialog box will ask if you want to erase the existing storage pools to create the new policy. Select **Yes** to rebuild all storage pools or **No** to cancel the change. See Rebuilding all Storage Pools.

7. Click **Finish**.

Viewing the Storage Pool

To view the storage pool information from Command View VLS:

1. Select the **System** tab.
2. Expand **Storage Pools** in the navigation tree.
3. Select the storage pool of interest in the navigation tree. The storage pool details window opens.

Rebuilding all Storage Pools

To delete all information on the VLS9200 arrays and reformat them, perform a Rebuild All Storage Pools from Command View VLS.

△ **CAUTION:** Rebuild All Storage Pools destroys all current virtual tape cartridges in the system.

To rebuild all storage pools from Command View VLS:

1. Select the **System** tab.
2. Select **Storage Pools** in the navigation tree.
3. Select **Rebuild All Storage Pools** from the task bar.
4. Select **Rebuild**, or, if your system has deduplication enabled, select **Restart Emulations in Maintenance Mode** from the task bar.

   Systems with deduplication enabled must enter Maintenance Mode before rebuilding the storage pools. Maintenance Mode reboots the system with deduplication disabled and the front fibre ports down.
5. If your system has deduplication enabled, wait until the system has completed rebooting into Maintenance Mode, then follow steps 1 through 3. The system will reboot again; when the system is back up, deduplication is enabled and the front fibre ports are back up.

Rebuilding a Single Storage Pool

To delete all information on the VLS9200 arrays for one specific storage pool and reformat them, perform a Rebuild Storage Pool from Command View VLS.

△ **CAUTION:** Selecting Rebuild Storage Pool destroys all current virtual tape cartridges in that storage pool.

To rebuild a storage pool from Command View VLS:

1. Select the **System** tab.
2. Select **Storage Pools** in the navigation tree.
3. Select the specific storage pool you want to rebuild.
4. Select **Rebuild Storage Pool** from the task bar.
5. Click **Rebuild**, or, if your system has deduplication enabled, select **Restart Emulations in Maintenance Mode** from the task bar.

   Systems with deduplication enabled must enter Maintenance Mode before rebuilding the storage pools. Maintenance Mode reboots the system with deduplication disabled and the front fibre ports down.

△ **CAUTION:** Do not resume backup operations until the rebuilt arrays have finished initializing (can take up to 24 hours). View the “Disk Array x” details page on the Systems tab of Command View VLS to view the array state. The disk array is still initializing when the array state is “Initializing.”

Adding New Arrays to the Storage Pool

If you add a new array or disk array enclosure and run the Discover Unconfigured Storage task (see "Adding VLS Capacity" (page 45)) but cancel the process without adding the LUN capacity, you can resume the process later.

1. Select the **System** tab.
2. Select **Storage Pools** in the navigation tree.
3. On the Storage Pools screen, select **Run Pool Policy** from the task bar. (The task is only available if you previously used the Discover Unconfigured Storage task, or if you added storage and then rebooted the entire VLS system.)

   The VLS locates the new array or disk array enclosure and the screen displays the LUN capacity that will be added to the storage pools, based on the storage pool policy, as a result of the new storage.
4. Click **Accept** to continue. The VLS adds the new storage to the storage pools.
5. Click **Return** to return to the Storage Pools screen.

Installing Additional Licenses

Your VLS system may require any of the following licenses:

- Capacity:

  A VLS capacity license must be installed on the VLS when you add additional disk array enclosures. Each enclosure, whether a base or capacity enclosure, comes with its own capacity license. (This is new for the VLS9200. Previously, the node and the capacity bundle each came with a base license that covered an array.)

  If you are in a license violation state, all VLS read/write operations are disabled until either sufficient licenses are installed to support the storage, or the excess storage is removed. When you have cleared a license violation by installing an upgrade capacity license, the VLS read/write operations are automatically enabled without requiring a reboot.

  The base license on the node enables the storage that is part of the base SKU. The capacity bundle includes the capacity license and the registration materials necessary for installing capacity licenses.

  NOTE: Do not discard the registration materials included in the capacity bundle.

- Deduplication:

  A VLS deduplication license must be installed on the VLS before you can use the deduplication feature. The number of deduplication licenses must match or exceed the number of capacity licenses installed. After you install the deduplication licenses, the VLS system automatically enables the deduplication feature for all supported backup types.

- Replication:

  A VLS replication license must be installed on the VLS before you can use deduplication-enabled replication. Without the license, you may replicate whole backups across the LAN/WAN. However, you need the replication license to replicate backups that have been deduplicated. Deduplication-enabled replication requires one license per node on the target site.

- Secure Erasure:

  When you delete a cartridge, this feature overwrites deleted cartridge data with a specific data pattern so the data cannot be recovered. This is comparable to tape shredding of physical tapes. This only applies to firmware version 6.0 and higher.

- iLO 2 Advanced

  VLS nodes are shipped with the HP Integrated Lights-Out (iLO) Standard feature for remote management. However, you need a license to use the iLO 2 Advanced features including Virtual Media and Remote Console.

Follow these steps to install the licenses described above:

1. Use Command View VLS to obtain the VLS system serial number from the **Identity** tab.
2. Locate the paper or email entitlement certificate for the licenses you purchased. (You selected the delivery method during the ordering process.)

   HP recommends purchasing electronic certificates over physical certificates for faster delivery and the convenience of not having to manage (either file away or throw away) confidential paper certificates.
3. Log on to http://www.webware.hp.com.
4. Select **Generate Licenses**.
5. Sign in. If you are a new user, follow the onscreen instructions.
6. Enter the order number from the entitlement certificate.
7. Enter the VLS serial number. You will receive a license key immediately onscreen and via email.
8. Copy the license key.
9. In Command View VLS, select the **System** tab.
10. Select **Chassis** on the navigation tree.
11. Select **Licensing** from the task bar.

    The **Manage Upgrade Licenses** screen displays all of the existing licenses.
12. Select **Add License**.
13. In the empty field that displays, paste the license key.
14. Select **OK**.

    The screen returns to the **Manage Upgrade Licenses** list and includes the newly installed licenses.

NOTE: When installing deduplication or Secure Erasure licenses, the VLS system will automatically reboot. This may take a few minutes to begin; when it does, you will see a message on the **Notifications** tab.

5 Automigration/Replication

Instead of the preferred method of copying virtual media to physical media via the backup application, another option is to perform transparent tape migration via the VLS device using *automigration*. Automigration describes the feature in which the Virtual Library System acts as a tape copy engine that transfers data from virtual cartridges on disk to a physical tape library connected to the VLS device. The VLS automigration feature uses *Echo copy*, which automatically synchronizes the physical cartridges to matching virtual cartridges (with the same barcodes) based on user-defined policies and is totally transparent to the backup application.

You can also copy virtual media using *replication*. Replication provides automigration from the source VLS across the LAN/WAN to a remote virtual destination library. See Replication Concepts (page 51).

This section describes automigration topics from overall automigration concepts to specific operations you can perform on your system.

NOTE: Throughout the automigration windows, a *SAN library* refers to a destination library that is connected to the source library through the SAN and uses the automigration feature. A *LAN/WAN library* refers to a remote destination library that is connected to the source through the LAN/WAN and uses the replication feature.

NOTE: When a list of slots is displayed, the message, "[#] items found, displaying 1 to 20." appears. If there are more than 20 items found, scroll through them using the arrows pointing right and left at the far right-hand side at the top of the list. Also, in some cases, only available slots or only slots containing tapes appear in the list.

NOTE: For each procedure described in this chapter, at least one means of access to the relevant screen or menu is specified. However, links are often provided in the main window that can be used as a shortcut to other windows or menus.

Understanding Automigration Concepts

Before using automigration, review the information in this section. This will allow you to create copy pools and automigration policies appropriate to meet your storage needs.

Echo Copy Concepts

Echo copy acts as a transparent disk cache to the physical library, so that the backup application writes to virtual cartridges in the virtual library. Automigration then automatically schedules the copies from virtual cartridges to physical cartridges with matching barcodes, based on the automigration policies the user establishes.

Echo copy is managed through the automigration software, not the backup application. For that reason:

- The destination library is not visible to the backup application, so it does not need licensing.
- Copy traffic is no longer routed through the SAN.
- All destination tapes created by echo copy are in the native tape format, so they can be restored directly from any tape drive or library that is visible to the backup application.

When determining whether to use echo copy pools, remember:

- The backup application will not be aware of any copy failures.
- Any mistakes in destination library media management will also affect the virtual cartridges. For example, if new tapes are not loaded into the destination library, the physical copy will not exist.

- The destination library can only be used for copy operations.
- Echo copy is a full tape copy, rather than an incremental change copy, so it can be an inefficient use of media if you are using non-appending copy pools in your backup jobs.

An echo copy pool is used to define which destination library slots are to be echoed into a specified virtual library. Automigration then monitors the echo copy pool slots to detect cartridge loads/ejects in the destination library, and automatically synchronizes the virtual cartridges to the destination cartridges, creating the matching virtual cartridges as needed.

This means that when new destination tapes are loaded, automigration will automatically scan them (read the backup application headers) and then automatically create matching virtual cartridges in the virtual library specified for that echo copy pool.

NOTE: The automatic scanning of new cartridges can take a long time if all the tape drives in the destination library are busy with higher priority operations such as copies. Therefore, it is best to load new tapes when copies are not running.

Data written to echoed virtual cartridges will be automatically copied onto matching destination tapes based on the echo copy policy. An echo copy policy defines for each source virtual library the copy window (start and end times), the copy on eject option, and the time in days for expiration after eject. If destination tapes are ejected, the matching virtual tapes are automatically moved to the firesafe and are deleted at the policy-defined expiration time. This ensures the device does not fill up its disk space with older cartridges. See Creating an Echo Copy Pool (page 56) to create a policy. If virtual tapes are ejected by a backup application, the matching destination tapes are also automatically ejected into the destination library mailslot when the copy operation is complete. When an echo copy is ejected (mailslot eject box is checked), the echo copy is performed, then the eject is carried out. This results in the echo copy being placed in the device's firesafe and maintained according to the established policy. If a destination tape was ejected while a copy was pending, then notifications in the VLS GUI will inform the user that they have interrupted the copy process.

Replication Concepts

Replication provides automigration via LAN/WAN between two VLS devices. Because replication is a feature of automigration and uses the same Echo Copy policies that allow flexible cartridge/slot based configuration, any number of different replication configurations can be supported. You establish a replication policy and echo copy pools using Command View VLS in the same way you set up automigration with a destination library on the SAN.

During replication, the source VLS copies data to the echo copy pools on a replication library that is on the source. During the user-defined availability window, this replication library migrates data to the destination library, known as the LAN/WAN replication target.

The following are two of many possible replication configurations:

- Data center to data center

  Designate one VLS as the source and a second VLS as the destination. Configure the destination VLS to present a LAN/WAN replication target that is visible to the source VLS. The source VLS performs normal backups during the regular backup window, and during the availability window the source virtual cartridges automatically migrate to matching virtual cartridges on the destination VLS. The same configuration is also used in the other direction so there is a backup library and a LAN/WAN replication target library on both devices.

- Branch office to a main data center

  Divide a single destination target into multiple slot ranges to allow a many-to-one configuration without needing a separate replication library for each branch office. In this way, the VLS replication can scale to hundreds of branch offices all replicating to a single large device.

Replication can be configured to operate in one of two modes:

- *Deduplication-enabled replication*, known simply as replication — the virtual cartridge on the source VLS is deduplicated against the virtual cartridge on the target VLS. In this manner, only data that has changed is transmitted over the network to the target VLS. This mode requires that deduplication is licensed and enabled on both the source and the target VLS.
- *Whole cartridge replication* — the entire virtual cartridge is copied from the source VLS to the target VLS.

NOTE: All of the information on automigration also applies to replication except where specifically dealing with physical tapes (e.g., ejecting media) and where noted. Otherwise, where the information refers to physical cartridges, for replication assume virtual cartridges instead.

NOTE: Replication is deduplication-enabled if you have purchased the appropriate replication and deduplication licenses, and your backup ISVs and data types are supported for deduplication. Check the *Accelerated deduplication ISV support matrix* at http://www.hp.com/go/ebs/ to see if your system supports deduplication.

Tape Initialization

When you first configure deduplication-enabled replication on your VLS and set up an echo copy pool to a LAN/WAN destination, the first round of data migration is not deduplicated because there is not yet a set of backups on the target VLS to deduplicate against. Because the first full set of backups can be very large, the VLS system includes a tape initialization process. You can transport the first full set of backups to the target VLS using physical tapes rather than the network. This tape initialization process is optional and must be enabled by the administrator when creating the echo copy pool.

The tape initialization process works, very generally, like this:

1. Set up the LAN/WAN replication target on the remote site
2. Set up an echo copy pool on the source site
3. Run a standard deduplication backup on the source site
4. Export the full backup to physical tapes
5. Transfer the physical tapes to the remote site
6. Import data from the tapes onto the remote LAN/WAN replication target

Once the tape initialization process is complete, the automatic migration of deduplicated data from the source site to the target site over the LAN/WAN begins. See Exporting Data to Physical tapes for Tape Initialization (page 74) and Importing Data from Physical Tapes for Tape Initialization (page 75) for the specific procedures.

Connecting a Destination Library

Automigration requires one or more dedicated destination libraries to be connected to the VLS device.

Supported Destination Library Configurations

Automigration is supported on:

- HP MSL series tape libraries
- HP EML series tape libraries or library partitions
- HP ESL E-series tape libraries or library partitions
- HP ESL G3 tape libraries or library partitions
- HP VLS virtual libraries

Using automigration, you can share a single destination library across multiple virtual libraries (maximum of 20 drives on the physical libraries), or configure multiple destination libraries to be used in a single virtual library.

△ **CAUTION:** Automigration only supports destination libraries that have homogeneous drive types; for example, all drives are LTO-2. A mixture of drive types in the destination library, such as LTO-3 and LTO-2, is not supported.

NOTE: Automigration allows you to use a VLS as a destination library. Because of this feature, it can also be used as a device-to-device local replication scheme.

Connecting a Destination Library to a VLS9000

To connect the destination library to the VLS9000:

1. Connect your destination library to the VLS by connecting the library to the Fibre Channel switches in the VLS connectivity kit.
2. Reboot the VLS. Upon reboot, the device detects the newly connected destination library.

Managing and Unmanaging a Destination Library

To manage a library is to enable automigration by connecting the source library to a destination library that is already on the VLS. Until you manage the destination library, it cannot communicate with the source. The process for managing destination libraries is different for SAN libraries than for LAN/WAN libraries. See Managing a SAN Library (page 53) or Managing a LAN/WAN Replication Library (page 53).

An unmanaged library is a library that is not recognized by and using automigration or replication. The process for unmanaging destination libraries is the same for both SAN and LAN/WAN libraries. See Unmanaging a SAN or LAN/WAN Library (page 54).

Managing a SAN Library

To manage a SAN library:

1. Open the **Automigration/Replication** tab.
2. From the task bar, select **Manage SAN Automigration Library**.

   The screen displays all eligible libraries. Libraries that appear on the list but are greyed out either have no drives or have multiple drive types and therefore cannot be managed. Also, if there are no unmanaged drives, the system will return the message, "There are no unmanaged libraries."
3. If the library you wish to manage is not already selected, select it now.

   NOTE: You can only select one library to manage at a time. To manage additional libraries, repeat the procedure for each library to add.
4. Select **Submit**.

   The **Destination Library Details** screen displays, with the message, "The library, [library name], was managed successfully."

You can now create pools for the library and manage your data on the library using automigration.

You can also unmanage the library at any time. See Unmanaging a SAN or LAN/WAN Library (page 54) for instructions.

Managing a LAN/WAN Replication Library

To manage a LAN/WAN replication target:

1. Select the **Automigration/Replication** tab.

   The **Summary for All Managed Destination Libraries** screen displays.
2. Select **Manage LAN/WAN Replication Library** from the task bar.
3. Enter the name or IP address of the host containing the LAN/WAN replication target you just created.
4. Select **Submit**.
5. On the next screen, select the LAN/WAN replication target to manage.
6. Enter the password you created for that target.
7. Select **Submit**.

   The LAN/WAN replication target is now associated with the source.

You must re-manage a LAN/WAN replication target if you change the password for security reasons; see "Re-managing a LAN/WAN Replication Library" (page 54).

You can now create pools for the library and manage your data on the library using replication.

You can also unmanage the library at any time. See Unmanaging a SAN or LAN/WAN Library (page 54) for instructions.

Re-managing a LAN/WAN Replication Library

You must re-manage a LAN/WAN replication target if you change the password for security reasons. To re-manage a LAN/WAN replication target:

1. Select the **Automigration/Replication** tab.
2. Expand **Destination Libraries** in the navigation tree.
3. Select the library of interest to open the **Destination Library Details** screen.
4. From the task bar, select **Re-manage LAN/WAN Replication Target**.
5. Enter the host name of the LAN/WAN replication target *only if* the LAN/WAN replication target's host name has changed.
6. Enter the LAN/WAN replication target password.
7. Select **Submit**.

   The LAN/WAN replication target is now re-managed with the source using the new password.

You can now create pools for the library and manage your data on the library using replication.

You can also unmanage the library at any time. See Unmanaging a SAN or LAN/WAN Library (page 54) for instructions.

Unmanaging a SAN or LAN/WAN Library

Use one of the following two ways to unmanage a library:

Unmanage a library from the **Destination Library Details** window.

1. From the navigation tree, select the specific library to unmanage.

   NOTE: You can only select one library to unmanage at a time. To unmanage additional libraries, repeat the procedure for each library to unmanage.
2. Select **Unmanage** from the task bar.
3. Select **OK** from the dialog box.

   The **Destination Libraries** window displays and provides the message, "The library, [library name], was unmanaged successfully."

Unmanage the library from the **Destination Libraries** window.

1. Select **Destination Libraries** from the navigation tree.

2. From the task bar, select **Unmanage Library**.

   The **Unmanage Destination Library** screen displays, showing all managed libraries. If there are no managed libraries, the system will return the message: "There are no managed libraries".

3. If the library you wish to unmanage is not already selected, select it now.

   NOTE: You can only select one library to unmanage at a time. To unmanage additional libraries, repeat the procedure for each library to unmanage.

4. Select **Submit**.

   The **Destination Library Details** screen displays, with the message, "The library, [library name], was unmanaged successfully."

Echo Copy Pool Operations

Echo copy acts as a transparent disk cache to the physical library, so that the backup application writes to virtual cartridges in the virtual library. Automigration then automatically schedules the copies from virtual cartridges to their matching physical cartridges (with the same barcodes) based on the automigration policies.

For creating echo copies, automigration supports the following backup software on the physical libraries:

- CA ARCserve Backup
- Commvault Galaxy
- HP DataProtector
- HP DataProtector Express
- Legato Networker
- Tivoli Storage Manager
- Veritas Net Backup
- Veritas Backup Exec

△ **CAUTION:** Automigration does not support tar formatting. A tar file will not load if the first file on the tape is larger than 1 MB unless you perform a Load for Restore. HP strongly recommends against using automigration with tar-based backup software.

After connecting your destination library to the VLS and adding it as a Managed Library, follow these steps to operate echo copy:

1. Identify the Virtual Library you will associate with this managed library.
2. Create an echo copy pool between the virtual library and this managed library.

   Any cartridges loaded (or already present) in the managed library will be automatically detected, and matching virtual cartridges will be automatically created in the associated virtual library.

   NOTE: The automatic scanning of new cartridges can take a long time if all the tape drives in the destination library are busy with higher priority operations such as copies. For this reason, it is best to load new tapes when copies are not running.

3. Check for the auto-created virtual cartridges in the virtual library. On the **Automigration/Replication** tab, expand **Source Cartridges** in the navigation tree and then select the library of interest. The screen displays the cartridges created by automigration.
4. Any data written to the automigration virtual cartridges will be automatically mirrored onto the matching destination tapes based on the automigration policy settings. Monitor the status

of the mirror by using a Command View VLS Console and viewing the destination tapes in **Slots** in the expanded list under **Destination Library**.

5. In order to restore from a destination cartridge, either load it into a physical drive that is visible to the backup application, or perform a Load for Restore. Load for Restore copies the destination tape back into the virtual cartridge so that the backup application can then restore from the virtual cartridge.

Creating an Echo Copy Pool

Echo copy pools are created from physical library slots after a destination tape library is added to the VLS automigration configuration. Each echo copy pool defines:

- The single destination library
- The single source virtual library
- The slot range
- The echo copy pool policy

Each virtual library has a SAN policy, and those used as a replication library will also have a LAN/WAN policy. These policies are set up during the creation procedure.

To create an echo copy pool:

1. On the **Automigration/Replication** tab, expand **Destination Libraries** on the navigation tree so that you can see all the related items.
2. Expand the destination library for which you want to create a pool.
3. Select **Copy Pools** on the navigation tree.
4. From the task bar, select **Create Echo Copy Pool**.

   The **CREATE ECHO COPY POOL** screen displays.
5. Enter a start slot number and an end slot number for the copy pool from within the available slot range shown.
6. Select the local library where your echoed virtual cartridges will be placed from the Local Library list.
7. Select the storage pool where your echoed virtual cartridges will be stored from the Storage Pool list.
8. For LAN/WAN echo copy pools, select whether your replication is for deduplicated or non-deduplicated backups.
9. For LAN/WAN echo copy pools, select “Initialize via Tape Transport” only if you intend to use this echo copy pool for the one-time process of tape initialization. (See Tape Initialization (page 52).)
10. Select **Next Step** to set the policies.
11. Type the desired policy settings in the corresponding fields. The policy settings differ for SAN libraries and LAN/WAN libraries, and are as follows:

    SAN libraries:

    - **Retention days** – the number of days information is kept in the firesafe before it is deleted. The default is two days.
    - **Sizing factor** – the percentage of space, compared to the actual size of a disk, allocated on the virtual tape for the copy job. For example, if the sizing factor is set to 90% and the physical tape is 100 GB, the allocated space for the virtual tape will be 90 GB.

NOTE: The sizing factor is crucial to creating the right size virtual tapes. When determining the sizing factor of the virtual tapes, keep in mind the following:

- The sizing factor should be based on the size of the physical tape or the tape type if possible. Common tape types and their sizes are: LTO-1 – 100 GB, LTO-2 — 200 GB, LTO-3 — 400 GB, LTO-4 — 800 GB, DLT-IV — 80 GB, DLT-VS1 — 160 GB, SDLT-I — 320 GB, SDLT-II — 600 GB.
- HP recommends against setting the sizing factor too high (for example 110%). Although the virtual copy can be made, if the drive compression is too low the data might not fit back onto the physical tape.
- The sizing factor applies to all operations except Load for Restore, in which case the sizing factor is ignored and the virtual copy is exactly the size of the physical cartridge.
- In general, the virtual cartridge is approximately 90% of the actual cartridge size. Base the size of the copy on the eventual maximum size of the actual cartridge that is to be copied.

- **Source cartridge size limit** — the size of all newly created source cartridges, regardless of the physical cartridge size, on VLS systems with deduplication enabled. The default size is 200 GB; the maximum size is 300 GB.

  Certain operations, such as loading physical cartridges into a copy pool with pre-existing source cartridges, will require you to accept resizing the existing cartridges if they exceed the size limit set here. In this case, a warning message indicates the number of cartridges to be resized if you proceed. If you opt to continue and resize the source cartridges, no data will be lost; you can still access data beyond the end of the newly set capacity limit.

  The Sizing Factor also controls the size of the source cartridge. The system will size the source cartridge using the Source cartridge size limit or the sizing factor, whichever value is the smallest.

- **Echo Copy on Source Cartridge Eject** – When the backup application ejects an out of sync virtual cartridge, the matching destination cartridge will not be ejected until the copy is complete. When the copy on eject option is not checked, then the time to complete the copy and eject the destination cartridge will depend on your start time and window size. When this option is checked, then the copy will be started as soon as possible (depending on available drives) regardless of start time and window size. Then the destination cartridge will be ejected.
- **Send notification if cartridge not migrated in** — the copy pool threshold. The system will send a notification if this many hours have passed and the cartridges have not migrated.
- **Start mirror of Out of Synch cartridges** — When a cartridge goes into the 'Out of Sync' state, you can schedule the mirror operation to begin only at the start of the policy window, or to wait for the specified number of hours to pass after it enters the 'Out of Sync' state (provided the time is within the policy window). The default is to schedule mirror jobs immediately upon entering the 'Out of Sync' state provided the current time is within the policy window. Set this value to a number greater than zero to prevent aborted or multiple mirror operations on a cartridge where the backup application mounts the cartridge, writes to it, unmounts the cartridge, and then repeats this cycle multiple times during a backup window.
- **At End of the Policy Window** – what happens to active jobs when the policy window is over. The options are Allow Active Jobs to Complete, Cancel Active Jobs, and Cancel Active Jobs if Less Than 0% complete. If you select the last option, enter the percentage completion in the field.

LAN/WAN libraries:

- **Priority** — the priority this echo copy pool takes over other copy pools during the backup window. This can be High, Medium, or Low.
- **Deduplication Timeout** (only if you selected deduplicated replication on the previous screen) — if the cartridge fails to deduplicate within the timeout limit you set, the entire cartridge is copied over in non-deduplicated mode.
- **Send notification if cartridge not replicated in** — the copy pool threshold. The system will send a notification if this many hours have passed and the cartridges have not replicated.
- **Start mirror of Out of Synch cartridges** — see above for LAN libraries.
- **At End of the Policy Window** – see above for LAN libraries.

12. Select **Next**.
13. Beneath the policy settings you just entered, enter the details of the window duration:
    - **Start Day** – the day of the week on which the echo copy job begins. HP recommends that copies are scheduled on a different day and/or time window from other backup activities.
    - **Start Time** – the time at which the echo copy job begins. HP recommends that copies are scheduled within a different time window from other backup activities.
    - **Window Duration** – the number of hours available during which the echo copy job can take place. If the migration does not take place during this window, the job is maintained in the queue until the next start time.

    For SAN destinations, HP recommends that you schedule mirror copies on a different day/time window than backup activities. For LAN/WAN destinations, HP recommends that you allow mirror copies to run 24 hours a day unless there is a need to restrict the use of LAN/WAN bandwidth during certain periods of the day.
14. Select **Add**.

    The window refreshes, and the availability window you just added is moved to the Current Availability Windows section of the screen.

    Repeat steps 12 through 14 for as many availability windows as you need.
15. If you need to delete an availability window you just created, select **Delete** corresponding to that window.
16. Select **Submit**.

    If the pool was successfully created, the **Copy Pools** screen displays, along with the message, "The echo copy pool [echo copy pool name] was successfully created."

    If the pool was not created, the **CREATE NEW ECHO COPY POOLS** screen refreshes and provides an error message at the bottom of the screen. Failure to create the pool most often occurs because the slot numbers chosen are outside the available slot range. "The start slot is not in a free range of slots" displays if only the start slot or both the start and end slots are out of range. "The end slot is not in a free range of slots" displays if only the end slot is out of range.
17. If the new pool is not created due to a slot range error, repeat this procedure and select slots within an available range.

Creating Virtual Tapes

Virtual tapes are created automatically when:

- A pool is created that includes physical tapes.
- A **Load Media for Restore**, **Load Blank Media**, or **Load Media for Overwrite** is performed.
- A tape is moved into an echo copy pool by some means other than automigration.

NOTE: The tape is only created if a header exists and is legible by the system.

Restoring from a SAN Physical Cartridge

If the destination tape is still loaded in the destination library, then its matching virtual cartridge will still be present in the virtual library. In this case, you can simply restore from the virtual cartridge using the backup application.

If the destination tape has been ejected from the destination library, you must use one of the following options:

1. If the automigration virtual cartridge still exists in the firesafe (for example, if the policy-defined retention period has not expired), use Command View VLS to manually move the cartridge back into the virtual library. You can then restore from the virtual cartridge using the backup application, and then move the cartridge back to the firesafe.
2. If the automigration virtual cartridge has been deleted from the firesafe, retrieve the physical cartridge by one of the following methods:
   - Load the physical cartridge into any compatible physical drive or library that is visible to the backup application and restore from that tape using the backup application.
   - Load the physical cartridge into the destination library and perform a **Load Media for Restore**, which copies the entire destination tape back into a virtual cartridge. You can then restore from the virtual cartridge using the backup application.

To perform **Load Media for Restore**:

1. Select the **Automigration/Replication** tab.
2. In the navigation tree, expand **Destination Libraries** and then the library of interest.
3. Select **Mailslot** to display the list of mailslots on that library.
4. From the task bar, select **Load Media for Restore** to open the Load Media for Restore screen.
5. From the drop-down box, select the copy pool you want to load the media into. You can choose among the echo copy pools.
6. For all mailslots, the destination slots are automatically populated with the first available slots. To keep the automatic assignment, skip to Step 10. To assign the destination slots manually, continue to the next step.

   If the Destination Slot Number for each mailslot displays “None,” the copy pool you selected is full. Select another copy pool and the Destination Slot Number column will show the automatic assignment.
7. Click **Clear All** to clear the automatic assignments.
8. Hover over the first **Select Slot** link to display a list of the available destination slots. Select a slot number from the list.

   After you select a slot from the available destination slots, that slot no longer appears in the list.
9. Hover over each **Select Slot** link until you have selected a destination slot for each mailslot.
10. Click **Next Step**. A confirmation screen displays.
11. Click **Load**.

    The **Media Move History** screen displays the current status of the move. The possible status messages are Moving, Waiting, Successful, and Failed.

    If the status of the move is still Waiting, you can click **Cancel** to stop the move.

NOTE: Using **Load Media for Restore** will create a virtual tape if one does not already exist.

Restoring from a LAN/WAN Virtual Cartridge

From Command View VLS:

1. Click the **Automigration/Replication** tab.
2. Under **Destination Libraries** in the navigation tree, expand the library you want to restore.
3. From the navigation tree, select **Slots**.
4. On the task bar, select **Restore Media**.
5. Select the slot numbers you wish to restore.
6. Click **Submit**.

   The **Restore Media** screen refreshes with a message that indicates the restores were successful.

Loading Blank Media into an Echo Copy Pool

To move a blank tape (or a tape that should be considered blank) from a mailslot on a destination library into an echo copy pool, use **Load Blank Media**. From Command View VLS:

1. Select the **Automigration/Replication** tab.
2. In the navigation tree, expand **Destination Libraries** and then the library of interest.
3. Select **Mailslot** to display the list of mailslots on that library.
4. From the task bar, select **Load Blank Media** to open the Load Blank Media screen.
5. From the drop-down box, select the copy pool you want to load the media into. You can also choose unmanaged slots that are not in a copy pool.
6. For all mailslots, the destination slots are automatically populated with the first available slots. To keep the automatic assignment, skip to Step 10. To assign the destination slots manually, continue to the next step.

   If the Destination Slot Number for each mailslot displays "None," the copy pool you selected is full. Select another copy pool and the Destination Slot Number column will show the automatic assignment.
7. Click **Clear All** to clear the automatic assignments.
8. Hover over the first **Select Slot** link to display a list of the available destination slots. Select a slot number from the list.

   After you select a slot from the available destination slots, that slot no longer appears in the list.
9. Hover over each **Select Slot** link until you have selected a destination slot for each mailslot.
10. Click **Next Step**. A confirmation screen displays.
11. Click **Load**. The **Media Move History** screen displays the current status of the move. The possible status messages are Moving, Waiting, Successful, and Failed.

    If the status of the move is still Moving or Waiting, you can click **Cancel** to stop the move.

    Automigration will then automatically create a matching blank virtual cartridge in the source virtual library defined for this echo copy pool if one does not already exist.

△ **CAUTION:** Any tape moved into an echo copy pool in this way will be considered blank even if it contains data.

Loading Media into an Echo Copy Pool for Overwrite

To load an expired tape (a tape that was previously backed-up to and is being reused) from a mailslot on a destination library into an echo copy pool, use **Load Media for Overwrite**. From Command View VLS:

1. Select the **Automigration/Replication** tab.
2. In the navigation tree, expand **Destination Libraries** and then the library of interest.
3. Select **Mailslot** to display the list of mailslots on that library.

4. From the task bar, select **Load Media for Overwrite** to open the Load Media for Overwrite screen.
5. From the drop-down box, select the copy pool you want to load the media into.
6. For all mailslots, the destination slots are automatically populated with the first available slots. To keep the automatic assignment, skip to Step 10. To assign the destination slots manually, continue to the next step.

   If the Destination Slot Number for each mailslot displays "None," the copy pool you selected is full. Select another copy pool and the Destination Slot Number column will show the automatic assignment.
7. Click **Clear All** to clear the automatic assignments.
8. Hover over the first **Select Slot** link to display a pop-up box of the available destination slots. Select a slot number from the box.

   After you select a slot from the available destination slots, that slot no longer appears in the pop-up box.
9. Hover over each **Select Slot** link until you have selected a destination slot for each mailslot.
10. Click **Next Step**. A confirmation screen displays.
11. Click **Load**.

    The **Media Move History** screen displays the current status of the move. The possible status messages are Moving, Waiting, Successful, and Failed.

    If the status of the move is still Waiting, you can click **Cancel** to stop the move.

    Automigration will then automatically scan the header from the loaded tape when a drive becomes available. The amount of time this takes varies depending on how busy the destination library is. After scanning the tape header, it will automatically create a matching virtual cartridge (if one does not already exist) in the source virtual library defined for this echo copy pool that is blank except for the header written at the beginning of the tape.

NOTE: Because no data has been stored, you cannot restore from this virtual tape.

Restarting a Broken Mirror

The "mirror broken" state can occur when there is not enough room on the virtual tape to create the copy, there are no available slots to create the copy, the library cannot read the header of the physical tape, the library cannot determine that a tape without a header is blank, or the library cannot successfully write the header to the virtual tape.

When a physical cartridge in a destination library is in this state, you must restart the broken mirror for the automigration to continue. The Restart Broken Mirror task triggers a job to run which clears out the problem.

1. From the task bar, select **Restart Broken Mirror**. The Restart Broken Mirror screen opens and displays all cartridges with the Mirror Broken status.
2. Select the cartridges you want to restart.
3. Select **Submit**. The Result screen indicates that the operation was successful. The cartridge is now in the UpToDate status.

Viewing Cartridges in Automigration Source Libraries

When a tape is still present in the destination library, you can view the matching automigration virtual cartridge in the associated source virtual library. To view cartridges in the source libraries:

1. On the **Automigration/Replication** tab, select **Source Cartridges** from the navigation tree.
2. The right hand pane then shows all the automigration virtual cartridges (alphabetically by bar code) in the source libraries and information including the cartridge state, last written date, destination library, and destination slot.

Viewing Automigration Cartridges in the Firesafe

When a cartridge is ejected from the destination library, its matching virtual cartridge is automatically ejected out of the virtual library and moved into the device's firesafe. The firesafe acts as a virtual offline location for the automigration virtual cartridges. Once they are in the firesafe, the automigration virtual cartridges are retained according to their automigration policies, which define how many days the virtual cartridges remain in the firesafe before being automatically deleted.

NOTE: From the **Automigration/Replication** tab of Command View VLS, the firesafe in the window shows items placed in the firesafe by automigration only; items placed in the firesafe from different functions of the VLS are not shown here.

To view cartridges in the firesafe, from the **Automigration/Replication** tab, select **Firesafe** from the navigation tree. For mirror copies, the firesafe date is the date of the most recent copy.

When the physical tape is moved back into the physical library, the corresponding virtual tape is immediately moved from the firesafe back to the appropriate location (based on the location of the physical tape). The physical tape is not read upon load and is not synchronized to the virtual tape. Therefore, if you have modified the physical tape while it was outside of the library, then it is now out-of-sync with the virtual tape in the firesafe. If you want to keep these modifications to the physical tape, you will need to ensure that the data is copied to the virtual tape. Either manually delete the virtual tape from the firesafe or perform a **Load Media for Restore**. This forces the system to read the physical tape upon load and causes automigration to create a new virtual copy. See Restoring from a SAN Physical Cartridge (page 59).

Editing Copy Pools

The following sections describe the copy pool edit operations available to the user.

Moving a Copy Pool

When there is not enough space left on a virtual library, a copy pool can be moved to a different virtual library. To move a copy pool from one virtual library to another:

1. Select the **Automigration/Replication** tab and expand the task bar of the navigation tree.
2. Under **Destination Libraries**, select **Copy Pools**.
3. From the **Name** column in the copy pools lists, select the copy pool to be moved.
4. From the **Copy Pool Details** window task bar, select **Change Local Library**.
5. From the **CHANGE LOCAL LIBRARY** window, verify the current local library on which the pool resides.
6. Select the new local library, then select **Submit**.

   The **Echo Copy Pool Details** window displays, along with the message, "The local library was successfully changed."

NOTE: When an echo copy pool moves to a different local library, the associated automigration tapes automatically move with it.

Changing the Slot Mapping for a SAN Library

Slot mapping refers to the assignment of physical slots in a library to correspond to a specific virtual copy pool. Mapping occurs as a copy pool is created; however, mapping can be changed at any time. Reasons to change the slot mapping include the need for a group of slots to expand to match the corresponding virtual copy pool, the need to shrink an existing pool to make more room for a growing pool, and the need to rearrange the mapping so that the pools correspond to a consecutive set of slots.

To remove the slot mapping of any copy pool:

1. Select **Slots** in the appropriate library from the navigation tree.

2. In the **Copy Pool** column, select any instance of the appropriate pool.

   The **ECHO COPY POOL DETAILS** screen displays.
3. Select **Delete** in the taskbar.
4. Select **OK** from the dialog box.

   The copy pool details screen refreshes and the message, "The slot map was successfully deleted from [copy pool name]" displays.

NOTE: If a tape is in a newly unmapped section of a library, the tape will be moved to the firesafe. If the tape has not expired and been deleted from the firesafe, upon remapping of the section, the tape will move back and be removed from the firesafe.

To add slot mapping to any copy pool which does not have slots mapped:

1. Under **Destination Libraries**, select **Copy Pools** from the navigator pane.
2. Select the appropriate copy pool to display the copy pool details screen.
3. From the task bar, select **Edit Slot Maps**.
4. On the **Edit Slot Map** screen, in the Add Additional Slots section, enter a start slot and end slot for the copy pool from the available slot ranges listed.
5. Select **Add**.

   The copy pool details screen refreshes and the message, "The slot map was successfully added to [copy pool name]" displays.

To change slot mapping on a copy pool that already has slots mapped:

1. On the **System** tab, check the capacity of the copy pool to ensure there is room for copies.
2. From the copy pool details screen on the **Automigration/Replication** tab, select **Edit Slot Maps** on the taskbar.

   The **Edit Slot Map** window displays.
3. In the Current Slots section, select **Edit** for the slots you want to edit. The **EDIT SLOT MAP** window opens.
4. Change the Start and End slots.
5. Select **Submit**.

   If the change is successful, the copy pool details window displays, including the message, "The slot map was successfully changed".

   If the start and/or end slot is outside the available range, the **EDIT SLOT MAP** window refreshes and displays "The start and end slot define an invalid range."
6. If the slot map is not changed due to a slot range error, repeat this procedure and select slots within an available range.

Changing the Slot Mapping for a LAN/WAN Library

Slot mapping in the case of replication refers to the assignment of virtual slots in a library to correspond to a specific LAN/WAN replication target. Mapping occurs as a LAN/WAN replication target is created; however, mapping can be changed at any time. Reasons to change the slot mapping include the need for a group of slots to expand the number of slots on the LAN/WAN replication target, the need to shrink an existing LAN/WAN replication target, and the desire to rearrange the mapping so that the LAN/WAN replication targets correspond to a consecutive set of slots.

To remove the slot mapping of any copy pool:

1. Select the **Automigration/Replication** tab.
2. Expand **LAN/WAN Replication Libraries** in the navigation tree, and then expand the appropriate library.
3. Select **Copy Pools** in the navigation tree.

4. On the **Summary for Copy Pools** screen, select the echo copy pool if interest to open the **Echo Copy Pool Details** screen for that copy pool.
5. From the task bar, select **Edit Slot Maps**.
6. On the **Edit Slot Maps** screen, select **Delete** corresponding to the slot map to remove.
7. Select **OK** in the dialog box.

   The copy pool details screen refreshes and the message, "The slot map was successfully deleted from [copy pool name]" displays.

To add slot mapping to any copy pool which does not have slots mapped:

1. Follow steps 1 through 5 above.
2. In the Add Additional Slots section of the screen, enter the start slot and end slot for the new copy pool from the available slot ranges listed.
3. Select **Add**.

   The slot range you just added moves to the Current Slots section of the screen.

   Repeat this step for as many slot maps as you need.
4. Select **Submit**.

   The copy pool details screen refreshes and the message, "The slot map was successfully added to [copy pool name]" displays.

To change the slot mapping on a copy pool that already has slots mapped:

1. On the **System** tab, check the capacity of the copy pool to ensure there is room for copies.
2. Follow steps 1 through 5 in the "To remove the slot mapping of any copy pool" section above.
3. On the **Edit Slot Maps** screen, select **Edit** corresponding to the slot map to change.
4. Enter the new start and/or end slots into the appropriate fields.
5. Select **Submit**.

   If the change is successful, the copy pool details window displays, including the message, "The slot map was successfully changed."

Editing the SAN or LAN/WAN Policy

1. Select **Copy Pools** in the appropriate library from the navigation tree.
2. Select the appropriate copy pool to open the **Echo Copy Details** screen.
3. In the task bar, select Edit **Policy**.
4. Make the appropriate changes. For explanations of the options, see Creating an Echo Copy Pool (page 56).
5. Select **Submit**.

   The **Echo Copy Details** screen displays the new policy information.

Editing the SAN or LAN/WAN Availability Windows

1. Select **Copy Pools** in the appropriate library from the navigation tree.
2. Select the appropriate copy pool to open the **Echo Copy Details** screen.
3. In the task bar, select **Edit Policy**.
4. In the task bar, select **Edit Policy Windows**.
5. Make the appropriate changes. For explanations of the procedure, see Creating an Echo Copy Pool (page 56).
6. Select **Submit**.

   The **Echo Copy Details** screen displays the new policy information.

To add or delete policy windows, see Creating an Echo Copy Pool (page 56).

Deleting a Copy Pool

You should delete a copy pool when you no longer need it. To delete a copy pool:

1. Select **Copy Pools** under the appropriate library from the navigation tree.
2. Select the copy pool on the **Summary for Copy Pools screen** to open the **Echo Copy Details** screen.
3. From the task bar, select **Delete**.
4. Select **OK** from the dialog box.

   The **Copy Pools** screen is refreshed and the deleted pool is no longer listed.

NOTE: Deleting a copy pool moves the associated virtual tapes into the firesafe. At the end of the retention period, the system deletes the source cartridges from the firesafe. If you need to retrieve the cartridges for any reason, you must do so before the retention period ends.

SAN Destination Library Operations

This section describe all of the SAN destination library operations available to the user.

Monitoring Destination Library Status

This section describes how to locate the Command View VLS automigration status messages of a destination library. This applies to both SAN automigration libraries and LAN/WAN replication libraries.

VLS hardware, environmental, and virtual device (library, tape drive, cartridge) status is constantly monitored by the VLS software and displayed on the VLS web user interface, Command View VLS.

Monitoring All Libraries

While the device status icon in the Command View VLS status banner indicates the overall VLS device health on other tabs, the icon on the **Automigration/Replication** tab indicates the status of the destination libraries.

A destination library status icon can be one of five states:

- **Error**—An error occurred while the system was determining the status of the destination libraries.
- **Unknown**—A destination library's operating condition is unknown. Contact HP Technical Support.
- **Normal**—All destination libraries are operating normally.
- **Warning**—At least one destination library is in a good state while at least one destination library is any state other than good.
- **Warning for All**—All destination libraries are in any state other than good.

Monitoring a Specific Library

A notification alert is generated by the VLS software when a hardware or environmental failure is detected or predicted. VLS notification alerts are displayed on the Notifications screen of Command View VLS, and can also be sent as mail to the addresses you specify and/or as SNMP traps to the management consoles you specify. Status is also provided, where appropriate, on some screens under the **Automigration/Replication** tab.

To view the automigration status of a particular destination library:

1. Select the **Automigration/Replication** tab.
2. In the navigation tree, select the destination library to view. This opens the **Destination Library Details** screen.

   This screen displays the state of the destination library. For SAN automigration libraries the options are Good, Degraded, Critical, Failed, or Missing; for LAN/WAN replication libraries

the options are Connected, Configuration Out of Sync, and Unreachable. The screen also provides the name and model of the library, number of simultaneous transfers, number of slots, management URL, and availability.

3. Expand the destination library in the navigation tree to access more specific information.

Cartridge Status and Slot Details

To view the status of the destination library's slots, expand the library in the navigation tree and select **Slots**.

The **Summary for Slots** screen displays the drive name, barcode, cartridge status, local library, copy pool, and last mirrored date for each slot number in use. Select a barcode from the list to see more details on the job history and status for that barcode.

Quickly locate slots of interest using the **Advanced Search**. See Advanced Search for Slots (page 68).

You can also select **Slots State Summary** from the navigation tree to see which of all the possible statuses have slots in that status; if a status is not listed, there are no slots currently in that status. The number of slots in each status is displayed. Select a status to see a list of the specific slots in that status.

The Cartridge Status column of the **Summary for Slots** screen is particularly useful with echo copy because the backup application is not aware of any copy failures. The status of the physical cartridges in the destination library will be one of the following:

Status message	Pool type	Description
Unmanaged	None	This cartridge is not part of any pool.
Adding Cartridge	Echo Copy	Copying the header from the target cartridge to this newly created source cartridge. If the barcode of the target cartridge exists anywhere on the VLS, it is moved into the source library for the copy pool.
Up To Date	Echo Copy	The target and source cartridges have the same contents.
Waiting for Backup Data*	Echo Copy	Waiting for the backup application to update the source cartridge by appending or overwriting the cartridge over the SAN. A cartridge will get into this state when the barcode for the source cartridge already existed on the source VLS when the (LBR) Echo Copy pool was created and the source cartridge contained data. It is not possible to replicate that preexisting content in a deduplicated manner.
In Use	Echo Copy	The cartridge has been loaded into a drive by the backup application.
Backup Postprocessing*	Echo Copy	Creating deduplication instructions.
Out of Sync	Echo Copy	The source virtual cartridge has been updated by the backup application since the target cartridge was updated. Instruction creation is complete.
Mirror Scheduled	Echo Copy	Waiting to acquire resources to run the job to synchronize the target cartridge with the source cartridge.
Mirroring	Echo Copy	Mirroring from the target cartridge to the source cartridge.
Mirror Broken	Echo Copy	A problem was encountered mirroring the cartridge.
Restoring	Echo Copy	Mirroring from the source cartridge to the target cartridge.
Eject Pending	Echo Copy	Ejecting the target cartridge and about to put the source cartridge into the firesafe.
Mirror/Eject Pending	Echo Copy	About to eject the target cartridge and then put the source cartridge into the firesafe.
Mirroring before Eject	Echo Copy	Synchronizing the cartridge in the Destination Library with the source virtual cartridge. When the mirror job is complete, the target cartridge will be ejected and the source cartridge will be moved to the firesafe.

Status message	Pool type	Description
Export Preprocessing*	Echo Copy	Gathering deduplication instructions needed for replication using tape transport.
Exporting*	Echo Copy	Copying content from the source cartridge onto a physical tape.
Partially Exported*	Echo Copy	Copying content from the source cartridge will continue on another physical tape.
Export In Use*	Echo Copy	Waiting for the remaining cartridges in the pool to finish exporting.
In Transit/Importing*	Echo Copy	Importing status on the destination library, In Sync status on the source VLS.
Importing/In Use*	Echo Copy	Importing status on the destination library, loaded into a drive by the backup application the source VLS.
Importing/Backup Postprocessing*	Echo Copy	Importing status on the destination library, creating deduplication instructions on the source VLS.
Importing/Out of Sync*	Echo Copy	Importing status on the destination library, Out Of Sync status on the source VLS.
Mirror Preprocessing*	Echo Copy	Gathering the deduplication instructions needed for replication.
Mirror Preprocess Pending*	Echo Copy	A mirror preprocess job is awaiting resources in order to run.
Mirror Postprocessing*	Echo Copy	Expanding deduplication instructions to update the target cartridge.
Cleanup*	Echo Copy	Cleaning up replication data on the source.
Eject Broken	Echo Copy	A problem occurred when attempting to eject a physical cartridge.
Header Broken	Echo Copy	A problem occurred during source cartridge creation process.
Restore Broken	Echo Copy	A problem occurred while restoring a cartridge.
Restore Pending	Echo Copy	A restore job is awaiting resources in order to run.
Paused	Echo Copy	A mirror job was paused.
Empty Tape	Tape Export	The physical tape has not yet been used yet.
Copying	Tape Export	Copying a source virtual cartridge onto this physical tape.
Used Tape	Tape Export	Tape contains export data.
Full Tape	Tape Export	Tape contains export data and is ready to be ejected. Signal to tape operator to unload this tape from the physical library.
Unloaded Full Tape	Tape Export	Tape contains export data and has been ejected. This tape should be included in the collection to be sent to the target site.
Waiting for Load	Tape Export	Tape that contains data that will be imported when the tape operator moves it into an Import pool slot. Signal to tape operator to load this tape into the physical library.
Tape Currently Not Needed	Tape Export	Tape in an Import pool slot that is in the catalog, but not needed yet. Signal to tape operator to remove the tape from the physical library.
Bad Tape	Tape Export	Unable to write tape. It does not contain any export data and is ready to be ejected. This tape should NOT be sent to the target site.
Unloaded Tape	Tape Import	Tape that contains data that will be imported later.
Waiting for Load	Tape Import	Tape that contains data that will be imported when the tape operator moves it into an Import pool slot. Signal to tape operator to load this tape into the physical library.
Tape Currently Not Needed	Tape Import	Tape in an Import pool slot that is in the catalog, but not needed yet. Signal to tape operator to remove the tape from the physical library.

Status message	Pool type	Description
Ready For Import	Tape Import	Tape in an Import pool slot that is in the catalog.
Importing	Tape Import	Actively copying data from the physical tape to the target virtual cartridge.
Import Complete	Tape Import	All data has been copied from the physical tape to the target virtual cartridges. Signal to tape operator to remove the tape from the physical library.
Unloaded Completed Tape	Tape Import	All data has been copied and the tape has been ejected.
Bad Tape	Tape Import	Unable to read the physical tape. Signal to tape operator to remove the tape from the physical library.
Unloaded Bad Tape	Tape Import	Unable to read the physical tape and the tape has been ejected.
Skipped	Tape Import	The tape operator skipped this tape (possibly because it was missing in the collection received from the source site).
Unloaded Skipped Tape	Tape Import	The tape operator skipped this tape and the tape has been ejected.
Unknown Tape	Tape Import	There is a physical tape in an Import pool slot that is not part of the pool; it is not in the catalog. Signal to tape operator to remove the tape from the physical library.
* Indicates status messages that are only valid for replication (deduplication-enabled).		

Advanced Search for Slots

Quickly locate slots of interest using the **Advanced Search** link on the task bar. Enter a specific barcode or filter by status, local library, and/or copy pools. Choose options from the lists and select **Submit**. The slots meeting your criteria are displayed.

Mailslot Details

Select **Mailslot** from the expanded destination library list to view the destination library mailslots. The screen displays the barcode and local library for each slot. The task bar includes further actions you can take.

This screen is only available for SAN automigration libraries.

Copy Pool Details

Select **Copy Pools** from the expanded destination library list to view the **Echo Copy** pools. The screen displays the priority, local library, storage pools, slot maps, and policy windows for each copy pool. Select a copy pool from the list to see more details and to access further actions.

Import/Export Pool Details

Select **Import/Export Pools** from the expanded destination library list to view the destination library import and export pools. The screen displays the priority, local library, storage pools, slot maps, and policy windows for each pool. Select an import or export pool from the list to see more details and to access further actions.

This screen is only available for SAN automigration libraries.

Tape Drive Details

Select **Drives** from the expanded destination library to view the destination library tape drives. The screen displays the drive status, name, drive type, serial number, availability, state, and barcode. Select a drive from this list or from the navigation tree to see more details and to access further tasks.

This screen is only available for SAN automigration libraries.

Forcing a Replication Job

The **Copy Now** task allows you to schedule a replication (or automigration) job that forces the cartridge to replicate immediately regardless of whether or not the cartridge is within the policy window. You can only perform this task when the cartridge is holding in the Out of Synch state.

In Command View VLS:

1. On the **Automigration/Replication** tab, expand the destination library in the navigation tree and select **Slots** to open the **Summary for Slots** screen.
2. Select **Copy Now** from the task bar.
3. On the **Copy Now** screen, select the slots you want to replicate.
4. Select **Submit**.

   The system immediately registers the selected cartridges into the queue to replicate when resources are available regardless of the policy windows.

Placing a Library Offline or Online

Place the library offline in order to deploy firmware, create a support ticket, or run a library assessment test. You can place a LAN/WAN destination library offline as well. To do so:

1. From the navigation tree under **Destination Libraries**, select the library to place offline.
2. From the task bar, select **Offline**.

   A dialog box opens to confirm the selection and warn that placing the library offline will cancel all active jobs.

3. Select **OK** from the dialog box.

   The **Destination Library Details** screen refreshes and displays the message, "The destination library was successfully placed offline." In addition, the **Offline** option in the task bar is replaced with **Online**.

NOTE: When placing the library offline from the **Automigration/Replication** tab, the library is not truly offline. Instead, it is offline for automigration or replication jobs only.

Place the library online to resume scheduled automigration or replication:

1. From the navigation tree under **Destination Libraries**, select the library to place online.
2. From the task bar, select **Online**.

   A dialog box opens to confirm the selection and warn that placing the library online will allow jobs to resume.

3. Select **OK** from the dialog box.

   The **Destination Library Details** screen refreshes and displays the message, "The destination library was successfully placed online." In addition, the **Online** option in the task bar is replaced with **Offline**.

Moving Media from One Slot to Another

From Command View VLS:

1. Select the **Automigration/Replication** tab.
2. In the navigation tree, expand **Destination Libraries** and then the library of interest.
3. Select **Slots** to display the list of slots on that library.
4. From the task bar, select **Move Media**. The screen displays a list of slots and the copy pools to which they currently belong.

5. Hover over the **Select Slot** link for the first slot you want to edit. The screen displays a list of the available destination slots. Select a slot number from the list.

   After you select a slot from the available destination slots, that slot no longer appears in the list.
6. Hover over each **Select Slot** link until you have selected a destination slot for each slot you want to edit.
7. Click **Next Step**. The screen displays a confirmation.
8. Click **Move**.

   The **Move Media History** screen displays the current status of the move. The possible status messages are Moving, Waiting, Successful, and Failed.

   If the status of the move is still Waiting, you can click **Cancel** to stop the move.

Ejecting Media from a Slot into an Empty Mailslot

You can eject media from a slot into an empty mailslot within the same library using Eject Media.

From Command View VLS:

1. Select the **Automigration/Replication** tab.
2. In the navigation tree, expand **Destination Libraries** and then the library of interest.
3. Select **Slots** to display the list of slots on that library.
4. From the task bar, select **Eject Media**. The screen displays a list of slots that are full.
5. From the list of full slots, select the source slots of the media you want to eject.

   The Available Mailslots displays the number of mailslots currently available. As you select and deselect slot numbers from the list, the number changes.
6. Click **Next Step**. The screen displays a confirmation.
7. Select the **Copy before Eject if Out of Sync** box if you want to force a mirror of any cartridge before it is ejected.

   This determines what the system does when the library policy includes a copy on eject and the media being ejected is either not synchronized or has a status of "Mirror Broken." If deselected, the slot will eject immediately without running a copy. If selected, a copy job is put in the queue and the system will wait to eject the media until after the copy is complete. Scheduling the copy requires that you wait for the copy to complete before moving another tape into the slot. Although a status message may display indicating that the copy has begun, it may still be in the queue.
8. Click **Eject**.

   The **Move Media History** screen displays the current status of the eject. The possible status messages are Moving, Waiting, Successful, and Failed.

   If the status of the move is still Waiting, you can click **Cancel** to stop the eject.

Ejecting Media from a Drive into an Empty Mailslot

To eject media from a drive into an empty mailslot within the same library:

1. Expand the navigation tree. On the appropriate library, expand **Drives** and then select the drive from which to eject the media.

   The **TAPE DRIVE DETAILS** screen is displayed in the main window.
2. From the task bar, select **Eject Media**.
3. From the list of empty mailslots that displays, select the destination slot for the ejected media.
4. Select **Submit**.
5. After the media is ejected, the **TAPE DRIVE DETAILS** screen displays along with the message, "The media was successfully ejected from the drive into slot [destination mailslot number]."

Restarting Automigration/Replication Services

If you replace a tape drive on your physical tape library, you must restart automigration/replication services afterwards. This resets the services to acknowledge the new tape drive.

1. In Command View VLS, select the **System** tab.
2. In the navigation tree, select **Chassis**.
3. Under **Maintenance Tasks**, select **System Maintenance**.
4. In the task bar, select **Restart Automigration/Replication Services**. The screen displays a warning.
5. Select **Restart**. (You can select **Return** to cancel the restart.) The screen displays a summary of the restarted services.
6. Select **Return**.

Scanning a SAN Destination Library

For an initial setup, or to force an immediate synchronization of data, scan the appropriate destination library. This immediately forces the scan of a specific physical library:

NOTE: The status message is returned as soon as the scan is successfully scheduled; however, the scan may not yet be complete. There is no way to determine whether the scan has been performed.

---

1. From the navigation tree under **Destination Libraries**, select the library to scan.
2. From the task bar, select **Scan**.

   The **Destination Library Details** screen refreshes, and the message, "Scan of destination library successfully scheduled" displays.

Editing the Management URL

In order to view the management software for a SAN destination library from the Automigration interface, provide the destination library URL:

1. From the navigation tree under **Destination Libraries**, select the library with the URL to add.
2. From the task bar, select **Edit Management URL**.
3. Type the URL into the **Management URL** field, then select **Submit**.

   If the management URL is accepted, the **Destination Library Details** screen refreshes and displays the message, "The management URL was successfully changed." If not, the **Edit Management URL** screen refreshes and displays the error message, "Please enter a valid management URL."
4. If the URL is not changed, repeat this procedure using a valid URL.

After the Management URL has been successfully added, it creates a link to the management software. Click on the URL in the **Destination Library Details** list to launch the management software in a new window.

Uploading SAN Destination Library or Tape Drive Firmware

To load firmware for a physical library or disk drive to a destination library:

1. From the navigation tree, select the appropriate destination library or disk drive.
2. From the task bar, select **Upload Firmware**.
3. Select the firmware by either of these methods:
   - Type the file name in the "Select file to upload:" field.
   - Select **Browse** to locate the appropriate file.

4. Select **Submit**.

   The **SUMMARY FOR ALL DESTINATION LIBRARIES** screen refreshes, along with the message, "File [file name] successfully uploaded."

Deploying SAN Destination Library or Tape Drive Firmware

After uploading the firmware for a physical library or disk drive on a destination library (see Uploading SAN Destination Library or Tape Drive Firmware (page 71)), install the firmware:

1. Place the appropriate library offline (see Placing a Library Offline or Online (page 69)).
2. From the navigation tree, select the appropriate destination library or disk drive.
3. From the task bar, select **Deploy Firmware**.
4. From the **DEPLOY LIBRARY FIRMWARE** screen firmware list, select the firmware to install.

   A dialog box displays to confirm the selection.
5. From the dialog box, select **OK**.

   The **Destination Library Details** screen displays, along with the message, "File [filename] successfully deployed."
6. Place the library online (see Placing a Library Offline or Online (page 69)).

Generating a SAN Destination Library Support Ticket

To generate a support ticket for a library:

1. Place the appropriate library offline (see Placing a Library Offline or Online (page 69)).
2. From the task bar in the **Destination Library Details** window, select **Support Ticket**.

   A dialog box displays to confirm the selection.
3. From the dialog box, select **OK**.

   The screen refreshes and displays the message, "Please wait, action in progress. Do not refresh this page." When the support ticket has been generated, the **Support Ticket Results** screen displays. Select **Download Support Ticket Results File** to view the command sent to the library.
4. Place the library online (see Placing a Library Offline or Online (page 69)).

Generating a SAN Destination Library Drive Support Ticket

To generate a support ticket for a drive:

1. Place the appropriate library offline (see Placing a Library Offline or Online (page 69)).
2. Select the appropriate drive from the navigation tree under Destination Libraries and the library containing the drive.
3. From the task bar (in the **TAPE DRIVE DETAILS** window), select **Support Ticket**.

   A dialog box displays to confirm the selection.
4. From the dialog box, select **OK**.

   The screen refreshes and displays the message, "Please wait, action in progress. Do not refresh this page." When the support ticket has been generated, the **Support Ticket Results** screen displays. From this screen, you can select **Display results of executing the LTT command** to view the command sent to the library or **Download support ticket** to download the actual support ticket file.
5. Select **Finish**.
6. Place the library online (see Placing a Library Offline or Online (page 69)).

Running a SAN Destination Library Assessment Test

To run a library assessment test:

1. Place the appropriate library offline (see Placing a Library Offline or Online (page 69)).

2. From the task bar (in the **Destination Library Details** window), select **Library Assessment Test**.

   A dialog box displays to confirm the selection.
3. From the dialog box, select **OK**.

   The **Library Assessment Test Results** window displays.
4. To view the results of the assessment, select **Download Library Assessment Test Results**.
5. Select **Finish** to return to the **Destination Library Details** window.
6. Place the library online (see Placing a Library Offline or Online (page 69)).

Running a SAN Destination Library Drive Assessment Test

To run a drive assessment test:

1. Place the appropriate library offline (see Placing a Library Offline or Online (page 69)).
2. In the navigation tree, select the drive to be tested.
3. From the task bar, select **Drive Assessment Test**.

   A dialog box displays, warning that the test will erase all data on a cartridge, if there is a cartridge on that drive.
4. Select **OK**.

   The **DRIVE ASSESSMENT TEST** screen displays and asks for a mailslot containing a known-good-cartridge to use for the test.
5. Enter the appropriate mailslot.
6. Select **Submit**.
7. The **Drive Test Results** screen displays, with a message indicating a successful test.
8. Select **Download drive assessment results** to view the command sent to the drive.
9. Select **Finish**.
10. Place the library online (see Placing a Library Offline or Online (page 69)).

Replacing a Library

When a library fails, or when the library robotics card must be changed, the replacement will have a different serial number from the original. To assign it the same pools, mapping, etc. as the original:

NOTE: While the virtual tapes are in the firesafe, scheduled backups for those tapes will not occur.

1. Make a note of all pool configuration information for pools associated with the library to be replaced.
2. Delete all pools associated with the library (see Deleting a Copy Pool).

   NOTE: Deleting the pools automatically moves all virtual cartridges from within the pool to the firesafe.
3. Unmanage the physical library to be replaced (see Managing and Unmanaging a Destination Library).
4. Replace the library or robotics card.
5. Manage the new physical library (see Managing and Unmanaging a Destination Library).
6. Manually recreate the storage pools associated with the new library using the information written down at the beginning of this procedure.

   The virtual tapes that were moved into the firesafe will automatically return to their previous locations.

LAN/WAN Destination Library Operations

The following sections describe the destination library operations for LAN/WAN libraries available to the user.

Several operations also apply to SAN destination libraries and are explained in SAN Destination Library Operations:

- Monitoring Destination Library Status (page 65)
- Placing a Library Offline or Online (page 69)
- Forcing a Replication Job (page 69)

Exporting Data to Physical tapes for Tape Initialization

NOTE: Before beginning the export process, verify that the physical tape library exporting the data uses the same number of barcode characters as the physical tape library that will import the data. If the barcodes do not match exactly, the import process will not work. See your tape library user manuals for information on checking and configuring the number of barcode characters used.

1. Create a LAN/WAN replication target on the remote site. See Creating a LAN/WAN Replication Target (page 76).
2. Create a virtual library on the source site. See Creating a Virtual Library (page 116).
3. On the source site, create an echo copy pool on the newly created LAN/WAN replication target. See Creating an Echo Copy Pool (page 56). Be sure to check the "Initialize via Tape Transport" box.
4. From the **Copy Pools** screen, select the newly created copy pool to open the **Echo Copy Pool Details** screen. Note that the state of the copy pool is "Awaiting Initialization."
5. Allow your regularly scheduled full backups to complete. Cartridges that need to be transported via physical tape become "Out of sync."
6. From the task bar, select **Initiate Tape Transport**. The **Create Tape Export Pool** screen opens.
7. From the **SAN Automigration Library** list, select the physical library from which you want to copy the tapes.
8. Enter a Start and End Slot from the available slot range.
9. Select **Submit**. The status of the copy pool changes to "Exporting."
10. From the navigation tree, select **Import/Export Pools**, and then select the newly created export pool to see the **Tape Export Pool Details** screen.

    The data from the selected library slots is copying to the physical tapes. When the data has finished exporting to the tapes, the status of the copy pool changes to "Importing." The screen prompts you to load empty tapes and unload full tapes as needed.
11. Once the export is finished, select **Import Handling Instructions** from the task bar. This produces information needed for the data import process. Print this information and ship it to the remote location with the physical tapes.

Stopping a Tape Export

1. On the navigation tree, expand Destination Libraries and select **Import/Export Pools** to open the list of all import and export pools.
2. Select the export pool you wish to stop to open the **Tape Export Pool Details** screen.
3. From the task bar, select **Stop Tape Export**.

   The export process stops immediately and all echo copy pool cartridges move to the "Out of sync" state.

4. From the **Echo Copy Pool Details** screen, you can:
   - Select **Initiate Tape Transport** in the task bar to restart the export.
   - Select **Cancel Tape Transport** in the task bar to cancel the process and place the echo copy pool into the "Ready" state.

Importing Data from Physical Tapes for Tape Initialization

1. Complete the export process. See Exporting Data to Physical tapes for Tape Initialization (page 74).
2. On the target site, open the **Automigration/Replication** tab and select **Import Tapes** from the navigation tree.
3. Select the export pool you want to import.
4. From the **Local Library** list, select the physical library from which to copy the tapes.
5. Enter the start and end slots from the available slot range.
6. Select **Submit**.
7. Select **Import/Export Pools** from the navigation tree, then select the newly created import pool to see the **Tape Import Pool Details** screen.

   The screen prompts you to load full tapes and unload finished tapes as needed. If a physical tape is damaged or otherwise unavailable, you can select **Skip** for that tape and transmit the data over the LAN/WAN after the import process completes.
8. After the import process completes:
   - The tape import pool is automatically destroyed on the target site
   - The tape export pool is automatically destroyed on the source site
   - The echo copy pool on the source will change to the "Ready" state and deduplication-enabled replication over the LAN/WAN will begin at the next screen

Forcing Non-Deduplicated Replication

For systems using replication with deduplication, the **Non Deduplicated Copy** and **Forced Non Deduplicated Copy** tasks allow you to schedule a replication job that forces the whole cartridge (non-deduplicated data) to replicate immediately regardless of whether or not the cartridge is within the policy window. You can only perform this task when the cartridge is in the Backup Postprocessing state (Non Deduplicated Copy task), or when the cartridge has not successfully migrated in the deduplication timeout limit or is being "forced" into a whole cartridge copy (Forced Non Deduplicated Copy task).

NOTE: The whole cartridge copy of the data will not deduplicate. This data will consume additional space on the target VLS until the cartridge is overwritten with new data by the backup application.

Non Deduplicated Copy Task

In Command View VLS:

1. On the **Automigration/Replication** tab, expand the destination library in the navigation tree and select **Slots** to open the **Summary for Slots** screen.
2. Select **Non Deduplicated Copy** from the task bar.
3. On the **Non Deduplicated Copy** screen, select the slots you want to replicate.
4. Select **Submit**.

   The system immediately registers the selected cartridges into the queue to replicate the whole cartridge when resources are available regardless of the policy windows.

Forced Non Deduplicated Copy Task

In Command View VLS:

1. On the **Automigration/Replication** tab, select "Not migrated in Deduplication timeout limit/Forced Copies" from the **Summary of All Cartridges** screen.
2. Select **Forced Non Deduplicated Copy** from the task bar.
3. On the **Forced Non Deduplicated Copy** screen, select the cartridges you want to replicate.
4. Select **Submit**.

   The system immediately registers the selected cartridges into the queue to replicate the whole cartridge when resources are available regardless of the policy windows.

Pausing, Resuming, and Canceling Replication Jobs

Each replication job is actually split into smaller jobs: Mirror Preprocessing (preparing to move data), Mirror (moving the data), and Mirror Postprocessing (clean-up process). This saves resources because each job type uses only the resources it needs instead of reserving resources for the entire job. (Whole cartridge replication is not divided into smaller jobs.) The source VLS displays the Mirror Preprocessing and Mirror jobs, while the target VLS displays the Mirror and Mirror Postprocessing jobs.

From Command View VLS, select the **Automigration/Replication** tab, then select **Job Reporting** in the navigation tree. This opens the Current Status screen where you can control the jobs.

On the source VLS, you can pause Mirror and Restore jobs and resume them at a later time, for example when there are more resources available. At any point during the job, click the Pause Job icon (⏸) in the Action column. The job pauses, and the Pause Job icon is replaced by the Resume Job icon (▶). When you are ready, click the Resume Job icon and the job will continue where it left off.

You can cancel all job types at any point by clicking the Cancel Job icon (✖) in the Action column.

NOTE: When a replication library goes offline, all active mirror jobs pause. When the replication library comes back online, all paused jobs resume.

LAN/WAN Replication Target Operations

The following sections describe the operations for LAN/WAN replication target.

Creating a LAN/WAN Replication Target

The first step in configuring replication is the creation of the LAN/WAN replication target. Do this via Command View VLS on the destination VLS. Any virtual library (or slot range within a virtual library) can be configured to act as a LAN/WAN replication target.

1. In Command View VLS, select the **Automigration/Replication** tab.
2. Expand **LAN/WAN Replication Targets** in the navigation tree.
3. If the library on which you want to add a LAN/WAN replication target appears in the list, select that library. The **Summary for all LAN/WAN Replication Targets** screen displays all LAN/WAN replication targets created for that library.

   If the library does not appear in the navigation tree, it means that the library does not yet have any LAN/WAN replication targets on it. Select **LAN/WAN Replication Targets** in the navigation tree instead. The **Summary for All LAN/WAN Replication Targets** screen displays all LAN/WAN replication targets created for all libraries.
4. Select **Create LAN/WAN Replication Target** from the task bar to open the **Create LAN/WAN Replication Target** screen.
5. Enter a name for the LAN/WAN replication target.
6. If you did not select your library from the navigation tree, select the library on which you want to add the target from the **Local Library** menu.

   The Available Slot Ranges section indicates the slots that are available on the library you just selected.

NOTE: If you selected your library from the navigation tree, this pull-down field does not appear because you have already selected the appropriate library.

7. Enter a start slot and an end slot for the copy pool from within the available ranges.
8. Enter the number of maximum simultaneous transfers permitted.

   This allows you to limit the replication activity on that target. This field defaults to the maximum number of transfers allowed by the VLS.
9. The Maximum TCP/IP Bandwidth for this replication target defaults to Unlimited; enter a value in Mb/second if you want to limit the bandwidth.

   Adding a limit restricts the total bandwidth used by this replication target regardless of the number of jobs running or on which nodes the jobs are executing. For example, if one job is running it uses the total bandwidth allowed; if two jobs are running they split the total bandwidth allowed. It is possible to set the total bandwidth limit to a value greater than what your network supports. In this case, the behavior is the same as if the Maximum TCP/IP Bandwidth is set to Unlimited.
10. Select a Compress option from the pull-down field.

    The options are Global Setting, Yes (compression is on), and No (compression is off). See Setting the Global LAN/WAN Replication Target Configuration (page 78) to set the global default.
11. Enter a registration password, and then retype it in the next field.
12. Select **Add Availability Windows** to open a new screen.

    This takes you to a new screen.
13. In the Add Availability Window section of the screen, select the day and enter the time the replication process should begin.
14. Enter the allowable duration of the replication jobs in hours and minutes.

    Replication jobs can only begin during the availability window. When the availability window ends, any replication jobs currently in progress will continue until they complete. No replication jobs can begin until the next availability window opens.
15. Click **Add**.

    The window refreshes, and the availability window you just added is moved to the Current Availability Windows section of the screen.

    Repeat steps 12 through 14 for as many availability windows as you need.
16. Click **Submit**.

    The screen returns to the selected library's list of LAN/WAN replication targets.
17. Assign the LAN/WAN replication target to the source library. See Managing a LAN/WAN Replication Library (page 53).

NOTE: When you configure a virtual library as a LAN/WAN replication target with Echo Copy, you may also need to hide it (e.g., using LUN masking or port mapping/zoning) from the front-end SAN in the case where the same backup application instance sees both the source and destination VLS devices. (The backup application must not see the same tape barcode in two places at the same time.) See LUN Mapping (page 112) for details.

Viewing the Replication Target Slot Details

On the navigation tree, select **Slots** from the expanded replication target list to view the replication target slots. The screen displays the barcode and last successful echo copy for each slot.

The last successful echo copy is intended to notify you of problems with the echo copy, but is not necessarily related to the Cartridge Status or Last Mirrored fields on the Summary for Slots or

Summary for Cartridges screens. The state can be “unknown” when only the header transferred to the tape, when nothing transferred to the tape, during the transfer of data, or when a data transfer has failed.

Setting the Global LAN/WAN Replication Target Configuration

1. Click the **Automigration/Replication** tab.
2. In the navigation tree, expand **Configuration Summary**.
3. Select **Global LAN/WAN Target Configuration**.
4. From the **Default Compression Setting for LAN/WAN Replication Targets** menu, select whether the compression for LAN/WAN replication targets is on (Yes) or off (No) by default.

   If your network has a WAN accelerator that performs compression installed between the source VLS and the target VLS, setting this to No will usually speed up data transfers during replication.
5. Enter a new port number for unencrypted data transfer *only* if you need to change it from the default.

   Your firewall may require that the data transfer use a different port number.
6. Click **Submit**.

Editing a LAN/WAN Replication Target

To edit the LAN/WAN replication target settings:

1. Select the **Automigration/Replication** tab.
2. Expand **LAN/WAN Replication Targets** on the navigation tree, and then select the target of interest. The **LAN/WAN Replication Target Details** screen displays.
3. Select **Edit** from the task bar.
4. On the **Edit LAN/WAN Replication Target Settings** screen, edit the target settings as needed. For an explanation of the settings, see Creating a LAN/WAN Replication Target.
5. Select **Submit**.

To edit the slot mapping, see Changing the Slot Mapping for a LAN/WAN Library (page 63).

To edit the availability window:

1. Follow steps 1 through 3 above.
2. Select **Edit Availability Windows** from the task bar to open that screen.

   The **Edit Availability Windows** screen displays.
3. To delete a availability window, select **Delete** in the row of that policy window in the **Current Availability Windows** section of the screen.
4. To add a availability window, enter the information in the **Add Availability Window** section of the screen, and then select **Add**.

   Repeat this step for as many availability windows as you need.

   NOTE: When adding multiple availability windows, you must select **Add** for each new availability window or the system will not record it.
5. Select **Submit**.

Deleting a LAN/WAN Replication Target

1. Select the **Automigration/Replication** tab.
2. Expand **LAN/WAN Replication Targets** on the navigation tree.
3. Select the LAN/WAN replication target you wish to delete.
4. On the **LAN/WAN Replication Target Details** screen, select **Delete** on the task bar.

5. Select **OK** from the dialog box.

   The **LAN/WAN Replication Targets** screen displays with the deleted target removed from the list.

Changing the LAN/WAN Replication Target Password

You may need to change the LAN/WAN replication target's password in the event of a security breach. The following steps will stop all communication between the source and the target, and then re-establish secure communication.

1. Change the password on the LAN/WAN replication target.

   See Editing a LAN/WAN Replication Target (page 78) to reach the **Edit LAN/WAN Replication Target Settings** screen. Enter a new password for the target.

2. Change the LAN/WAN replication target's password on the source to the new password.

   See Managing a LAN/WAN Replication Library (page 53) to reach the **Re-manage LAN/WAN Library** screen. Enter the same password you just created for the target.

Clearing the Source VLS from the LAN/WAN Replication Target

You may want to clear the connection between a source library and its LAN/WAN replication target in order to use the target with a different source library. The target library maintains all of its default settings in the change.

On the destination library:

1. Select the **Automigration/Replication** tab.
2. Expand **LAN/WAN Replication Targets** on the navigation tree.
3. Select the LAN/WAN replication target you wish to clear from its source.
4. On the **LAN/WAN Replication Target Details** screen, select **Clear Managed Source VLS** on the task bar.
5. The screen refreshes, and a message indicates that the connection has been cleared.
6. Connect the target with a different source library. See Managing a LAN/WAN Replication Library (page 53).

NOTE: Clearing the connection leaves both the source and destination libraries intact. This is different from unmanaging a library, where the source library is deleted.

Automigration/Replication Reporting

The VLS stores job status and history for all automigration and replication jobs, allowing reports to be generated and displayed online or exported in a comma-separated values (CSV) file format. You can customize and view job status and history reports for the VLS automigration feature in Command View VLS.

Status of all Cartridges

The **Summary of All Cartridges Managed by Automigration/Replication** screen provides a quick view of the status of all cartridges that are managed by automigration/replication. Each managed cartridge is counted among only one of the listed statuses with the exception of the first status which can contain cartridges listed elsewhere.

Echo Copy Pool Summary:

- **Not migrated in Copy Pools notification limit** — contains cartridges that have not successfully mirrored within the time limit set for the echo copy pool (assigned in the policy when the echo copy pool is created). A successful mirror is a cartridge that transitions from the “Backup Postprocessing” state to the “Up to Date” state with several intermediate states. A notification is sent once a day that identifies the number of cartridges that have not successfully mirrored within the threshold time.

Cartridges in this category can also be listed in the following categories: Mirror Failed, Pending, Mirror Active, In Use/Deduplicating, and Waiting for Policy Window. This category displays a green (no cartridges in this category) or red (one or more cartridges in this category) icon.

- **Mirror failed — Corrective action needed** — contains cartridges for which the copy to the mirror has failed. This category displays a green (no cartridges in this category) or red (one or more cartridges in this category) icon.
- **Not migrated in Deduplication timeout limit/Forced Copies** — contains cartridges that have not successfully migrated in the deduplication timeout limit and cartridges currently being "forced" into a whole cartridge (non-deduplicated) copy.
- **In Use/Deduplicating** — contains cartridges that are currently being used by the system.
- **Pending** — contains cartridges that are ready for copy but have not started, for example, because the system does not have enough resources available or because they are waiting for the dependent cartridges to replicate.
- **Paused** — contains cartridges that have been paused.
- **Waiting for policy window** — contains cartridges that are waiting for the policy window to open for replication to begin.
- **Mirror Active** — contains cartridges that are currently copying to the destination library.
- **Mirror Complete** — contains cartridges that have completed copying to the destination library.
- **Waiting for first backup** — contains cartridges that do not yet have a stored backup.
- **Initializing** — contains cartridges that are currently initializing.

Target Copy Pool Summary:

- **Mirror Active** — contains cartridges that are currently copying to the mirror.
- **Mirror Complete** — contains cartridges that have completed copying to the mirror.

Use the **Group By** menu to filter the status list, or click a particular status to view the summary list of cartridges that it contains.

Summary of Cartridges by Status

Selecting a particular status from the Cartridge Status screen opens the **Summary of <category> Cartridges** screen. The summary screen displays the cartridge barcodes and other information such as the local library and destination library for each cartridge.

There are a number of tasks available in the task bar of the cartridge summary screens, and the tasks displayed depend on the Cartridge Status category in which the cartridges belong.

- Copy Now — see Forcing a Replication Job (page 69).
- Non Deduplicated Copy — see Copying the Whole Cartridge Outside of the Policy Window (page 75).
- Forced Non Deduplicated Copy — see Copying the Whole Cartridge Outside of the Policy Window (page 75).
- Reset Deduplication Timer — resets the system's timer (default is 48 hours). If the time limit is reached again, the system forces a whole cartridge replication.
- Refresh — refreshes the current screen.
- Restart Broken Mirror — see Restarting a Broken Mirror (page 61).
- Restore Media — see Restoring from a LAN/WAN Virtual Cartridge (page 60).
- Pause Job — pause one or more Mirror jobs. See (page 76).

- Cancel Job — cancel one or more Mirror jobs. See (page 76).
- Resume Job — resume one or more paused Mirror jobs. See (page 76).

From the summary screen you can also click a specific barcode or an echo copy pool to see the details of that selection.

Cartridge Details

View the details of a particular cartridge by clicking the barcode from the cartridge summary screen. The details include the last time the cartridge was in the In Sync state, the current physical and logical size, and the job history.

Some Cartridge Status categories provide a section of Additional Details on the cartridge details screens. The additional details depend on the category. For example, cartridges in the Pending category display a list of dependent cartridges while cartridges in the Out of Sync category display whether or not the cartridge is ready to replicate.

You can export the details displayed on the screen to a text file by selecting **Export Cartridge Details** in the task bar.

You can view the activity log of the cartridge, which lists the important events, operations, and state transitions, by selecting **View Log** in the task bar. The list displays the most recent activity first. To download the entire log file, select **Export Log File** from the task bar.

Configuring the Cartridge Status

To configure the cartridge status (Summary of all Cartridges Managed by Automigration/Replication) screen:

1. Select the **Automigration/Replication** tab.
2. In the navigation tree, expand **Configuration Summary**.
3. Select **Cartridge Summary** from the expanded list.
4. Enter the time you want the system to check for cartridges not migrated within the copy pools threshold limit. Use the HH:MM format, then select AM or PM from the list. Each day, at the specified time, if one or more cartridges have not migrated within the threshold limit, the system sends a notification that indicates the number of cartridges that have not migrated in time.
5. Check the Send Notification box if you want a notification when cartridges are not migrated in the copy pools threshold limit. (Unselect it to cancel notifications.)
6. Click **Submit**.

Viewing the Current Status of Jobs

To view the current status of jobs:

1. Select the **Automigration/Replication** tab.
2. In the navigation tree, select **Job reporting**.

The screen opens to the Current Status report which displays information on all pending and active automigration jobs. The report includes:

- Barcode
- Action – pause, resume, or cancel job (see (page 76))
- Job type – Mirror Preprocessing or Mirror
- Start time
- % complete
- Time of the last update
- Source and target locations

- The node the job is running on
- Status – active or pending
- Expected completion time
- The drive the job is running on

Change the number of rows displaying on the screen using the Page Size menu. You can also use the Filter by View menu to display a specific, predefined set of information; see Configuring Automigration Job Reports (page 82) to create the views. After making a choice from one or both of these menus, click **Refresh**.

Configuring Automigration Job Reports

The **Configuration** screen allows you to assign default settings for reports.

1. Select the **Automigration/Replication** tab.
2. In the navigation tree, expand **Configuration Summary**.
3. Select **Job Reporting Configuration** from the expanded list.

You can customize the following defaults:

- Refresh time for the display (1 to 15 minutes)
- Duration of the job status graphs to display (1 to 90 days)
- Reporting data retention period (1 to 90 days)
- Duration of the CSV format export file (1 to 90 days)
- Name for the CSV format export file

You can also create a pre-defined custom view based on the locations you choose:

1. Select a location category.
2. Select the specific locations of interest from the **Available Locations** box. You can select multiple devices by using Ctrl+click.
3. Using the **>>** button, or by double-clicking, move the locations of interest into the **Selected Locations** box. These are the locations that will display in the report. You can use **<<** button to remove locations from the **Selected Locations** box.
4. Select another location category and repeat steps 2 and 3.
5. Enter a name for this view in the Create a New View field.
6. Select **Create View**. This view is now available as a selection in the Views list on the **Job History** screen.

To update an existing view, select it from the Update existing view list, adjust the selected locations, rename the view (if desired) in the name field, and select **Update View**. Select **Delete View** if you want to remove that view from your pre-defined options.

At any time, you can change any of these default settings.

Viewing the Job History

The **Job History** screen displays the history of the completed library jobs. It defaults to SAN jobs only, and displays the number of days set as the default on the **Configuration** screen.

The job history table displays for each job:

- Barcode
- Start and end times
- Size in MB
- Data transfer time
- Total processing time

- Transfer rate
- Source and target locations
- The node the job is running on
- Completion status
- Compression (yes or no)

The performance graph maps the MB per second against the time it took the jobs to complete.

To change the jobs included in the job history report, select a View previously created on the **Configuration** screen. If you haven't set up any views:

1. Select a location category. The options are SAN, LAN/WAN, All locations, and predefined Views.
2. Select the specific locations of interest from the **Available Locations** box. You can select multiple devices by using Ctrl+click.
3. Using the **>>** button, or by double-clicking, move the locations of interest into the **Selected Locations** box. These are the locations that will display in the report. You can use **<<** button to remove locations from the **Selected Locations** box.
4. Enter the number of days the report should include.

   NOTE: Changing the number of days here does not affect the default number set on the **Configuration** screen.

5. Select a new location type; the default is Both. You can change the report to include only the jobs where the selected devices acted as:
   - Target — the selected device receives the data.
   - Source — the selected device sends the data.
6. Select **Update**. The job history table and performance graph update to include jobs based on the new criteria.

Exporting the Job History to a CSV File

The CSV export file is a text file, delivered as a .zip. Each line is the record for one device, and the data fields are separated by commas or columns depending on the program used to view the file.

You can export the data currently displayed in the history by selecting **Export Displayed Data** from the task bar, or select **Export All Data** which allows you to choose the number of days included in the exported file. In both cases, the **File Download** window opens for you to determine where to save the file.

Viewing the Job Summary

On the **Job Summary** screen you can see the number of successful, failed, and rescheduled jobs both coming in and going out from the current device. By default, it displays one day of data with the device acting as the Source.

To change the display, change the number of days for which you want to see the summary, and/or select to view the device data as it acts as the Target, and select **Update**. The table refreshes to reflect the new information.

You can export the data currently displayed by selecting **Export Displayed Data** in the task bar.

Configuring the GUI Displays

The **Automigration/Replication GUI Configuration** screen allows you to assign default settings for certain GUI displays.

1. Select the **Automigration/Replication** tab.

2. In the navigation tree, expand **Configuration Summary**.
3. Select **GUI Configuration** from the expanded list.
4. In the Default Number of Rows in Slot/Cartridge Table box, enter the number of table rows you want to display on the slot and cartridge summary screens. Changing the number of rows to display from the actual display screens does not change the default value added here.
5. In the Default Number of Rows in Job box, enter the number of table rows you want to display on the job screens. Changing the number of rows to display from the actual display screens does not change the default value added here.
6. In the Default Refresh Time for GUI Pages box, enter the frequency in minutes that you want the GUI screens to refresh.
7. Click **Submit**.

Testing the VLS Connectivity

The connectivity test allows you to test whether all of the nodes on the source VLS and target VLS can communicate with each other.

To text existing connections, from Command View VLS:

1. Select the **Automigration/Replication** tab.
2. Select **Connectivity Test** from the navigation tree.

   The screen lists all of the VLS systems currently connected to the one you are viewing.
3. Click **Expand** to see the source and target IP addresses. This also shows the status of the last connectivity test.
4. Click **Verify Connection**.

   The screen displays the result of the test (Success or Failure). If the test failed, details are provided.

To test an IP address before replication is set up, from Command View VLS:

1. Follow Step 1 and Step 2 above.
2. Under **Other VLS**, enter the IP address or host name of the intended target.
3. If the target is a multi-node device and you want to test every node, select Check All IPs.
4. Click **Verify Connection**.

   The screen displays the result of the test (Success or Failure). If the test failed, details are provided.

NOTE: The connectivity test only works if the replication target VLS is at the same firmware version or higher than the source VLS.

6 Deduplication

Deduplication is the functionality in which only a single copy of a data block is stored on a device. Duplicate information is removed, allowing you to store more data in a given amount of space and restore data using lower bandwidth links. The HP virtual library system uses *Accelerated deduplication*.

NOTE: The deduplication feature is only available on systems running VLS software version 3.0 or later.

This section describes deduplication including getting deduplication running on your system, configuring deduplication, and viewing reports.

NOTE: See the *HP VLS Solutions Guide* for more detailed information.

How It Works

HP Accelerated deduplication compares the most recent version of a backup to the previous version using object-level differencing code. It places pointers in the earlier version that identify duplicated content in the new version. Deduplication then eliminates the redundant data in the earlier version while retaining the complete, new version. You can improve deduplication performance simply by adding additional nodes.

NOTE: Deduplication takes place after the data has been processed to the backup tapes. Therefore, any data backed up to compression-enabled virtual tape drives (both software and hardware compression) is compressed before it is deduplicated.

The following is an overview of the deduplication process. See the *HP VLS Solutions Guide* for more detailed information.

1. When a backup runs, a data grooming exercise is performed on the fly. Using meta-data attached by the backup application, data grooming maps the content or "objects" of the backup, and assembles a content database. This process has minimal performance impact.
2. After the scheduled backups have completed, the content database is used to "delta-difference" (compare) objects in current and previous backups from the same hosts. There are different levels of comparison. For example, files may be compared using a strong hashing function, while other objects may be compared at a byte level.
3. When duplicate data is found in an older backup, it is replaced by a pointer to the most recent copy of the same data. Because the most recent backup is a full version, you achieve the fastest possible restores.
4. Space reclamation occurs when duplicate data from previous backups is removed from the disk. This can take some time, but results in previously consumed capacity being returned to a free pool on the device.

Getting Deduplication Running on the VLS

This section explains how to get deduplication running on your VLS system including some considerations for setting up the system, installing the firmware, and installing the deduplication licenses.

Considerations

To make the most of the deduplication benefits, review these considerations before setting it up on your VLS system:

- Virtual cartridge sizing — The system cannot deduplicate versions of a backup that are on the same cartridge; the versions are not deduplicated until a new version is written to a different virtual cartridge. Therefore, you want the cartridges to be sized big enough to contain an

entire backup job and to prevent too many backup jobs from piling up on the same cartridge, but small enough that you are not wasting overall cartridge space.

- Additional nodes — For systems with long backup windows, you may want to include additional nodes to speed up the post-processing deduplication. A VLS system using deduplication can support up to six nodes nodes.
- Additional capacity — Because you must store two full backups before the delta-differencing begins, you may want to include additional disk capacity at least the size of the sum of the backups. A VLS system using deduplication can support up to eight arrays with four 1U or 2U nodes.

Installing the Firmware

The deduplication feature requires an upgrade to the VLS firmware version 3.0 or higher. Download the *VLS Firmware and Quick Restore CD Image* appropriate for your VLS system from the HP website, and burn it to a DVD (or CD). Then follow the instructions for using the Quick Restore DVD.

1. Save your configuration settings. See Saving Configuration Settings (page 133).
2. Download the *VLS Firmware and Quick Restore CD Image* appropriate for your VLS system from the HP website.
3. Burn the image to CD to create your own Quick Restore DVD.
4. Follow the Recovering from Operating System Failure (page 230) procedure for re-installing the operating system, including the instructions specific to restoring primary nodes.

NOTE: You must install the Quick Restore DVD on each node of the VLS.

Installing the Deduplication Licenses

The deduplication feature is a licensed option. The number of deduplication licenses must match or exceed the number of capacity licenses (based on LTU) on the VLS device. See Installing Additional Licenses (page 48) for installation instructions.

After installing the required deduplication licenses, the VLS automatically reboots. When the system is back up, it first checks the standard capacity licenses and then the deduplication licenses. Once the deduplication licenses are verified, the deduplication feature is automatically enabled for all supported backup types.

No further setup is required. When the next backup begins, the deduplication process begins mapping the content of that backup. After the second backup, the system delta-differences (compares) the two backups and the deduplication proceeds.

You may choose to disable some backup types; see Configuring Deduplication Options (page 86) for details.

Configuring Deduplication Options

You can include or exclude specific backups or types of backup (e.g., server type) from the deduplication process and choose the deduplication algorithm used.

NOTE: These options are not available until you have installed the appropriate number of deduplication licenses.

1. Select the **System** tab.
2. On the navigation tree, navigate to **Chassis→Deduplication→Configuration** .

   The **Configuration** screen displays.
3. For each data type, select the appropriate deduplication algorithm from the list. The defaults depend on the backup application and the file type; in each case, the algorithm most likely

to result in the best deduplication ratio is used. Depending on your current setting, the options are:

- Backup — Useful when file-level differencing is less space efficient (for example, if the file server is full of very small files).
- File — Useful for file servers.
- Enhanced Backup — Useful for databases that are:
  - Striped
  - Multiplexed
  - Large (greater than 14 TB)
  - Flat-file with deduplication speed or ratio problems

  NOTE: Once you change the algorithm from Backup to Enhanced Backup, you cannot revert to Backup again. However, you can still disable the policy.
- Enabled — Available if the algorithm is currently set to Disabled.
- Disabled — Turns off deduplication.

4. Select Policy-Based Matching for data types where appropriate (unchecked by default).

   With this option, the deduplication algorithm compares data sets based on the backup policy (job) name, and then compares them based on the client name, before deduplicating. Leave this unchecked to have the deduplication engine match the data sets based on the client name only.
5. Click **Update**.

   The screen refreshes and updates the information.

NOTE: You can set the backup algorithm at the individual backup job level. On the **Configuration** screen, select a specific data type to display all the backup jobs of that type, then follow Step 3 through Step 5 above.

Editing the Data Protector Configuration

Data Protector adds one suffix to the backup job names of full backups and a different suffix to the backup job names of incremental backups. Because the job names are not identical, full backups will not deduplicate against incremental backups. However, you can set up deduplication to strip off the suffixes so the two types of jobs will deduplicate.

From Command View VLS:

1. Select the **System** tab.
2. In the navigation tree, select **Chassis**. The chassis details screen opens
3. Under the **Maintenance Tasks** list, select **System Maintenance**.
4. From the task bar, select **Edit Data Protector Configuration**.
5. Enter the suffix of the full backup job names in the text box.
6. Select **Submit**. The suffix appears in a list beneath the text box.
7. Enter the suffix of the incremental backup job names in the text box.
8. Select **Submit**. The suffix is added to the list on the screen.
9. Repeat this procedure for all of the suffixes you want deduplication to ignore.
10. When you have added all of the necessary suffixes, select **Return**.

Viewing Deduplication Statistics and Reports

In Command View VLS, you can view statistics on the deduplication process by summary, backup report, cartridge report, or system capacity.

Deduplication Summary

The **Deduplication Summary** displays a graph depicting the storage savings achieved with data that has been fully deduplicated.

1. Select the **System** tab.
2. Select **Chassis** on the navigation tree to expand it.
3. Select **Deduplication**.

   The deduplication summary displays.

   In the graph displayed, the *logical data* is the uncompressed physical size of all user data that has fully deduplicated; the *used capacity* is the actual physical storage space consumed by the original data after it has been both compressed (if enabled) and fully deduplicated.

Deduplication Backup Report

The backup report provides information on the deduplication of your backup jobs.

1. Select **Backup Report** from the navigation tree or from the task bar of the **Deduplication Summary** screen.

   The backup report options display.
2. Unselect any agents, backup types, or states you want to exclude from the report. By default, all supported and enabled backup jobs are selected and display in the report.
3. Select **View Backups**.

   The screen displays a list of backup jobs meeting the set criteria and includes the following information:

   - State — the state of the backup job (see below)
   - Backup Name
   - Policy
   - Backup Time
   - Type
   - Logical Size (version 3.4.x) — the size of the backup data sent to the VLS (before deduplication and compression)
   - Physical Size Estimate (version 3.4.x) — the disk space currently used to store the compressed backup, which varies over time as deduplication processes the backup and reclaims redundant disk space
   - Dedupe Ratio Estimate — the estimated deduplication ratio (based on the Logical Size divided by Physical Size Estimate)
4. From the results list, select a backup name to see the backup statistics for that particular job.

   The backup information includes a graph depicting the original data size (shown as zero prior to the deduplication), the deduplicated size, and the unprocessed data. In the **Cartridge Details**, select a barcode to see its cartridge report.

The deduplication reports show the following states:

 Waiting for Next Backup — the backup has nothing to difference against and is therefore waiting for a new backup. Incr/diff backups difference against the new full backup, not the old full backup.

 Delta-diff in Process — the backup has identified another version of itself to difference against and is now running differencing to identify the duplicate data between the two versions. With multi-stream backups, this process may take multiple tries (going back to "Waiting for Next Backup" state each time) until the differencing locates the correct stream.

 Pending Reclamation — the differencing is complete (duplicate data has been identified) and space reclamation is now waiting for full cartridges before it can begin.

 Partially Reclaimed — in a backup job that spanned multiple cartridges, the full cartridges have been space reclaimed but the last tape in the spanned set (which is partially full) is waiting until that tape is full before it can reclaim space.

 Dedupe Complete — deduplication, including all space reclamation, is complete for this backup job.

 No Match Found — indicates backups that cannot be deduplicated because they were unable to match with their previous version due to large-scale modification.

In the detailed Backup and Cartridge reports, the Dedupe Ratio Estimate represents the overall compression ratio (including both deduplication and compression) of that backup/cartridge based on the amount of logical backup data stored versus the amount of physical disk space used. If the backup job status is “Waiting for next backup,” “Delta-diff in Progress,” or “Pending Reclamation,” the ratio will *only* include the compression because deduplication will not have actually space reclaimed that tape and therefore will not have saved any disk space. If the status is “Partially Reclaimed” or “Dedupe Complete,” the backup disk space has been partially or full reduced by deduplication and the ratio represents compression plus deduplication. The Dedupe Estimate in GB follows the same logic.

Deduplication Cartridge Report (version 3.4.x)

The cartridge report provides information on the deduplication of your backup jobs at the cartridge level.

1. Select **Cartridge Report** from the navigation tree or from the task bar of the **Deduplication Summary** screen.

   The cartridge report options display.

2. Select **View** corresponding to the report you want to view. You can view all cartridges, or view a specific barcode prefix or virtual library.

   The screen displays the list of cartridges meeting the set criteria.

3. From the results list, select a cartridge to see all of the backup jobs on that cartridge.

   The report includes the following information:

   - Library
   - Barcode
   - Logical Size — the size of the backup data sent to the VLS (before deduplication and compression)
   - Physical Size — the disk space currently used to store the compressed backup, which varies over time as deduplication processes the backup and reclaims redundant disk space
   - Dedupe Ratio Estimate — the estimated deduplication ratio (based on the Logical Size divided by Physical Size)

NOTE: If a cartridge is full and all jobs on it have been delta-differenced except for one job that is waiting for another backup, you can have the cartridge reclaimed by temporarily disabling the one remaining backup job. Disabling the backup type disables all instances of that backup type on all cartridges that have not yet been delta-differenced. When you re-enable the backup type, it allows deduplication for future instances of that backup type.

Deduplication System Capacity (version 3.4.x)

You can view specific details about the system capacity using deduplication.

Select **System Capacity** from the navigation tree or from the task bar of the **Deduplication Summary** screen.

The screen displays the following information:

- Total physical capacity — the capacity of the entire VLS system
- Reserved for system — the amount of capacity needed to perform system functions (for example, storing the meta-data)
- Usable capacity — the total capacity that can be used for deduplication (Total Physical Capacity minus Reserved for System)
- Used capacity — the capacity currently in use
- Available capacity — the capacity currently available (Usable Capacity minus Used Capacity)
- Logical Data — the amount of backup data sent to the VLS (before deduplication and compression)
- Used Capacity — the capacity currently in use
- System Ratio — the ratio of the Logical Data divided by the Used Capacity
- Space Savings — the percentage of capacity saved by deduplication

7 Operation

This section describes how to power on and power off the VLS nodes and arrays.

Powering On VLS Arrays

The order in which you power up the disk array enclosures in an array is important. Power on the base enclosure last in order to ensure that the disks in the capacity enclosures have enough time to spin completely before being scanned by the RAID controllers in the base enclosure.

CAUTION: Power on only one array enclosure at a time to avoid overloading the AC power source.

To power on an array:

1. Turn both power switches on the rear of each array enclosure to On.

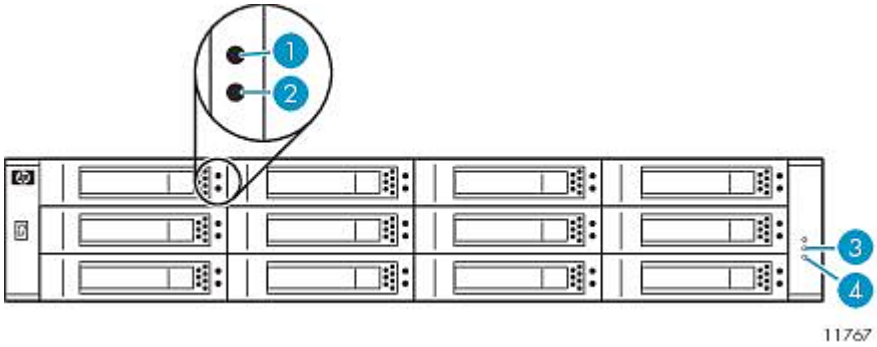
   Some power supply models do not have a power switch; in this case, the power cords were unplugged from the enclosure to power it down. Plug the cords back into the enclosure.

   Start with the capacity enclosure farthest from the base enclosure and working toward the base enclosure. Then power on the base enclosure.

2. If you just replaced a capacity enclosure, check the enclosure ID displayed on the front of the enclosures. Each array contains a base enclosure with an enclosure ID of 0. The capacity enclosure installed just below the base enclosure should have an enclosure ID of 1. The next capacity enclosure down in the rack should have an enclosure ID of 2, and the next should have an enclosure ID of 3. (The numbering works the same way regardless of the number of enclosures in your system.) If the enclosure IDs displayed are not correct after replacing a capacity enclosure, you must rescan the enclosures and assign them enclosure IDs based on their rack positions. Follow these steps from Command View VLS:
   a. Click the **System** tab.
   b. Select the disk array in the navigation tree with the new capacity enclosure.
   c. Record either RAID controller's IP address displayed on the disk array details window.
   d. Open a secure shell session. See "Opening a Secure Shell Session" (page 102).
   e. Telnet to one of the RAID controllers in the array by entering: `telnet <IP address of RAID controller>` and then press **Enter**.
   f. At the `Login as:` prompt, enter `manage` and then press **Enter**.
   g. At the `Password:` prompt, enter `!manage` and then press **Enter**.
   h. Enter `rescan` and then press **Enter**.
   i. Verify that the new capacity enclosure's ID is correct.
   j. Power off the new capacity enclosure, leaving the power switch off for at least 60 seconds. Then, power the capacity enclosure back on.
3. Confirm that the disk array enclosures are all functioning normally by observing the condition of their status LEDs. The LED status should match those shown in the following tables.

   If an LED status does not match the status shown in the following tables, a component needs attention.

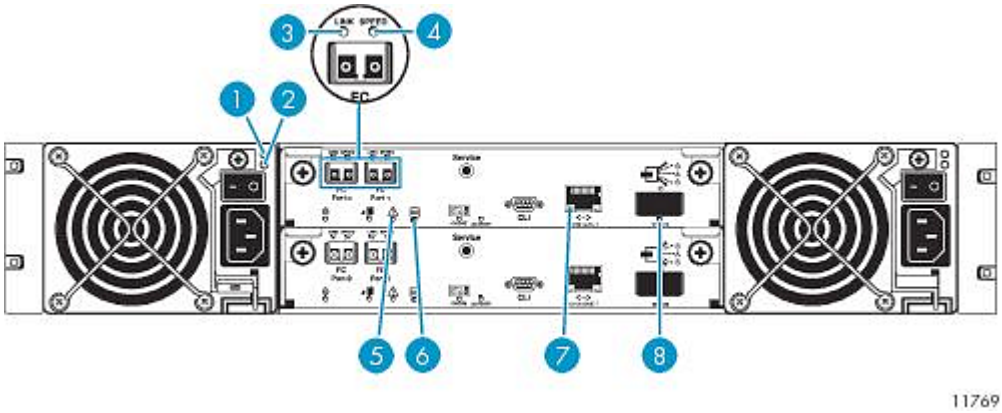
Figure 2 Base and Capacity Enclosure Front Panel LED Status – Normal Operation



Item	Location	LED	LED state
1	Hard drives	Status (blue or yellow)	Off or blue
2		Power/Activity (green)	On or blinking
3	Right ear	Fault/Service Required	Off
4		Power On/OK	On

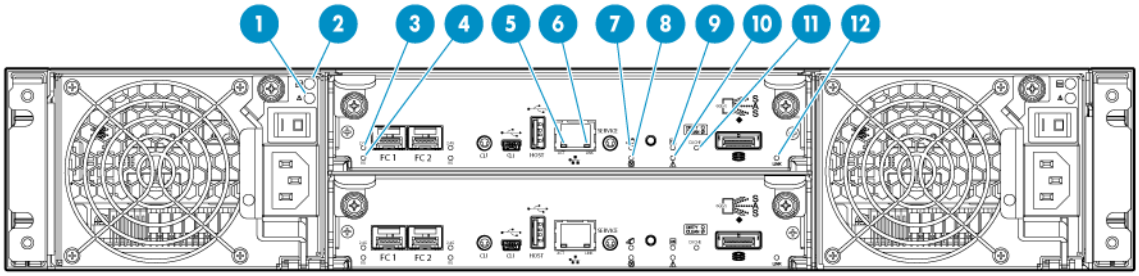
NOTE: The hard drive LEDs may not immediately illuminate when the enclosure is powered on. The LEDs illuminate after the hard drives are configured by the VLS firmware.

Figure 3 VLS9000 Base Enclosure Rear Panel LED Status – Normal Operation



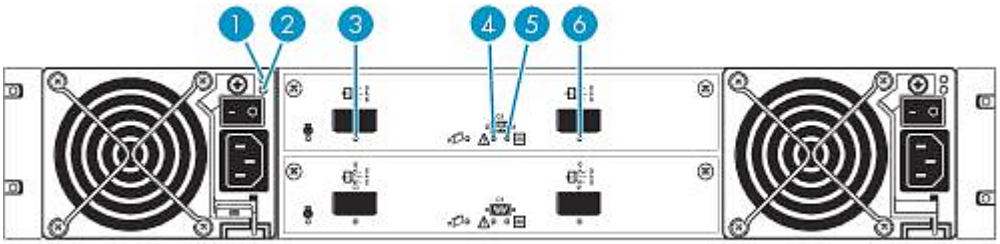
Item	Location	LED	LED state
1	Power module	AC Power Good (green)	On
2		DC-Fan Fault/ Service Required (yellow)	Off
3	RAID controller	FC link status (L) (green)	On
4		FC link speed (S) (green)	On
5		Fault/Service required (yellow)	Off
6		Power On/OK (green)	On
7		Ethernet link status (green)	On
8		Expansion port status (green)	On

Figure 4 VLS9200 Base Enclosure Rear Panel LED Status – Normal Operation



Item	Location	LED	LED state
1	Power module	Voltage/Fan Fault/Service Required (amber)	Off
2		Input Source Power Good (green)	On
3	RAID controller	Host 2/4 Gb FC Link Status/Link Activity (green)	On, if link speed is 2 or 4 Gbps
4		Host 8 Gb FC Link Status/Link Activity (green)	On, if link speed is 8 Gbps
5		Network Port Activity (green)	On
6		Network Port Link Status (green)	On
7		OK to Remove (blue)	Off
8		Unit Locator (white)	Off
9		FRU OK (green)	On
10		Fault/Service Required (amber)	Off
11		Cache Status (green)	On, if cache contains unwritten data Off, if cache does not contain unwritten data
12		Expansion Port Status (green)	On

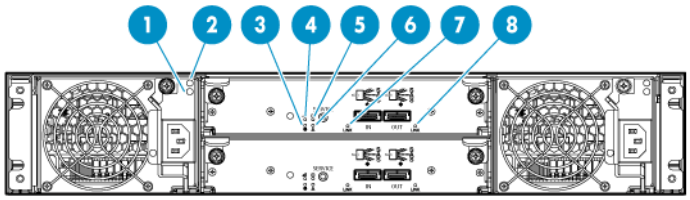
Figure 5 VLS9000 Capacity Enclosure Rear Panel LED Status – Normal Operation



Item	Location	LED	LED state
1	Power module	AC power good (green)	On
2		DC-Fan Fault/Service Required (yellow)	Off
3	Expansion controller	SAS In port status (green)	On
4		Fault/Service Required (yellow)	Off

Item	Location	LED	LED state
5		Power On/OK (green)	On
6		SAS Out port status (green)	On

Figure 6 VLS9200 Capacity Enclosure Rear Panel LED Status – Normal Operation



Item	Location	LED	LED state
1	Power module	Voltage/Fan Fault/Service Required (amber)	Off
2		Input Source Power Good (green)	On
3	Expansion controller	Unit Locator (white)	Off
4		OK to Remove (blue)	Off
5		FRU OK (green)	On
6		Fault/Service Required (amber)	Off
7		SAS In Port Status (green)	On
8		SAS Out Port Status (green)	On

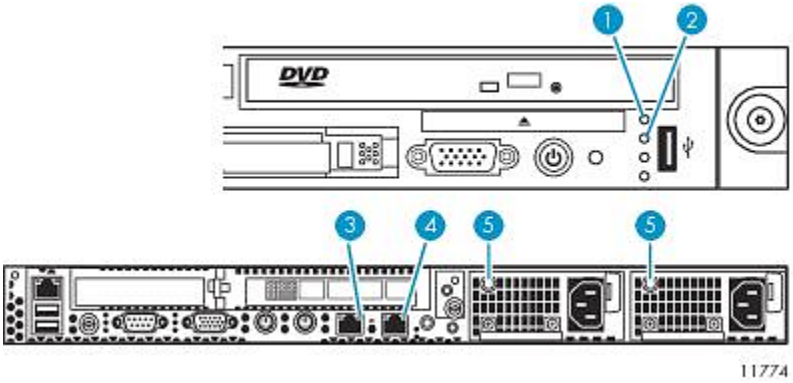
Powering On the VLS System

To power on the system:

1. Power on the two private LAN switches connected to the VLS. (VLS9000 7.5 TB and 10 TB systems only include one LAN switch.)
2. Power on the two private Fibre Channel switches connected to the VLS. (VLS9000 7.5 TB and 10 TB systems do not include Fibre Channel switches.)
3. Power on all arrays in the VLS. See "Powering on VLS Arrays" (page 91).
4. Press the Power On/Standby button on all of the secondary nodes.
5. After the secondary nodes are powering up, press the Power On/Standby button on the primary node.
6. Confirm that the VLS components are all functioning normally and the VLS is cabled correctly by observing their status LEDs.

   The LED status should match those shown in the following table. If it does not, a component needs attention.

Figure 7 VLS Node LED Status During Normal Operation



Item	Description	Status
1	Internal health LED	LED is green.
2	External health LED (power supply)	LED is green.
3	NIC 1 link LED	LED is green if primary node. LED is off if secondary node.
4	NIC 2 link LED	LED is green.
5	Power supply LEDs	LED is green.

7. Rebooting the system is complete when you receive the "Initializing node#", then "Initializing for node# completed." messages for all nodes in the systems notifications in Command View VLS.

NOTE: Under problem conditions, you can use iLO Standard (non-licensed) to power on the system. You can also use it to determine if the nodes are powered on or off.

Rebooting the VLS System

From VLS CLI:

1. Verify that any backup or restore operation has completed and that the VLS is idle.
2. Open a secure shell session and log in as the administrator. See "Opening a Secure Shell Session" (page 102).
3. Initiate a reboot of the VLS by entering:

   ```
   restartSystem
   ```

From Command View VLS:

1. Verify that any backup or restore operation has completed and that the VLS is idle.
2. Click the **System** tab.
3. Select **Chassis** in the navigation tree.
4. Under **Maintenance Tasks**, select **System Maintenance**.
5. Select **Restart All Nodes** from the task bar.

   Restart Head Wizard displays.
6. Select **Yes** to reboot all nodes.

△ **CAUTION:** Rebooting the VLS device places the VLS cartridges back into the same library slots and tape drives they were in at the time of reboot. To move the cartridges from tape drives back into the appropriate slots, use **Force Unload** from the task bar visible when you select the tape drive from the navigation tree.

Powering Off the System

WARNING!  To reduce the risk of personal injury, electric shock, or damage to the equipment, remove the power cord to remove power from the node before removing the access panel. The front panel Power On/Standby button does not completely shut off system power. Portions of the power supply and some internal circuitry remain active until AC power is removed.

From the VLS CLI:

1. Verify that any backup or restore operation has completed and that the VLS is idle.
2. Initiate a shutdown of the VLS by entering:

   ```
   shutdownSystem
   ```

   The primary node will report when it has powered down. Amber system power LEDs indicate that nodes are in standby mode.
3. Press the **Power On/Standby** button on any nodes not in standby mode. Amber system power LEDs indicate that nodes are in standby mode.
4. If removing the access panel from a node:
   a. Wait until the VLS has completed its shutdown operation, then press the UID LED button on the front of the node. Blue LEDs illuminate on the front and rear panels of the node.
   b. Go to the back of the rack and locate the node by identifying the illuminated rear UID LED button.
   c. Unplug the node AC power cords from the power source. The node is now without power.

From Command View VLS:

1. Verify that any backup or restore operation has completed and that the VLS is idle.
2. Under the System tab, select **Chassis** in the navigation tree.
3. Under **Maintenance Tasks**, select **System Maintenance**.
4. Select **Shutdown All Nodes** from the task bar.

   Shutdown Head Wizard displays.
5. Click **Yes** to shut down all nodes.
6. If removing the access panel from a node, wait until the VLS has completed its shutdown operation, then press the UID LED button on the front of the node.

   Blue LEDs illuminate on the front and rear panels of the node. Amber system power LEDs indicate that nodes are in standby mode.
7. Press the **Power On/Standby** button on any nodes that are not in standby mode.
8. If removing the access panel from a node:
   a. Go to the back of the rack and locate the node by identifying the illuminated rear UID LED button.
   b. Unplug the node AC power cords from the power source. The node is now without power.

NOTE: Under problem conditions, you can use iLO Standard (non-licensed) to power off the system. You can also use it to determine if the nodes are powered on or off.

Powering Off VLS Arrays

CAUTION: Always power off the system before disconnecting disk array cables or powering off a disk array enclosure to prevent the appliance from erroneously detecting a disk array RAID volume failure.

NOTE: It is not necessary to power off a disk array enclosure when replacing a power module, hard drive, RAID controller, or expansion controller.

To power off a VLS array:

1. Power off the system. See "Powering Off the System" (page 96).
2. Turn both power switches on the rear of each disk array enclosure off. Some power supply models do not have a power switch; in this case, power down the enclosure by unplugging the power cord from the enclosure.

   Always power off the base enclosure first. Then power off the capacity enclosures, starting with the capacity enclosure at the beginning of the SAS chain and working away from the base enclosure.

8 User Interfaces

This section describes the three user interfaces (UIs) that can be used to configure, manage, and monitor the VLS over the web, remotely over the LAN, or through a serial connection. It also provides instructions on how to open and close a connection to the VLS for each type of user interface.

User Interface Requirements

VLS user interfaces lists the VLS user interfaces and their requirements. Of the three user interfaces, Command View VLS should be used in most circumstances. It is the most intuitive and easiest to learn and use.

Multiple user interface sessions may be open at once.

Table 13 VLS user interface requirements

User interface	Requirements	Configuration	For more information
Command View VLS	PC or workstation network attached to the VLS node 0 running Microsoft Internet Explorer 6.0 or higher, or Netscape Navigator 4.7 or higher.	10/100/1000 BaseT Ethernet port configured with an appropriate IP address, host name, domain name, subnet mask, and gateway. Can login as Administrator or User.	See Command View VLS (page 98).
Secure shell (ssh)	Secure shell client (such as PuTTY) network attached to the VLS node 0.	10/100/1000 BaseT Ethernet port configured with an appropriate IP address, subnet mask, and gateway. Can login as Administrator only.	See Secure Shell and Serial User Interfaces (page 101).
Serial	Null-modem cable attached to the VLS node 0 and terminal emulation program (such as Windows Hyperterminal™) configured to 115200 baud.	Only one serial connection at a time is permissible. Can login as Administrator or Emergency user.	See Secure Shell and Serial User Interfaces (page 101).

Command View VLS

Command View VLS is a web browser-based GUI that you can use to configure, manage, and monitor your VLS through a LAN. Command View VLS provides the following:

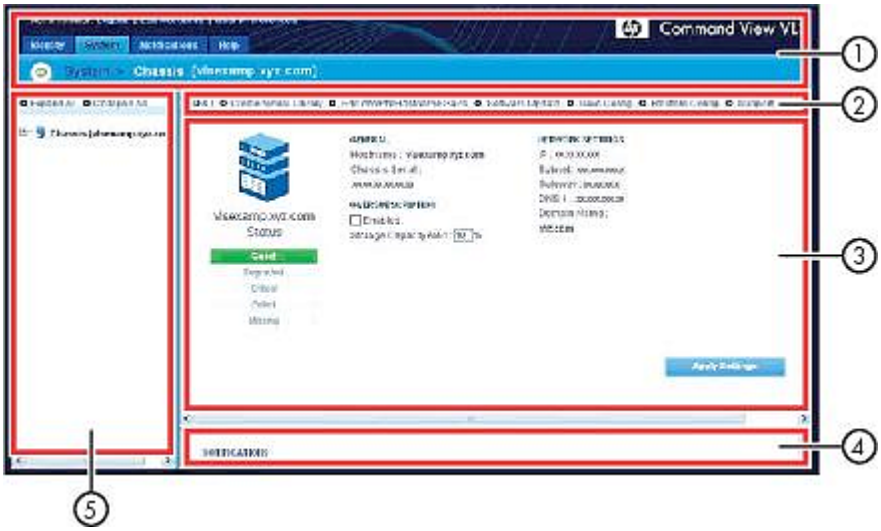
- Configuration and management of VLS virtual devices (libraries and tape drives) and cartridges, including LUN masking and LUN mapping
- Changing of the default Fibre Channel host port settings
- Viewing and deleting VLS notification alerts
- Configuring VLS mail and SNMP notification alert settings
- Editing VLS account passwords
- Enabling and disabling storage capacity oversubscription
- Managing storage pools
- Establishing automigration policies and copy pools, and performing destination library operations
- Viewing VLS hardware and virtual device status

- Installing VLS firmware updates
- Saving and restoring VLS network settings and virtual library configurations
- Restarting VLS device emulations and Command View VLS
- Viewing and saving VLS trace log files

Command View VLS is installed on the VLS and communicates through the LAN. Users can open a Command View VLS session from a web browser on the LAN, or HP Systems Insight Manager.

Window Regions

Command View VLS windows consist of five regions. Not all regions are displayed on all windows.



Item	Description
1	status banner
2	task bar
3	status pane
4	notifications pane
5	navigation tree

NOTE: You can enlarge or reduce any region on the window. To change the size of a region, position your cursor on the border of a pane, and press the left mouse button while simultaneously dragging the border.

Opening a Command View VLS Session from a Web Browser

NOTE: Before you can open a Command View VLS session, you must set the VLS network settings. See Setting the Network Settings (page 105).

To open a Command View VLS session from a web browser:

1. Launch a web browser.
2. In the web browser URL box, enter:

   `https://<fully qualified name of the VLS>`

NOTE: Entering "`http://<fully qualified name>`" instead of the above URL automatically redirects you to the secure "`https://<fully qualified name>`" connection. All communications are over a secure connection.

3. If a Security Alert window opens and prompts you to accept the Secure Sockets Layer (SSL) certificate, install the SSL certificate as described in Installing the SSL Certificate into your Web Browser (page 100).

   The first time you open a Command View VLS session (and the first time you open a Command View VLS session after changing the fully qualified name of the VLS), a Security Alert window opens and prompts you to accept the Secure Sockets Layer (SSL) certificate.

4. Enter `administrator` or `user` in the **Username** box. The user name is case sensitive.

NOTE: Logging in as administrator gives you full privileges to all VLS functions available through Command View VLS. Logging in as a user gives you only viewing and cartridge management privileges.

5. Enter the appropriate password in the **Password** box for the username entered.

   The default administrator password is `admin`. The default user password is `guest`. The password is case sensitive.

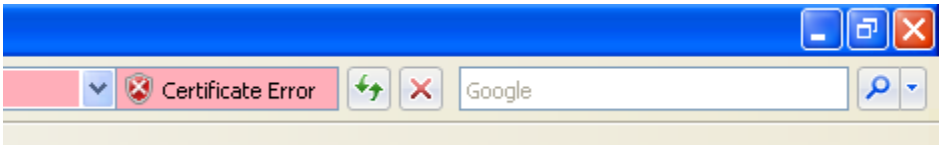
6. Click **Login**.

Installing the SSL Certificate into your Web Browser

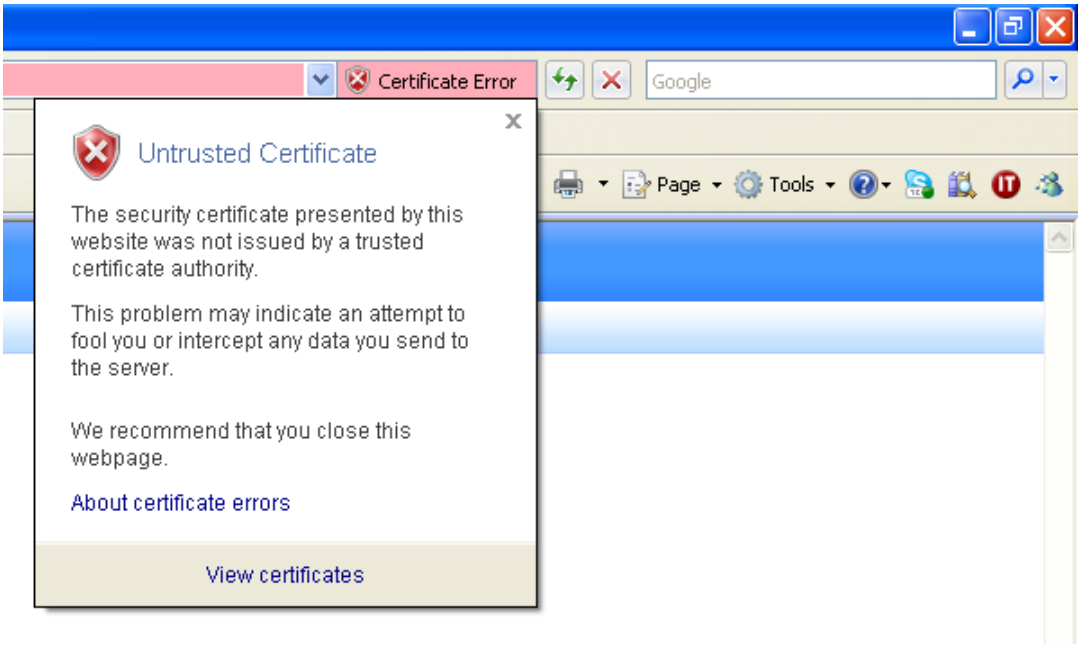
The first time you open a Command View VLS session (and the first time you open a Command View VLS session after changing the fully qualified name of the VLS), a message that reads "There is a problem with this website's security certificate." appears on the screen. Although you can continue to the login screen, you will get this message every time you access the login screen until you install the SSL certificate into your web browser.

The following procedure describes how to install the certificate for Internet Explorer 7. Other browsers may have a different process.

1. Select **Continue to this website (not recommended)**. A pink Certificate Error appears to the right of the URL. (Your browser window may look slightly different from the images below.)



2. Select the Certificate Error. An Untrusted Certificate window opens.



3. Select **View certificates**. A Certificate window opens.
4. Select **Install Certificate...** to launch the Certificate Wizard.
5. Select **Next**.
6. Make sure that **Automatically select the certificate store based on the type of certificate** (the default) is chosen and select **Next**.
7. Select **Finish**.
8. A Security Window opens. Select **Yes**.
9. Select **OK** or **Finish** on each window that displays until the Command View VLS login window displays.
10.

Restarting Command View VLS

To restart Command View VLS:

1. Under the System tab, select **Chassis** in the navigation tree.
2. Under **Maintenance Tasks**, select **System Maintenance**.
3. Click **Restart Command View VLS** in the task bar.

   The **Restart Command View VLS** window opens.
4. Click **Restart** to confirm.

Closing a Command View VLS Session

To close a Command View VLS session, click **Logout** in the status banner or simply close the web browser.

Secure Shell and Serial User Interfaces

The secure shell user interface provides remote configuration and management of your VLS over a LAN using the VLS command-line interface (CLI) command set. The serial user interface provides local configuration and management of your VLS through the serial connector on the rear of the VLS node 0 using the same VLS CLI command set.

A secure shell or serial session provides the following:

- Setting the VLS network settings
- Configuration and management of VLS virtual devices (libraries and tape drives) and cartridges
- Changing of the default Fibre Channel host port settings
- Viewing and deleting VLS notification alerts
- Configuring VLS mail and SNMP notification alert settings
- Editing VLS account passwords
- Enabling and disabling storage capacity oversubscription
- Viewing VLS hardware status
- Saving and restoring VLS network settings and virtual library configurations
- Restarting VLS device emulations and Command View VLS
- Rebooting and powering off the VLS

The serial user interface also provides emergency login access that allows you to change the administrator password if it is forgotten.

Opening a Secure Shell Session

NOTE: Before you can open a secure shell session, you must set the VLS network settings. See Setting the Network Settings (page 105).

To open a secure shell session:

1. Open a secure shell session to the VLS using a secure shell program (such as PuTTY) or by entering:

   `ssh <fully qualified VLS name>` and then press **Enter**.
2. At the `Login as:` prompt, enter `administrator` and then press **Enter**.
3. At the `Password:` prompt, enter the administrator password and then press **Enter**.

   The default administrator password is `admin`.

Closing a Secure Shell Session

To close a secure shell session enter `logout`, `done`, `quit`, `bye`, or `exit`, and then press **Enter**.

Opening a Serial Session

To open a serial session:

1. Connect a PC or workstation to the serial port on the rear of the VLS using the null-modem (serial) cable provided.
2. Establish a CLI session using a terminal emulation program, such as Windows Hyperterminal.
3. Enter `administrator` or `emergency` for username. Both logins gives you full privileges to all VLS functions available through the CLI command set.
4. Enter the administrator or emergency password.

   The default administrator password is `admin`. The emergency password is `repair`.

Closing a Serial Session

To close a serial session, click **Logout** at the top of the Console Manager window. This logs you out of the Console Manager and displays the Logon window.

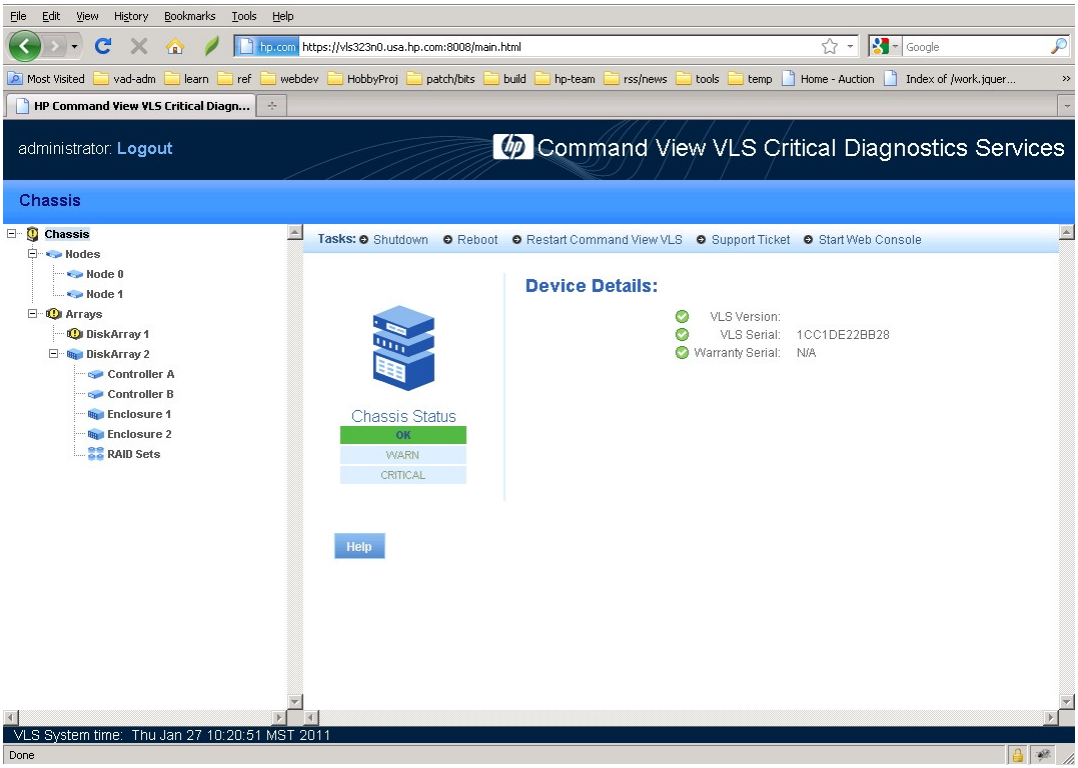
VLS Critical Diagnostics Services

VLS Critical Diagnostics Services is a mini HTTP service built into VLS to provide the status and details of the hardware, console access, and a support ticket service so you can check the VLS vitals before the main GUI is running. You can also use it to examine the VLS if it hangs during a bootup and does not come all the way up. However, you cannot use it to diagnose master node hardware issues or network connectivity issues because this service relies on those to operate.

To access the Diagnostic Services:

1. Go to https://hostname:8008/.
2. Log in using the Command View VLS user name and password.

   At the initial installation, the login default is “administrator” (user name) and “admin” (password). You must change this password within Command View VLS; you cannot change it in the diagnostic services.
3. Wait until all of the hardware components are populated; this can take up to 15 seconds.



In the screen shot above, the Diagnostic Services screen is fully loaded. This system has two nodes and two arrays. Note that there is a problem with array 1.

To view information about any hardware component, select it from the navigation tree; the screen displays the status and details about that item.

Diagnostic Services tasks are available on the task bar:

- Shutdown — shuts down the VLS system as it would from Command View VLS or VLS CLI.
- Reboot — reboots the VLS system as it would from Command View VLS or VLS CLI.
- Restart Command View VLS — restarts Command View VLS.
- Support Ticket

  The support ticket task allows you to generate and download a support ticket. Click **Create New Support Ticket**. The ticket is listed under Active Ticket Collection Process until it completes.

After completion, the ticket is listed under Available Tickets; click **Download** to download the ticket or **Delete** to delete it.

- Start Web Console

  Enter the service (administrator) password. You can use the web console just as you use a serial session when connected to the serial port of the VLS node. The web console may be slower than a serial session depending on the condition of the network.

9 Configuration

This section describes how to configure and manage the VLS network settings, user preferences, Fibre Channel host ports (optional), virtual libraries, tape drives, and cartridges.

Setting the Network Settings

Before you can open a Command View VLS or secure shell session, set the network settings. The network settings can be set using either the VLS discovery utility (see "Setting the Network Settings using the VLS Discovery Utility" (page 105)) or the CLI command set using the serial user interface (see "Setting the Network Settings using the CLI Command Set" (page 106)).

Setting the Network Settings using the VLS Discovery Utility

The VLS discovery utility looks for all the devices on the same subnet as the Windows computer on which it is running. It then lists the devices and indicates whether they are configured (have an IP address) or unconfigured.

You can use the VLS discovery utility to set the network settings on an unconfigured VLS, and to view the network settings of configured devices. The utility can also be used to remove LUNs from the user interface after one or more LUNs are no longer configured or have been removed from the VLS.

NOTE: The VLS discovery utility can only be used to change the network settings on a VLS with no IP address. Once a VLS has an IP address, either through the DHCP or the VLS discovery utility, its network settings cannot be changed using the VLS discovery utility. Use the CLI command set or Command View VLS to change the network settings on a VLS that has an IP address. See "Setting the Network Settings using the CLI Command Set" (page 106).

To set the network settings using the VLS discovery utility:

1. Insert the VLS Documentation CD into the CD drive on a Windows system that is on the same subnet as the VLS.

   The CD auto-launches.

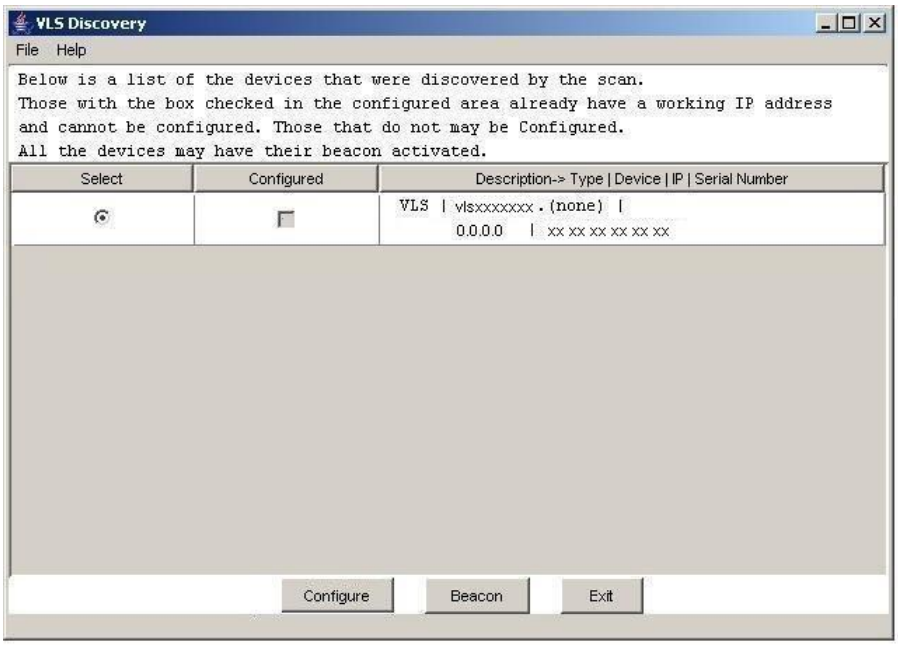
2. Click **VLS discovery utility**.

   The VLS discovery utility opens and lists all the devices it sees on the subnet (Figure 8 (page 106)).

   The **Configured** box for a device is checked if the device has an IP address.

   The device type, host name, IP address (if available), and serial number are displayed for each device listed.

Figure 8 VLS discovery utility — main window



3. To visually identify a device listed, select the device from the list and click **Beacon**. This will illuminate an LED on the device for the specified length of time.

   In the case of the VLS, the UID LED button on the VLS node illuminates.
4. Select the VLS from the list of devices and click **Configure**.

   The Device Configuration window opens.
5. Leave the default host name or enter a new host name in the **Host Name** box.

   The default VLS host name is `VLS<VLS serial number>`.

   The host name cannot contain spaces.
6. Enter an IP address in the **IP Address** box.
7. Enter the subnet mask in the **Subnet Mask** box.

   NOTE: To display the correct subnet mask, gateway, DNS server, and domain name settings for the VLS, open a DOS window on the computer running the VLS discovery utility and type `ipconfig /all`
8. Enter the gateway in the **Gateway** box.
9. Enter the DNS server IP address in the **DNS IP Address** box.
10. Enter the domain name in the **Domain Name** box.
11. Click **Configure** to save the network settings to the VLS.
12. Click **Exit** to close the VLS discovery utility.

Setting the Network Settings using the CLI Command Set

To set the network settings using the CLI command set, set either the:

- DHCP usage and host name, or
- Fully qualified host name (or host name and DNS domain name separately), DNS server address, IP address, gateway, and netmask

To set the network settings using the CLI command set:

1. Open a serial session and log in to the administrator account. See "Opening a Serial Session" (page 102).

2. To see the current configuration settings, at the prompt enter:

   `showConfig`

3. Set each desired configuration value by entering:

   `setConfigValue <-tag> [value]`

   where `<-tag>` can be any of the following:

Tag	Description
`-host`	Host name (such as vlsexamp) (unqualified)
`-domain`	DNS domain name (such as xyz.com)
`-fullhost`	Fully qualified name (such as vlsexamp.xyz.com)
`-dnsaddr`	DNS server address (replaces all addresses with one line)
`-dnsaddr1`	First DNS server address (cannot use with dnsaddr)
`-dnsaddr2`	Second DNS server address (cannot use with dnsaddr)
`-dhcp`	Has no value, indicates you want to configure the public Ethernet connection using DHCP (reset is -dhcp=false)
`-ipaddr`	IP address of public Ethernet connection
`-gate`	Gateway to network (xx.xx.xx.x)
`-mask`	Netmask. Default is 255.255.255.0
`–ntpPrimary`	First NTP Server Address
`–ntpSecondary`	Second NTP Server Address

   NOTE: More than one network value can be set at a time or you can set them individually. To reset a value, enter " " (quoted space) as the value.

   NOTE: If you need to clear the DNS completely, set the DHCP to `false` and enter `0.0.0.0` for both the first and second DNS server addresses.

4. When all the network parameters are set to your desired values, save the settings by entering:

   `commitConfig`

   NOTE: The system automatically reboots after any change.

5. Verify the network settings have been changed by entering:

   `showConfig`

Setting the Network Settings using Command View VLS

To set the network settings using Command View VLS, set either the:

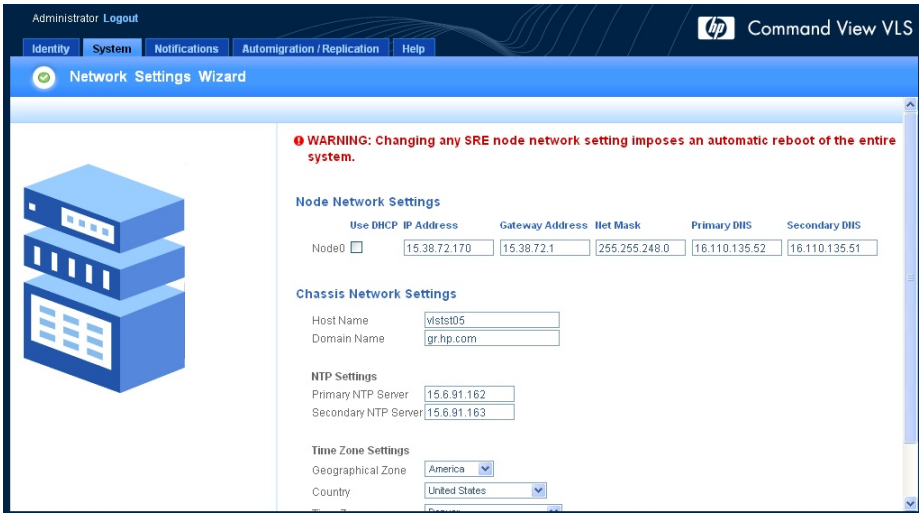
- DHCP usage and host name, or
- Fully qualified host name (or host name and DNS domain name separately), DNS server address, IP address, gateway, and netmask

To set the network settings using Command View VLS:

1. Click the **System** tab.
2. Select **Chassis** in the navigation tree.
3. Select **Set Network Configuration** under **Maintenance Tasks**.

4. Current network configuration, NTP settings, and time zone settings are displayed. Modify these as needed (Figure 9 (page 108)).

Figure 9 Set Network Configuration Wizard window



5. Click **Finish** to apply the settings.

NOTE: The system automatically reboots after any change.

NOTE: If you need to clear the DNS completely, clear the **Use DHCP** checkbox and enter `0.0.0.0` for both the primary and secondary DNS server addresses.

Setting the User Preferences

Setting the user preferences allows you to:

- Set the frequency at which the system state is checked and the browser is refreshed
- Add the VLS administrator's name, company, mail, and phone number, and the VLS location to the Identity tab window
- Set the maximum number of notification alerts to store

To set the user preferences, from Command View VLS:

1. From the **System** tab, select **Chassis** in the navigation tree.
2. Click **User Preferences** under **Maintenance Tasks**. The User Preferences window opens.
3. Enter a value (in seconds) in the **State Polling Frequency** box.

   The default state polling frequency is 15 seconds.
4. Enter the appropriate numeric value in the Number of Notifications dialog box.
5. Enter the company name in the Company dialog box.
6. Enter the city and state where the VLS is located in the Location dialog box. This is displayed on the Identity tab.
7. Enter the VLS administrator's name in the Contact dialog box. This is displayed on the Identity tab.
8. Enter the VLS administrator's phone number, including area code, in the Contact Phone dialog box. This is displayed on the Identity tab.
9. Enter the VLS administrator's E-mail address in the E-mail dialog box. This is displayed on the Identity tab.

   The E-mail address entered is assigned to the Email Administrator link on the Login window. Users can click this link to send an E-mail to the administrator when they need help or are unable to log in to Command View VLS.

10. Enter the warranty serial number in the Warranty Serial Number dialog box. This is displayed on the Identity tab and is saved and restored as part of the VLS device configuration.
11. Click **Apply Settings**.

Editing the Default Fibre Channel Host Port Settings

Only edit the Fibre Channel host port settings if you do not want to use the default settings, if some system problem is occurring, or if the "AUTO" setting is not working properly.

NOTE: The values displayed under **Actual** are the actual values found by the VLS for the Fibre Channel host port.

NOTE: If you enter a value that is not supported by the Fibre Channel port (for example, you enter Fabric in the Topology column but the port uses the Loop topology), your entry remains in the Preferred box, but the Actual column will display the correct value when Command View VLS performs its occasional status checks.

To change the default Fibre Channel host port settings, from Command View VLS:

1. Click the **System** tab.
2. Expand **Chassis** in the navigation tree.
3. Expand the **Node** to modify in the navigation tree.
4. Select **Fibre Channel** in the navigation tree.

   The Fibre Channel Host Ports window opens.
5. Enter a value for the Loop ID in the **Loop ID Preferred** box for each Fibre Channel host port to use for prioritizing communication requests with the VLS.

   If the Fibre Channel host port's topology is Fabric, the Loop ID value is ignored.
6. Select the Fibre Channel host port's topology in the **Topology Preferred** box for each Fibre Channel host port.

   Auto — Allows the VLS to determine the Fibre Channel port's topology

   Loop — Sets the topology type to an arbitrated loop

   Fabric — Sets the topology type to fabric
7. Select a link speed in the **Link Speed Preferred** box for each Fibre Channel host port.

   Auto—Allows the VLS to determine the Fibre Channel port's link speed

   1 — 1 Gb per second

   2 — 2 Gb per second

   4 — 4 Gb per second
8. When you are finished configuring the Fibre Channel ports, click **Apply Settings**.
9. Restart the VLS device emulations to make the changes take effect. See "Restarting VLS Device Emulations" (page 131).

Managing Oversubscription

Because the VLS dynamically allocates storage space as data is written to virtual media, the VLS allows you to allocate more cartridge capacity than is physically installed. This feature, called oversubscription, permits configuring your system for anticipated storage growth; configure cartridges beyond your current capacity and then seamlessly add physical storage later.

By default, oversubscription is disabled.

NOTE: Using oversubscription, you run the risk of running out of physical storage capacity and requires careful planning of your storage needs and a review of your current storage policy.

Enabling and Disabling Oversubscription

To enable oversubscription:

In Command View VLS:

1. Select the **System** tab.
2. Select **Chassis** in the navigation tree.

   The chassis details window opens.
3. In the Oversubscription section, select **Enabled**.
4. The **Notify when storage capacity is [x] % Full** box defaults to 90. You may change the value or leave it at 90.

   This percentage value is the threshold of storage space consumed that when reached triggers a storage capacity notification alert. If this threshold is set to zero (0), an alert will be sent only when existing capacity has been reached.
5. Click **Apply Settings**.

To disable oversubscription, deselect the **Enabled** box.

NOTE: Oversubscription cannot be disabled while cartridge capacity is oversubscribed.

Shutdown at 98% Capacity

The system displays warnings on the Notifications screen when the backend storage capacity consumed reaches the user-defined threshold (determined when you enabled oversubscription). Additional notifications are sent when the capacity consumed reaches 95% and again at 98%.

At the level of 98%, the system will reject all attempts to write data from the backup application. Free up storage space or add more storage before reaching this point to ensure that no data is lost. All read operations remain unaffected.

Once you reduce the capacity consumed to a level below the user-defined threshold, writes from the backup application resume automatically. However, if you reduce the capacity consumed to less than 98% but still above the threshold, you can manually resume writes by selecting **Enable Writes** (now visible) from the task bar of the Chassis status screen.

When the storage capacity consumed exceeds the user-defined threshold, the system:

- Displays warnings on the Notifications screen
- Sends emails (if configured) to specified users
- Sends alerts to the management consoles (if SNMP traps are configured)
- Displays the **Reclaim Space** link on the Chassis status screen

At this point, you can perform the following tasks:

- Erase cartridges — erase or relabel expired cartridges to free up storage space. See your backup application manual for details.

  NOTE: Use the Cartridge Utilization report to identify cartridges that are consuming more space and can be erased to create more storage space. See "Receiving Automated Reports" (page 154).

  Erasing data from cartridges containing data that is not deduplicated will free up more storage space than erasing from cartridges with deduplicated data.
- Reclaim space — see "Reclaiming Storage Space" (page 111).
- Add more storage

  NOTE: You cannot hot-add storage while the VLS is deduplicating data.

Reclaiming Storage Space

The Reclaim Space task appears on the Chassis status screen when the storage capacity consumed reaches the user-defined threshold (or the default of 90%). This allows you to schedule reclamation of the additional storage you make available by erasing cartridges. First erase cartridges from your backup application, then follow the procedure below.

From Command View VLS:

1. On the **System** tab, select **Chassis** from the navigation screen to open the Chassis status screen.
2. Select **Reclaim Space** in the task bar.

   The VLS system initiates space reclamation and the Notifications screen displays a notification of the scheduled reclamation.

Managing Virtual Device LUNs

The VLS has a LUN masking, a LUN mapping, and a port mapping feature that allows you to restrict host access to the LUNs (virtual libraries and tape drives) configured on the VLS and assign each virtual device to a specific Fibre Channel host port. These features allow you to allocate the virtual devices to individual hosts and distribute the virtual tape drives across the Fibre Channel host ports to achieve maximum bandwidth. See "Managing high availability" (page 122) for more information.

You can set a global default so that either the VLS allows all hosts connected to the VLS through the SAN to access all virtual devices configured on the VLS, or the VLS prevents all hosts from viewing any virtual devices until they are explicitly mapped to the host. Each time you add a new host to the VLS, it takes the global default you have set. The VLS firmware also manages the LUN numbering so that the virtual device LUN assignments always meet operating system requirements and restrictions. See "Default LUN Numbering" (page 111) and "Operating System LUN Requirements and Restrictions" (page 112).

Port mapping is required and allows you to assign each virtual device to one of the Fibre Channel host ports or a pair of Fibre Channel host ports (if your backup solution supports this).

Default LUN Numbering

The VLS automatically assigns a logical unit number (LUN) to each virtual library and tape drive created on the VLS in the order in which they are created by you, starting with LUN0 and increasing incrementally by one as each new virtual library or tape drive is created on an Fibre Channel host port (LUN1, LUN2, and so on). The first virtual device port mapped to any of the Fibre Channel host ports is assigned the LUN number LUN0. The second virtual device port mapped to an Fibre Channel host port is assigned the LUN number LUN1, and so on.

The default LUN numbers are changed by the VLS firmware when the VLS device emulations are restarted if:

- A virtual device has been deleted since the last restart, creating a gap in the LUN numbering, or
- A virtual tape drive has been added to a library since the last restart and the default LUN number it was assigned is not consecutive with the other virtual tape drives in the same library.

Restarting VLS device emulations changes the default LUN numbers as necessary to remove the gap or to make the virtual tape drive LUN numbers consecutive in each library. This is done so that the virtual device LUN numbering meets the operating system LUN requirements.

NOTE: When a LUN has been unconfigured or otherwise deleted, it may still show up in the VLS user interface. Use the VLS discovery utility to refresh the list of LUNs that are present.

Operating System LUN Requirements and Restrictions

Most operating systems require that each VLS Fibre Channel host port connected to the SAN has a virtual device with the LUN number LUN0 and no gaps in the LUN numbering (LUN0, LUN1, LUN2, and so on). If the operating system does not see a LUN0 on a VLS Fibre Channel host port when it is scanning for new hardware on the SAN, it will stop looking for LUNs on that port and erroneously report that there are no LUNs (virtual devices) on that port. If the operating system sees a LUN0, LUN1, and LUN2 but not a LUN3 on the port, it will stop looking for LUNs on that port when the gap in the LUN numbering is encountered. Even though there may be more LUNs, such as LUN4, the operating system will erroneously report that there are only three LUNs on the port.

In addition, operating systems are configured to only look for a maximum number of LUNs per device and no more. Once the maximum number of LUNs is detected, the operating system stops looking. In the case of the VLS, the operating system considers each Fibre Channel host port to be one device with its own set of LUNs. So, if the maximum number of LUNs an operating system is configured to see is eight, the operating system will only see LUN0 through LUN7 and will not see LUN8, LUN9, and up on each Fibre Channel host port.

To get around the maximum LUNs per device restriction, you can either:

- Increase the maximum LUNs per device setting for the operating system. See "Troubleshooting" (page 241) for more information.
- Enable LUN mapping on the VLS to restrict the number of virtual devices the host's operating system sees on the VLS Fibre Channel host ports. See "LUN Mapping" (page 112) for more information.

LUN Masking

LUN masking restricts a host's access to the virtual devices (virtual libraries and/or tape drives) on the VLS. You should use it when there are more virtual device LUNs mapped to an Fibre Channel host port than the operating system LUN restrictions support. You can limit the LUNs the host's operating system can see on the port, so that only the virtual devices the host needs to see are visible.

For example, if a host's operating system is configured to only see up to eight LUNs per Fibre Channel host port, the host will not be able to see the virtual devices numbered LUN8, LUN9, and up. Suppose that you need the host to see LUN0 through LUN5, LUN8, and LUN9. You can enable LUN mapping, thereby hiding all of the LUNs from the host. Then you can map LUN0 through LUN5, LUN8, and LUN9 to the host. The VLS will automatically renumber the mapped LUNs so that LUNs 8 and 9 become LUNs 6 and 7 and they are now within the eight the host can see. See LUN Mapping.

In the VLS, LUN masking occurs automatically for all hosts when you enable LUN mapping using the global enable/disable LUN mapping setting. See "Setting the Default LUN Mapping" (page 113).

LUN Mapping

LUN mapping is used to present only a subset of the VLS virtual devices to a host. If LUN mapping is enabled, the VLS prevents all hosts connected to the VLS through the SAN from viewing any virtual devices until they are explicitly mapped to the host. By disabling LUN mapping, the VLS allows all hosts connected to the VLS to access all virtual devices configured on the VLS. By default, LUN mapping is disabled. The setting you choose will apply to every new host that you add to the VLS. See Setting the Default LUN Mapping.

Setting the Default LUN Mapping

You can set a global default to disable or enable LUN mapping. The setting you choose will apply to every new host that you add to the VLS.

- All Devices (LUN mapping disabled) – The default. The VLS allows all hosts connected to the VLS through the SAN to access all virtual devices configured on the VLS.
- User-Defined (LUN mapping enabled) – the VLS prevents all hosts connected to the VLS through the SAN from viewing any virtual devices until they are explicitly mapped to the host.

To set the default status of LUN mapping, from Command View VLS:

1. Click the **System** tab.
2. Expand **Chassis** in the navigation tree.
3. Select **LUN Mapping** in the navigation tree.
4. If this is not your first time changing the setting, select **Change Host Access Mode** in the task bar.
5. Initially, **All Devices** is selected, and LUN mapping is disabled.
6. To enable LUN mapping, select **User-Defined**.
7. Select **Apply**.

   The global default is now set. For every host you add, LUN mapping is automatically enabled or disabled as you chose.

NOTE: Both modes allow you to disable a host so that it cannot see any virtual devices regardless of any other settings.

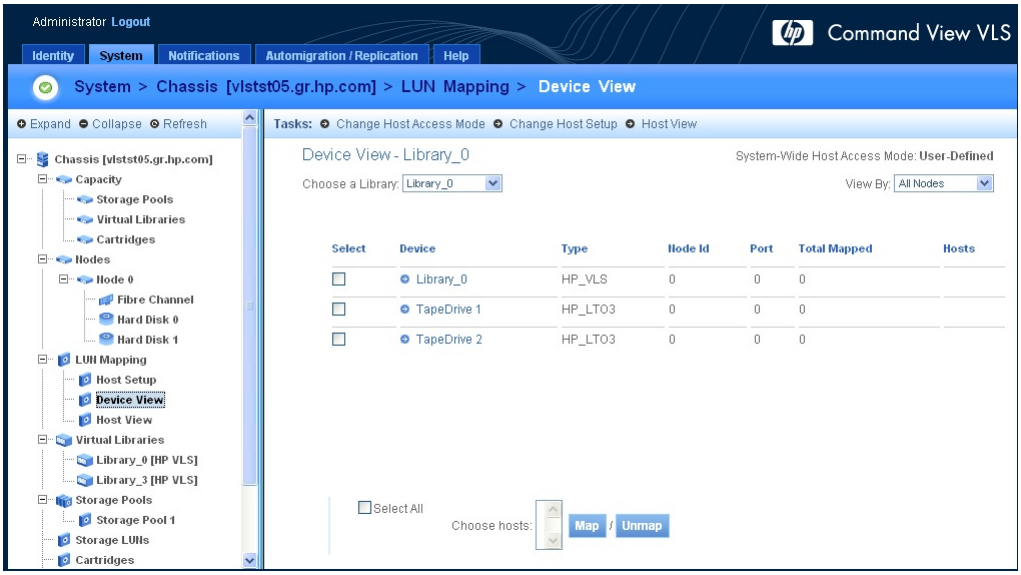
Mapping LUNs by Device

To map LUNs by device:

1. Select the **System** tab.
2. Expand **Chassis** in the navigation tree.
3. Expand **LUN Mapping** in the navigation tree.
4. Select **Device View**.

   The **Device View** window displays all of the devices that have been mapped to a host (Figure 10 (page 113)).

Figure 10 LUN Mapping Device View window



5. Select a library from the **Choose a Library** list to view its mapped devices.

   The window refreshes to show the appropriate list.
6. Use the **View By** list to narrow the list of devices based on the node.
7. Select the devices you want to map to a particular host.
8. Select the host in the **Choose hosts** list at the bottom of the window. These hosts currently do not have any of the devices shown mapped to them.

   You can select multiple hosts using **Ctrl+click**.
9. Select **Map** next to **Choose hosts**.

   The window refreshes and the host appears in the device list for the appropriate devices. The selected devices are now visible to the new hosts.

To unmap LUNs by device:

1. Navigate to the **Device View** window. See the mapping procedure above.
2. Select the appropriate library from the **Choose a Library** list.
3. Select the devices to unmap.
4. Select **Unmap** next to the **Choose hosts** list.

   The window refreshes and the newly unmapped devices disappear from the device list. They are no longer visible to the hosts.

NOTE: After you map or unmap the virtual devices, the VLS automatically reassigns a logical unit number (LUN) to each virtual library and tape drive created on the VLS to ensure that the virtual device LUN numbering meets the operating system LUN requirements.

Mapping LUNs by Host

To map LUNs by host:

1. Select the **System** tab.
2. Expand **Chassis** in the navigation tree.
3. Expand **LUN Mapping** in the navigation tree.
4. Select **Host View**.

   The **Host View** window displays all of the devices that can be seen by a selected host.
5. Select a host from the **Choose Host** list to view the devices mapped to it.

   The window refreshes to show the appropriate device list.
6. Use the **View By** to narrow the list of devices based on the node.
7. Select the devices to map in the field at the bottom of the window. These devices are currently not mapped to the viewed host.

   You can select multiple devices using **Ctrl+click**.
8. Select **GO** next to **Map devices**.

   The window refreshes and the newly mapped devices appear in the list. These devices are now visible to the host.

To unmap LUNs by host:

1. Navigate to the **Host View** window. See the mapping procedure above.
2. Select the appropriate host from the **Choose Host** list.
3. Select the devices to unmap.
4. Select **GO** next to **Unmap selected devices**.

   The window refreshes and the newly unmapped devices disappear from the list. These devices are no longer visible to the host.

NOTE: After you map or unmap the virtual devices, the VLS automatically reassigns a logical unit number (LUN) to each virtual library and tape drive created on the VLS to ensure that the virtual device LUN numbering meets the operating system LUN requirements.

Setting Up the Hosts

You can configure the hosts in Command View VLS. You will make all of the changes to the hosts from the **Host Setup** window.

To open the **Host Setup** window:

1. Select the **System** tab.
2. Expand **Chassis** in the navigation tree.
3. Expand **LUN Mapping** in the navigation tree.
4. Select **Host Setup**.

   The **Host Setup** window displays a list of the host world wide port numbers (WWPNs) seen by the VLS Fibre Channel host ports on the SAN.

To add a host WWPN:

1. Open the **Host Setup** window.
2. In the top row, select the state of the new host in the **State** list.
3. Enter the WWPN in the **World Wide Port Number** box.

   The WWPN must be exactly 16 numerals long and cannot contain any letters or special characters.

4. Enter a hostname in the **Hostname** box.
5. Select **Add**.

   The window refreshes and displays a message indicating the host was added successfully. The new host WWPN is listed with the others.

NOTE: The VLS only supports up to 128 hosts per Fibre Channel port.

To rename or newly assign a host name alias to a host WWPN:

1. Open the **Host Setup** window.
2. Select the hosts to rename.
3. Enter the new hostname in the **Hostname** box for each selected host.
4. Select **Rename Hosts**.

   The window refreshes and displays a message indicating the hosts were renamed successfully. The new names are visible in the box.

To disable or enable host WWPNs:

1. Open the **Host Setup** window.
2. Select the hosts to change.
3. Select **Disable Hosts** or **Enable Hosts** as appropriate.

   The window refreshes and displays a message indicating the hosts were disabled or enabled successfully. Note that the state now reflects the change.

To remove host WWPNs:

1. Open the **Host Setup** window.
2. Select the hosts to remove.
3. Select **Remove Hosts**.

   The window refreshes and displays a message indicating the hosts were removed successfully. The hosts no longer appear on the list.

Dual Port Virtual Devices

When creating a library robot LUN or tape drive LUNs, you can present the virtual devices to a pair of host ports rather than just one port. Both ports must be on the same node. The **Port Mapping** list displays selections for each individual port plus possible port pairs (for example: `0`, `1`, `0&1`). The benefit of dual port virtual devices is that they are still accessible when one path fails.

△ **CAUTION:** Many operating systems and backup applications do not support more than one path to a tape library device. Only use this feature if you are certain that it is supported.

When creating dual port virtual devices, the LUN numbering on both ports follows the conventions for default LUN numbering (see "Default LUN Numbering" (page 111)). However, if you use LUN mapping for a dual port device, the defined LUN number for that device for a specified host applies to both device paths. Follow the operating system LUN requirements (see "Operating System LUN Requirements and Restrictions" (page 112)) when configuring the paths.

Creating a Virtual Library

Before creating a virtual library, you must first:

- Determine the best way to manage VLS virtual library and tape drive LUNs for your environment (see "Managing Virtual Device LUNs" (page 111)).
- Determine the best way to configure virtual libraries and tape drives on your VLS for your environment. See the *HP VLS Solutions Guide*.

You can configure any combination of virtual tape libraries and virtual tape drives up to the maximum number supported on the VLS. You can configure one node with up to 16 libraries with a total of up to 180 virtual tape drives. With multiple nodes, a single library can span across nodes.

To create a new virtual library, from Command View VLS:

1. Click the **System** tab.
2. Select **Chassis** in the navigation tree.
3. Select **Create Virtual Library** in the task bar.

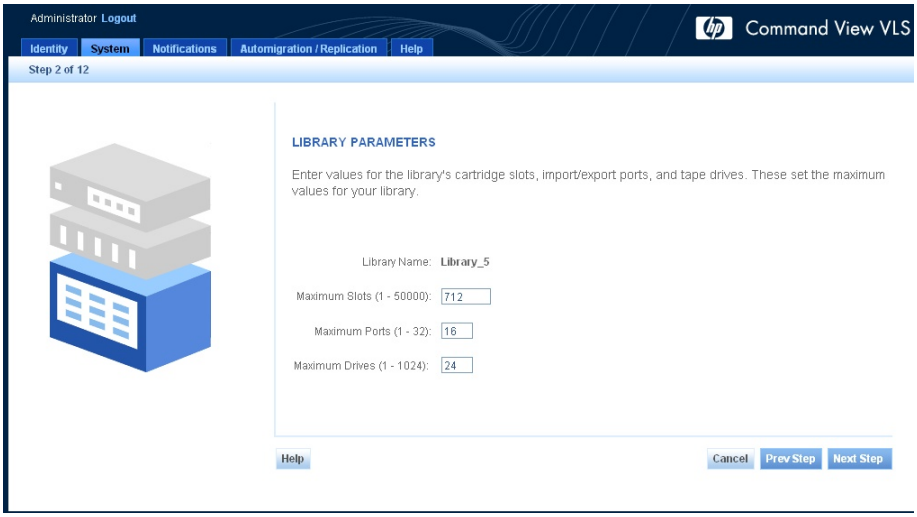
   The **Create Virtual Library Wizard** opens.
4. Select the Fibre Channel host port and node on which to present the virtual library.

   Only one port or port pair may be selected.
5. Select the type of tape library to emulate.

   NOTE: The only library emulation Veritas supports for use with Netbackup is the HP VLS emulation. IBM supports using the HP VLS emulation for TSM version 5.5.1 or higher. The HP VLS emulation is not intended for use with other backup applications.
6. Click **Next Step**.

   The window displays the default library name and the default number of Maximum Slots, Maximum Ports, and Maximum Drives based on the physical tape library emulation selected (Figure 11 (page 117)).

Figure 11 Create Virtual Library Wizard window (2 of 12)



7. Change the library name if you prefer. You can use letters, numbers, and underscores (no blank spaces).
8. Enter the maximum number of cartridge slots that may be added to the library in the **Maximum Slots** box.

   The default values in the **Maximum Slots** box is based on the physical tape library you selected.

⚠ **CAUTION:** Changing the defaults can have unpredictable results if your backup application expects a certain number of slots in a specific library type.

9. Enter the maximum number of input/export ports on which the library may be configured to be visible in the **Maximum Ports** box.
10. Enter the maximum number of tape drives the library may contain in the **Maximum Drives** box.

    NOTE: The maximum values entered cannot be changed later. So, consider your potential future requirements when entering values.

    Not all of the tape drives and cartridges must be created at this time. You may add tape drives later.

11. Click **Next Step**.

    A window opens indicating that by default all libraries connected to the VLS have access to all hosts.
12. Click **Create Library**.

    A summary window opens and displays details about the library emulation created.
13. Choose one of the following options:
    - To perform LUN mapping for the virtual library, click **Map LUNs** and proceed to "LUN Mapping" (page 112) for further instructions.
    - To continue creating the virtual library, click **Create Tape Drives** and proceed to "Creating Tape Drives" (page 118).
    - To exit the wizard, click **Cancel**.

      The library is created but does not contain any tape drives or cartridges. You can add tape drives and cartridges later.

Editing a Virtual Library

To edit the slots and drives of a virtual library, from Command View VLS:

1. Click the **System** tab.
2. Expand **Chassis** in the navigation tree.
3. Expand **Virtual Libraries** in the navigation tree.
4. Select the virtual library you want to edit.
5. Select **Edit Virtual Library** in the task bar.
6. On the **Library Parameters** screen, change the values as appropriate. You can change the maximum number of slots, maximum number of ports, and maximum number of drives.
7. Select **Next Step**. The screen displays a confirmation.
8. Select **Yes** to continue. The screen displays a "success" message.

Creating Tape Drives

NOTE: If you add a virtual tape drive to a library after another library has been created, the default LUN number assigned to the tape drive will not be consecutive with the other virtual tape drives in the same library. To correct this, restart the VLS device emulations. See "Restarting VLS Device Emulations" (page 131). The VLS firmware will change the virtual device LUN numbers on the VLS so that all the default tape drive LUNs in a library are consecutive.

NOTE: A virtual library may only contain one type of tape drive.

To add tape drives to a virtual library:

1. If you are already in the **Create Library Wizard** window, click **Create Tape Drives**.

   The **Tape Drive Parameters** window opens.
2. If not:
   a. Click the **System** tab.
   b. Select the library in the navigation tree to which you want to add tape drives.
   c. Click **Create Tape Drive** in the task bar.

      The **Tape Drive Parameters** window opens.
3. Select the type of physical tape drive to emulate.
4. Enter the Fibre Channel host port and node on which to present the tape drives in the **Port Mapping** box.

   Only one port or port pair may be selected.
5. Click **Next Step**.

   The next **Tape Drive Parameters** window opens.
6. Enter the number of tape drives you want to create in the library at this time in the **Tape Drives** box, if different from the default value.

   You can add more tape drives to the library later. The **Tape Drives** box defaults to the standard number of drives for the library type.

   NOTE: All the tape drives created at one time are mapped to the same Fibre Channel host ports. Make sure to load-balance the tape drives across the Fibre Channel host ports to obtain maximum performance. Tape drives in a library do not have to be mapped to the same port as the library.
7. Click **Create Tape Drive**.

   A summary window opens and displays details about the tape drives created.

8. Choose one of the following options:
   - To perform LUN mapping for the virtual tape drive, click **Map LUNs** and proceed to "LUN Mapping" (page 112) for further instructions.
   - To create more tape drives, click **Create More Tape Drives**.
   - To add cartridges to the virtual library, click **Create Cartridges** and proceed to "Creating Cartridges" (page 119).
   - To exit the wizard, click **Cancel**.

     At this point the library and tape drives have been created, but the library does not contain any cartridges. You can add cartridges later.

Creating Cartridges

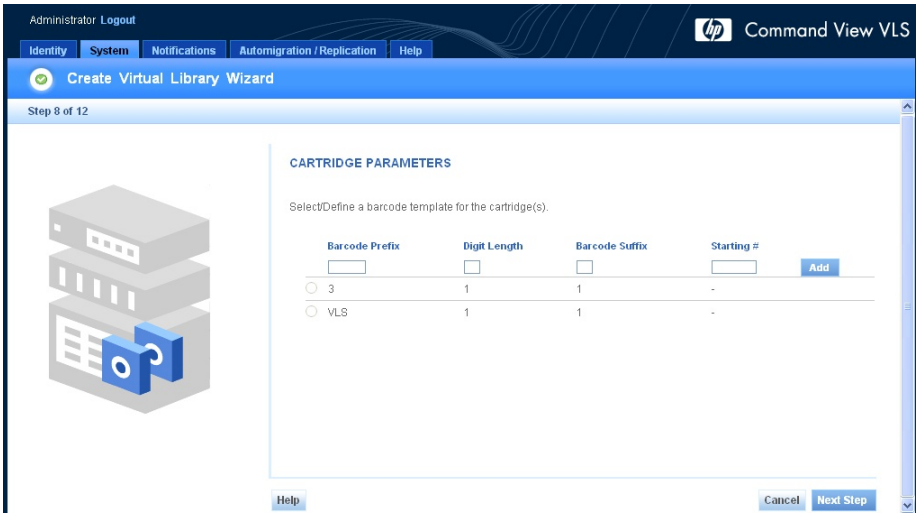
To add cartridges to a virtual library:

1. If you are already in the **Create Library Wizard** window, select **Create Cartridges**.

   The **Cartridge Parameters** window opens (Figure 12 (page 119)).
2. If not:
   a. Click the **System** tab.
   b. Select the virtual library in the navigation tree to which you are adding cartridges.
   c. Click **Create Cartridge** in the task bar.

      The Cartridge Parameters window opens (Figure 12 (page 119)).

Figure 12 Create Virtual Library Wizard window (8 of 12)



3. To add a barcode template:
   a. Enter the barcode prefix (one to six alphanumeric characters) in the **Barcode Prefix** box. No special characters are permitted.
   b. Enter the number of digits for the barcode number in the **Digit Length** box. For example, if you enter "3" the barcode numbers will be 001, 002, 003, etc.
   c. Enter the barcode suffix (one or two alphanumeric characters) in the **Barcode Suffix** box. No special characters are permitted.
   d. Enter the starting barcode number in the **Starting #** box.
   e. Click **Add** to add the new barcode template.
   f. To add another barcode template, repeat these steps.
4. Click the radio button next to the barcode template you want to use to create the cartridges.

NOTE: NetBackup has total barcode limit of eight characters. HP Data Protector has a total barcode limit of 16 characters. Check your user guide for other backup applications.

5. Click **Next Step**.
6. Select the type of physical cartridge to emulate.
7. Click **Next Step**.
8. Enter the number of cartridges and the cartridge size in the appropriate boxes (Figure 13 (page 120)).

   The default number of cartridges is based on the maximum number of slots configured for the virtual library. The default cartridge size is based on the actual size of the type of cartridge emulated.

   If there are multiple storage pools on your system, you must select the pool in which to create cartridges from the **—> Available capacity** list.

   The system calculates and displays the amount of required storage. If the required storage exceeds what is available, the overage appears in red. You can allow the oversubscription of storage capacity (see "Enabling and Disabling Oversubscription" (page 110)), or you can change either the number of cartridges or the cartridge size (or both) to correct the overage condition.

Figure 13 Create Virtual Library Wizard window (10 of 12)

9. Click **Next Step**.

   A summary window opens and displays details about the cartridges you created.
10. Click **Next**.
11. Click **Return**.

    The System tab window opens. You can now select the new library, tape drives, and cartridges in the navigation tree to view their configuration information, such as their default LUN numbers.

Destroying a Virtual Library

NOTE: Destroying a virtual library may create a gap in the default LUN numbering on the Fibre Channel host port to which it was mapped. If a gap is created, restart the VLS device emulations to remove the gap. See "Restarting VLS Device Emulations" (page 131).

Most operating systems will ignore (cannot access) any virtual devices with LUN numbers that follow a gap in the LUN numbering on an Fibre Channel host port.

NOTE: You cannot destroy a library that is currently being accessed by a backup application.

When a virtual library is destroyed, all the tape drives associated with the library are also destroyed. The cartridges in the virtual library, however, are not destroyed. They are moved to the Firesafe where they are stored until you either destroy them or associate them with a virtual library. See "Managing Cartridges" (page 127).

To destroy (delete) a virtual library, from Command View VLS:

1. Click the **System** tab.
2. Select the virtual library in the navigation tree.

   The virtual library details window opens.
3. Click **Destroy Virtual Library** in the task bar.
4. Click **Yes** to confirm.
5. Click **Finish**.

Destroying a Tape Drive

NOTE: Destroying a tape drive may create a gap in the default LUN numbering on the Fibre Channel host port to which it was mapped. If a gap is created, restart the VLS device emulations to remove the gap. See "Restarting VLS Device Emulations" (page 131).

Most operating systems will ignore (cannot access) any virtual devices with LUN numbers that follow a gap in the LUN numbering on an Fibre Channel host port.

NOTE: You cannot destroy a tape drive that is currently being used by a backup application.

To destroy a tape drive, from Command View VLS:

1. Click the **System** tab.
2. Select the tape drive in the navigation tree.

   The tape drive details window opens.
3. Click **Destroy Tape Drive** in the task bar.
4. Click **Yes** to confirm.
5. Click **Finish**.

10 Management

This section details the VLS management procedures such as changing the account passwords, managing high availability, and saving configuration settings.

Changing the Account Passwords

To change the administrator and/or user account password, from Command View VLS:

1. Click the **System** tab.
2. Select **Chassis** from the navigation tree.
3. Click **Edit Accounts** under **Maintenance Tasks**. The **Edit Accounts** window opens.
4. Enter the current password in the **Old Password** box. The password is case sensitive.
5. Enter a new password in the **New Password** box.
6. Enter the new password again in the **Retype New Password** box.
7. Click **Apply Settings**.

   Command View VLS restarts automatically.

   NOTE: You can change the user or administrator account password separately, or change both at the same time.

NOTE: The password can also be changed from the VLS CLI. See "CLI Management commands" (page 170).

Managing High Availability

This section describes the methods to maintain high availability with your VLS.

Array Dual Pathing

The VLS system supports dual pathing to the arrays which provides path balancing and transparent path failover on the VLS. Having followed the setup recommendations in the *HP VLS Solutions Guide* and the installation instructions in this guide, each node on the VLS is connected to two fabrics/zones which are each connected to the arrays by two paths. This assures that the VLS can establish two paths per LUN, each path on a separate fabric/zone.

Load Balancing

For load balancing the VLS system, half of the data transfer (from a specific node through a fabric to the array) is conducted over one path; half over a second fabric, hence another path. The paths are selected as follows: Once configured, the device recognizes all paths to each node on the device. From all potential preferred paths and all potential secondary paths, the array assigns one preferred path and one secondary path.

NOTE: During each reboot the device is re-analyzed and the preferred and secondary paths are reassigned.

To view the preferred path for each LUN in the **Storage LUN Details**:

1. In Command View VLS, select the System tab.
2. Select **Storage LUNs** in the navigation tree.
3. Select the **View** button for either **All** LUNs or the LUNs in the desired **<Storage Pool #>**.

   Summary information displays at the top of the list. Preferred and secondary paths are listed after the summary information in the **Storage LUN Details Per Node** sections.

   NOTE: It may take several minutes to display this information if there are many LUNs.

LUN Path Failover

LUN path failover allows the VLS to automatically reroute data traffic usually assigned to one (preferred) path to another (secondary) path when the preferred path fails. Path status is shown in Command View VLS under **Storage LUN Details**.

A failover is indicated in the **Storage LUN Details** screen by the yellow warning icon and the notification message: **Fibre Channel Path Failed Over to {#:#:#:#}**. The #s stand for the node port; bus number (always 0); the target id (an array port); and the LUN number on the array.

When one path fails, automatic failover reroutes data traffic to the secondary path so the data transfer still happens, but potentially at a slower rate. It is advised that you restore the path as soon as possible to avoid a double path failure.

To restore the failed path:

1. Determine the cause of the failure and repair it if needed.
2. In Command View VLS, access the System tab.
3. Select **Storage LUNs** from the navigation tree.
4. Select **View** to display the storage LUN details.
5. Select **Fix Primary Paths** from the task bar to display the **Fix Primary Paths Wizard**.
6. Select **Apply** to set all paths back to their primary paths.

Failure of both paths (double path failure) is indicated by the red critical icon and a specific notification message. The notification message differs based on whether the failure occurs while running or upon booting the system.

- A double path failure that occurs while running results in the critical alert **Fibre Channel Paths Failed for Lun, ulid <numerical LUN id number> wwnn <numerical wwnn>**.
- A double path failure that occurs upon booting the system results in the critical alert **Missing Storage LUN paths on node #**.

This means the node can not communicate with the LUN at all. If the failed paths are on the primary node, the whole storage pool containing that LUN is off-line; if the failed paths are on a secondary node, the storage pool is on-line until reboot, but the storage pool is inaccessible from that node. In this case, you can still get to the LUNs, but only from a different node.

To repair double path failure (assuming there has been no reboot during the failure):

1. Determine the cause of the failures and repair them if needed.
2. In Command View VLS, access the System tab.
3. Select **Storage LUNs** from the navigation tree.
4. Select **Fix Primary Paths** from the task bar to display the **Fix Primary Paths Wizard**.
5. Select **Apply** to set all paths back to their original settings.

Private LAN Dual Pathing

The private LAN on the VLS has dual pathing which consists of a cable from each switch to each node. If a LAN switch or a path to a LAN switch fails, the data transfer will automatically fail-over to the other available switch.

- The primary path is through NIC 2 of the switch and is referred to in the error notification as `eth1`. If the LAN switch associated with NIC2 fails, the Notifications tab will display all `eth1` failures.
- The secondary path is through the USB LAN cable and is identified as `eth2` in the error notification. If the LAN switch associated with the USB LAN cable fails, the Notifications tab will display all `eth2` failures.
- If both paths fail, the critical alert will identify `bond 0` as the combined failed path. If both paths from the private LAN to a secondary node fails, the node is off-line; but if both paths to a primary node fails, the whole device is off-line.

When a failure occurs, repair the failure. In most cases, the system will automatically recognize that the repair is complete and restore the path or paths without having to reboot the system; however, you may need to reboot the system if the repair includes installing a new USB LAN adapter.

Managing Disk Arrays

Some VLS firmware versions allow you to manage the disk arrays. The disk array management screens allow you to view the status and other details of a virtual disk, delete unused virtual disks, and clear the metadata on leftover disks.

To access the disk array management screens, from Command View VLS:

1. Select the **System** tab.
2. In the navigation tree, expand **Chassis**.
3. In the navigation tree, select **Disk Arrays**.
4. In the task bar, select **Service**.

   The screen provides a caution about using the Disk Array Management service.
5. Click **Accept**.

   The screen opens to the Manage Virtual Disks screen and displays details about the virtual disk array including the disk array number and IP address, virtual disk name, total capacity, free capacity, owning controller, RAID level, status, background array activity (and percentage complete), and the serial number. You can access the Clear Leftover Disks, Update Firmware, Reset Array Information, and Set RAID Mode screens from the task bar.

Viewing the Virtual Disk Status

The Manage Virtual Disks screen displays details about the virtual disks in the disk arrays. By default, it lists all of the virtual disks in the arrays. You can narrow the list by using the Select Disk Arrays list and then selecting **Update**.

The status of the disk array is one of the following:

- Online, Not Fault Tolerant, some disks down — The virtual disk is online. However, some drives are down and the virtual disk is not fault tolerant.
- Online, Fault Tolerant, some disks down — The virtual disk is online and fault tolerant. However, some of the drives are down.
- Online, Fault Tolerant — The virtual disk is online and fault tolerant.
- Offline, either due to initialization or because disks are down and data may be lost — The virtual disk is offline either because of initialization or because drives are down and data may be lost.
- Critical, Quarantined due to missing disks — The virtual disk is in a critical state and has been quarantined because three or more drives are missing.
- Offline, Quarantined due to missing disks — The virtual disk is offline and has been quarantined because three or more drives are missing.
- Online, Not Fault Tolerant — The virtual disk is online and does not have fault tolerant attributes.
- Unknown — The state of the virtual disk is not known.

Possible background activity running on the virtual disks:

- Disks Scrubbing — Disks within the virtual disk are being scrubbed.
- Expanding — The virtual disk is being expanded.
- Initializing — The virtual disk is initializing.
- Low-level formatting — A low level format is in progress.

- Reconstructing — The virtual disk is being reconstructed.
- Verifying — The virtual disk is being verified.
- VDisk Scrubbing — The virtual disk is being scrubbed.

Deleting Unused Virtual Disks

On the Manage Virtual Disks screen, you can delete an unused virtual disk. By default, it lists the virtual disks in all of the disk arrays.

1. Select the virtual disks you want to delete.

   To narrow the list of disks displayed, use the Select Disk Array list, then select **Update**.
2. Select Delete Unused VDisk from the Select Operation list.
3. Select **Submit**. A warning screen displays.
4. Select **Continue**. The screen displays the status of the deletion.

NOTE: You can only delete virtual disks that are currently not in use or that have two or fewer disks.

Clearing the Leftover Disks

The Clear Leftover Disks screen displays details about the disks including the disk array number and IP address, enclosure number, disk slot number, serial number, disk state, disk revision (firmware version), and disk drive size in TB.

Each disk drive contains metadata that the system uses to identify the drive's owning virtual disk, if any. Disks will go into the Leftover state when they are removed and inserted into the same array. This is caused by the difference in timestamp between the reinserted drive and the timestamp present with the virtual disk. You must clear the disk's metadata before you can use the leftover disk in a different virtual disk or as a spare.

The status of the disk is one of the following:

- Available — Disk is available for use in a virtual disk
- Global spare — Disk is available as a global spare
- Leftover — Disk contains metadata but is not part of a virtual disk
- Part of virtual disk — Disk is part of a virtual disk
- Spare assigned to virtual disk — Disk is a spare assigned to a virtual disk

To clear the Leftover disks:

1. Navigate to the Manage Virtual Disks screen (see "Managing Disk Arrays" (page 124)).
2. Select **Clear Leftover Disks** from the task bar.
3. Select the disks you want to clear from the list.

   To narrow the list of disks in the Leftover state displayed, use the Select Disk Array or Select Enclosure list, then select **Update**.
4. Select **Submit**. A warning screen displays.
5. Select **Continue**. The screen displays the status of the disk clearing.

Updating the Disk Firmware

Some VLS firmware versions allow you to update the firmware on the disk arrays. The Update Firmware screen lists the available disk array firmware upgrade. It provides the disk model and revision numbers of the disks that are able to receive the upgrade. Only disks meeting the upgrade criteria display on this screen.

To update the firmware on the array disks:

1. Navigate to the Manage Virtual Disks screen (see "Managing Disk Arrays" (page 124)).
2. Select **Update Firmware** from the task bar.
3. Select the disks you want to update to the new firmware.

   To narrow the list of disks displayed by disk array, enclosure, or revision, use the Select Disks list, then select **Update**.
4. Select Submit. A warning message displays.
5. Review the warning and select **Continue**. The Update Firmware screen displays.

   You can select **Cancel** to cancel the update process or select different disks.
6. If necessary, click the "De-select disks pending for update" link to remove certain disks from the update process.
7. Reboot the system. See "Rebooting the System" (page 95). The firmware update begins after the reboot.
8. Go to `http://<vls-hostname>` (where <vls-hostname> is the hostname of the system running the firmware update) to open the **Disk firmware update progress** screen and monitor the progress.

   If you are only updating SAS drives, when all of the disks have been updated to the new firmware the VLS automatically reboots.

   If you are updating any SATA drives, when all of the disks have been updated to the new firmware a **Done** button appears. Do not select **Done** until you complete the next step.
9. Manually power cycle the disk arrays.
10. When the power cycle is complete, select **Done**. It may take several minutes until the system is back online.

Resetting the Disk Array Information

Use the Reset Array Information function to reconstruct the display of array components in the Command View VLS navigation tree following the removal of a disk array or enclosure.

△ **CAUTION:** Follow the procedure in "Removing VLS Capacity" (page 46) when removing an array from the system or removing an enclosure from an array.

1. Navigate to the Manage Virtual Disks screen (see "Managing Disk Arrays" (page 124)).
2. Select **Reset Array Information** from the task bar.

   The screen provides a caution about resetting the disk array information.
3. Click **Accept**.

   The screen displays a message that the reset has completed successfully.

Setting the RAID Mode

If your VLS is located at a remote data center and failed hard drives cannot be replaced in a timely manner (48 to 72 hours), you can set the global VLS RAID6 configuration to include a hot-spare for each RAID set. This feature allocates one spare hard drive per enclosure that will automatically take over for a failed drive. After you replace the failed drive, the new drive becomes the spare.

△ **CAUTION:** This feature requires running the Rebuild All Storage Pools operation. Rebuild All Storage Pools destroys all current virtual tape cartridges in the system. HP recommends only changing this mode on a new installation before creating any virtual cartridges.

To change the RAID mode, in Command View VLS:

1. Navigate to the Manage Virtual Disks screen (see "Managing Disk Arrays" (page 124)).
2. Select **Set RAID Mode** from the task bar.

3. Select the RAID Mode.
   - Default – No Hot-spare: the system uses a 10+2 configuration where ten disks are part of the available virtual disks and two are parity disks.
   - Hot-spare: the system uses a 9+2+1 configuration where nine disks are part of the available virtual disks, two are parity disks, and one is a hot-spare disk.

   NOTE: Using the hot-spare mode reduces the VLS capacity and performance by 10%.
4. Click **Submit**.

   The screen displays a warning.
5. Click **Submit**.

   The screen displays a confirmation that the mode was changed.

   For all existing arrays, the change is made only when you use the Rebuild All Storage Pools operation; see "Rebuilding all Storage Pools" (page 47). After the global change is made, any new disk array enclosures added to the configuration will use the selected mode. If you change the mode and do not rebuild all the storage pools, the system will continue to use the mode selected before your change.

Setting the Disk Beaconing

Disk beaconing allows you to turn on the identification LED for any disk on a disk array enclosure. You can also turn on LEDs by enclosures or arrays. This can help identify a specific disk that needs to be replaced.

To access the disk beaconing screens, from Command View VLS:

1. Select the **System** tab.
2. In the navigation tree, expand **Chassis**.
3. In the navigation tree, select **Disk Arrays**.
4. In the task bar, select **Disk Beaconing**.

   The screen opens to the Summary of all Disks in the VLS screen and displays details about the virtual disks including the total number of disks, number of disks in an error state, and the number of disks with beaconing set to On.
5. Drill down from **Disk Beaconing** in the navigation tree to view the disk arrays, enclosures within an array, or disks within an enclosure.
6. Select the array, enclosure, or disks you want to change. (The default is disk beaconing off.)
7. Click **ON** (or OFF) to change the status of the disk beaconing.

   The screen lists the disks that have changed.

Managing Cartridges

You can change the following parameters for existing cartridges from the Cartridge Parameters window:

- Library with which they are associated
- Capacity
- Write access

Accessing the Cartridge Parameters Window

To access the Cartridge Paramenters window, from Command View VLS:

1. Click the **System** tab.

2. Select **Cartridges** in the navigation tree.

   The **Cartridge Details** window opens.
3. Select the number of cartridges to display from the Cartridges per Page list beside the group of cartridges you wish to edit. Options are 10, 50, 100 (default), 500, or 1024 cartridges.
4. Click the **View** button beside the group of cartridges you want to edit.

   If viewing by barcode, enter a cartridge range to view a specific cartridges or leave the default values to view all the cartridges with the barcode.

   The **Cartridges Parameters** window opens. This displays information about the cartridge such as the barcodes on it, the type of cartridge, the total capacity, and the read/write access.

Changing Cartridge Capacity

To change a cartridge's total capacity, from Command View VLS:

1. Click the **System** tab.
2. Select **Cartridges** in the navigation tree. The **Cartridge Details** screen opens.
3. Select the number of cartridges to display from the menu beside the category of cartridges you wish to move. The options are 10, 50, 100 (default), 500, or 1024 cartridges.
4. Click **View** beside the category. The cartridges parameters window opens.
5. Choose the cartridges that you want to edit by using the Select boxes.
6. Enter a new value, in GB, in the **Total** box.
7. Click **Update** in the cartridge row.

Changing Cartridge Read and Write Access

To change a cartridges' read and write access, from Command View VLS:

1. Click the **System** tab.
2. Select **Cartridges** in the navigation tree. The **Cartridge Details** screen opens.
3. Select the number of cartridges to display from the menu beside the category of cartridges you wish to move. The options are 10, 50, 100 (default), 500, or 1024 cartridges.
4. Click **View** beside the category. The cartridges parameters window opens.
5. From the Cartridges Parameters window, select the **Select** box next to each cartridge that you want to edit.
6. Select the desired access from the **Access** box.
7. Click **Update** in the cartridge row.

To change the read/write access for all cartridges displayed:

1. Select the **Select All** box.
2. Select the read/write setting for the cartridges from the **Change selected** box.
3. Click the **Go** button next to the **Change selected** box.

Moving Cartridges

You can move one or more cartridges at a time from one library to another or from a library to the firesafe.

You may delete replication cartridges on either the source or the target VLS with the following results:

- Moving a source cartridge from its existing slot to a different slot in the same library does not move the target cartridge.
- Moving a target cartridge from its existing slot to a different slot in the same library, within the same replication target and copy pool, results in the source cartridge moving to the new slot.

- Moving a source cartridge from its existing library to a different library or to the firesafe results in the target cartridge disappearing from the echo copy pool and moving to the firesafe.
- Moving a target cartridge from its existing library to a different library or to the firesafe, or to a different slot that is not part of the echo copy pool, does not move the source cartridge.
- Moving a target cartridge from its existing library to a different library, or to a new slot in the same library within a new echo copy pool, results in the source cartridge disappearing from the echo copy pool but not moving from its existing library.

To move cartridges, from Command View VLS:

1. Click the **System** tab.
2. Select **Cartridges** in the navigation tree. The cartridges details window opens.
3. Select the number of cartridges to display from the menu beside the category of cartridges you wish to move. The options are 10, 50, 100 (default), 500, or 1024 cartridges.
4. Click **View** beside the category. The cartridges parameters window opens.
5. Select the **Select** box next to each cartridge that you want to delete, or use **Select All** to delete all the cartridges listed.
6. Select the destination from the Move Selected To menu.
7. Click **Go** to the right of the Move Selected To menu.

NOTE: If you have moved a large number of cartridges, allow approximately 20–30 minutes for the VLS system to fully free up the resources from the move before making changes based on the move.

Deleting Cartridges

You can delete one or more cartridges at a time from the VLS. The delete cartridge operation removes the specified cartridges from the VLS, freeing the storage space previously consumed by those cartridges for new data. For more security, you can use the licensed Secure Erasure feature.

Secure Erasure provides guaranteed erasure of information on virtual tape cartridges. (You must purchase a separate license for this feature.) You can schedule all or selected cartridges for a total data overwrite to ensure that no data can be retrieved. The erasure procedure conforms to NIST guidelines as required in many regulated industries and government agencies that mandate that data must be destroyed after a certain period of time. This erasure is comparable to tape shredding of physical tapes.

△ **CAUTION:** If you want to keep data that is currently on a cartridge that you are going to delete, copy the data to another cartridge using a backup application before performing this task.

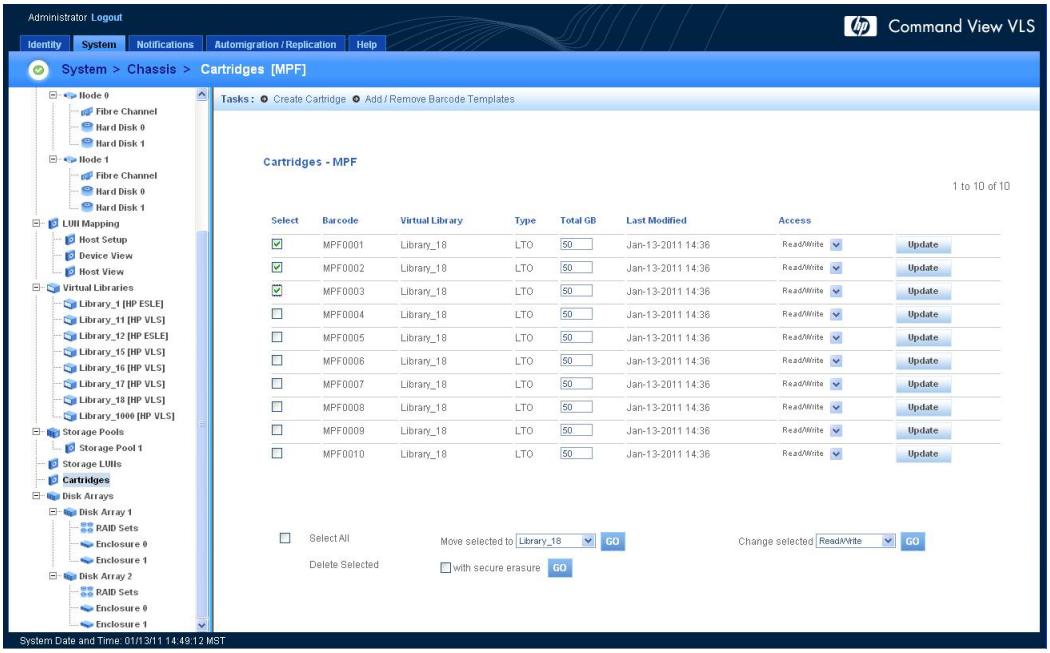
NOTE: You cannot delete a cartridge that is currently being accessed by a backup application. Cancel all replication and deduplication jobs associated with this cartridge first.

You may delete replication cartridges on either the source or the target VLS with the following results:

- Deleting a source cartridge results in the mirror copy pool on the target VLS moving to the Mirror Broken state.
- Deleting a target cartridge results in the cartridge disappearing from the mirror copy pool on the source VLS.

To delete cartridges, from Command View VLS:

1. On the **Cartridge Details** screen, select all the cartridges that you want to delete and erase.



2. If you have installed a Secure Erasure license, select the **With Secure Erasure** option if you want to use Secure Erasure. This option is only available if you have the license installed.
3. Click **Go**.

   The **Destroy Cartridge** wizard opens and requests confirmation.
4. Click **Yes** to continue. (You can click **No** or **Cancel** to return to the Cartridge Details screen without deleting any cartridges.)

   The system deletes the selected cartridges, and the progress of the delete operation is indicated on the **Destroy Cartridge** wizard. Secure Erasure occurs in the background after a cartridge is deleted.

   When the delete operation is complete, a success message appears.
5. Click **Finish** to exit the wizard and return to the **Cartridge Details** screen.

   When Secure Erase has completed on the cartridges, an alert notification appears on the **Notifications** screen.

Unloading a Cartridge from a Drive

If a tape becomes stuck in a drive and cannot be removed using the backup application, unload the tape using Command View VLS:

1. Select the tape drive from the navigation tree
2. From the task bar, select **Force Unload**.

   This will return the tape to its original slot.

NOTE: Upon reboot of the VLS or restart emulations, all cartridges that were in drives will NOT be returned to their original slots. They will be loaded back into the drives. Use **Force Unload** to return them to their original slots if needed.

Adding and Removing Barcode Templates

You can add and remove (delete), but not edit, cartridge barcode templates at any time.

NOTE: Deleting a barcode template does not affect the cartridges that were created using it.

To add or delete a barcode template, from Command View VLS:

1. Click the **System** tab.
2. Select **Cartridges** in the navigation tree.
3. Click **Add/Remove Barcode Templates** in the task bar. The **Add/Remove Barcode Templates** window opens.
4. To delete a barcode template, click the **Remove** button for the barcode template.

   The window refreshes when the deletion operation is finished.
5. To add a barcode template:
   a. Enter the barcode prefix (one to five alpha characters) in the **Barcode Prefix** box.
   b. Enter the number of digits for the barcode number in the **Digit Length** box.
   c. Enter the barcode suffix (one to two alpha characters) in the **Barcode Suffix** box.
   d. Enter the starting barcode number in the **Starting #** box.
   e. Click **Add** to add the new barcode template.
   f. To add another barcode template, repeat these steps.

Freeing up Storage Space

Storage space can be freed up by erasing the data on or destroying virtual media that is no longer used, such as:

- Cartridges that are no longer used by a backup application
- Cartridges that have been moved to the Firesafe that are no longer needed

Use the backup application to erase data on virtual media that is no longer used.

Destroy virtual media that is no longer needed using Command View VLS. See "Destroying Cartridges" (page 129).

NOTE: Reducing the size of the cartridges in a virtual library will not free up disk space. Storage space is dynamically assigned by the VLS as it is used. It is not reserved.

Restarting VLS Device Emulations

Restart VLS device emulations:

- If the VLS locks up
- After destroying a virtual device (library or tape drive) on the VLS and doing so leaves a gap in the virtual device LUN numbering on an Fibre Channel host port

- After adding a virtual tape drive and the default LUN number assigned to it is not consecutive with the other virtual tape drives in the same library
- After deleting external array LUNs.

CAUTION: Restarting VLS device emulations changes the default virtual device LUN numbers if there is a gap in the LUN numbering, or if there is a tape drive whose LUN number is not consecutive with the other tape drives in the same library. The firmware changes the LUN numbers as necessary to remove the gap or to make the virtual tape drive LUN numbers consecutive in each library, so that the virtual device LUN numbering meets the operating system LUN requirements. When this occurs, on each host:

- Rescan the SAN with the operating system for hardware changes.
- Rescan for new devices with the backup application and update the backup application device files.

CAUTION: Restarting VLS device emulations places the VLS cartridges back into the same library slots and tape drives they were in at the time of reboot/restart. To move the cartridges from tape drives back into the appropriate slots, use **Force Unload** from the task bar visible when you select the tape drive from the navigation tree.

To restart the VLS device emulations, from Command View VLS:

1. Click the **System** tab.
2. Select **Chassis** in the navigation tree.
3. Select **System Maintenance** under **Maintenance Tasks**.
4. Select **Restart Emulations** in the task bar. The **Restart Emulations** window opens.
5. Click **Restart Emulations** to confirm.

Updating the Firmware

CAUTION: The VLS restarts automatically when you install a firmware update.

To update the VLS firmware:

1. Obtain the VLS firmware update zip file from HP.
2. Verify the file integrity of the downloaded file. See the firmware release notes for details.
3. In Command View VLS, click the **System** tab.
4. Select **Chassis** in the navigation tree.
5. Select **Software Update** under **Maintenance Tasks**. The **Software Update** window opens.
6. Select **Browse**.
7. Select the zipped firmware upgrade file.
8. Select **Next Step**. The window displays information about the upgrade.
9. Select **Next Step** to continue. The EULA displays.
10. Select **Accept and Install** to continue.

    The screen displays a message that the upgrade was successfully installed and reboots automatically. The reboot may take several minutes.

Saving Configuration Settings

NOTE: The VLS firmware ensures a persistent VLS serial number and Fibre Channel port WWPNs, so that in the event of any hardware failure and replacement (such as the system board or Fibre Channel host bus adapter card), the VLS still appears exactly the same to the external SAN. It does this by generating a VLS serial number and Fibre Channel port WWPNs at first boot, which are based on the system board's MAC address. The VLS serial number and Fibre Channel port WWPNs are saved on the VLS hard drives and with the virtual library configuration settings in the configuration file.

HP highly recommends that you save your virtual library configuration and the VLS network settings to an external configuration file, so they can be restored in the event of a disaster.

To save your virtual library configuration and the VLS network settings to an external configuration file, from Command View VLS:

1. Click the **System** tab.
2. Select **Chassis** in the navigation tree.
3. Select **Save Config** under **Maintenance Tasks**. The **Save Configuration** window opens.
4. Right-click **Download Configuration Files**.
5. Select **Save Target As**.

   A zip file is displayed in the **File name** box.
6. Click **Save**, wait for the file to finish downloading, and then click **Close**. The **Save Configuration** window re-opens.
7. Click **Finish**.

NOTE: Optionally, you can set the device to automatically save and E-mail the configuration file at midnight after the configuration is modified. See "Edit the Email Settings" (page 137).

11 Monitoring

This section describes the various tools you can use to monitor the status of the VLS hardware and virtual devices (libraries and tape drives) and how to use them.

Status Information in the Status Pane

Status information for the VLS hardware components and virtual devices is displayed in Command View VLS on the status pane when an individual hardware component or virtual device is selected in the navigation tree.

The device status possibilities are:

- **Good**— The component, part of the component, or the virtual device is operating normally.
- **Degraded**—The component, or one or more parts of the component, has failed or is operating outside of its normal range but is still operational.
- **Critical** —The component, or one or more parts of the component, has failed or exceeded its limits. Although it is still operational, VLS failure is imminent.
- **Failed**—The component, or one or more parts of the component, has failed and the VLS is inoperable. Immediate service is needed.
- **Missing** —The VLS cannot detect the component or a part of the component.

In addition to the device status, a red or yellow alert bar will highlight specific parts of a component when that particular element within the component has failed (red) or is operating outside its normal range (yellow).

To view the status information for a VLS hardware component or virtual device, from Command View VLS:

1. Click the **System** tab.
2. Click the object in the navigation tree that represents the hardware component or virtual device that you want to view.

   The status information for the object selected, and its subobjects in the navigation tree, is displayed in the status pane.

Status Icons

The current overall status of the VLS is displayed on Command View VLS as an icon in the status banner. In addition, components or parts of a component whose condition is not **Good** are marked with the corresponding icon in the navigation tree.

Device Status Icon

The device status icon in the Command View VLS status banner indicates the overall VLS device health. The device status icon is displayed in the status banner regardless of the tab selected.

NOTE: On the **Automigration/Replication** tab, the status icon represents the health of the destination libraries, not the overall VLS device health. See Monitoring Destination Library Status (page 65).

If multiple system health conditions exist simultaneously (for example, two components are experiencing problems and have a status of warning and error, respectively), the icon representing the most serious status is displayed in the status banner.

Figure 14 Device status icon in the status banner

A device status icon can be one of four states:

Unknown—A component's operating condition is unknown. Contact HP Technical Support.

Normal—All components within the VLS are operating normally.

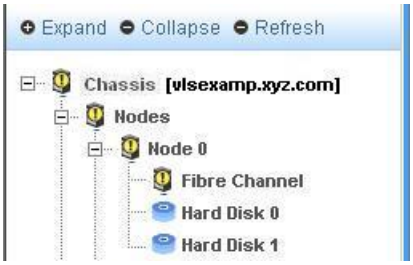
Warning—A component's operating condition has degraded.

Error—A component has failed.

Navigation Tree Icon

An icon appears just to the left of objects in the navigation tree when an unknown, warning, or error condition is present with a component. It also appears just to the left of the parent objects of that component. For example, if the icon is displayed by Fibre Channel in the navigation tree, it will also be displayed by its parent objects (for example: Node 0, Nodes, and Chassis).

Figure 15 Navigation tree icon

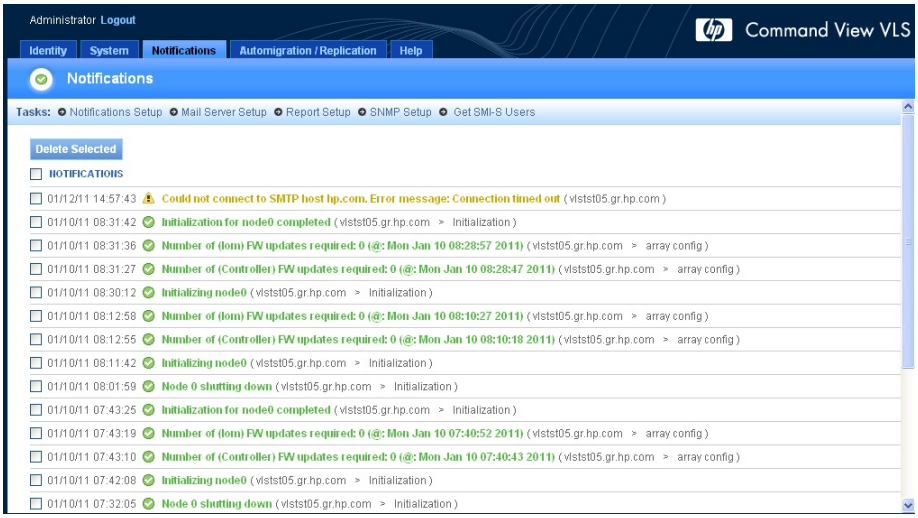


Notification Alerts

If a VLS hardware component or an environmental condition degrades or fails, the VLS generates a notification alert. Notification alerts are displayed on Command View VLS in the notification pane and on the **Notification** tab. Click the **View Details** link to view the details of a notification alert.

Notification alerts are also e-mailed to the addresses you specify and sent as SNMP traps to the management consoles you specify.

Figure 16 Notification alert examples



A notification alert can be one of four states:

Unknown—The operating condition of the component or component part is unknown. Contact HP Technical Support.

Info—The component or component part's operating condition has improved to good (OK).

Warning—The component or component part's operating condition has degraded.

Error—The component or component part has failed.

Command View VLS

To view the current and historical notification alerts for all the VLS hardware components:

1. Click the **Notifications** tab. The **Notifications** window displays.
2. Click the **View Details** link for a notification alert to view more information about the notification alert.

To view the notification alerts for a specific VLS hardware component:

1. Click the **System** tab.
2. Select the object in the navigation tree that represents the hardware component that you want to view.

   The notification alerts relevant to the object selected and its subobjects in the navigation tree are listed in the notifications pane.
3. Click the **View Details** link for a notification alert to view more information about that notification alert.

To delete notification alerts:

1. Click the **Notifications** tab. The **Notifications** window displays.
2. Select the boxes next to the notification alerts that you want to delete.
3. Click **Delete Selected**.

   The notification alerts are deleted from the **Notification** window and can no longer be viewed.

E-mail Notification

To receive VLS notification alerts by e-mail, you must edit the e-mail server settings and then edit the e-mail settings.

Editing the Email Server Settings

NOTE: You must enter the email server settings before editing the email settings.

To edit the email server settings, from Command View VLS:

1. Click the **Notifications** tab. The **Notifications** window displays.
2. Select **Edit Mail Server Settings** in the task bar. The **Edit Mail Server Settings** window opens.
3. To add a mail server:
   a. Enter the domain name for a mail server with an SMTP gateway that will process mail from the VLS in the **Outgoing Mail Server** box.
   b. If you want to change the **From** address, which defaults to `administrator@<device name>`, type the preferred address in the **Sender Email Address** box.
   c. Click **Add**.
   d. To add another email server, repeat these steps.
4. To delete an email server from the list, click the **Remove** button for the email server.

Edit the Email Settings

Email notification is sent to the persons you include on the email distribution list in the email settings. You specify the email notification alert severity and format settings for each person on the distribution list.

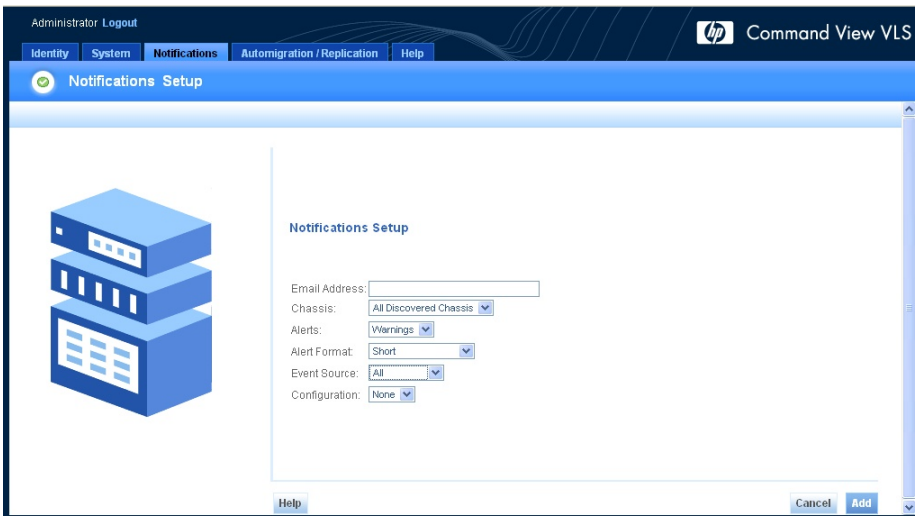
To create an email distribution list for notification alerts, add an email address to the list, or remove an email address from the list:

1. Log in to Command View VLS as the administrator. See Opening a Command View VLS Session from a Web Browser (page 99).
2. Click the **Notifications** tab.

   The **Notifications** window displays.
3. Click **Edit Email Settings** in the task bar.

   The **Edit Email Settings** window opens (Figure 17 (page 137)).

Figure 17 Edit Email Settings window



4. To add an email address:
   a. Enter an email address in the **Email Address** box.
   b. Select the chassis you want to monitor in the **Chassis** box.
   c. Select the type of notification alerts to send in the **Alerts** box.
      - **All**—Sends all notifications
      - **Errors**—Sends only errors
      - **Warnings**—Sends only warnings
      - **None**—Sends no notifications
   d. Select a notification alert format in the **Format** box.
      - **Short**—Sends short mail messages
      - **Long**—Sends detailed mail messages
      - **Long + Attachment**—Sends detailed mail messages and relevant log files
      - **Configuration**—Saves the VLS configuration and emails it at midnight after any configuration change.
   e. Click **Add**.
   f. To add another email address, repeat these steps.
5. To delete an email address, click the **Remove** button for the email address.

6. To test an email address entry, click **Test Email**.

   If the test message is not received at the email address, check the email server settings.

SNMP Notification

To receive VLS notification alerts on a management consoles, you must edit the SNMP settings to specify the management consoles you want to receive VLS SNMP traps.

Editing the SNMP Settings

NOTE: To display VLS notification alerts on a management console, the management console must be running HP Systems Insight Manager, and be configured to receive SNMP traps from the VLS.

To add a management consoles to the SNMP alert distribution list from Command View VLS:

1. Click the **Notifications** tab.

   The **Notifications** window displays.
2. Select **SNMP Setup** in the task bar.

   The **SNMP Setup** window opens.
3. To add management consoles:
   a. Enter the host name of a management console that you want to receive VLS SNMP traps in the **Hostname** box.
   b. Enter the string name that is passed with the set to get commands from the management console in the **Community String** box.

      This value is typically set to **Public**.
   c. Select the Event Source from the drop-down list to determine which types of notifications to receive (All, Nodes, Disk Arrays, or Deduplication).
   d. Select the appropriate trap version for the management application that will receive the SNMP traps in the **Trap Version** box.

      Select **1** for the trap version if your management application is HP Systems Insight Manager.
   e. Select the Severity of notifications to receive (Errors, Warnings, or All) from the drop-down list.
   f. Select the Chassis of interest (All Discovered Chassis or a specific chassis) from the drop-down list.
   g. Click **Add**.
   h. To add another management console, repeat these steps.

      You can add up to eight management consoles.
4. To delete a management console from the list, click the **Remove** button for the management console.

Editing the SNMP Community String

To change the SNMP community string:

1. Click the **Notifications** tab.
2. Select **SNMP Setup** in the task bar.
3. Select **Change Community String** in the task bar.
4. In the dialog box, enter the new Read and Read-Write community strings.
5. Click **Save**.

   The SNMP restarts automatically.

6. Test the system using the new community strings to ensure your changes were applied.

SMI-S Support

SMI-S support allows applications attached to the VLS to detect the virtual library configuration and to allow some users to change the state of the VLS.

To protect access to the VLS via the SMI-S agent, and to allow a higher level of security for the device, there are two access categories:

- Read-only access allows you to view SMI-S objects but not change them. This is used by 3rd party monitoring products, ISEE, and other components that need visibilty but not control of the VLS configuration.
- Read and write access allows complete control of the device including the ability to reboot, move tapes, change port map settings, etc.

△ **CAUTION:** Because of its destructive potential, this functionality should be strictly controlled.

To disable an SMI-S user:

1. From the **Notifications** tab task bar, select **Get SMI-S users**.

   The **SMI-S Users** screen displays listing **Read Only Users** and **Read Write Users**.
2. Under the user's name, select **disable**.

   The **SMIS-Users** screen refreshes and displays the message, “The [Read Write or Read Only] User was successfully disabled.” The **disable** button for that user is replaced by the **enable** button.

To enable a user:

1. From the **Notifications** tab task bar, select **Get SMI-S users**.

   The **SMI-S Users** screen displays listing **Read Only Users** and **Read Write Users**.
2. Under the user's name, select **enable**.

   The **SMIS-Users** screen refreshes and displays the message, “The [Read Write or Read Only] User was successfully enabled.” The **enable** button for that user is replaced by the **disable** button.

To change a user's password:

1. From the **Notifications** tab task bar, select **Get SMI-S users**.

   The **SMI-S Users** screen displays listing **Read Only Users** and **Read Write Users**.
2. Under the appropriate user's name, select **change password**.

   The **change password** screen displays.
3. Enter the new password for the user in both fields.
4. Select **Submit**.

   The **SMIS-Users** screen refreshes and displays the message, “The [Read Write or Read Only] User's password was successfully changed.”

NOTE: Viewing and managing users with SMI-S access is the only SMI-S-associated functionality on the VLS itself. The benefits of SMI-S are evident on applications attached to the VLS.

Monitoring Storage Capacity

The Capacity Manager is a tool that constantly monitors your VLS storage utilization. The Capacity Manager provides a centralized graphical view of the storage capacity utilization by devices in your VLS. The graphical representation of the data allows easy, in-depth capacity monitoring by providing overall system capacity view, storage pool view, library view, and cartridge view.

The Capacity Manager screens are designed to provide quick information for monitoring and diagnostic purposes. The overall data reduction (compression plus optional deduplication) of your VLS is displayed by the ratio provided under the various views. Capacity Manager screens are accessible to both the administrator and guest users.

The Capacity Manager provides storage statistics based on the existing backup data on your VLS. The Capacity Manager screens are interactive and allow real-time reporting to facilitate information sharing. The comprehensive view of storage capacity allows you to keep track of the amount of storage that has been allocated to the different storage pools.

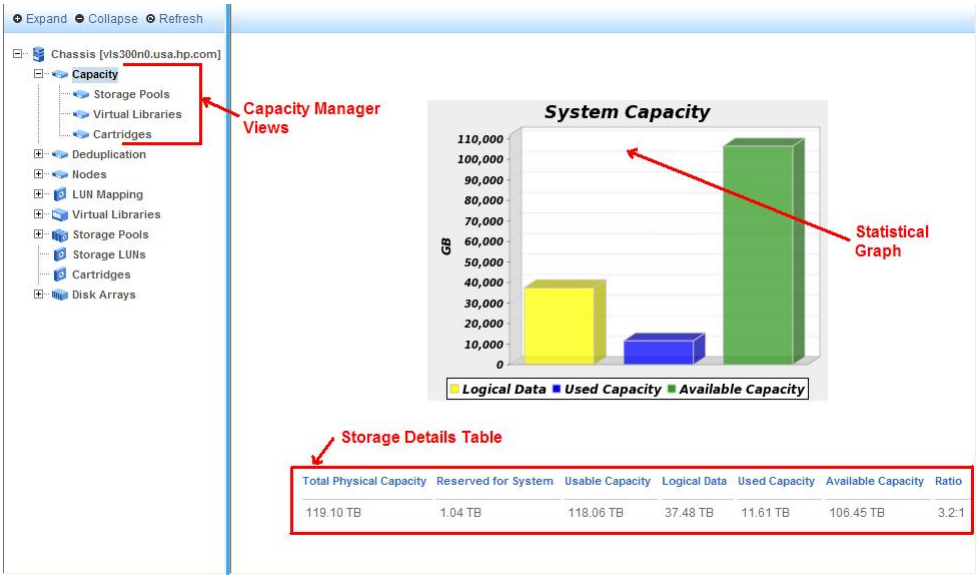
The Capacity Manager is designed to assist you in identifying future storage requirements from a storage pool perspective.

Accessing the Capacity Manager

To access the Capacity Manager screens with different capacity usage views:

1. Log into Command View VLS.
2. From the side bar Navigation Tree, select **Capacity** to display the **System Capacity** screen.

Figure 18 System Capacity Screen



3. Expand the navigation tree to display the usage view options.

The Statistical Graph provides information for the component's overall storage utilization. The Storage Details table provides a detailed storage utilization listing of the selected component.

Capacity Usage Views

This section describes the various information screens related to the system capacity.

System Capacity View

The System Capacity screen presents a summary of the system's overall storage capacity utilization. The Statistical Graph on the System Capacity view displays the Logical, Used and Available capacity in your VLS. The System Capacity table lists the following capacity values:

Table 14 System Capacity Table

Total Physical Capacity	Total physical storage capacity purchased and installed on the system. This is the sum of all LUN capacity in the pool, minus the space reserved for formatting overhead.
Reserved for System	The space required for system overhead and metadata. Storage Pool 1 or the FireSafe can have more space reserved than other storage pools due to Deduplication metadata that can be up to 2 TB.
Usable Capacity	The physical storage capacity available for user data. This is the total Physical Capacity less the space reserved for the system.
Logical Data	The size of all backup data currently retained and visible to the backup application.
Used Capacity	The physical storage used for data whether or not it is deduplicated.
Available Capacity	The physical storage currently available for additional backup data. This is the total Usable Capacity less the Used Capacity.
Ratio	The ratio of Logical Data to Used Capacity.

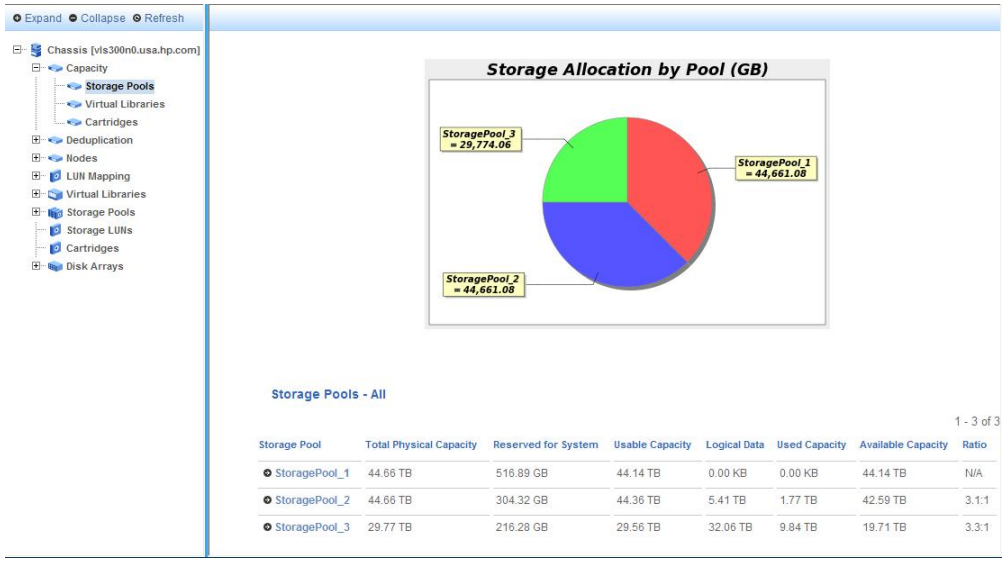
Storage Pool View

To navigate to the Storage Pools link:

- On the navigation tree, select System > Chassis > Capacity > Storage Pools.

The **Storage Allocation by Pool** screen displays the statistical graph that depicts all the storage pools in your VLS. The graph also displays the total capacity of each storage pool.

Figure 19 Storage Allocation by Pool Screen



The **Storage Pool Capacity** table lists the following capacity values:

Table 15 Storage Pool Capacity Table

Storage Pool	The name of the storage pool. This is a link to display information about the storage pool.
Total Physical Capacity	Total physical storage capacity purchased and installed on the system. This is the sum of all LUN capacity in the pool, minus the space reserved for formatting overhead.

Table 15 Storage Pool Capacity Table *(continued)*

Reserved for System	The space required for system overhead and metadata. Storage Pool 1 or the FireSafe can have more space reserved than other storage pools due to Deduplication metadata that can be up to 2 TB.
Usable Capacity	The physical storage capacity available for user data. This is the total Physical Capacity less the space reserved for the system.
Logical Data	The size of all backup data currently retained and visible to the backup application.
Used Capacity	The physical storage used for data whether or not it is deduplicated.
Available Capacity	The physical storage currently available for additional backup data. This is the total Usable Capacity less the Used Capacity.
Ratio	The ratio of Logical Data to Used Capacity.

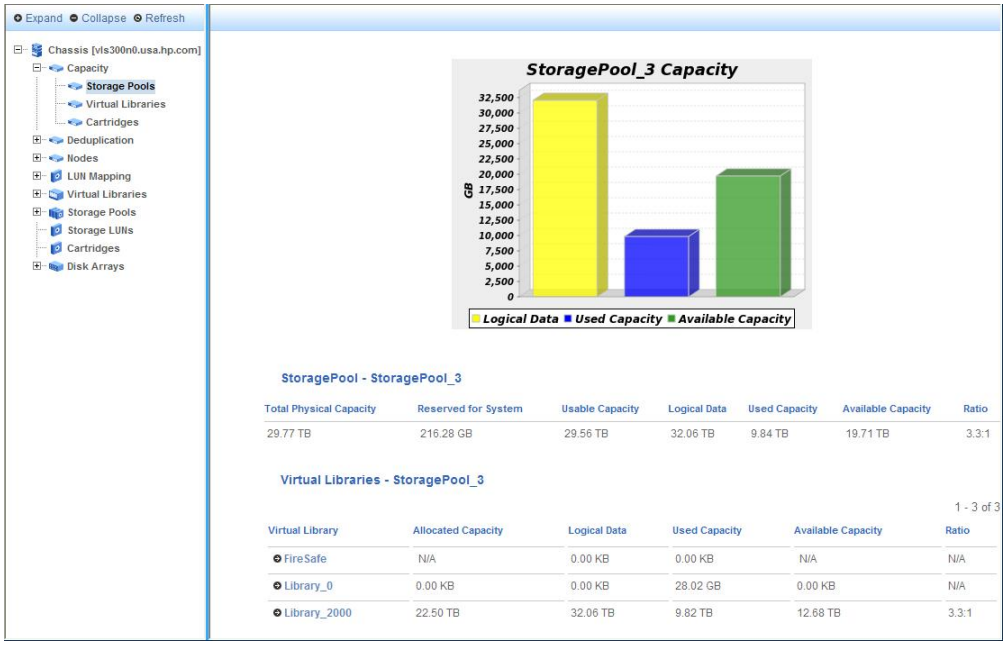
Viewing Additional Information about a Storage Pool

To view additional capacity information for a particular storage pool:

- On the **Storage Allocation by Pool** screen, click the Storage Pool name field.

The **Storage Pool Capacity** screen displays the over all capacity information for the selected storage pool and a graphical representation showing the Logical, Used, and Available storage capacity.

Figure 20 Storage Pool Capacity Screen



The **Storage Pool Capacity** table lists the following capacity values:

Table 16 Storage Pool Capacity Table

Total Physical Capacity	Total physical storage capacity purchased and installed on the system. This is the sum of all LUN capacity in the pool, minus the space reserved for formatting overhead.
Reserved for System	The space required for system overhead and metadata. Storage Pool 1 or the FireSafe can have more space

Table 16 Storage Pool Capacity Table *(continued)*

	reserved than other storage pools due to Deduplication metadata that can be up to 2 TB.
Usable Capacity	The physical storage capacity available for user data. This is the total Physical Capacity less the space reserved for the system.
Logical Data	The size of all backup data currently retained and visible to the backup application.
Used Capacity	The physical storage used for data whether or not it is deduplicated.
Available Capacity	The physical storage currently available for additional backup data. This is the total Usable Capacity less the Used Capacity.
Ratio	The ratio of Logical Data to Used Capacity.

If there are libraries in this storage pool, a table listing the library and FireSafe capacity information is displayed. You may need to scroll down to view additional capacity information.

The **Libraries Capacity** table lists the following capacity values:

Table 17 Libraries Capacity Table

Library	The name of the library or FireSafe in the storage pool *n*.
Allocated Capacity	Total storage capacity allocated to the Library. This is the product of the number and size of the cartridges in the Library. This value might be oversubscribed.
Logical Data	The size of all backup data currently retained and visible to the backup application.
Used Capacity	The physical storage used for data whether or not it is deduplicated.
Available Capacity	The physical storage currently available for additional backup data. This is the total Usable Capacity less the Used Capacity.
Ratio	The ratio of Logical Data to Used Capacity.

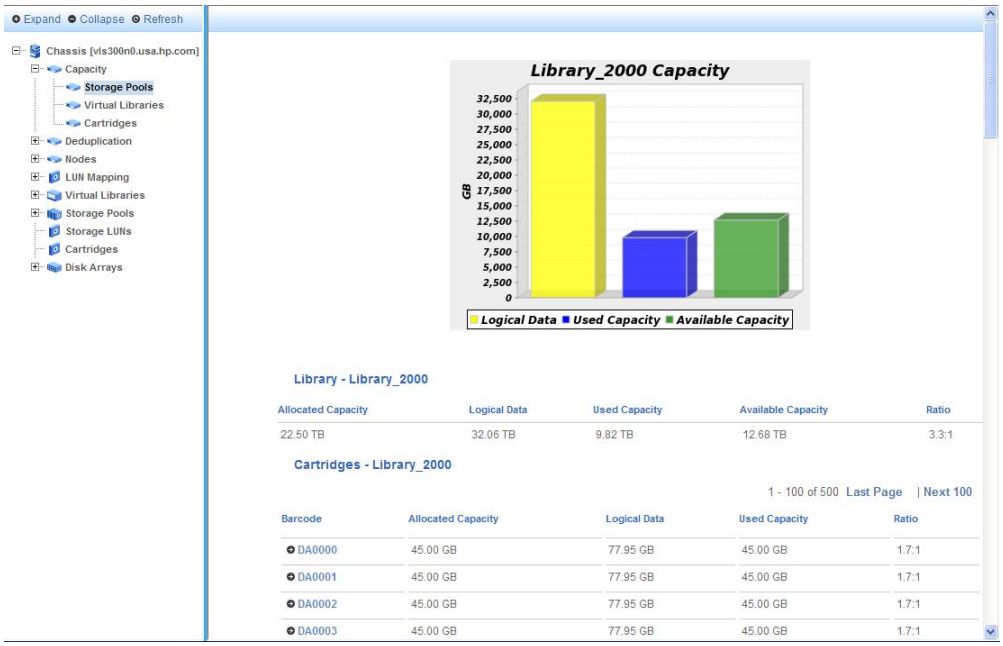
Viewing Additional Information about a Library

To view additional capacity information about a Library:

- On the information screen, click the Library name field.

The **Library Capacity** screen displays capacity information for this Library, which is a graphical representation showing the Logical, Used, and Available storage capacity.

Figure 21 Library Capacity Screen



The **Library Capacity** table lists the following capacity values:

Table 18 Library Capacity Table

Allocated Capacity	Total storage capacity allocated to the Library. This is the product of the number and size of the cartridges in the Library. This value might be oversubscribed.
Logical Data	The size of all backup data currently retained and visible to the backup application.
Used Capacity	The physical storage used for data whether or not it is deduplicated.
Available Capacity	The physical storage currently available for additional backup data. This is the total Allocated Capacity less the Used Capacity.
Ratio	The ratio of Logical Data to Used Capacity.

If there are cartridges in this library, a table listing the cartridge capacity information is displayed. You may need to scroll down to view additional capacity information.

The **Cartridges Capacity** table lists the following capacity values:

Table 19 Cartridges Capacity Table

Barcode	The barcode of the cartridges in the library. The barcode name is a link to display the capacity information about the cartridge.
Allocated Capacity	Total storage capacity allocated to the Cartridge.
Logical Data	The size of all backup data currently retained and visible to the backup application.
Used Capacity	The physical storage capacity consumed in the cartridge.
Ratio	The ratio of Logical Data to Used Capacity.

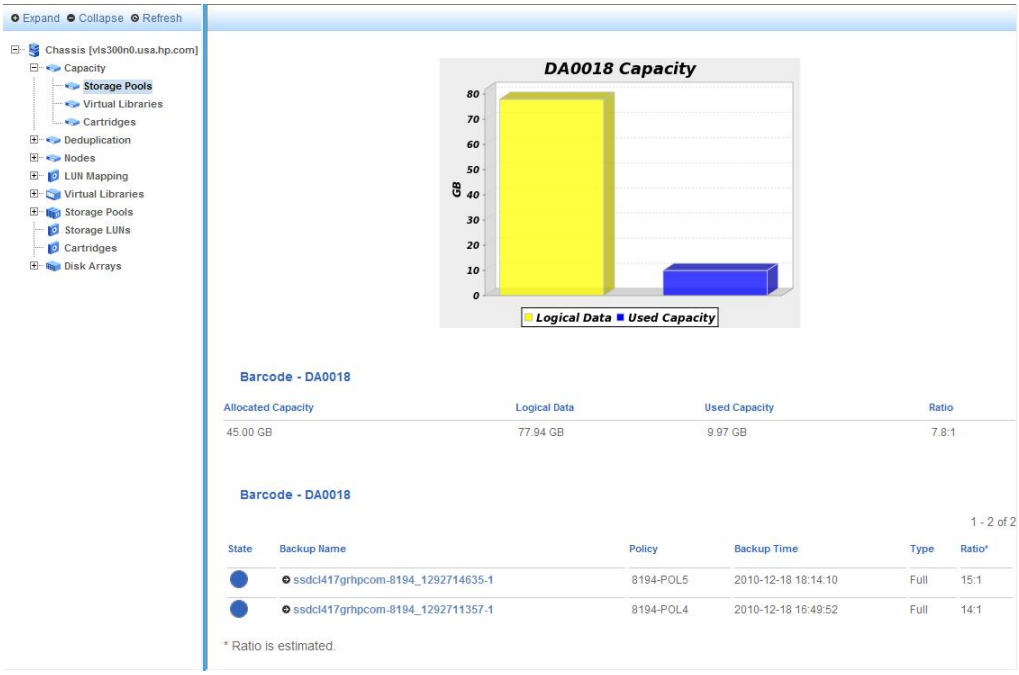
Viewing Additional Information about a Cartridge

To view additional capacity information about a cartridge:

- On the information screen, click the Barcode name field link.

The **Cartridge Capacity** screen displays capacity information for this cartridge and a graphical representation showing the Logical and Used storage capacity.

Figure 22 Cartridge Capacity Screen



The **Cartridge Capacity** table lists the following capacity values:

Table 20 Cartridge Capacity Table

Allocated Capacity	Total storage capacity allocated to the Cartridge.
Logical Data	The size of all backup data currently retained and visible to the backup application.
Used Capacity	The physical storage capacity consumed in the cartridge.
Ratio	The ratio of Logical Data to Used Capacity.

If there are backups on this cartridge, a table listing the backup information is displayed. You may need to scroll down to view additional capacity information.

The **Cartridge Backup Capacity** table lists the following capacity values:

Table 21 Cartridge Backup Capacity Table

State	The current deduplication state of the backup.
Backup Name	The name of the backup set.
Policy	The name of the policy used for the backup.
Backup Time	The time when the data was backed up.
Type	The backup type.
Dedupe Ratio	The deduplication ratio obtained.

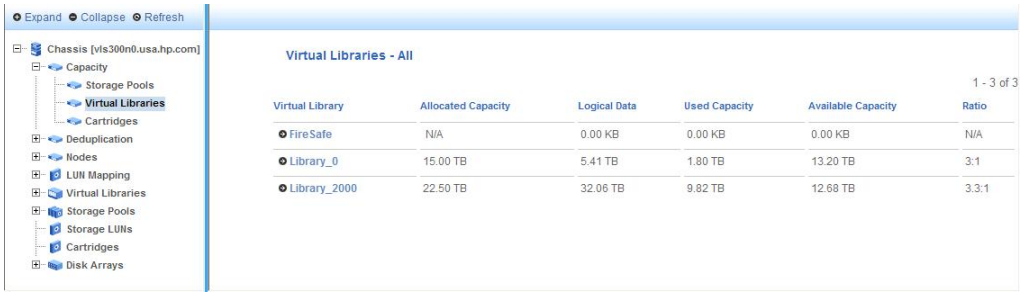
Libraries View

To navigate to the Libraries link:

- On the navigation tree, select System > Chassis > Capacity > Libraries.

The **Libraries** screen displays the list of libraries and FireSafe capacity utilization in your VLS.

Figure 23 Libraries Screen



The **Libraries Capacity** table lists the following capacity values:

Table 22 Libraries Capacity Table

Library	The name of the library or FireSafe. This is a link to display capacity information about the library or FireSafe.
Allocated Capacity	Total storage capacity allocated to the Library. This is the product of the number and size of the cartridges in the Library. This value might be oversubscribed.
Logical Data	The size of all backup data currently retained and visible to the backup application.
Used Capacity	The physical storage used for data whether or not it is deduplicated.
Available Capacity	The physical storage currently available for additional backup data. This is the total Allocated Capacity less the Used Capacity.
Ratio	The ratio of Logical Data to Used Capacity.

See "Viewing Additional Information about a Library" (page 143) for detailed library capacity utilization.

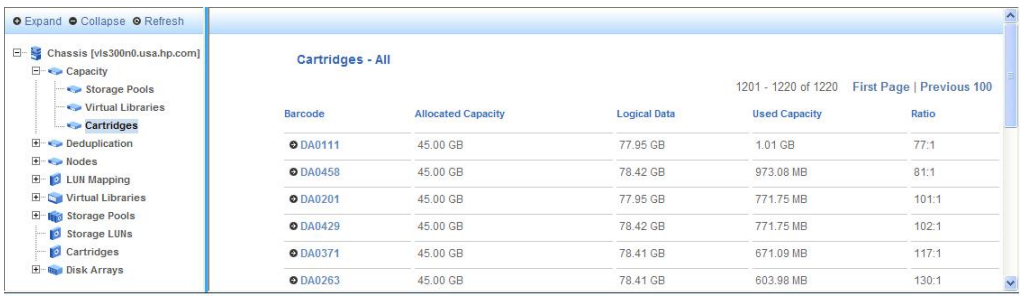
Cartridges View

To navigate to the Cartridges link:

- On the navigation tree, select System > Chassis > Capacity > Cartridges.

The **Cartridges Capacity** screen displays the list of cartridges in your VLS.

Figure 24 Cartridges Capacity Screen



The **Cartridges Capacity** table lists the following capacity values:

Table 23 Cartridges Capacity Table

Barcode	The barcode of the cartridges in the library. The barcode name is a link to display the capacity information about the cartridge.
Allocated Capacity	Total storage capacity allocated to the Cartridge.
Logical Data	The size of all backup data currently retained and visible to the backup application.
Used Capacity	The physical storage capacity consumed in the cartridge.
Ratio	The ratio of Logical Data to Used Capacity.

NOTE: The Used Capacity value for some cartridges may be greater than the Logical Data. This can be due to relabeling of a cartridge that consumes 32 MB of physical space. The Extent Size of a relabeled cartridge is fixed at 32 MB. This is added to the Used Capacity value of the relabeled cartridge, even when the cartridge has no data.

See "Viewing Additional Information about a Cartridge" (page 144) for detailed cartridge capacity utilization.

Performance and Storage Use Reports

You can customize and view current status, performance, and storage use reports for the entire VLS, for individual nodes, and for selected devices in Command View VLS. You can also view information on the overall health of the SAN.

You can generate and display the reports online, or export the report data in a comma-separated values (CSV) file-format; see Exporting CSV Data. You can also set up automated reports that the system emails to you on a regular basis; see Receiving Automated Reports (page 154).

To view and configure VLS performance, storage use, and SAN health reports:

1. From the **System** tab, select **Chassis** at the top of the navigation tree.
2. From the **Tasks** displayed at the top of the main window, select **Reporting**. The reporting tabs open to **Performance History** by default.

Exporting CSV Data

Many of the reports allow you to export the data in a comma-separated values (CSV) file-format. Determine the information you want exported and select the **Export** (or similar) button. The **File Download** window opens for you to indicate where to save the file.

The CSV export file is a text file delivered as a .zip. Each line is the record for one device, and the data fields are separated by commas or columns depending on the program used to view the file.

Configuring Performance Reports and Notifications

On the **Configuration** tab, you can assign default settings for reports and notifications. At any time, you can change any of these default settings.

Current Status Tab

For the **Current Status** tab, you can customize the default refresh time for the display.

You can also create a pre-defined custom view based on the devices you choose. At the bottom of the **Configuration** tab:

1. Select a device category.
2. Select the specific devices of interest from the **Available Devices** box.

3. Using the **>>** button, move the devices of interest into the **Selected Devices** box. These are the devices that will display in the report. You can use **<<** button to remove devices from the **Selected Devices** box.
4. Select another device category and repeat steps 2 and 3.
5. Enter a name for this view in the Create a New View field.
6. Select **Create View**.

   This view is now available as a selection in the Pre-defined Views list on the **Current Status** and **Performance History** tabs.

To edit an existing view, select it from the Update Existing View list, adjust the selected devices, rename the view (if desired) in the name field, and select **Update View**. Select **Delete View** if you want to remove that view from your Pre-defined options.

Performance History Tab

For the **Performance History** tab, you can customize:

- The default duration of the performance graphs to display
- The default duration of the CSV format export file
- The default name for the CSV format export file

You can also create a pre-defined custom view based on the devices you choose. See Current Status Tab (page 147).

SAN Health Tab and Notifications

For the **SAN Health** tab, you can customize:

- The number of SRRs (Sequence Retransmission Requests) for an item above which a notification is generated
- The number of SRRs for an item below which the item does not display in the report
- The number of Aborts for an item above which a notification is generated
- The number of Aborts for an item below which the item does not display in the report

Physical Capacity Notifications

You can determine when the system sends notifications related to the physical capacity. Set up notifications for when the physical capacity exceeds a chosen percentage.

Logical Capacity Notifications

You can determine when the system sends notifications related to the logical capacity. Set up notifications for when:

- The logical capacity usage exceeds a chosen percentage
- The system ratio falls below a chosen percentage
- The deduplication ratio falls below a chosen percentage

Current Status

The **Current Status** tab displays the overall performance and storage capacity information of the VLS in gauges at the top of the page.

You can also select specific devices to display either the performance or the storage capacity used.

Show the performance of:

- **All Nodes**
- **Pre-defined Views**

  Select one of the views from the list. You can create these views on the **Configuration** tab.
- **Most Active** (node, library, and tape drive)

Show the storage capacity (total and used) of:

- **All Storage Pools**
- **All Virtual Libraries**
- **Virtual Libraries per Storage Pool** (displays a pie chart instead of a gauge)
- **Storage Pools per Virtual Library** (displays a pie chart instead of a gauge)

Performance History

The **Performance History** tab displays a table of performance data for the selected nodes or devices as designated in the **Configuration** tab.

To determine which devices display, select one of the following:

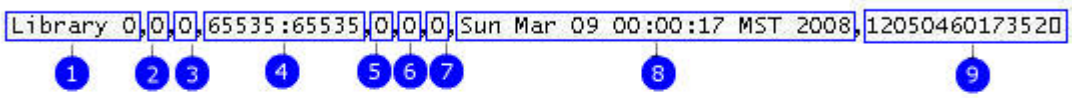
- **Nodes**
- **Pre-defined Views**, and then select a view from the list

Determine the duration of the data reported in the graphs. Valid entries are whole numbers between one and 15.

NOTE: The longer the duration you select, or the more nodes or devices your system has, the longer it may take to generate a report.

To export the CSV data, enter the number of days to include in the report and click **Export**. (See Exporting CSV Data (page 147) for more information on exporting CSV data.) See Figure 25 (page 149) for an explanation of each field in a line of CSV data.

Figure 25 CSV data fields for VLS performance reports



Item	Data
1	Device name
2	Node number
3	Target/device ID
4	Ignore this field
5	Writes
6	Bytes written/read
7	Bytes written/read in last minute

Item	Data
8	Time stamp
9	Ignore this field

SAN Health

The SAN Health tab displays information on the number and types of errors encountered on the SAN. See (page 151).

To export the CSV data, in the Export Data section of the screen enter the number of days to include in the report and click **Export**.

When you open the SAN Health tab, the graph at the bottom of the screen displays information for the top 16 locations from all location categories with the most errors. You can change the information displayed in the graph:

1. Select a location category.
2. Select the specific locations of interest from the **Available Locations** box.
3. Using the **>>** button, move the locations of interest into the **Selected Locations** box. These are the locations that will display in the report. You can use the **<<** button to remove locations from the **Selected Locations** box.
4. Select another location category and repeat steps 2 and 3.
5. Select **Update Graph**. The graph updates to reflect the information you chose.

You can also create a pre-defined custom view based on the locations you choose:

1. Follow steps 1 through 4 above.
2. Enter a name for this view in the Create a New View field.
3. Select **Create View**.

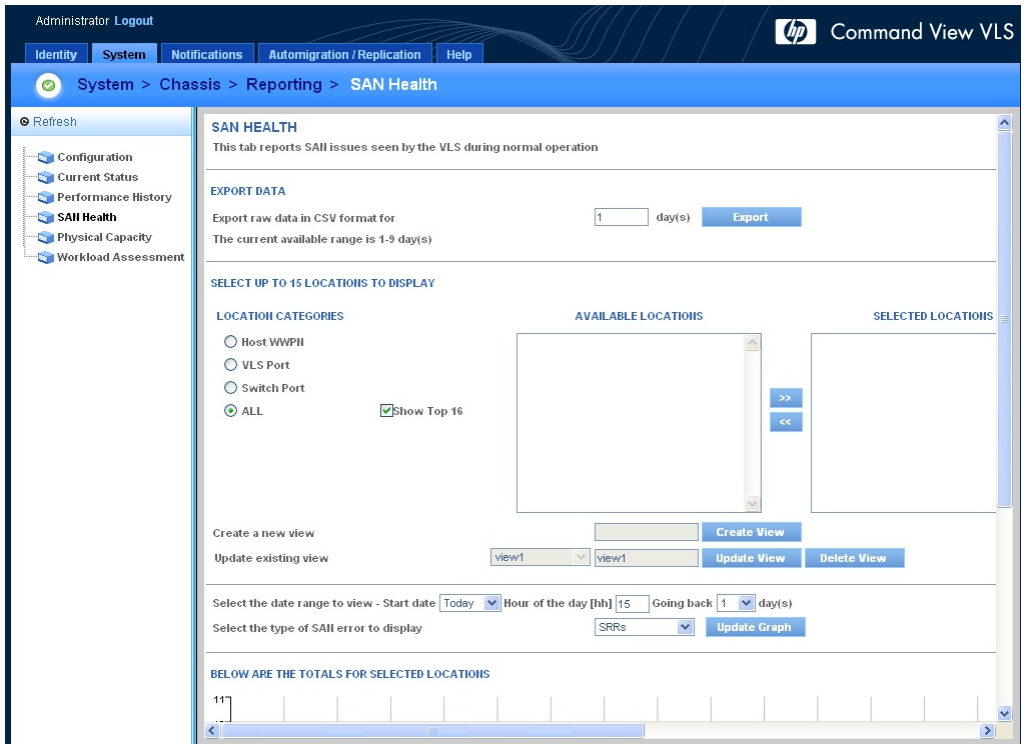
   This view is now available as a selection in the Update Existing View list.

To edit an existing view, select it from the Update Existing View list, adjust the selected locations, rename the view (if desired) in the name field, and select **Update View**. Select **Delete View** if you want to remove that view from your Pre-defined options.

To see the graph for a particular pre-defined view, select it from the Update Existing View list. The graph immediately updates to the data for that view.

To further refine a report, you can change the number of days reflected in the graph and the type of error to include in the display. Enter the information for either or both of these options and select **Update Graph**. The graph applies those boundaries to the data for the previously selected locations or pre-defined view.

Figure 26 SAN Health tab



Logical Capacity

This tab displays different views of the current logical capacity usage for an individual library or the entire VLS system. Logical capacity is the amount of data the backup application wrote, while the physical capacity is the amount of data actually stored on the disk.

Select the **Show Details** link in the first section to display the breakdown of the logical and physical capacity and the deduplication ratio. To export the deduplication CSV data, enter the number of days to include in the report and select **Export**. (See Exporting CSV Data (page 147) for more information.)

To change the information displayed in the graphs:

1. Select the date range to include in the report:
   - Start date — the date you want as the starting point for stepping back into the past by some number of days to establish a particular date range. This is effectively the end date of the date range.
   - Hour of the day — the hour of the day, in 24 hour time, to use in conjunction with the Start date.
   - Going back — the number of days to step back from the selected start date to establish a date range.

   For example, if you select June 20 at 10 going back 3 days, the graph will include data from June 17 at 10:00 a.m. to June 20th at 10:00 a.m.

   NOTE: The greater the number of days included in the date range, the fewer the data points for each day will display in the graphs. For example, for two days of data the graphs will show one data point for every two hours, while for seven days of data the graphs will show one data point for every seven hours.

2. In some cases, there are more data points than the graphs can display. You must select how the system chooses which data point to use for each time period displayed. For example, if

you show four days of data the graphs show one data point for every four-hour period. Use the Advanced Setting list to indicate which data point out of that four-hour period is used:

- First data point — the first data point for each time period.
- Maximum data point — the data point with the highest value for each time period.
- Minimum data point — the data point with the lowest value for each time period.

3. Select a specific virtual library to view from the list, or use "VLS Device" to include all libraries (Logical Capacity tab only).
4. Select **Update Graphs**. The graphs update to reflect the data options you chose.

NOTE: The final graph displays the history of the logical capacity for the entire VLS and does not change if you choose to view a specific library.

Physical Capacity

This tab displays different views of the physical capacity usage for an individual library or the entire VLS system. Physical capacity is the amount of data actually stored on the disk, while the logical capacity is the amount of data the backup application wrote. In a deduplicated environment, the physical capacity reported represents data after compression and deduplication; without deduplication it represents data after compression.

To export the physical capacity CSV data, enter the number of days to include in the report and select **Export**. (See Exporting CSV Data (page 147) for more information.)

To change the information displayed in the graphs, follow Step 1, Step 2, and Step 4 in Logical Capacity (page 151).

The final two graphs allow you to view the physical capacity for a specific storage pool or library. You can also change the graph type from stacked to line. Use the lists to make your selections and then select **Update Graphs**.

Workload Assessment

The Workload Assessment tab features a workload assessment simulation to ensure that a planned new backup will "fit" on the system with the existing backups before actually running the backup. The simulation tests the physical capacity and logical capacity thresholds; it also tests the Fibre Channel performance for each day of the week that runs an existing backup.

In addition, you can quickly see whether or not a particular library has notification alerts enabled and the alert threshold values. A threshold is a percentage or ratio value that when reached triggers the system to send a notification. For example, if you set the critical notification for the logical capacity to 90, the system will send a critical notification when the logical capacity exceeds 90% used. You can edit the notification alerts for specific libraries and for the entire VLS system on this screen. See Editing the Notification Alerts (page 153).

Running a Workload Assessment Simulation

1. Select the library of interest.
2. Select **Assess Workload**.
3. On the pop-up window, select **OK** to use a template or **Cancel** to enter all of the criteria values.
4. If you opted to use a template, select the template and then select **Run Simulation**. If you opted not to use a template, enter the criteria values and then select **Run Simulation**.

   You can add, edit, and delete templates; see Using the Workload Assessment Templates.
5. Enter the size of the full backup in GB at the top of the screen.
6. Select **Run Simulation**.

   Scroll to the bottom of the screen, if necessary, to view the simulation results. Each tested threshold receives either a green (threshold is fine) or red (threshold is exceeded) icon.

Using the Workload Assessment Templates

Deleting a workload assessment template:

1. Select the template from the template summary screen.
2. Select **Delete Template**. The template is removed from the template summary list.

Adding a new workload assessment template:

1. Select **Add New Template**.
2. Enter the template name and all other values.
3. For each day of the week, select the backup type and the start time and duration in 24–hour time.
4. Select **Create Template**. The screen displays the template summary list which now includes the one you just created.

Editing a workload assessment template:

1. Select the template from the template summary screen.
2. Select **Edit Template**.
3. Change the values as necessary.
4. Select **Update**. The screen returns to the template summary list.

Editing the Notification Alerts

To edit the notification alerts for libraries, the VLS system, and storage pools:

1. Select the VLS, or the library or storage pool of interest.
2. Select **Edit Thresholds** (libraries and VLS) or **Edit Pool Configuration** (storage pools). The screen lists the available notification alerts with default or previously set threshold values.
3. Check the top box to enable notification alerts (or uncheck it to disable alerts).
4. Enter the hour of the day for the system to send notifications in 24–hour time. For example, a value of 14 means 2:00 p.m.
5. Change the remaining values where necessary. Some values are a ratio, while others are a percentage. You can set both critical and warning notifications for:
   - System ratio — the logical data to used capacity
   - Deduplication ratio — the logical size to physical size
   - Logical capacity usage — the total amount of data written by the backup application
   - Replication traffic — the total replication data transferring across the LAN/WAN
   - Physical capacity usage — the total physical disk space used
   - Performance of the library — the overall performance of the library
6. Select **Submit**. The screen indicates that the notification alerts have been set.
7. Select **Back** to return to the Workload Assessment screen.

Replication History

This tab displays two views of the replication usage for the VLS system. The first graph shows the actual traffic; the y-axis displays the usage in MB and the x-axis displays the day of the month (dd) and time of day (hh) data points. The second graph shows the replication ratio (logical size of the backup to amount of data replicated) for each day/time data point.

To export the replication traffic CSV data, enter the number of days to include in the report and select **Export**. (See Exporting CSV Data (page 147) for more information.)

To change the information displayed in the graphs:

1. Follow Step 1 in Logical Capacity (page 151).
2. Select a specific virtual library to view from the list, or use “This Device” to include all libraries.

3. Select **Update Graphs**. The graphs update to reflect the data options you chose.

Deduplication Job History

This tab displays the count of both active and pending jobs over time to reveal trends in the deduplication jobs such as when the job load is usually light. This is useful information for job scheduling.

To export the replication traffic CSV data, enter the number of days to include in the report and select **Export**. (See Exporting CSV Data (page 147) for more information.)

To change the information displayed in the graphs:

1. Follow Step 1 in Logical Capacity (page 151).
2. Select **Update Graphs**. The graph updates to reflect the data options you chose.

Receiving Automated Reports

You can receive automated reports on a regular basis via email. To set up the automated reports:

1. In the GUI of the target VLS, select the **Notifications** tab.
2. In the task bar, select **Report Setup**.
3. Enter the email address to receive the reports.
4. Select the type of report you want to receive:
   - System Capacity — includes the initially available physical capacity, the capacity consumed, and the remaining capacity.
   - Backup Summary — includes the type of backup, the status, the before deduplication and after deduplication data size in GB, the amount of space saved by deduplication, and the amount of data unprocessed for all backup jobs in process or the queue at the time of the report.
   - Policy-Cartridge Summary — includes the cartridges involved in the policy of the backup application, the type of backup, the status, the before deduplication and after deduplication data size in GB, the amount of space saved by deduplication, and the amount of data unprocessed for all backup jobs in process or the queue at the time of the report.
   - Cartridge Utilization Report — lists the capacity used by each cartridge and includes the barcode, disk space usage in bytes, deduplication status, and dependent cartridges (if any).

     This report assists you in identifying cartridges that are consuming more storage space that you can expired to free up storage space.
   - Replication Job History — includes start and end times, data transfer time, source and target locations, and the job completion status for each job in process or in the job queue at the time the report was generated.
   - Performance History — includes performance data for all the applicable devices for each day in the reporting period. See Performance History (page 149) for a description of the CSV fields.
   - SAN Health History — includes information on the errors encountered on all the locations in the SAN including the number of service retry requests (SRR) and aborts.
   - Replication Data for ISV Import — sends an hourly email report listing which virtual cartridges have been successfully replicated in the last hour. Feed this cartridge list into a script that automatically triggers tape import jobs in the backup application (which read the new cartridge data and import this content into the media database). The target backup application can then restore from the imported virtual cartridges or copy them to physical tape, etc.

     The report fields are defined as:

ISV~<virtual cartridge barcode>~<virtual library serial number>~<virtual library slot number>

See the *HP VLS Solutions Guide* for import example scripts.

- Physical Capacity Usage — includes the total physical capacity and the physical capacity used by individual libraries and storage pools.
- Logical Capacity Usage — includes the total logical capacity and the logical capacity used by individual libraries.
- Replication Traffic — shows the total amount of replication data transferring across the LAN/WAN.

5. Select the report format you prefer. Some reports only use CVS format, while some include HTML as an option.
6. Select the frequency of the automated report. The options are one-time (as of the moment you add the report), hourly, daily, weekly, and monthly.
7. The Time, Day of Week, and Day of Month lists appear based on the frequency you selected. For example, if you select Weekly, you can then set the Time and Day of Week you want the reports to run.
8. Select **Add**. The system will run the report and email it to you at the next opportunity based on your settings.
9. Repeat the steps above to receive multiple reports.

Stress Testing Hard Disks using the Storage Exerciser

Systems running some VLS firmware versions can stress test physical storage to ensure the integrity of the hard disks using the Storage Exerciser tool. (Because it can affect overall performance, however, HP recommends not running the Storage Exerciser unless it is advised by HP support personnel.) The Storage Exerciser provides two types of test jobs:

- *Background* — enables a user to initiate a low resource test job that continually writes and reads a small amount of data at regular intervals.
- *Read-only* — reads and decompresses all data currently residing on the VLS by opening each non-empty, non-hidden cartridge. All data is decompressed but not copied to any other location or made available to any other device.

NOTE: Storage Exerciser jobs will slow down other VLS operations. Do not start a job when the performance of other VLS operations is critical.

Configuring the Storage Exerciser

In the **Configuration** tab, you can assign default settings for reports.

To customize the Storage Exerciser, from Command View VLS:

1. Select the **System** tab.
2. From the navigation tree, select **Chassis**.
3. From the task bar, select **Storage Exerciser**. A caution screen indicates that running a job will affect your system's overall performance.
4. Click **Accept**. The Storage Exerciser opens to the **Configuration** tab.
5. Choose an option or enter the information into the fields:
   - Storage Pool — the storage pool targeted in tests (All, or one specific storage pool).
   - Compressibility Ratio — the compressibility ratio for data written during a Background job. For instance, if 2:1 is selected, the data created will be compressible at 2:1 and decompressed when read back. This exercises the disks more thoroughly than without compression. A compressibility ratio of at least 2:1 is recommended.

- Number of Concurrent Jobs — the number of read or write operations (called streams) running at the same time. The larger the number, the more the storage system is stressed; you can run up to six at once.

  NOTE: A Background job can only involve one stream unless multiple storage pools are present.

- Notification Generation Options — the notifications displayed on the **Notifications** tab. Choose to generate notifications per time period (in hours and minutes) or per number of job iterations. The notifications provide links to detailed information about the jobs performed. (This configuration option is only available for some VLS firmware versions.)

6. Click **Save as Default**. The Storage Exerciser uses this information throughout the operation.

If you encounter problems with the Storage Exerciser, select **Restart Storage Exerciser Service** from the task bar. All jobs currently in progress will stop and report a status of Complete.

Storage Exerciser CLI Commands

If you have root access to the VLS, you can configure the jobs at the command line. You can also retrieve reports from `/var/log/hp/exerciser/exericser_report.log`; see Log File Fields (page 159) for an explanation of the report fields.

The command options are `start`, `stop`, and `status`.

Examples:

```
/S2100/hp/exerciser/sbin start -t readonly -p all -s 3
/S2100/hp/exerciser/sbin start -t background -p 1 -s 4 -c 3 -D 10 -T
01:30
/S2100/hp/exerciser/sbin stop -t readonly
/S2100/hp/exerciser/sbin status -t readonly
```

Where:

`-t`	test type: `readonly` or `background`
`-p`	storage pools: `all` or use the number of the individual storage pool
`-s`	concurrent streams: `1` to `6` (the default is 1)
`-c`	compressibility: `1` to `4`; 1=1:1, 2=2:1, 3=3:1, 4=4:1. Only applicable to a Background test.
`-D`	data limit in GB. Only applicable to a Background test.
`-T`	time limit: `HH:MM`. Only applicable to a Background test.

Starting and Reviewing Read-only Jobs

To run a Background job, from the **Configuration** tab:

1. Make changes to the default configuration if necessary; see "Configuring the Storage Exerciser" (page 155).
2. Select the **Read-Only Job** tab.

   This tab displays information for all previous and current Read-only jobs. The Storage Pool and Number of Concurrent Jobs fields contain the default information entered in the **Configuration** tab.

3. If you want to choose which nodes will be tested, follow the steps below. Otherwise, all available nodes are selected by default.
   a. Click the **Select Nodes** link.
   b. Select the nodes you want to test.
   c. Click **Done**.
4. If you want to choose by barcodes which cartridges to read , follow the steps below. Otherwise, all cartridges are read by default.
   a. Select Read by BarCode.
   b. Enter a search pattern in the empty field. A search pattern filters the barcodes to just those you want to the Storage Exerciser to read. You can use the following characters to enter a regular expression:
      - * = zero or more characters (standard wildcard)

        For example, enter *AB* to include all cartridges whose barcode contains the string "AB" anywhere in the barcode, or enter AB* to include all cartridges whose barcode begins with "AB."
      - ? = any single character

        For example, enter AB?CD to include all cartridges whose barcode begins with "AB," ends with "CD," and has any single character between "AB" and "CD."
   c. Click **Find**.

      If you are not satisfied with the list of barcodes to read, enter a new search pattern in the Barcode Regular Expression field at the top of the screen and click **Re-Query** to try again.
5. Click **Start**. The new job appears in the status table.
6. Click **Cancel** in the appropriate row to cancel a Read-only job.

The status table displays:

- Start Time — the date and time the job began.
- End Time — the date and time the job ended.
- Total Number of Cartridges — the number of cartridges the job will read.
- Cartridges Read — the number of cartridges read so far.
- Cartridge Read Errors — the number of read operations that failed. If the value in this column is red, select it to view a detailed list of the failed operations.
- Data Read — the amount of data in bytes read so far.
- Status — the state of the jobs can be In Progress, Cancelling, Cancelled, Complete, or Complete with Errors.

  The Complete with Errors status signifies that one or more read operations failed; this may mean the job uncovered a disk error. If a disk error has occurred, the Log Monitor Summary (page 158) on the **Background Job** tab displays a sum of errors and presents a link to view error detail and drive recommendations.
- % Complete — the percentage of cartridges read so far.

Click **Cancel** in the appropriate row to cancel a Read-only job. To delete jobs from the status table, check the jobs in the Select column, and then click **Delete Selected**.

Starting and Reviewing Background Jobs

To run a Background job, from the **Configuration** tab:

1. Make changes to the default configuration if necessary; see "Configuring the Storage Exerciser" (page 155).

2. Select the **Background Job** tab.

   This tab displays information for all previous and current Background jobs. The Storage Pool, Number of Concurrent Jobs, and Compressibility Ratio fields contain the default information entered in the **Configuration** tab.
3. If you want the job to stop after a particular time period, enter it in the Test Duration field. Otherwise, leave the Unlimited box checked to allow the test to run indefinitely.
4. If you want to restrict the maximum amount of data the job will write, enter the amount in GB in the Max Data to Write field. Otherwise, leave the Unlimited box checked to allow it to write any amount of data.
5. If you want to choose which nodes will be tested, follow the steps below. Otherwise, all available nodes are selected by default.
   a. Click the **Select Nodes** link.
   b. Select the nodes you want to test.
   c. Click **Done**.
6. Click **Start**. The job appears in the status table and will run, reading and writing data continuously, until the job duration is complete (if you added one) or until you cancel the job.

   Click **Cancel** in the appropriate row to cancel a Background job.

NOTE: During a job, one cartridge per storage pool involved in the job is created to support the background process. This cartridge can be found under the VLS cartridge list prefixed with "StorageExerciser_." You can only start one Background job at a time.

You must have at least 5 GB of free space on your VLS in order to run a Background job. If less than 5 GB is available, the Background job will fail.

The status table displays:

- Start Time — the date and time the job began.
- End Time — the date and time the job ended.
- Current Iteration — the number of the current iteration of the read/write process.
- Failed Iterations — the number of iterations that failed due to decompression error or other error.
- Data Written — the amount of data in bytes that has been written for all iterations combined.
- Data Read — the amount of data in bytes that has been read for all iterations combined.
- Status — the state of the jobs can be In Progress, Cancelling, Cancelled, Complete, or Complete with Errors.

  The Complete with Errors status signifies that one or more read operations failed; this may mean the job uncovered a disk error. If a disk error has occurred, view the Log Monitor Summary.

To delete jobs from the status table, check the jobs in the Select column, and then click **Delete Selected**.

Log Monitor Summary

The **Log Monitor Summary** displays decompression error details. You may sort the table by selecting a column header. You may delete errors by selecting the rows and then selecting **Delete Selected**.

When enclosure and/or IP address calculations are pending, select **Refresh** to refresh the information in the table. **Refresh Array Info** updates cached array information on the server. Use this if you make architectural changes such as adding arrays to the VLS.

The log monitor table displays:

- Time — the date and time the decompression error was logged in the system log.
- SDev Number — the Set Device number logged in the decompression error.
- LBA — Logical Block Address, representing the hex value of the logical location of the error in the RAID set.
- Offset — the distance in Hex from the beginning of the LBA, to the occurrence of the decompression error.
- Length — the length in Hex of the decompression error.
- Hard Disks — the calculated number of the bay in the enclosure in which the hard disk resides. The numbers start at 0 in the upper-left, increase down, and then increase to the right. For example, bay 11 is the most lower-right drive bay in the enclosure.
- Enclosure — the calculated number of the enclosure in which the hard disk that produced the error resides.
- IP — the IP address of the array in which the enclosure and hard disk reside.
- Drive part number — the part number of the particular drive.

Log File Fields

The log file is a comma-separated values (CSV) file-format. The data fields are separated by commas or columns depending on the program used to view the file.

Test summaries are logged at the beginning and end of a test. The data fields are in order as follows:

- Test_summary — indicates that this row of data is the test summary information
- Test summary ID
- Date of the test
- Test type — Background or Read-only
- Storage pools — All or the number of the storage pool tested
- Test start time
- Test end time
- Current job count
- Total job count
- Total amount of data written during the test
- Total amount of data read during the test
- Total number of successful jobs
- Total number of failed jobs
- Status of the test

Decompression errors will be logged once per occurrence. The data fields are in order as follows. See Log Monitor Summary (page 158) for descriptions not defined here:

- Decompression_error — indicates that this row of data is the decompression information.
- Decompression error ID
- Time the error occurred
- sDev Number
- LBA

- Offset
- Length
- UUID
- IP address
- Enclosure number
- Range of suggested disk numbers within the enclosure
- Part number of the faulty drive

Jobs are only logged in event of a job failure. The data fields are in order as follows:

- Job — indicates that this row of data is the job information
- Job ID
- Date of the test
- Generated job key
- Test start time
- Time of last update to the job
- Test end time
- Number of the storage pool tested
- Total amount of data written during the test at this point
- Direction — read or write
- Result — success or fail
- Message, if any, associated with the failed job
- External connect error, if any
- Source barcode of the job
- Target barcode of the job

Clearing All System Faults

If the VLS system is showing a degraded status even after the fault that lead to the degraded status has been cleared, you can force a rescan of the VLS system.

From Command View VLS:

1. On the **System** tab, select **Chassis** in the navigation tree.
2. On the task bar, select **Clear All Faults**.

   The screen refreshes and the correct status is displayed. (If the status does not change, it was already correct.) All fault notifications are cleared from the **Notifications** tab.

NOTE: This operation clears all of the arrays from Command View VLS. In about five minutes, the arrays return with an updated view.

Clearing the Hardware Compression Faults

If the VLS node is showing a hardware compression status that you think is incorrect, or if you want to verify the status shown, you can force a rescan of the node.

From Command View VLS:

1. On the **System** tab, expand **Chassis** in the navigation tree.
2. Expand **Nodes**.
3. Select the node of interest in the navigation tree.

4. On the task bar, select **Clear Compression Faults**.

   The screen refreshes and the correct status is displayed. (If the status does not change, it was already correct.) Any incorrect fault notifications are cleared from the **Notifications** tab.

Trace Log Files

You can view the current diagnostic VLS trace log files for troubleshooting purposes. You can also save one or more of the trace log files to external text files, or to a single zip file to create a support ticket.

Viewing Trace Log Files

You can view the current diagnostic VLS trace log files. From Command View VLS:

1. Click the **System** tab.
2. Select **Chassis** in the navigation tree.
3. Click **Log Viewer** under **Maintenance Tasks**.

   The **Log Viewer** window opens.
4. Click the trace log file that you want to view.

   The contents of the trace log file opens.

Saving a Trace Log File

You can save a trace log file to an external file. From Command View VLS:

1. Click the **System** tab.
2. Select **Chassis** in the navigation tree.
3. Click **Log Viewer** under **Maintenance Tasks**.

   The **Log Viewer** window opens.
4. Right-click the trace log file from the list and select **Save Target As**.
5. Enter a name for the file and click **Save**.

Creating a Support Ticket

You can save all the current diagnostic VLS trace log files to a single zipped file to create a support ticket, or pick modules to create a subset of a full ticket. From Command View VLS:

1. Click the **System** tab.
2. Select **Chassis** in the navigation tree.
3. Click **Support Ticket** under **Maintenance Tasks**.

   The **Support Ticket** screen opens. The screen displays the date and size of the last ticket you ran.
4. Click **New Ticket**.
5. Select one of the following options to determine the modules included in the support ticket:
   - Basic — includes Automigration/Replicaton, Configuration/Monitoring, VLS, Command View, and System
   - Full — includes all modules in the basic ticket plus Array and Core Files
   - Custom — includes only the modules you select. Clicking Select All runs a full ticket.
6. Click **Create Ticket**. The screen displays the progress of the support ticket for each module and each node.

   The more complex your VLS system, the longer the support ticket takes to generate. You can leave the support ticket screen and return later to check on the progress. The support ticket is complete when the **Download** button appears.

7. Right-click **Download**.
8. Select **Save Target As**.

   The name of a zip file is displayed in the **File name** box. Do not change the generated file name.
9. Click **Save**.
10. Click **Close**.
11. Click **Finish**.

NOTE: Some versions of Internet Explorer will not download support tickets with a file size greater than 2 GB. VLS systems that are large or have been running a long time may generate larger support tickets. If you try to create a support ticket in Internet Explorer and it displays a blank page, use another browser such as Firefox. Firefox will download larger support tickets but may have a delay of several minutes before allowing you to save the file.

12 CLI Command Set

This section describes the VLS command-line interface (CLI) command set. The CLI command allows you to remotely configure, manage, and monitor the VLS over the LAN using a secure shell session. It also allows you to locally configure, manage, and monitor the VLS through the serial connection.

Commands

There are two types of CLI commands:

- **CLI-only commands**

  Commands that are processed by the CLI and affect only the CLI.

- **VLS commands**

  Commands that are passed to the VLS to configure, manage, and monitor the VLS.

Conventions

All command arguments are case-sensitive and optional. They can be specified in any order. There are several option tags associated with a command. The following conventions are used in this section to identify option tags and arguments:

- An option tag is preceded by a `-`.
- The argument is separated from the option tag by a space.
- If an argument contains a space, it must be enclosed by either two single quotes or two double quotes.
- If there is no argument after an option tag, the option is a switch.
- An `*` after an argument means the argument (including its option tag) can be repeated.
- A `|` between a compound argument means one or the other argument.

CLI-only Commands

This section describes the CLI-only commands in the VLS CLI command set.

Connection Commands

Use the CLI commands in CLI connection commands to establish or close a VLS secure shell or serial user interface session.

Table 24 CLI Connection Commands

Command	Description
`bye | done | exit | logout | quit`	Terminates the CLI session.
`close`	Closes the connection to the VLS.
`getHost`	Displays the fully qualified name of the VLS and its IP address.
`connect`	Connects to a host. Where `<-tag>` can be: `-a<s>` - Host name (localhost is default) (optional) `-p<s>` - Password (optional) `-u<s>` - userid (optional)

Output Commands

Use the CLI commands in CLI output commands to control the output and display help information for the CLI commands.

Table 25 CLI Output Commands

Command	Description
`trace`	Displays the stack trace after an exception has occurred.
`verbose`	Toggles verbose output on and off. When on, all messages are output to the screen.
`version`	Indicates current CLI version. If verbose is on, the module revisions display also.
`help`	Displays CLI command usage information. Where *<-tag>* can be: `-c<command>` - Provides help information for the specified CLI command. `-all` - Lists all CLI commands and their help information.
`enableVlsLog`	Enables VLS logging. Where the options are: `-d<n>` - Debug level (1 to 9) (optional) `-h` - Displays command usage information (optional)
`disableVlsLog`	Disables VLS logging. Where the options are: `-d<n>` - Debug level (1 to 1) (optional) `-h` - Displays command usage information (optional)

VLS Commands

This section describes the VLS commands in the VLS CLI command set.

Network Settings Configuration Commands

Use the CLI commands in CLI network settings configuration commands to configure the VLS network settings via a serial session. See Opening a Serial Session (page 102).

Table 26 CLI Network Settings Configuration Commands

Command	Description
`showConfig`	Lists host name, DNS domain name, DNS address, and various other addresses. This command shows both the current internal values, as well as the original values. It also lists the current and new content of all files affected by the changes.
`setConfigValue <-tag> [value]`	Sets the value of the corresponding configuration parameter. To reset a value, enter " " (quoted space) as the value. More than one tag and value can be set at a time. Where *<-tag>* can be: `-host` - Host name (such as vlsexamp) (unqualified) `-domain` - DNS domain name (such as xyz.com) `-fullhost` - Fully qualified name (such as vlsexamp.xyz.com) `–ntpPrimary` - First NTP Server Address `–ntpSecondary` - Second NTP Server Address `-dnsaddr` - DNS server address (replaces all addresses with one line) `-dnsaddr1` - First DNS server address (cannot use with dnsaddr) `-dnsaddr2` - Second DNS server address (cannot use with dnsaddr) `-dhcp` - Has no value, indicates you want to configure the public Ethernet connection using DHCP (reset is -dhcp=false) `-ipaddr` - IP address of public Ethernet connection `-gate` - Gateway to network (xx.xx.xx.x) `-mask` - Netmask. Defaults to 255.255.255.0

Table 26 CLI Network Settings Configuration Commands *(continued)*

Command	Description
`getDateTime`	Displays the day, date, time, time zone, and year (such as Mon March 14 11:30:46 EST 2005).
`setDateTime`	Sets the date and time. Where the options are: `-d <"s">` - Date and time in yyyy-mm-dd hh:mm format (hh is 24 hour from 0) (required). Example: `setDateTime -d "2009-06-09 09:45:00"` `-h` - Displays command usage information (optional)
`commitConfig`	Saves the system values changed using `setConfigValue`.

NOTE: To reset a value to its default setting, set the option tag to " " (quoted space). For example:

```
fullhost=" "
```

The exception to this is the dhcp tag. DHCP is disabled by entering:

```
-dhcp=false
```

Any network configuration changes made using `setConfigValue` do not take effect until "committed", using the `commitConfig` command.

Configuration Commands

Use the CLI commands in CLI configuration commands to:

- Edit the Fibre Channel host port settings
- Enable oversubscription and view oversubscription settings
- View LUN mapping
- Create, view, and destroy virtual libraries, tape drives, or cartridges
- Add, view, or remove barcode templates

Table 27 CLI Configuration Commands

Command	Usage [1]
`discoverArray`	Discovers any new arrays added to the VLS.
`updateFC`	Changes the default FC host port connection settings. Where the options are: `-a <n>` - ID number of node to modify (0, ...) (optional) `-i <n>` - FC index (0, 1, ...) (required) `-l <n>` - If attached in arbitrated loop mode, specifies a hard ALPA value between 0 and 125. A value of -1 specifies a dynamically assigned ALPA. If not attached to an arbitrated loop, this parameter is ignored (required) `-r <n>` - Port number of the FC port to modify (required) `-s <n>` - Preferred speed (0-Auto, 1-One GB, 2-Two GB, 4-Four GB, or 10-Ten GB) (required) `-t <n>` - Preferred topology (0-Auto, 1-Point to Point, 2-Loop, 3-Fabric, or 4-Public Loop) (required) `-h` - Displays command usage information (optional)
`setOverSubscription`	Enables or disables oversubscription and specifies the percent storage remaining for notification. Where the options are: `-e <n>` - Enable/disable oversubscription (0-Disabled or 1-Enabled) (required) `-p <n>` - Percentage of capacity remaining for alert notification (required) `-h` - Displays command usage information (optional)

Table 27 CLI Configuration Commands *(continued)*

Command	Usage [1]
`getOverSubscription`	Returns whether the oversubscription feature is enabled or disabled and the capacity remaining percentage for notification alert. Oversubscription is enabled when `enabled = 0`. Oversubscription is disabled when `enabled = 1`.
`getLibTypes`	Returns a list of available library emulation types. Displays each library emulation's name, type, product, revision, and vendor information. Where the options are: `-l` - List only licensed types (optional) `-h` - Displays command usage information (optional)
`createLibrary`	Creates a new library with the specified maximum number of cartridge slots, input/export ports, and tape drives. Where the options are: `-a <n>` - Node ID of the node on which the library emulation will reside (0, ...) (required) `-l <n>` - LUN number to assign to library (-1 to 128) (optional) `-n <n>` - Maximum number of tape drives (required) `-p <s>` - Product (spaces allowed) (MSL6000, ...) (required) `-pm <n>` - FC port to which this library is mapped (0, 1, ...) (required) `-pt <n>` - Maximum number of input/export ports (required) `-r <s>` - Revision (0430, ...) (required) `-sl <n>` - Maximum number of cartridge slots (required) `-t <s>` - Library type name (required) `-v <s>` - Vendor (HP, ...) (required) `-y <n>` - Library type to emulate (2051, ...) (required) `-h` - Displays command usage information (optional)
`getLibs`	Returns a list of the libraries defined on the VLS.
`getLib`	Returns a summary of the specified library. Where the options are: `-a <s>` - Name of library (Library_0, ...) (required) `-h` - Displays command usage information (optional)
`getLibOpenSlots`	Returns a summary of the slot status for each defined library (open:used:total).
`destroyLib`	Deletes the specified library from the VLS. This operation takes several minutes to perform. Where the options are: `-a <n>` - Node number on which the library emulation resides (0, ...) (optional) `-f` - Force. This parameter is ignored and is present only for backward compatibility (optional) `-l <n>` - LUN number of the library to delete (required) `-h` - Displays command usage information (optional)
`getTapeTypes`	Returns a list of all tape drive emulation types available. Displays each tape drive emulation's name, type, product, revision, and vendor information. Where the options are: `-l` - List only licensed types (optional) `-h` - Displays command usage information (optional)
`createTapeDrive`	Creates the specified number of tape drives of a particular type and associates them with the specified library. Where the options are: `-a <n>` - Node ID of node on which the tape drive emulation will reside (0, ...) (required) `-c <n>` - Data compression (0=Disabled, 1=Enabled) (required) `-l <n>` - LUN number to assign to tape drive (-1 to 128) (optional) `-la <n>` - Node number on which the library emulation of the library to associate with the tape drives resides (0 to 3) (required) `-ll <n>` - LUN number of library with which to associate tape drive (0, 1, ...) (required) `-n <n>` - Number of tape drives (required)

Table 27 CLI Configuration Commands *(continued)*

Command	Usage [1]
	`-p <s>` - Product (DLT7000, SDLT320, ...) (required) `-pm <n>` - FC port to which this tape drive is mapped. (required) `-r <s>` - Revision (R138, ...) (required) `-t <s>` - Tape drive type name (required) `-v <s>` - Vendor (Quantum, HP, ...) (required) `-y <n>` - Tape drive type (3, 4, ...) (required) `-h` - Displays command usage information (optional)
`getTapeDrives`	Returns a list of all tape drives defined in the VLS. Where the options are: `-a <s>` - Library name (Library_0, ...) (required) `-h` - Displays command usage information (optional)
`getTapeDrive`	Returns the configuration information for the specified tape drive. Where the options are: `-a <s>` - Name of desired tape drive (TapeDrive_1, ...) (required) `-h` - Displays command usage information (optional)
`getTapeDriveStats`	Returns the R/W statistics of the specified tape drives.
`getAllTapeDriveStats`	Returns the R/W statistics of all existing tape drives.
`destroyTapeDrive`	Deletes the specified tape drive from the VLS. Where the options are: `-a <n>` - Node number on which the tape drive resides (0 to 3) (optional) `-f` - Force. This parameter is ignored and is present only for backward compatibility (optional) `-l <n>` - LUN number of the tape drive to delete (1, 2, ...) (required) `-la <n>` - Number of the node on which the library emulation to which the tape drive is associated resides (required) `-ll <n>` - LUN number of the library associated with the tape drive to delete (required) `-h` - Displays command usage information (optional)
`addBarCodes`	Creates a new barcode template. Where the options are: `-b <s>` - Barcode prefix to use for the barcode (up to 5 alpha characters) upper case and/or numeric (required) `-i <n>` - Starting numeric value for the cartridges created with this template (1 to 1024) (required) `-u <n>` - Barcode suffix length. Number of digits for cartridge sequencing (1 to 16) (required) `-s <n>` - Barcode suffix to use for the barcode upper case and/or numeric (required) `-h` - Displays command usage information (optional)
`getBarCodes`	Returns a list of all the barcode templates (and their settings) that have been defined. Displays each barcode template's name, prefix, start index, and suffix length.
`deleteBarCode`	Deletes the specified barcode template. Where the options are: `-a <s>` - Barcode prefix (required) `-f` - Force. This parameter is ignored and is present only for backward compatibility (optional) `-h` - Displays command usage information (optional)
`getCartsBySP`	Gets cartridges by storage pool name. Where the options are: `-a <s>` - Storage pool name (StoragePool_#) (optional) `-h` - Displays command usage information (optional)

Table 27 CLI Configuration Commands *(continued)*

Command	Usage [1]
`getCartTypes`	Returns a list of available cartridge emulation types. Displays each cartridge emulation's name, type, and capacity information. Where the options are: `-l` - List only licensed types (optional) `-h` - Displays command usage information (optional)
`getCartTypesByTape`	Returns a list of available cartridge emulation types for the tape drive specified. Displays each cartridge emulation's name, type, and capacity information. Where the options are: `-a <s>` - Name of tape drive type (required) `-h` - Displays command usage information (optional)
`createCartridge`	Creates the specified number of cartridges with the specified barcode and associated with the specified library. Note: If you specify more cartridges than slots defined for the library, this command only creates enough cartridges for the slots available. That is, if your library has 100 slots and you specify 125 total cartridges, this command creates 100 cartridges. Likewise, if 50 cartridges were already created for this library, this command would create only 50 more cartridges, even though 125 are specified by the command. Where the options are: `-a <s>` - Cartridge name (DLT, ...) (required) `-b <s>` - Barcode prefix (required) `-c <n>` - Capacity in gigabytes (required) `-l <s>` - Library name (Library_0, ...) (required) `-n <n>` - Number of cartridges (required) `-ov <n>` - Oversubscribe (0 or 1) (required) `-s <s>` - Storage pool name (StoragePool_#) (optional) `-y <n>` - Cartridge type (2, ...) (required) `-h` - Displays command usage information (optional)
`getCartridges`	Returns a list of the cartridges that have been created. All cartridges have both a VLS filename (cartridge name) and a barcode label. This command returns the following cartridge metadata: • Storage pool the cartridge resides (SD_1_0) • Cartridge VLS filename • Cartridge capacity (in GB) • Consumed capacity (in GB) • Cartridge type • Timestamp value for when it was last loaded • Whether or not it is write-enabled (0) or write-protected (1) • Library to which it belongs • Barcode label
`getCartsByLib`	Returns a list of the cartridges associated with the specified library. Where the options are: `-a <s>` - Name of library (Library_0, ...) (required) `-h` - Displays command usage information (optional)
`getCartsByBarcode`	Returns the cartridge metadata for the number of cartridges indicated having the specified barcode. Where options are: `-b<s>` - Barcode prefix (required) `-i<n>` - Starting numeric value for the cartridges created with this template (required) `-n <n>` - Ending numeric value for the cartridges to retrieve (required) `-h` - Displays command usage information (optional)

Table 27 CLI Configuration Commands *(continued)*

Command	Usage [1]
`removeCartridge`	Deletes the specified cartridge and its user data from the VLS. Where the options are: `-a <s>` - VLS filename of cartridge to delete (required) `-b <s>` - Barcode value of cartridge to delete (required) `-c <n>` - Capacity of cartridge to delete in gigabytes (required) `-f` - Force. This parameter is ignored and is present only for backward compatibility (optional) `-l <s>` - Name of library with which cartridge is associated (Library_0, ...) (required) `-s <s>` - Storage LUN name (SLun_#) (optional) `-h` - Displays command usage information (optional)
`getStorageCapacity`	Returns the total usable storage capacity of the storage pool. Where the options are: `-a <s>` - Storage pool name (StoragePool_#) (optional) `-h` - Displays command usage information (optional)
`getStorageCapacities`	Returns a list of the usable storage capacity of each storage pool on the VLS.
`getStorageLuns`	Returns a list of the storage LUNs on the VLS. List includes the storage LUN name, IP address, storage pool number, number in storage pool, and so on for each LUN.
`getStorageLunsByArray`	Returns a list of the storage LUNs in the disk array. Where the options are: `-a <s>` - Disk array IP address (required) `-h` - Displays command usage information (optional)
`getStorageLunsBySP`	Returns a list of the storage LUNs on the storage pool. Where the options are: `-a <s>` - Storage pool name (StoragePool_#) (optional) `-h` - Displays command usage information (optional)
`getStorageLunsByNode`	Returns a list of the storage LUNs on the node. Where the options are: `-a <n>` - Node ID (0, 1, 2, ... - default is 0)) (optional) `-h` - Displays command usage information (optional)
`createStoragePool`	Creates a new storage pool. Where the options are: `-n <n>` - maximum number of cartridges (1 to 8000) (optional) `-h` - Displays command usage information (optional)
`deleteStoragePool`	Deletes a storage pool. Where the options are: `-a <s>` - Storage pool name (StoragePool_#) (required) `-h` - Displays command usage information (optional)
`deleteAllStoragePools`	Deletes all storage pools on the VLS and all the LUNs in all storage pools.
`getStoragePoolNames`	Returns a list of the storage pool names on the VLS.
`getStoragePool`	Returns information about the storage pool, such as primary LUN name, allocated capacity, capacity, extent size, used capacity, and number of LUNs. Where the options are: `-a <s>` - Storage pool name (StoragePool_#) (optional) `-h` - Displays command usage information (optional)
`getStoragePoolSummary`	Returns summary of storage pool information for all storage pools on the VLS.
`addHost`	Adds the specified host in the SAN list.
`listHostState`	Lists the current host state for all hosts in the SAN list.
`setHostState`	Sets the host state for specified host.
`setHostStateAll`	Sets the host state for all hosts in the SAN list to the state specified.

Table 27 CLI Configuration Commands *(continued)*

Command	Usage [1]
`listAccessMode`	Lists the current host access mode for all enabled hosts in the system.
`setAccessMode`	Sets the host access mode for all enabled hosts in the system.
`setAlias`	Sets the alias for the hostname of the specified host.
`removeHost`	Deletes the specified host from the SAN list.
`addLunMap`	Adds the specified device to the host.
`listLunMap`	Lists the host LUN map for specified device.
`deleteLunMap`	Deletes the specified device from the host.
`getTapeSerialCompatibilityMode`	Returns the compatibility mode for the virtual serial numbers.
`setTapeSerialCompatibilityMode`	Sets the compatibility mode for the virtual serial numbers. Upgrading to VLS firmware version 3.3.0 cause the colons in serial numbers to change to periods. `-m <s>` - Compatibility mode • `Standard` = default, keeps change of using periods instead of colons • `Legacy` = changes periods to back to colons
`getWwnnCompatibilityMode`	Returns the firmware version compatibility mode for the WWNNs.

[1] <s> = string; <n> = number; <f> = filename

Management Commands

Use the CLI commands in CLI Management commands to:

- Change the account passwords
- Manage cartridges
- Restart the VLS device emulations
- Save configuration settings
- Restore configuration settings

Table 28 CLI Management Commands

Command	Usage [1]
`changePassword`	Resets the administrative password, or changes the administrative or user password. Command View VLS automatically restarts after changing the passwords to make the changes take effect. Where the options are: `-admin` - Reset the administrator password (-u and -p are ignored) (optional) `-p` - Password (no spaces) (optional) `-u` - Username (administrator or user). Default is current user. (optional) `-h` - Displays command usage information (optional)
`editCartridge`	Changes parameters on an existing cartridge. Where the options are: `-a <s>` - VLS filename of the cartridge (required) `-b <s>` - Barcode label of the cartridge (required) `-c <n>` - Current capacity of the cartridge in gigabytes (optional). Only required if changing the cartridge capacity. `-l <s>` - Name of library in which the cartridge resides (Library_0, ...) (required) `-nc <n>` - Desired new capacity of the cartridge in gigabytes (optional) `-nl <s>` - Name of the new library if moving cartridge (Library_1, ..) (optional) `-s<s>` - Storage LUN name (SLun_#) (required) `-w` - Write protect? (0-read/write or 1-read only) (optional)

Table 28 CLI Management Commands *(continued)*

Command	Usage [1]
	`-y <n>` - Cartridge emulation type (2, 3, ...) (required) `-h` - Displays command usage information (optional)
`restartEmulations`	Restarts the VLS device emulations.
`restartCommandViewVLS`	Restarts Command View VLS.
`restartSystem`	Shuts down and restarts the VLS node.
`shutdownSystem`	Shuts down the VLS node so it can be powered off.
`shutdownNode`	Shuts down the VLS node so it can be powered off.
`saveAllConfig`	Where the options are: `-o <s>` - Saves the VLS virtual library configuration and network settings to the specified external configuration file. `-h` - Displays command usage information (optional)
`restoreAllConfig`	Where the options are: `-in <s>` - Restores the VLS virtual library configuration and network settings from the specified external configuration file. `-h` - Displays command usage information (optional)

[1] <s> = string; <n> = number; <f> = filename

Monitoring Commands

Use the CLI commands in CLI monitoring commands to:

- View the VLS health status
- View or delete notification alerts
- Add, view, or delete E-mail servers to route notification alerts
- Add, view, or delete E-mail addresses for notification alerts
- Add, view, or delete SNMP management consoles to receive notification alerts

Table 29 CLI Monitoring Commands

Command	Usage [1]
`getHealth`	Returns the VLS health status as a number (0-good, 1-degraded, 2-critical, 3-failed, 4-missing).
`getChassis`	Returns information about the VLS displayed on the Identity Tab window.
`getNode`	Returns information on the node. Where the options are: `-a <s>` - Node name (Head_0, ...) (required) `-h` - Displays command usage information (optional)
`getNodeNames`	Returns the list of nodes in the VLS.
`getNodeFault`	Returns fault information for the specified node. Where the options are: `-a <s>` - Node name (Head_0, ...) (required) `-h` - Displays command usage information (optional)
`getNotificationsCount`	Returns the number of notification messages specified counting back from the most recent. Where the options are: `-n <n>` - Maximum number of notifications to return (required) `-h` - Displays command usage information (optional)

Table 29 CLI Monitoring Commands *(continued)*

Command	Usage [1]
`getNotificationsDate`	Returns all the notification alert messages that occurred starting with the specified date. Where the options are: `-d` - mm/dd/yy on or after this date (required) `-h` - Displays command usage information (optional)
`deleteNotifications`	Deletes the specified notification alerts from the VLS. Where the options are: `-id <s>` - ID number of notification to delete (required) `-h` - Displays command usage information (optional)
`addEmailServer`	Specifies an E-mail server with an SMTP gateway to route notification alerts from the VLS. Where the options are: `-a <s>` - E-mail server address (required) `-c <s>` - node IP address (required) `-s <s>` - Sender email address (optional) `-h` - Displays command usage information (optional)
`getEmailServer`	Returns the E-mail server configuration settings for notification alerts.
`deleteEmailServer`	Deletes the specified E-mail server from the E-mail notification alerts settings. Where the options are: `-a <s>` - E-mail server address (required) `-c <s>` - VLS node IP address (required) `-f` - Force - This parameter is ignored and is present only for backward compatibility (optional) `-h` - Displays command usage information (optional)
`addEmail`	Adds an E-mail address and desired report formatting to the E-mail notification alert settings. Where the options are: `-a <s>` - E-mail address (required) `-c <s>` - VLS IP address (required) `-s <n>` - Severity (1-Error, 2-Warning, 4-Info, or 8-Unknown) (optional) `-y <n>` - E-mail type (1-Long with attachment, 2-Long, 4-Short, or 8-Reports) (optional) `-h` - Displays command usage information (optional) `-f <n>` - Notification frequency (0-None, 1-Daily, 2-Weekly, 3-Bi-weekly, or 4-Monthly) (optional)
`getEmail`	Returns the report settings for each E-mail address configured for notification alerts.
`deleteEmail`	Deletes the specified E-mail address from the E-mail notification alert settings. Where the options are: `-a <s>` - E-mail address (required) `-c <s>` - VLS node IP address (required) `-f` - Force. This parameter is ignored and is present only for backward compatibility (optional) `-y <n>` - Email type (1-long with attachment, 2-long, 4-short, 8-reports, 16-configuration) (required) `-h` - Displays command usage information (optional)
`addSnmpServer`	Specifies an SNMP management console to receive SNMP traps from the VLS. Where the options are: `-a <s>` - SNMP server IP address (required) `-c <s>` - VLS node IP address (required) `-m <s>` - Community (Public, ...) (required) `-v <s>` - Trap version (required) `-s <n>` - Severity (1-Error, 2-Warning, 4-Info, or 8-Unknown) (required)

Table 29 CLI Monitoring Commands *(continued)*

Command	Usage [1]
	`-h` - Displays command usage information (optional)
`getSnmp`	Returns the SNMP management console configuration settings for notification alerts.
`deleteSnmpServer`	Deletes the specified SNMP management console from the SNMP notification alert settings. Where the options are: `-a <s>` - SNMP server IP address (required) `-c <s>` - VLS node IP address (required) `-f` - Force. This parameter is ignored and is present only for backward compatibility (optional) `-h` - Displays command usage information (optional)

[1] <s> = string; <n> = number; <f> = filename

13 Component Identification

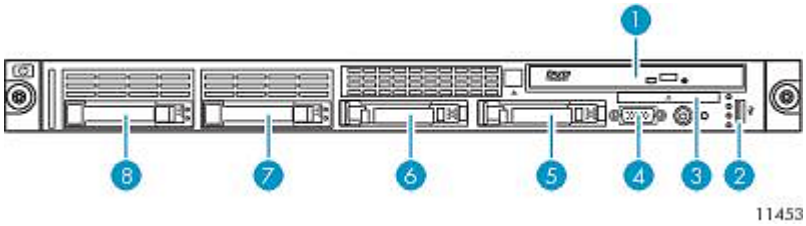
This section provides illustrations and descriptions of the node, disk array enclosure, Fibre Channel (FC) switch, and Ethernet switch components, LEDs, and buttons.

NOTE: For lights that blink or flash, the frequency of Hz is about the same number of blinks or flashes per second.

VLS9000 Node Components, LEDs, and Buttons

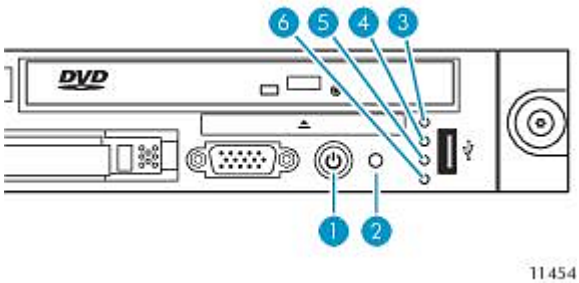
This section identifies and describes the front and rear panel components, LEDs, and buttons of the VLS nodes.

Front Panel Components



Item	Description
1	DVD-CD drive
2	Front USB connector
3	HP Systems Insight Display
4	Video connector
5	Hard drive blank
6	Hard drive blank
7	Hard drive 2
8	Hard drive 1

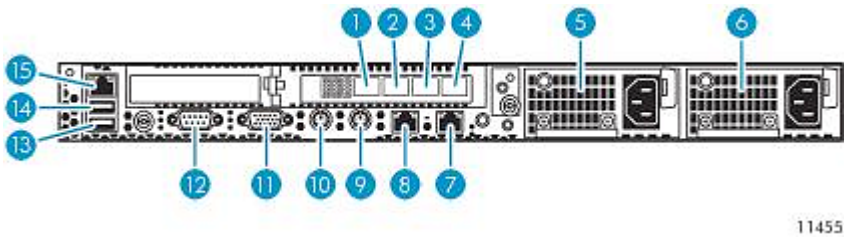
Front Panel LEDs and Buttons



Item	Description	Status
1	Power On/Standby button and system power LED	Green = System is on. Amber = System is shut down, but power is still applied.

Item	Description	Status
		Off = Power cord is not attached, power supply failure has occurred, no power supplies are installed, facility power is not available, or disconnected power button cable.
2	UID button/LED	Blue = Identification is activated. Flashing blue = System is being remotely managed. Off = Identification is deactivated.
3	Internal health LED	Green = System health is normal. Amber = System health is degraded. To identify the component in a degraded state, refer to HP Systems Insight Display LEDs and Internal Health LED Combinations. Red = System health is critical. To identify the component in a critical state, refer to HP Systems Insight Display LEDs and Internal Health LED Combinations. Off = System health is normal (when in standby mode).
4	External health LED (power supply)	Green = Power supply health is normal. Amber = Power redundancy failure occurred. Off = Power supply health is normal when in standby mode.
5	NIC 1 link/activity LED	Green = Network link exists. Flashing green = Network link and activity exist. Off = No link to network exists. If power is off, the front panel LED is not active. View the LEDs on the RJ-45 connector for status by referring to Rear Panel LEDs and Buttons.
6	NIC 2 link/activity LED	Green = Network link exists. Flashing green = Network link and activity exist. Off = No link to network exists. If power is off, the front panel LED is not active. View the LEDs on the RJ-45 connector for status by referring to Rear Panel LEDs and Buttons.

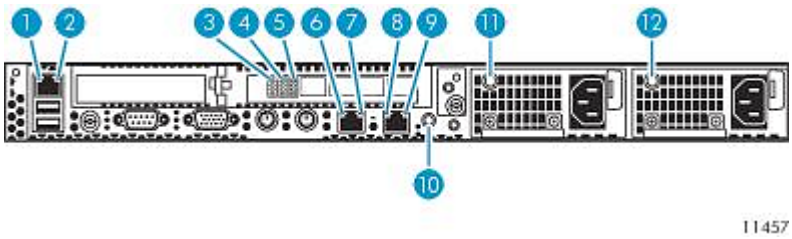
Rear Panel Components



Item	Description
1	Quad port FC card, storage port, port 4
2	Quad port FC card, storage port, port 3
3	Quad port FC card, host port, port 2

Item	Description
4	Quad port FC card, host port, port 1
5	Power supply 2
6	Power supply 1
7	NIC 2, on primary node connects to port 1 of switch 2810-24G
8	NIC 1, on primary node only, connects to the customer-provided external network (array)
9	Keyboard connector
10	Mouse connector
11	Video connector
12	Serial connector to access CLI
13	Rear USB connector
14	USB connector, on primary node connects to USB/Ethernet adapter, then to port 1 of switch 2510-24
15	iLO 2 NIC connector (service port)

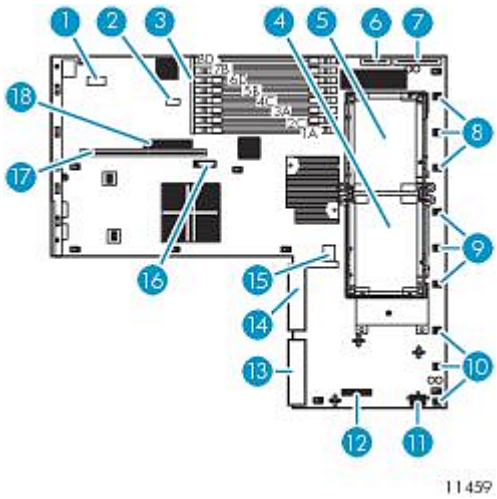
Rear Panel LEDs and Buttons



Item	Description	Status
1	iLO 2 NIC activity LED	Green = Activity exists. Flashing green = Activity exists. Off = No activity exists.
2	iLO 2 NIC link LED	Green = Link exists. Off = No link exists.
3–5	FC port LEDs	Red, green, and amber on or flashing = Power on. LED that is on/flashing represents the link speed (red = 1 Gbps, green = 2 Gbps, amber = 4 Gbps) = Online, I/O activity. Red, green, and amber flashing alternately = Firmware error. Red, green, and amber off = Power off.
6	10/100/1000 NIC 1 activity LED	Green = Activity exists. Flashing green = Activity exists. Off = No activity exists.
7	10/100/1000 NIC 1 link LED	Green = Link exists. Off = No link exists.
8	10/100/1000 NIC 2 activity LED	Green = Activity exists. Flashing green = Activity exists.

Item	Description	Status
		Off = No activity exists.
9	10/100/1000 NIC 2 link LED	Green = Link exists. Off = No link exists.
10	UID button/LED	Blue = Identification is activated. Flashing blue = System is being managed remotely. Off = Identification is deactivated.
11	Power supply 2 LED	Green = Normal Off = System is off or power supply has failed
12	Power supply 1 LED	Green = Normal Off = System is off or power supply has failed

System Board Components



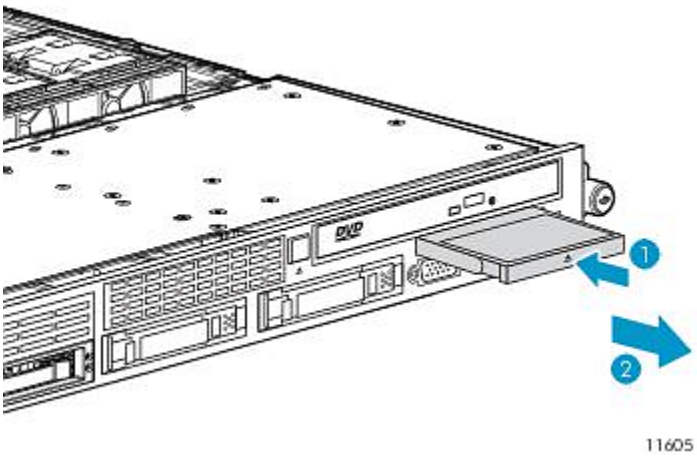
Item	Description
1	System maintenance switch (SW1)
2	NMI switch
3	FBDIMM slots (1-8)
4	Processor socket 2
5	Processor socket 1
6	DVD-CD drive connector
7	Power button connector
8	Fan module 3 connectors
9	Fan module 2 connectors
10	Fan module 1 connectors
11	SAS hard drive backplane power connector
12	Integrated Smart RAID controller connector
13	Power supply connector 1

Item	Description
14	Power supply connector 2
15	Internal USB connector
16	System battery
17	PCI riser board connector 2
18	PCI riser board connector 1

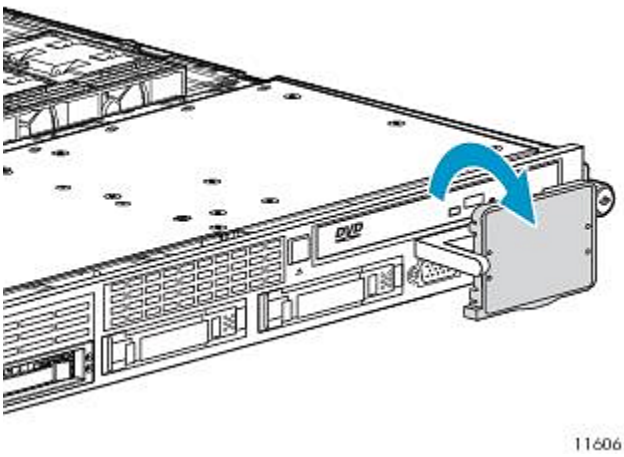
Accessing the HP Systems Insight Display

To eject the HP Systems Insight Display:

1. Press and release the display.
2. Extend the display from the chassis.



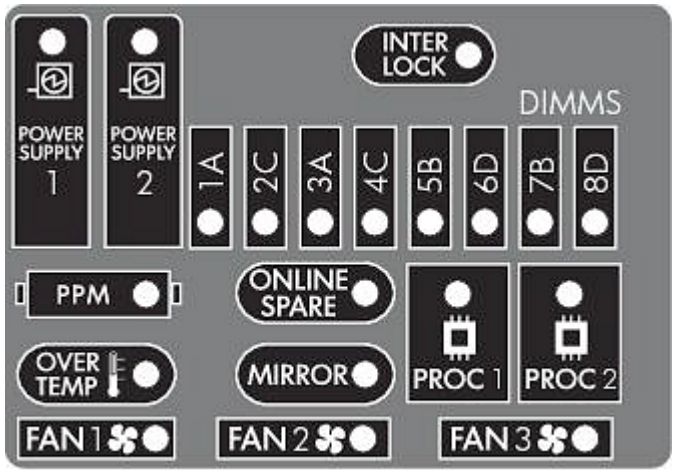
The display can be rotated up to 90 degrees.



HP Systems Insight Display and LEDs

The display provides status for all internal LEDs and enables diagnosis with the access panel installed.

To view the LEDs, access the HP Systems Insight Display.



Item	Description	Status
1	Online spare memory LED	Green = Protection enabled Flashing amber = Memory configuration error Amber = Memory failure occurred Off = No protection
2	Mirrored memory LED	Green = Protection enabled Flashing amber = Memory configuration error Amber = Memory failure occurred Off = No protection
	All other LEDs	Amber = Failure Off = Normal. For additional information detailing the causes for the activation of these LEDs, refer to HP Systems Insight Display LEDs and Internal Health LED Combinations.

NOTE: The HP Systems Insight Display LEDs represent the system board layout.

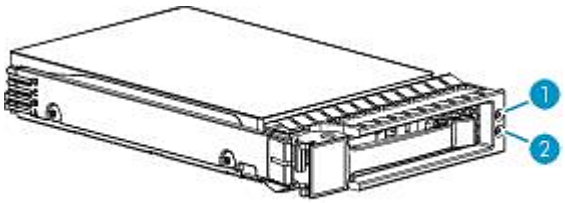
HP Systems Insight Display LEDs and Internal Health LED Combinations

When the internal health LED on the front panel illuminates either amber or red, the server is experiencing a health event. Combinations of illuminated system LEDs and the internal health LED indicate system status.

HP Systems Insight Display LED and color	Internal health LED color	Status
Processor failure, socket X (amber)	Red	One or more of the following conditions may exist: • Processor in socket X has failed. • Processor X is required yet not installed in the socket. • Processor X is unsupported. • ROM detects a failed processor during POST.
	Amber	Processor in socket X is in a pre-failure condition.

HP Systems Insight Display LED and color	Internal health LED color	Status
PPM failure, slot X (amber)	Red	One or more of the following conditions may exist: • PPM in slot X has failed. • PPM is not installed in slot X, but the corresponding processor is installed.
FBDIMM failure, slot X (amber)	Red	FBDIMM in slot X has failed.
	Amber	FBDIMM in slot X is in a pre-failure condition.
FBDIMM failure, all slots in one bank (amber)	Red	One or more FBDIMMs has failed. Test each bank of FBDIMMs by removing all other FBDIMMs. Isolate the failed FBDIMM by replacing each FBDIMM in a bank with a known working FBDIMM.
Online spare memory (amber)	Amber	Bank X failed over to the online spare memory bank.
Online spare memory (flashing amber)	Red	Invalid online spare memory configuration.
Online spare memory (green)	Green	Online spare memory enabled and not failed.
Mirrored memory (amber)	Amber	Bank X failed over to the mirrored memory bank.
Mirrored memory (flashing amber)	Red	Invalid mirrored memory configuration.
Mirrored memory (green)	Green	Mirrored memory enabled and not failed.
Overtemperature (amber)	Amber	The Health Driver has detected a cautionary temperature level.
	Red	The server has detected a hardware critical temperature level.
Riser interlock (amber)	Red	PCI riser cage is not seated.
Fan module (amber)	Amber	One fan is failed or removed.
	Red	Two or more fans have failed or are removed.

Hard Drive LEDs

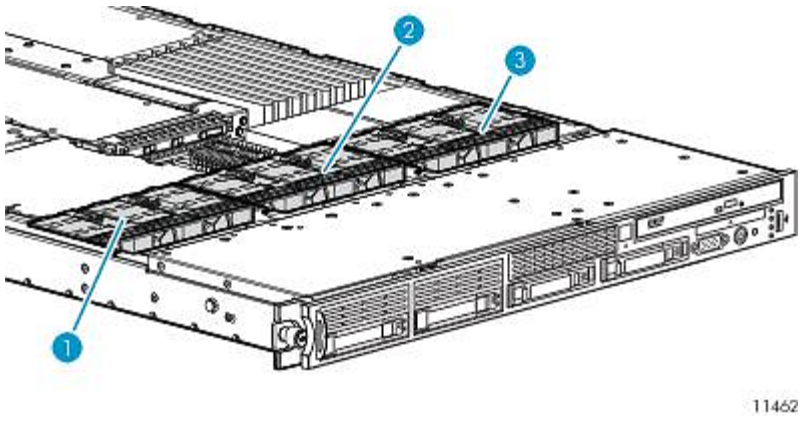


Item	Description
1	Fault/UID LED (amber/blue)
2	Online LED (green)

Hard Drive LED Combinations

Online/activity LED (green)	Fault/UID LED (amber/blue)	Interpretation
On, off, or flashing	Alternating amber and blue	The drive has failed, or a predictive failure alert has been received for this drive; it also has been selected by a management application.
On, off, or flashing	Steadily blue	The drive is operating normally, and it has been selected by a management application.
On	Amber, flashing regularly (1 Hz)	A predictive failure alert has been received for this drive. Replace the drive as soon as possible.
On	Off	The drive is online, but it is not active currently.
Flashing regularly (1 Hz)	Amber, flashing regularly (1 Hz)	**Do not remove the drive. Removing a drive may terminate the current operation and cause data loss.** The drive is part of an array that is undergoing capacity expansion or stripe migration, but a predictive failure alert has been received for this drive. To minimize the risk of data loss, do not replace the drive until the expansion or migration is complete.
Flashing regularly (1 Hz)	Off	**Do not remove the drive. Removing a drive may terminate the current operation and cause data loss.** The drive is rebuilding, or it is part of an array that is undergoing capacity expansion or stripe migration.
Flashing irregularly	Amber, flashing regularly (1 Hz)	The drive is active, but a predictive failure alert has been received for this drive. Replace the drive as soon as possible.
Flashing irregularly	Off	The drive is active, and it is operating normally.
Off	Steadily amber	A critical fault condition has been identified for this drive, and the controller has placed it offline. Replace the drive as soon as possible.
Off	Amber, flashing regularly (1 Hz)	A predictive failure alert has been received for this drive. Replace the drive as soon as possible.
Off	Off	The drive is offline, a spare, or not configured as part of an array.

Fan Locations

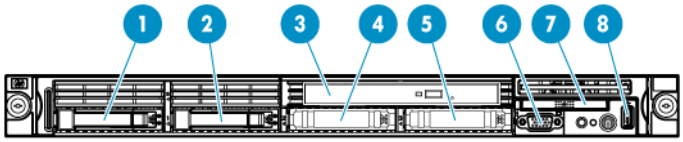


Item	Description
1	Fan module 1
2	Fan module 2
3	Fan module 3

VLS9200 Node Components, LEDs, and Buttons

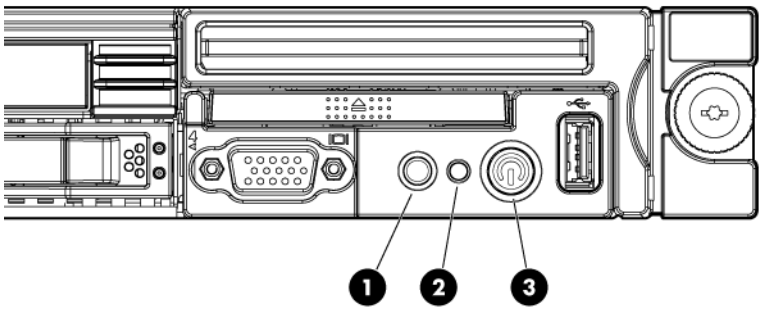
This section identifies and describes the front and rear panel components, LEDs, and buttons of the VLS nodes.

Front Panel Components



Item	Description
1	Hard drive 1
2	Hard drive 2
3	DVD-ROM drive
4	Hard drive blank
5	Hard drive blank
6	Video connector
7	HP Systems Insight Display
8	Front USB connector

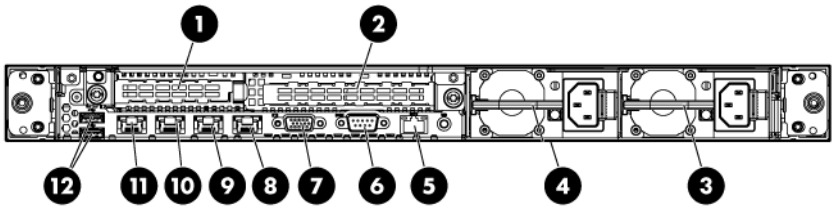
Front Panel LEDs and Buttons



Item	Description	Status
1	UID button/LED	Blue = Identification is activated. Flashing blue = System is being remotely managed. Off = Identification is deactivated.
2	Health LED	Green = System health is normal. Amber = System health is degraded. To identify the component in a degraded state, see HP Systems Insight Display LEDs and Internal Health LED Combinations. Red = System health is critical. To identify the component in a critical state, see HP Systems Insight Display LEDs and Internal Health LED Combinations.

Item	Description	Status
		Off = System health is normal (when in standby mode).
3	Power On/Standby button and system power LED	Green = System is on. Amber = System is in standby, but power is still applied. Off = Power cord is not attached, power supply failure has occurred, no power supplies are installed, facility power is not available, or the power button cable is disconnected.

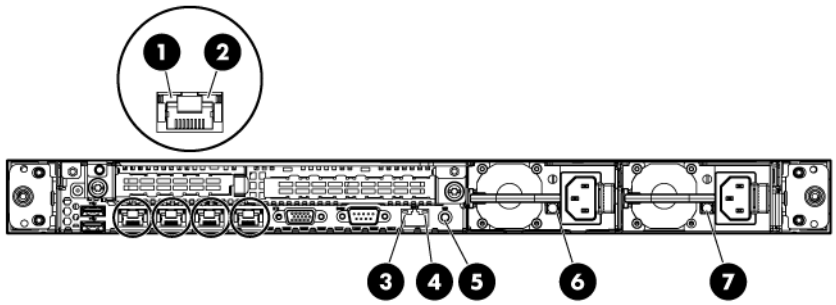
Rear Panel Components



Item	Description
1	Slot 1 PCIe2 x8 (8, 4, 2, 1)[1]
2	Slot 2 PCIe2 x16 (16, 8, 4, 2, 1)[1]
3	Power supply 1
4	Power supply 2
5	iLO 3 connector
6	Serial connector
7	Video connector
8	NIC 4 connector
9	NIC 3 connector
10	NIC 2 connector
11	NIC 1 connector
12	USB connectors (2)

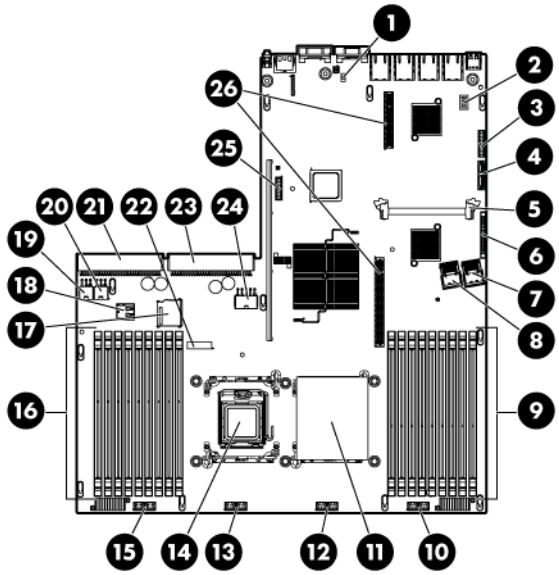
[1] (PCIe2 = Gen2 signaling rate, x8 = physical connector link width, (8, 4, 2, 1) = negotiable link widths)

Rear Panel LEDs and Buttons



Item	Description	Status
1	10/100/1000 NIC ctivity LED	Green = Activity exists. Flashing green = Activity exists. Off = No activity exists.
2	10/100/1000 NIC link LED	Green = Link exists. Off = No link exists.
3	iLO 3 NIC activity LED	Green = Activity exists. Flashing green = Activity exists. Off = No activity exists.
4	iLO 3 NIC link LED	Green = Link exists. Off = No link exists.
5	UID button/LED	Blue = Identification is activated. Flashing blue = System is being managed remotely. Off = Identification is deactivated.
6	Power supply 2 LED	Green = Normal Off = System is off or power supply has failed
7	Power supply 1 LED	Green = Normal Off = System is off or power supply has failed

System Board Components



Item	Description
1	NMI jumper
2	System maintenance switch
3	10 Gb sideband connector
4	SATA DVD-ROM drive connector
5	SAS cache module connector
6	Power button connector
7	Hard drive data connector 1 (drives 1–4)
8	Hard drive data connector 2 (drives 5–8)
9	Processor 1 DIMM slots (9)
10	Fan module 4 connector
11	Processor socket 1 (populated)
12	Fan module 3 connector
13	Fan module 2 connector
14	Processor socket 2
15	Fan module 1 connector
16	Processor 2 DIMM slots (9)
17	SD card slot
18	Internal USB connector
19	Hard drive power connector 1
20	Hard drive power connector 2
21	Power supply connector 1
22	System battery
23	Power supply connector 2

Item	Description
24	PCI power connector
25	TPM connector
26	PCIe riser board connectors (2)

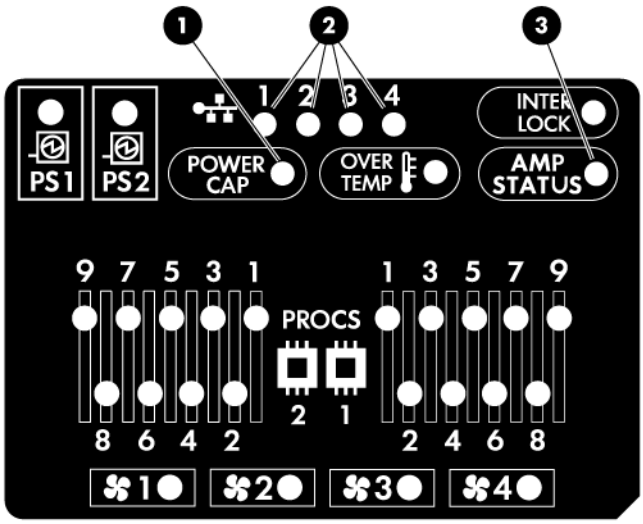
Accessing the HP System Insight Display

You access the HP System Insight Display the same way for the VLS9000 and VLS9200 systems. See "Accessing the HP Systems Insight Display" (page 178).

HP Systems Insight Display and LEDs

The display provides status for all internal LEDs and enables diagnosis with the access panel installed.

To view the LEDs, access the HP Systems Insight Display.



Item	Description	Status
1	Power cap LED	To determine Power cap status, see HP Systems Insight Display LEDs and Internal Health LED Combinations.
2	NIC LEDs	Green = Network link exists Flashing green = Network link and activity exist Off = No link to network exists If power is off, the front panel LED is not active. For status, see Rear Panel LEDs and Buttons.
3	AMP status	Green = AMP mode enabled Amber = Failover Flashing amber = Invalid configuration Off = AMP mode disabled
	All other LEDs	Amber = Failure Off = Normal. For possible failure causes, see HP Systems Insight Display LEDs and Internal Health LED Combinations.

NOTE: The HP Systems Insight Display LEDs represent the system board layout.

HP Systems Insight Display LEDs and Internal Health LED Combinations

When the internal health LED on the front panel illuminates either amber or red, the server is experiencing a health event. Combinations of illuminated system LEDs and the internal health LED indicate system status.

HP Systems Insight Display LED and color	Internal health LED color	System power LED	Status
Processor (amber)	Red	Amber	One or more of the following conditions may exist: • Processor in socket X has failed. • Processor X is required yet not installed in the socket. • Processor X is unsupported. • ROM detects a failed processor during POST.
	Amber	Green	Processor in socket X is in a pre-failure condition.
DIMM (amber)	Red	Green	One or more DIMMs have failed.
	Amber	Green	DIMM in slot X is in a pre-failure condition.
Overtemperature (amber)	Amber	Green	The Health Driver has detected a cautionary temperature level.
	Red	Green	The server has detected a hardware critical temperature level.
Interlock (amber)	Red	Green	The PCI riser board assembly is not seated properly.
Fan (amber)	Amber	Green	One fan is failed or removed.
	Red	Green	Two or more fans have failed or are removed.
Power supply (amber)	Red	Amber	• Only one power supply is installed and that power supply is in standby. • Power supply fault • System board fault
	Amber	Green	• Redundant power supply is installed and only one power supply is functional. • AC power cord is not plugged into redundant power supply. • Redundant power supply fault • Power supply mismatch at POST or power supply mismatch through hotplug addition.
Power cap (off)	—	Amber	Standby
Power cap (green)	—	Flashing green	Waiting for power
Power cap (flashing amber)	—	Amber	Power cap has been exceeded.
Power cap (green)	—	Green	Power is available.

IMPORTANT: If more than one DIMM slot LED is illuminated, further troubleshooting is required. Test each bank of DIMMs by removing all other DIMMs. Isolate the failed DIMM by replacing each DIMM in a bank with a known working DIMM.

Hard Drive LEDs

The hard drive LEDs are the same for the VLS9000 and VLS9200 systems. See "Hard Drive LEDs" (page 180).

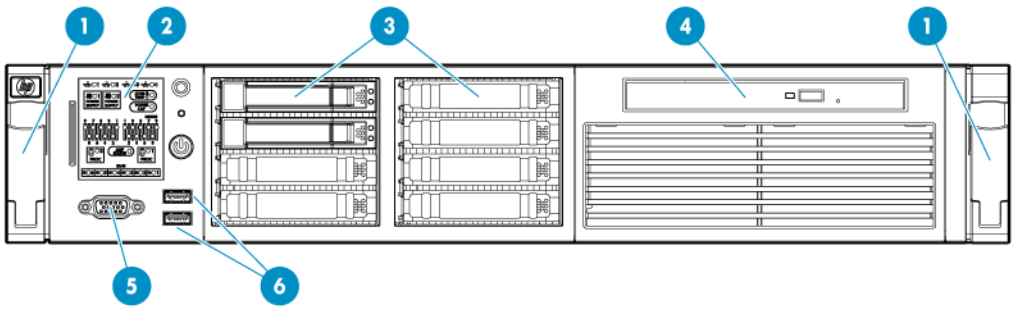
Hard Drive LED Combinations

The hard drive LED combinations are the same for the VLS9000 and VLS9200 systems. See "Hard Drive LED Combinations" (page 181).

VLS9200 High Performance Node Components, LEDs, and Buttons

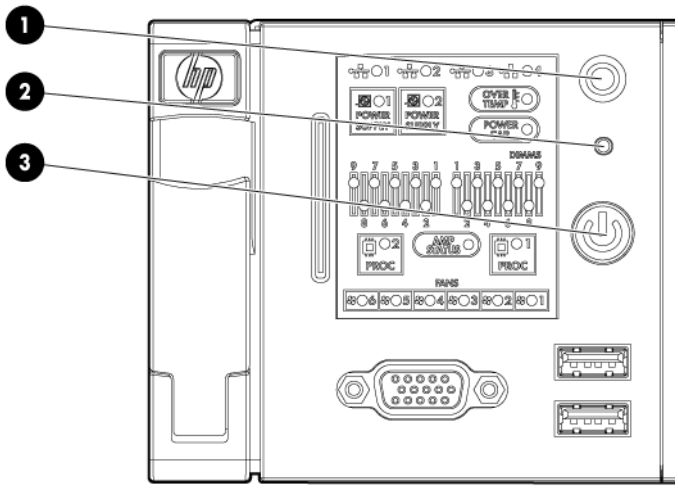
This section identifies and describes the front and rear panel components, LEDs, and buttons of the VLS nodes.

Front Panel Components



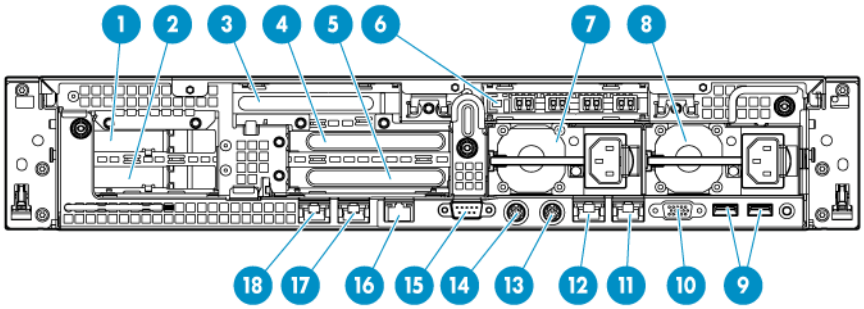
Item	Description
1	Quick release levers (2)
2	Systems Insight Display
3	Hard drives
4	DVD-ROM drive
5	Video connector
6	USB connectors (2)

Front Panel LEDs and Buttons



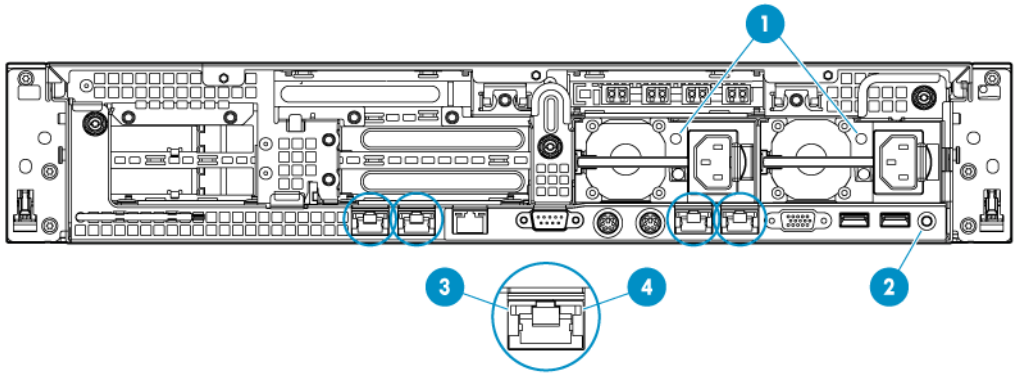
Item	Description	Status
1	UID button/LED	Blue = Identification is activated. Flashing blue = System is being remotely managed. Off = Identification is deactivated.
2	System health LED	Green = System health is normal. Amber = System health is degraded. To identify the component in a degraded state, see HP Systems Insight Display LEDs and Internal Health LED Combinations. Red = System health is critical. To identify the component in a critical state, see HP Systems Insight Display LEDs and Internal Health LED Combinations. Off = System health is normal (when in standby mode).
3	Power On/Standby button and system power LED	Green = System is on. Amber = System is in standby, but power is still applied. Off = Power cord is not attached, power supply failure has occurred, no power supplies are installed, facility power is not available, or the power button cable is disconnected.

Rear Panel Components



Item	Description
1	PCI slot 5
2	PCI slot 6
3	PCI slot 4
4	PCI slot 2
5	PCI slot 3
6	PCI slot 1
7	Power supply 2
8	Power supply 1
9	USB connectors (2)
10	Video connector
11	NIC 1 connector
12	NIC 2 connector
13	Mouse connector
14	Keyboard connector
15	Serial connector
16	iLO 3 connector
17	NIC 3 connector
18	NIC 4 connector

Rear Panel LEDs and Buttons

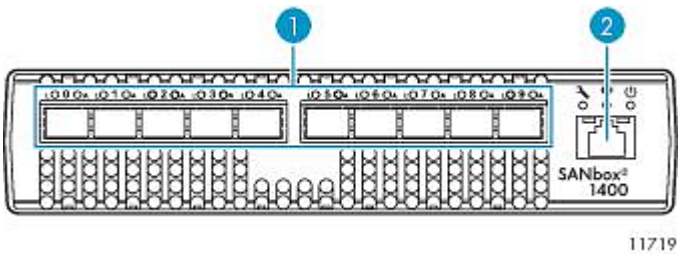


Item	Description	Status
1	Power supply LED	Green = Normal Off = System is off or power supply has failed
2	UID button/LED	Blue = Identification is activated. Flashing blue = System is being managed remotely. Off = Identification is deactivated.
3	iLO NIC activity LED	Green = Activity exists. Flashing green = Activity exists. Off = No activity exists.
4	iLO NIC link LED	Green = Link exists. Off = No link exists.

Fibre Channel Switch 4/10q Components, LEDs, and Buttons

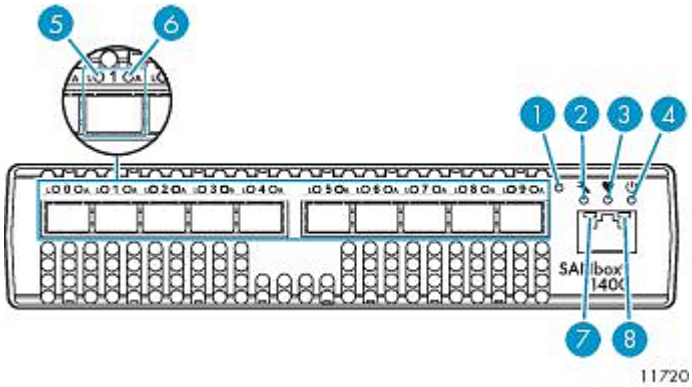
This section provides images and descriptions of the front and rear panels of the Fibre Channel Switch 4/10q.

Front Panel Components



Item	Description
1	Fibre Channel port 0 through 9 (numbered from left to right)
2	Ethernet port

Front Panel LEDs and Buttons



Item	Description	Status
1	Maintenance button	Dual-function momentary switch. Its purpose is to reset the switch or to place the switch in maintenance mode. To reset the switch, use a pointed tool to momentarily press and release (less than 2 seconds) the Maintenance button. The switch will respond as follows: 1. All the chassis LEDs will illuminate except the System Fault LED. 2. After approximately 1 minute, the power-on self test (POST) begins, extinguishing the Heartbeat LED. 3. When the POST is complete, the Input Power LED is illuminated and the Heartbeat LED is flashing once per second.
2	System fault LED	Amber = A fault exists in the switch firmware or hardware. Fault conditions include POST errors and over temperature conditions. Off = Switch is operating normally.
3	Heartbeat LED	Green = Switch is in maintenance mode. Blinking green (constant 1 Hz) = Switch passed the POST and the internal switch processor is running. 2 blinks = Internal firmware failure. 3 blinks = System error. 4 blinks = Configuration file system error. 5 blinks = Over temperature. See Heartbeat LED Blink Patterns for more information.
4	Input power LED	Green = Switch logic circuitry is receiving the proper DC voltages. Off = Switch is in maintenance mode.
5	Port logged-In LED	Green = A device is logged in to the port. Flashing green (constant 1 Hz) = A device is logging in to the port. Flashing green (constant 2 Hz) = The port is down, offline, or an error has occurred.
6	Port Activity LED	Green = Data is passing through the port. Each frame that the port transmits or receives causes LED to illuminate for 50 milliseconds.
7	Ethernet port link status LED	Green = Ethernet connection has been established. Off = No connection.
8	Ethernet port activity LED	Green = Data is being transmitted or received over the Ethernet connection. Off = No data being transmitted or received.

Heartbeat LED Blink Patterns

The Heartbeat LED indicates the operational status of the switch. When the POST completes with no errors, the Heartbeat LED blinks at steady rate of once per second. When the switch is in maintenance mode, the Heartbeat LED illuminates continuously. All other blink patterns indicate critical errors. In addition to producing a Heartbeat error blink patterns, a critical error also illuminates the System Fault LED. The Heartbeat LED shows an error blink pattern for the following conditions:

- 2 blinks - Internal Firmware Failure Blink Pattern
- 3 blinks - System Error Blink Pattern
- 4 blinks - Configuration File System Error Blink Pattern
- 5 blinks - Over Temperature Blink Pattern

Internal Firmware Failure Blink Pattern—An internal firmware failure blink pattern is 2 blinks followed by a two second pause. The 2-blink error pattern indicates that the firmware has failed, and that the switch must be reset. Momentarily press and release the Maintenance button to reset the switch.

System Error Blink Pattern—A system error blink pattern is 3 blinks followed by a two second pause. The 3-blink error pattern indicates that a POST failure or a system error has left the switch inoperable. If a system error occurs, contact HP support. Momentarily press and release the Maintenance button to reset the switch.

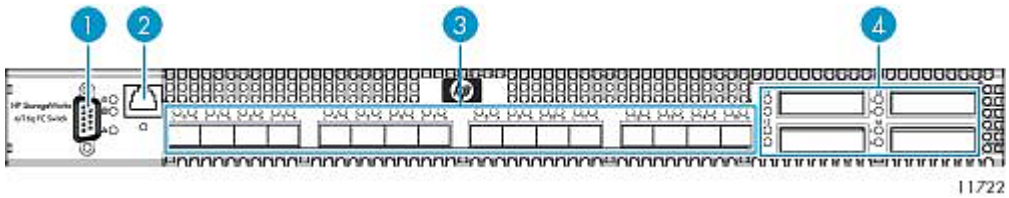
Configuration File System Error Blink Pattern—A configuration file system error blink pattern is 4 blinks followed by a two second pause. The 4-blink error pattern indicates that a configuration file system error has occurred. Contact HP support.

Over temperature blink pattern—An over temperature blink pattern is 5 blinks followed by a two second pause. The 5-blink error pattern indicates that the air temperature inside the switch has exceeded the failure temperature threshold. The failure temperature threshold is 70° C.

Fibre Channel Switch 4/16q Components, LEDs, and Buttons

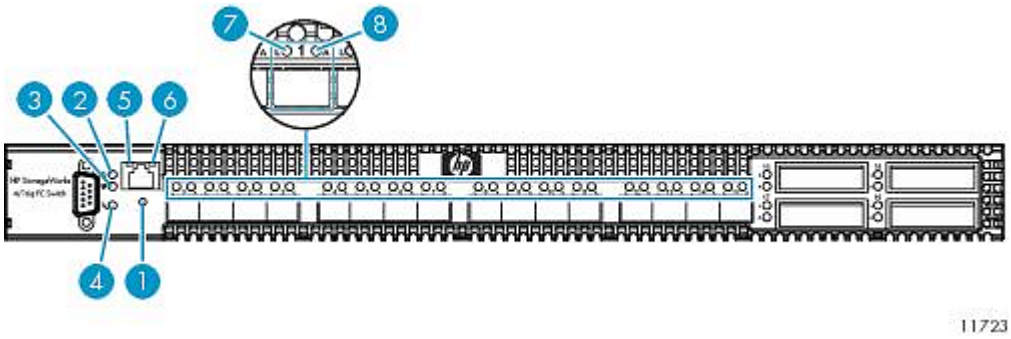
This section provides images and descriptions of the front and rear panels of the Fibre Channel Switch 4/16q.

Front Panel Components



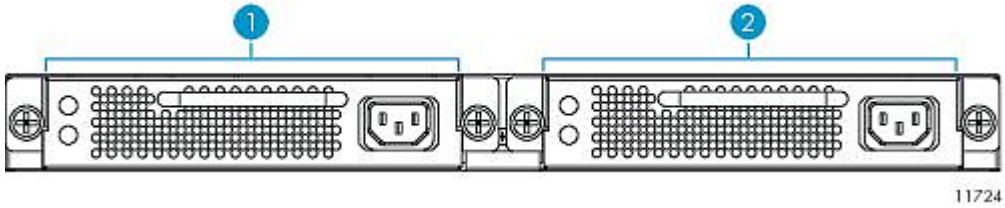
Item	Description
1	Serial port (not used)
2	Ethernet port
3	4 GB FC ports, port 0 through 15 (numbered from left to right)
4	10 GB FC ports, port 16 through 19 (not used)

Front Panel LEDs and Buttons



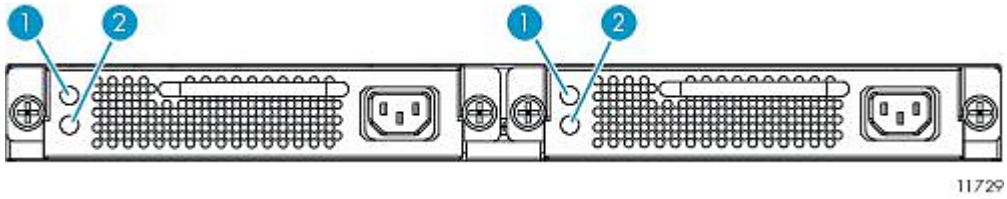
Item	Description	Status
1	Maintenance button	Dual-function momentary switch. Its purpose is to reset the switch or to place the switch in maintenance mode. To reset the switch, use a pointed tool to momentarily press and release (less than 2 seconds) the Maintenance button. The switch will respond as follows: 1. All the chassis LEDs will illuminate except the System Fault LED. 2. After approximately 1 minute, the power-on self test (POST) begins, extinguishing the Heartbeat LED. 3. When the POST is complete, the Input Power LED is illuminated and the Heartbeat LED is flashing once per second.
2	Input power LED	Green = Switch logic circuitry is receiving the proper DC voltages. Off = Switch is in maintenance mode.
3	Heartbeat LED	Green = Switch is in maintenance mode. Blinking green (constant 1 Hz) = Switch passed the POST and the internal switch processor is running. 2 blinks = Internal firmware failure. 3 blinks = System error. 4 blinks = Configuration file system error. 5 blinks = Over temperature. See Heartbeat LED Blink Patterns for more information.
4	System fault LED	Amber = A fault exists in the switch firmware or hardware. Fault conditions include POST errors and over temperature conditions. Off = Switch is operating normally.
5	Ethernet port activity LED	Green = Data is being transmitted or received over the Ethernet connection. Off = No data being transmitted or received.
6	Ethernet port link status LED	Green = Ethernet connection has been established. Off = No connection.
7	Port logged-In LED	Green = A device is logged in to the port. Flashing green (constant 1 Hz) = A device is logging in to the port. Flashing green (constant 2 Hz) = The port is down, offline, or an error has occurred.
8	Port activity LED	Green = Data is passing through the port. Each frame that the port transmits or receives causes LED to illuminate for 50 milliseconds.

Rear Panel Components



Item	Description
1	Power supply 0
2	Power supply 1

Rear Panel LEDs and Buttons



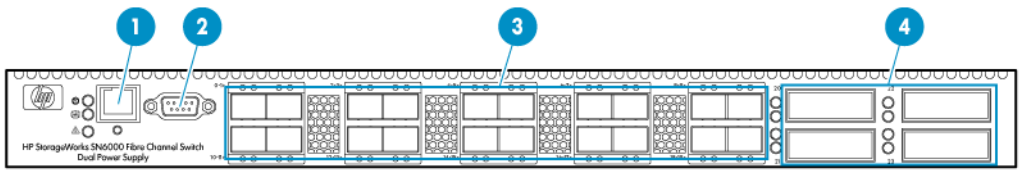
Item	Description	Status
1	Power supply status LED	Green = Power supply is receiving AC voltage and producing the proper DC voltages. Off = Power supply is not receiving AC voltage.
2	Power supply fault LED	Amber = Power supply fault exists and requires attention. Off = Power supply is operating normally.

Fibre Channel Switch 8/20q Components, LEDs, and Buttons

This section provides images and descriptions of the front and rear panels of the Fibre Channel Switch 8/20q.

Front Panel Components

This section provides images and descriptions of the front panel components of the Fibre Channel Switch 8/20q.

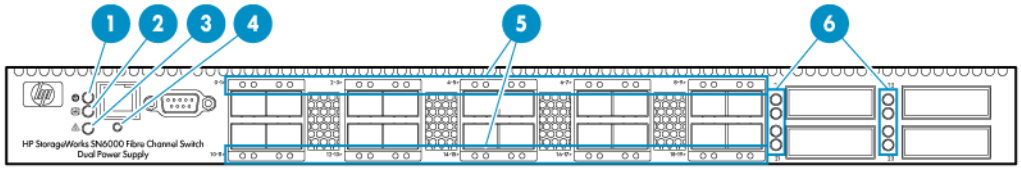


Item	Description
1	Ethernet port
2	Serial port

Item	Description
3	Fibre Channel ports
4	XPAK transponder ports (not in use)

Front Panel LEDs and Buttons

This section provides images and descriptions of the front panel LEDs and buttons of the Fibre Channel Switch 8/20q.



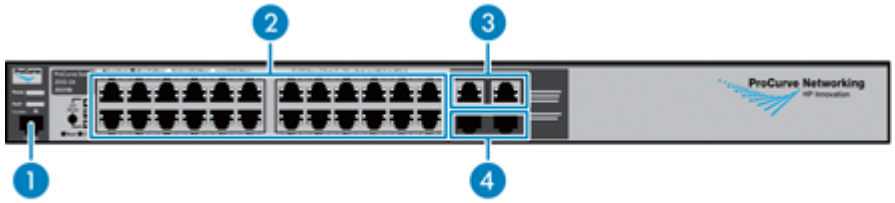
Item	Description	Status
1	Input Power LED	Green = The switch is receiving power. Off = One of these conditions exist: • The switch is NOT receiving power. • The switch is in maintenance mode.
2	Heartbeat LED	Green = The switch is in maintenance mode. Blinking green (once per second) = the switch is operational. Other blink patterns indicate critical errors: • 2 blinks — internal firmware failure • 3 blinks — Fatal power-on self test error • 4 blinks — configuration file system error • 5 blnks — over-temperature A critical error also illuminates the System Fault LED.
3	System Fault LED	Amber = a fault exists in the switch firmware or hardware. See the Heartbeat LED blink pattern for details.
4	Maintenance button	• To reset the switch — press and hold the Maintenance button for less than two seconds. This action clears any temporary error conditions that may have occurred and executes the switch self test. • To place the switch in Maintenance mode — press and hold the Maintenance button for several seconds until the Heartbeat LED illuminates and then extinguishes.
5	Port Logged-in LED (on left for each port)	Green = The port is properly connected and able to communicate with its attached devices. Off = One of these conditions exist: • The port connection is broken. • An error occurred that disabled the port.
	Port Activity LED (on right for each port)	Green = data is passing through the port.
6	Port Logged-in LED (on top for each port)	Green = The port is properly connected and able to communicate with its attached devices.

Item	Description	Status
		Off = One of these conditions exist: • The port connection is broken. • An error occurred that disabled the port.
	Port Activity LED (on bottom for each port)	Green = data is passing through the port.

Ethernet Switch 2510–24 Components, LEDs, and Buttons

This section provides images and descriptions of the front and rear panels of the Ethernet Switch 2510–24.

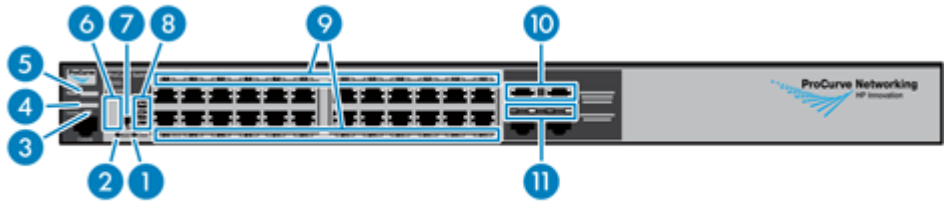
Front Panel Components



11981

Item	Description
1	Console port
2	10/100Base-TX RJ-45 Ethernet ports 1 through 24 (numbered from left to right, top to bottom)
3	10/100/1000–T dual-personality ports 25 and 26
4	mini—GBIC dual-personality ports 25 and 26

Front Panel LEDs and Buttons



11982

Item	Description	Status
1	Clear button	When pressed with the Reset button in a specific pattern, any configuration changes you may have made through the switch console, the web browser interface, and SNMP management are removed, and the factory default configuration is restored to the switch.
2	Reset button	Press to reset the switch while it is powered on. This action clears any temporary error conditions that may have occurred and executes the switch self test. Also resets all network activity counters to zero.
3	Locator LED	Blinking blue = Locate function is active. Firmware controlled, can be set to on or blinking. Off = Locate function is disabled.

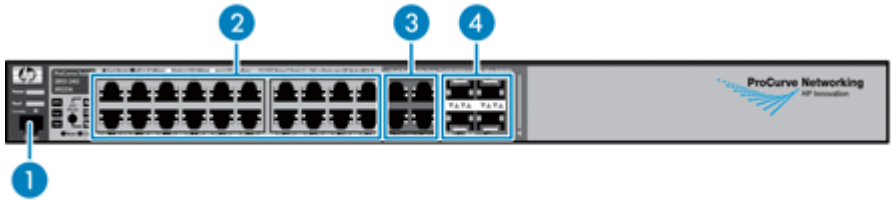
Item	Description	Status
4	Fault LED	Orange = On briefly after the switch is powered on or reset, at the beginning of switch self test. If this LED is on for a prolonged time, the switch has encountered a fatal hardware failure, or has failed its self test. Blinking orange[1] = A fault has occurred on the switch, one of the switch ports, or the fan. The Status LED for the component with the fault will blink simultaneously. Off = The normal state; indicates that there are no fault conditions on the switch.
5	Power LED	Green = The switch is receiving power. Off = The switch is NOT receiving power.
6	Self test LED	Green = The switch self test and initialization are in progress after you have power cycled or reset the switch. The switch is not operational until this LED goes off. Blinking green[1] = A component of the switch has failed its self test. The status LED for that component, for example an RJ-45 port, and the switch Fault LED will blink simultaneously. Off = The normal operational state; the switch is not undergoing self test.
6	Fan status LED	Blinking green[1] = The cooling fan has failed. The switch Fault LED will be blinking simultaneously. Off = The cooling fan is operating normally.
7	Mode select button	Press the button to step from one mode to the next. The current mode setting is indicated by the Mode select LEDs near the button.
8	Mode select LEDs	Act = Indicates that the port Mode LEDs are displaying network activity information. FDx = Indicates that the port Mode LEDs are lit for ports that are in Full Duplex Mode. Spd = Indicates that the port Mode LEDs are lit for ports that are operating at their maximum possible link speed. For the 10/100TX ports, that is 100 Mbps. ! = Indicates that the port Mode LEDs are displaying network events that could require operator attention, for example CRC errors or late collisions.
9, 10	Link LED	On = Indicates the port is enabled and receiving a link indication from the connected device. Off = One of these conditions exists: • No active network cable is connected to the port • The port is not receiving link beat or sufficient light • The port has been disabled through the switch console, the web browser interface, or HP TopTools. Blinking = If the LED is blinking simultaneously with the Fault LED, the corresponding port has failed its self test.
9, 11	Mode LED	Displays network activity information, or whether the port is configured for Full Duplex operation, or maximum link speed operation, or is experiencing network events requiring operator intervention depending on the mode selected. • If the Activity (Act) indicator LED is lit, each Mode LED displays activity information for the associated port—it flickers as network traffic is received and transmitted through the port. • If the Full Duplex (FDx) indicator LED is lit, the Mode LEDs light for those ports that are operating in full duplex. • If the maximum speed (Max) indicator LED is lit, the Mode LEDs light for those ports that are operating at their maximum possible link speed: 100 Mbps for 10/100 ports and 100-FX fiber-optic ports, and 1000 Mbps for 100/1000Base-T or gigabit fiber-optic ports. • If the attention (!) indicator LED is lit, each Mode LED lights briefly for each network event that could require operator attention, for example, late collisions or CRC errors.

[1] The blinking behavior is an on/off cycle once every 1.6 seconds, approximately.

Ethernet Switch 2810–24G Components, LEDs, and Buttons

This section provides images and descriptions of the front and rear panels of the Ethernet Switch 2810–24G.

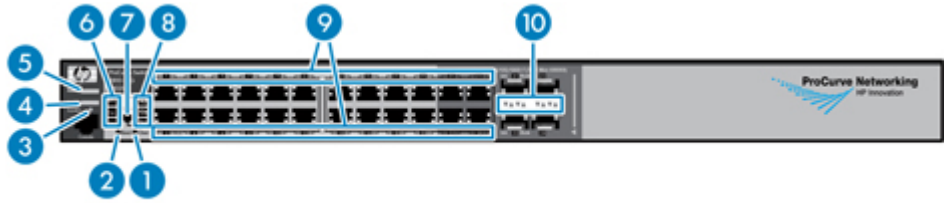
Front Panel Components



11980

Item	Description
1	Console port
2	10/100/1000Base-T RJ-45 ports 1 through 20 (numbered from top to bottom, left to right)
3	10/100/1000–T dual-personality ports 21 through 24
4	10/100/1000 mini-GBIC dual-personality ports 21 through 24

Front Panel LEDs and Buttons



11983

Item	Description	Status
1	Clear button	When pressed with the Reset button in a specific pattern, any configuration changes you may have made through the switch console, the Web browser interface, and SNMP management are removed, and the factory default configuration is restored to the switch.
2	Reset button	Used to reset the switch while it is turned on. This action clears any temporary error conditions that may have occurred and executes the switch self-test.
3	Locator LED	Blinking blue = Locate function is active. Firmware controlled, can be set to on or blinking. Off = Locate function is disabled.
4	Fault LED	Orange = The switch has encountered a fatal hardware failure or has failed its self-test. This LED comes on briefly after the switch is powered on or reset, at the beginning of switch self test. Blinking orange[1] = A fault has occurred on the switch, one of the switch ports, or the fan. The status LED for the component with the fault will blink simultaneously. If just the Fault LED is blinking, the switch could be attached to an RPS but not receiving power. Off = Indicates that there are no fault conditions on the switch.

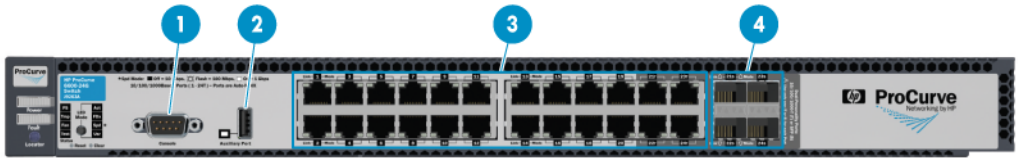
Item	Description	Status
5	Power LED	Green = The switch is receiving power. Off = The switch is not receiving power.
6	RPS status LED	Green = An HP ProCurve EPS/RPS unit is connected and operating correctly. The EPS/RPS could be powering the unit. Blinking green[1] = The EPS/RPS is connected but may be powering another switch or the EPS/RPS has experienced a fault. Off = The EPS/RPS is not connected or is not powered.
6	Fan status LED	Green = The cooling fan is working properly. Off = One of the unit's fans has failed. The switch Fault LED will be blinking simultaneously.
6	Self test LED	Green = The switch self test and initialization are in progress after the switch has been power cycled or reset. The switch is not operational until this LED goes off. Blinking green[1] = A component of the switch has failed its self-test. The status LED for that component and the switch Fault LED will blink simultaneously. Off = The switch is not undergoing self test.
7	Mode select button	Press the button to step from one mode to the next. The current mode setting is indicated by the Mode select LEDs near the button.
8	Mode select LEDs	Link = Indicates that the port LEDs are displaying link information. If the port LED is on, the port is enabled and receiving a link indication from the connected device. If the port LED is off, the port has no active network cable connected, or is not receiving link beat or sufficient light. Otherwise, the port may have been disabled through the switch console, the Web browser interface. If the port LED is blinking 1 simultaneously with the Fault LED, the corresponding port has failed its self-test. Act = Indicates that the port LEDs are displaying network activity information. FDx = Indicates that the port LEDs are lit for ports that are in full-duplex mode. Off indicates half duplex. Spd = Indicates that the port LEDs are displaying the connection speed at which each port is operating. If the port LED is off, the port is operating at 10 Mb/s. If the port LED is flashing2, the port is operating at 100 Mb/s, and if the port LED is on continuously, the port is operating at 1000 Mb/s.
9	Port LEDs (Green — overlaid with the port number)	Displays port link information, network activity information, whether the port is configured for full-duplex operation, or the speed of the connection, depending on the LED Mode selected. • If the Link (Lnk) indicator LED is lit, each port LED displays link information for the associated port. If the port LED is in Link mode and it is blinking, the port has failed its self test. The Fault and Self-Test LEDs will be blinking simultaneously. • If the Activity (Act) indicator LED is lit, each port LED displays activity information for the associated port — it flickers as network traffic is received and transmitted through the port.

Item	Description	Status
		• If the Full Duplex (FDx) indicator LED is lit, the port LEDs light for those ports that are operating in full duplex mode. • If the Speed (Spd) indicator LED is lit, the port LEDs behave as follows to indicate the connection speed for the port: ◦ OFF = 10 Mb/s ◦ Flashing = 100 Mb/s (the flashing behavior is a repeated on/off cycle once every 0.5 sec.) ◦ ON = 1000 Mb/s
10	T/M LEDs	For the dual-personality ports (ports 21 through 24), indicates which connector is enabled: • T = Indicates the 10/100/1000Base-T RJ-45 port is enabled. • M = Indicates the mini-GBIC port is enabled.

[1] The blinking behavior is an on/off cycle once every 1.6 seconds, approximately.

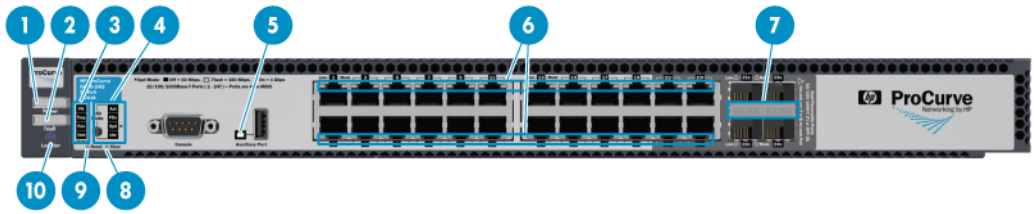
Ethernet Switch E6600 Components, LEDs, and Buttons

Front Panel Components



Item	Description
1	Console port
2	Auxiliary port
3	10/100/1000Base-T RJ-45 ports 1 through 24 (numbered from top to bottom, left to right)
4	10/100/1000 mini-GBIC dual-personality ports 21 through 24

Front Panel LEDs and Buttons



Item	Description	Status
1	Power LED	Green = The switch is operating correctly.

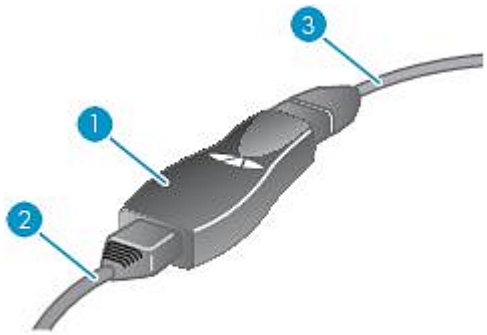
Item	Description	Status
		Off = The switch is not operating correctly or is not receiving power.
2	Fault LED	Orange = The switch has encountered a fatal hardware failure or has failed its self-test. This LED comes on briefly after the switch is powered on or reset, at the beginning of switch self test. Blinking orange = A fault has occurred on the switch, one of the switch ports, or the fan. The status LED for the component with the fault will blink simultaneously. If just the Fault LED is blinking, the switch could be attached to an RPS but not receiving power. Off = Indicates that there are no fault conditions on the switch.
3	PS, Temperature, Fan, and Test Status LEDs	PS: Green = The switch is receiving power. Blinking orange = A fault has occurred on one of the power supplies. The PS Status LED, Fault LED, and on the back of the switch the failed power supply LED (PS1 or PS2) will all blink simultaneously. Off = The switch is not receiving power.
		Temperature: Green = The switch temperature is normal. Blinking orange (blinks every 1.6 seconds) = An over temperature condition has been detected. This is a Fault condition indicating elevated internal temperatures. The Fault LED will blink simultaneously. Blinking orange = (blinks every 0.8 seconds) = This indicates an alert condition indicating critical internal temperatures. The Fault LED will blink simultaneously.
		Fan: Green: All fans are operating normally. Blinking orange (blinks every 1.6 seconds) = One of the unit's fans has failed. The switch Fault LED will be blinking simultaneously. Blinking orange = (blinks every 0.8 seconds) = One of the unit's fans has failed and the switch is in an overtemp condition. The switch Fault LED will be blinking simultaneously.
		Test Status: Green = The switch self-test and initialization are in progress after the switch has been power cycled or reset. The switch is not operational until this LED goes off. The Self-Test LED also comes on briefly when you "hot swap" a transceiver into the switch; the transceiver is self-tested when it is hot swapped. Blinking orange = A component of the switch has failed its self-test. The status LED for that component, for example an RJ-45 port, and the switch Fault LED will blink simultaneously. Off = The normal operational state; the switch is not undergoing self-test.
4	Port LED Mode select button and indicator LED	Mode select button: Press the button to step from one mode to the next. The current mode setting is indicated by the Mode select LEDs near the button.
		Mode select LED: Link = Indicates that the port LEDs are displaying link information. If the port LED is on, the port is enabled and receiving a link indication from the connected device. If the port LED is off, the port has no active network cable connected, or is not receiving link beat or sufficient light. Otherwise, the port may have been disabled through the switch console, the Web browser interface. If the port LED is blinking 1 simultaneously with the Fault LED, the corresponding port has failed its self-test. Act = Indicates that the port LEDs are displaying network activity information. FDx = Indicates that the port LEDs are lit for ports that are in full-duplex mode. Off indicates half duplex.

Item	Description	Status
		Spd = Indicates that the port LEDs are displaying the connection speed at which each port is operating. If the port LED is off, the port is operating at 10 Mb/s. If the port LED is flashing, the port is operating at 100 Mb/s, and if the port LED is on continuously, the port is operating at 1000 Mb/s. Usr = Indicates the port is displaying customer-specified information.
5	Auxiliary LED	Blinking green = Data transfer between the switch and a USB device is occurring. Green = The USB device is connected to the switch but no data transfer operation is occurring. Blinking orange (blinks every 1.6 seconds) = Indicates an error condition. The switch Fault LED will be blinking simultaneously. There is a hardware fault associated with the USB device or the USB connector on the switch. Blinking orange = (blinks every 0.8 seconds) = Indicates an alert condition. The switch Fault LED should not be blinking simultaneously. An alert error occurred in the USB operation that is not caused by a hardware fault, such as a file transfer error. Off = Indicates that no USB device has been inserted, or that the inserted USB device cannot be recognized, or that no command file can be found on the inserted USB device.
6	Port LEDs Link (left) and Mode (right)	Link: • Green = The port is enabled and receiving a link indication from the connected device. • Off = The port has no active network cable connected, or is not receiving link beat or sufficient light. Otherwise, the port may have been disabled through the switch console, the web browser interface, or ProCurve Manager. • Blinking orange simultaneously with the Fault LED = The corresponding port has failed its self-test.
		Mode: The operation of the Mode LED is controlled by the LED Mode select button, and the current setting is indicated by the LED Mode indicator LEDs near the button. Press the button to step from one view mode to the next. The default view is Activity (Act).
7	Port LEDs Link and Mode (arrows pointing to appropriate port)	Link: • Green = The port is enabled and receiving a link indication from the connected device. • Off = The port has no active network cable connected, or is not receiving link beat or sufficient light. Otherwise, the port may have been disabled through the switch console, the web browser interface, or ProCurve Manager. • Blinking orange simultaneously with the Fault LED = The corresponding port has failed its self-test.
		Mode: The operation of the Mode LED is controlled by the LED Mode select button, and the current setting is indicated by the LED Mode indicator LEDs near the button. Press the button to step from one view mode to the next. The default view is Activity (Act).
8	Clear button	When pressed by itself for at least one second, the button deletes any switch console access passwords that you may have configured. Use this feature if you have misplaced the password and need console access. This button can be disabled by a CLI command. When pressed with the Reset button in a specific pattern, any configuration changes you may have made through the switch console, the Web browser interface, and SNMP management are removed, and the factory default configuration is restored to the switch.

Item	Description	Status
9	Reset button	Used to reset the switch while it is turned on. This action clears any temporary error conditions that may have occurred and executes the switch self-test. When pressed with the Clear button in a specific pattern, any configuration changes you may have made through the switch console, the Web browser interface, and SNMP management are removed, and the factory default configuration is restored to the switch.
10	Locator LED	Blinking blue = Locate function is active. Firmware controlled, can be set to on or blinking. Off = Locate function is disabled.

USB LAN Adapter Components

This section provides an image and description of the USB LAN adapter.



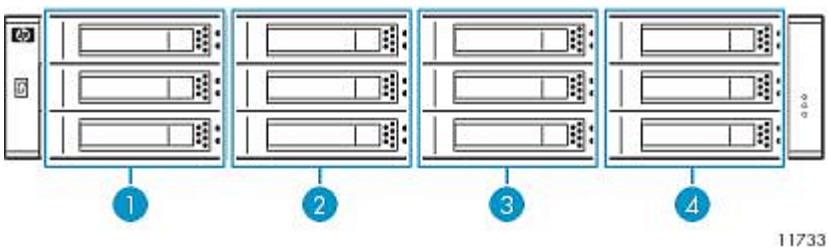
11191

Item	Description
1	USB LAN adapter
2	LAN cable
3	USB cable

VLS9000 Disk Array Components, LEDs, and Buttons

This section provides images and descriptions of the front and rear panels of the VLS9000 disk array enclosures.

Front Panel Components

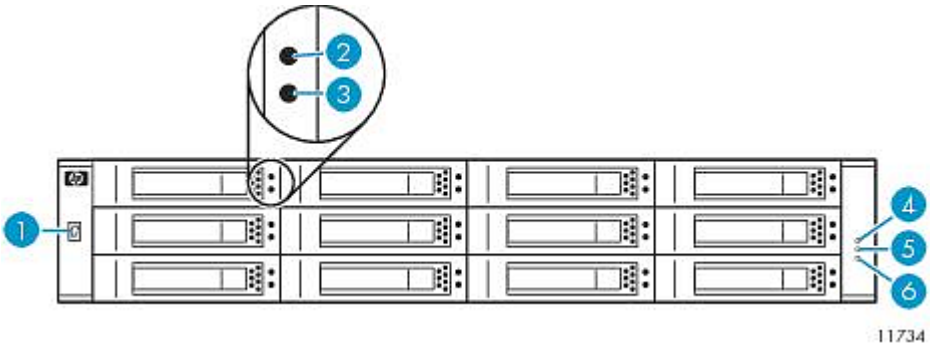


11733

Item	Description
1	Drives 0, 1, and 2 (numbered from top to bottom)
2	Drives 3, 4, and 5

Item	Description
3	Drives 6, 7, and 8
4	Drives 9, 10, and 11

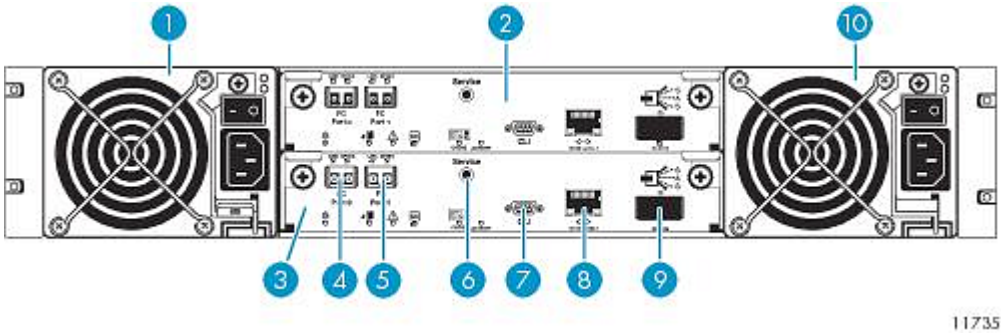
Front Panel LEDs



Item	Description	Status
1	Enclosure ID LED ("F" for 3–4 seconds at power up)	A hex LED shows the enclosure ID, which enables you to correlate an enclosure with logical views presented by Command View VLS. The enclosure ID for a base disk array enclosure is zero (0); the enclosure ID for an attached expansion disk array enclosure is nonzero. Continuous "F" = The display has a problem. If the Fault/Service required LED is also lit, an enclosure-level fault occurred.
2	Hard drive status LED	Blue = Hard drive is selected (for identification purposes only). Amber = Hard drive has failed. Flashing amber = Flashes at constant 1 Hz when hard drive is predicted to fail. Off = Hard drive is operating normally.
3	Hard drive activity LED	Green = Hard drive is online but there is no hard drive activity. Flashing green (constant 1 Hz) = Hard drive is rebuilding. Fluttering green = There is hard drive activity, or the array is running a background parity check of the data in the RAID set. Off = The hard drive has no power, is offline, or not configured.
4	Unit locator LED (on for 3–4 seconds at power up, then off)	Blinking white = Enclosure is selected (for identification purposes only). Off = Not active.
5	Fault/Service required LED (on for 3–4 seconds at power up, then off)	Amber = An enclosure-level fault occurred. Service action is required. The event has been acknowledged but the problem still needs attention. Off = No fault.
6	Power On/OK LED (on for 3–4 seconds at power up, blinks for up to 2 seconds during boot, then on)	Green = Enclosure is powered on with at least one power module operating normally. Off = Both power modules are off.

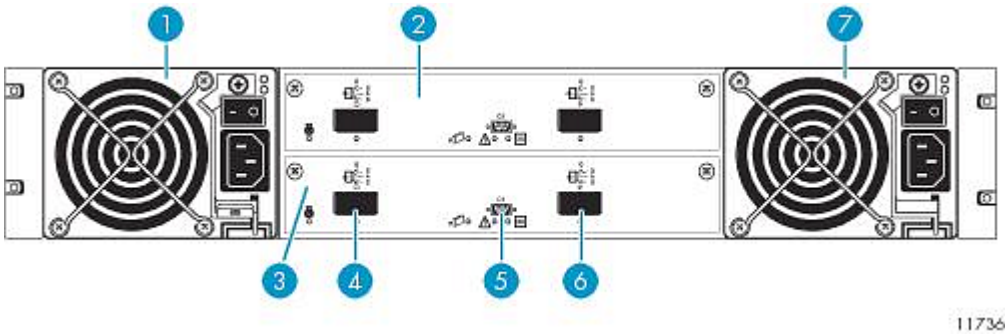
Rear Panel Components

Base Disk Array Enclosure



Item	Description
1	Power module 0
2	RAID controller 0
3	RAID controller 1
4	Fibre Channel port 0
5	Fibre Channel port 1 (not used)
6	Service port (for service only)
7	CLI port (not used)
8	Ethernet port
9	SAS output port
10	Power module 1

Expansion Disk Array Enclosure

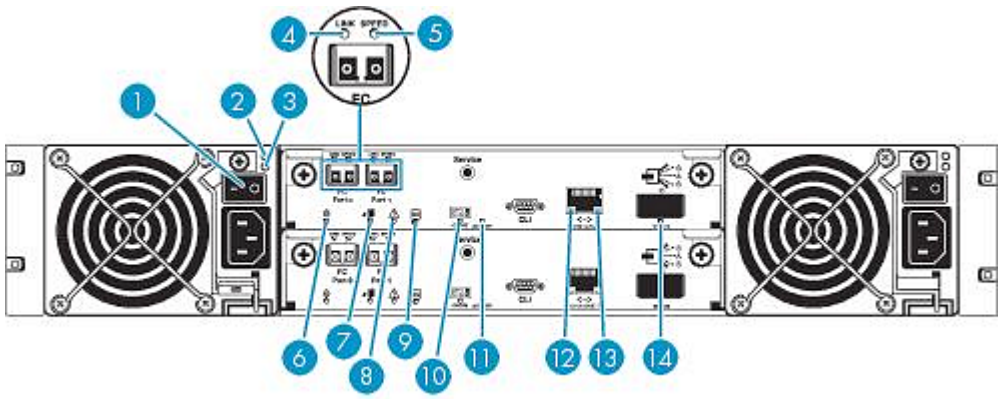


Item	Description
1	Power module 0
2	Expansion controller 0
3	Expansion controller 1
4	SAS port 0, input port
5	Service port (for service only)

Item	Description
6	SAS port 1, output port
7	Power module 1

Rear Panel LEDs and Buttons

Base Disk Array Enclosure

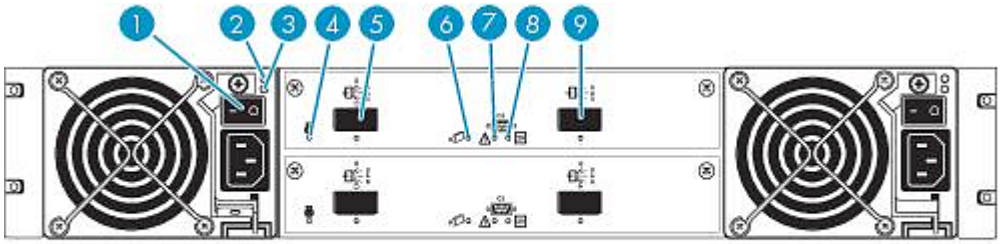


Item	Description	Status
1	Power switch[1]	Toggle, where O is Off.
2	AC Power Good LED	Green = AC power is on and input voltage is normal. Off = AC power is off or input voltage is below the minimum threshold.
3	DC-Fan Fault/ Service Required LED	Yellow = DC output voltage is out of range or a fan is operating below the minimum required RPM. Off = DC output voltage is normal.
4	FC link status (L) LED	Green = The port link is connected. Off = The port is empty or the link is down.
5	FC link speed (S) LED	Green = The data transfer rate is 4 Gbps. Off = The data transfer rate is 2 Gbps.
6	Unit locator LED	Blinking white = RAID controller is selected (for identification purposes only). Off = Not active.
7	OK to remove LED	Blue = The RAID controller can be removed. Off = The RAID controller is not prepared for removal.
8	Fault/Service required LED	Yellow = A fault has been detected or a service action is required. Blinking yellow = A hardware-controlled power on or a cache flush or restore error occurred.
9	Power On/OK LED	Green = RAID controller is operating normally. Off = RAID controller is not OK.
10	Cache status LED	Green = Cache is dirty (contains unwritten data) and operation is normal. Blinking green (1 Hz) = A Compact Flash flush is in progress. Blinking green (10 Hz) = A cache self-refresh is in progress. Valid data will remain until supercaps have drained, approximately 15 minutes. Off = Cache is clean (contains no unwritten data).

Item	Description	Status
11	Fibre Channel port activity LED	Blinking green = At least one FC port has I/O activity. Off = The FC ports have no I/O activity.
12	Ethernet link status LED	Green = The Ethernet link is up. Off = The Ethernet port is not connected or the link is down.
13	Ethernet activity LED	Blinking green = The Ethernet link has I/O activity. Off = The Ethernet link has no I/O activity.
14	SAS port status LED	Green = The port link is connected. Off = The port is empty or the link is down.

[1] Some power supply models do not have a power switch. In this case, power down the enclosure by unplugging the power cords from the enclosure.

Expansion Disk Array Enclosure



11738

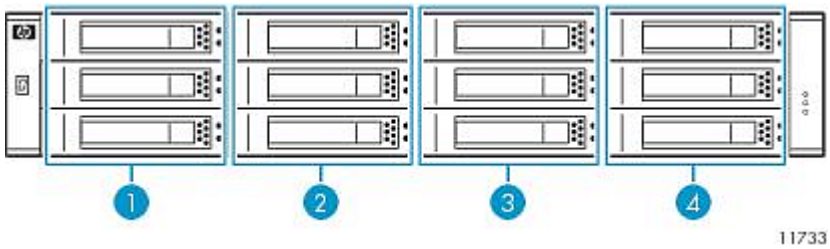
Item	Description	Status
1	Power switch[1]	Toggle, where O is Off.
2	AC Power Good LED	Green = AC power is on and input voltage is normal. Off = AC power is off or input voltage is below the minimum threshold.
3	DC-Fan Fault/ Service Required LED	Yellow = DC output voltage is out of range or a fan is operating below the minimum required RPM. Off = DC output voltage is normal.
4	Unit locator LED	Blinking white = Expansion controller is selected (for identification purposes only). Off = Not active.
5	SAS port 0, input port, status LED	Green = The port link is connected. Off = The port is empty or the link is down.
6	OK to remove LED	Blue = Not implemented.
7	Fault/Service required LED	Yellow = A fault has been detected or a service action is required. Blinking yellow = A hardware-controlled power on or a cache flush or restore error occurred.
8	Power On/OK LED	Green = Expansion controller is operating normally. Off = Expansion controller is not OK.
9	SAS port 1, output port, status LED	Green = The port link is connected. Off = The port is empty or the link is down.

[1] Some power supply models do not have a power switch. In this case, power down the enclosure by unplugging the power cords from the enclosure.

VLS9200 Disk Array Enclosure Components, LEDs, and Buttons

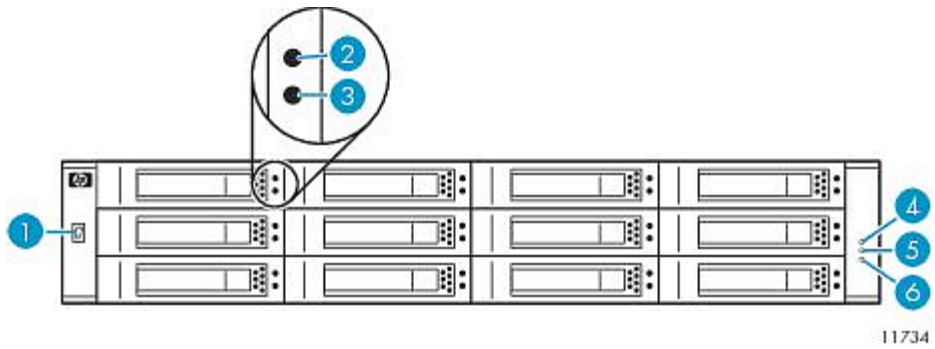
This section provides images and descriptions of the front and rear panels of the VLS9200 disk array enclosures.

Front Panel Components



Item	Description
1	Drives 0, 1, and 2 (numbered from top to bottom)
2	Drives 3, 4, and 5
3	Drives 6, 7, and 8
4	Drives 9, 10, and 11

Front Panel LEDs

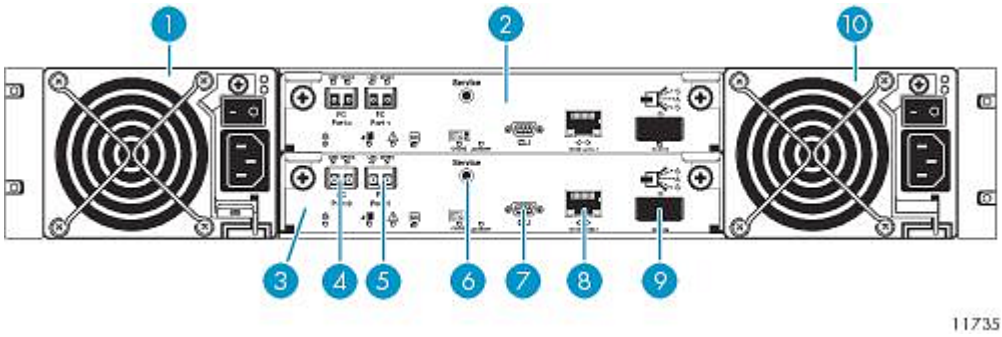


Item	Description	Status
1	Enclosure ID LED ("F" for 3–4 seconds at power up)	A hex LED shows the enclosure ID, which enables you to correlate an enclosure with logical views presented by Command View VLS. The enclosure ID for a base disk array enclosure is zero (0); the enclosure ID for an attached capacity enclosure is nonzero. Continuous "F" = The display has a problem. If the Fault/Service required LED is also lit, an enclosure-level fault occurred.
2	Hard drive status LED	Blue = Hard drive is selected (for identification purposes only). Amber = Hard drive has failed. Flashing amber = Flashes at constant 1 Hz when hard drive is predicted to fail. Off = Hard drive is operating normally.
3	Hard drive activity LED	Green = Hard drive is online but there is no hard drive activity. Flashing green (constant 1 Hz) = Hard drive is rebuilding.

Item	Description	Status
		Fluttering green = There is hard drive activity, or the array is running a background parity check of the data in the RAID set. Off = The hard drive has no power, is offline, or not configured.
4	Unit locator LED (on for 3–4 seconds at power up, then off)	Blinking white = Enclosure is selected (for identification purposes only). Off = Not active.
5	Fault/Service required LED (on for 3–4 seconds at power up, then off)	Amber = An enclosure-level fault occurred. Service action is required. The event has been acknowledged but the problem still needs attention. Off = No fault.
6	Power On/OK LED (on for 3–4 seconds at power up, blinks for up to 2 seconds during boot, then on)	Green = Enclosure is powered on with at least one power module operating normally. Off = Both power modules are off.

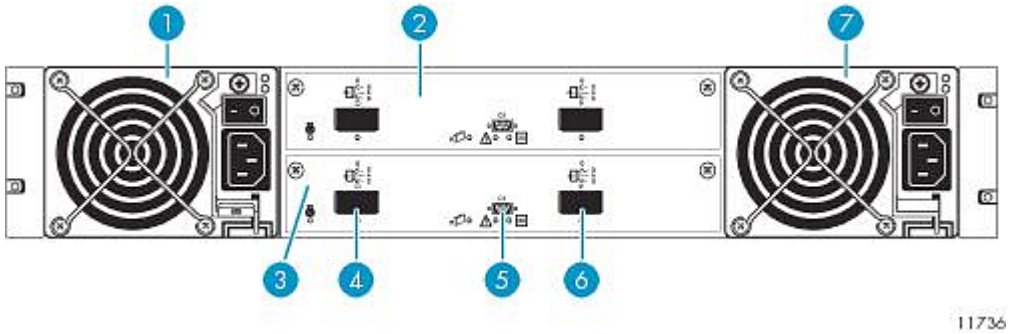
Rear Panel Components

Base Enclosure



Item	Description
1	Power module 0
2	RAID controller 0
3	RAID controller 1
4	Fibre Channel port 0
5	Fibre Channel port 1 (not used)
6	Service port (for service only)
7	CLI port (not used)
8	Ethernet port
9	SAS output port
10	Power module 1

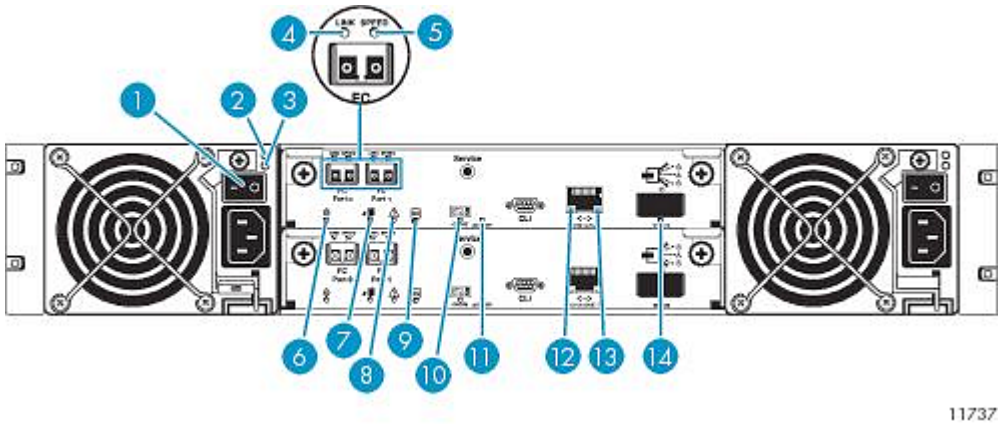
Capacity Enclosure



Item	Description
1	Power module 0
2	Expansion controller 0
3	Expansion controller 1
4	SAS port 0, input port
5	Service port (for service only)
6	SAS port 1, output port
7	Power module 1

Rear Panel LEDs and Buttons

Base Enclosure

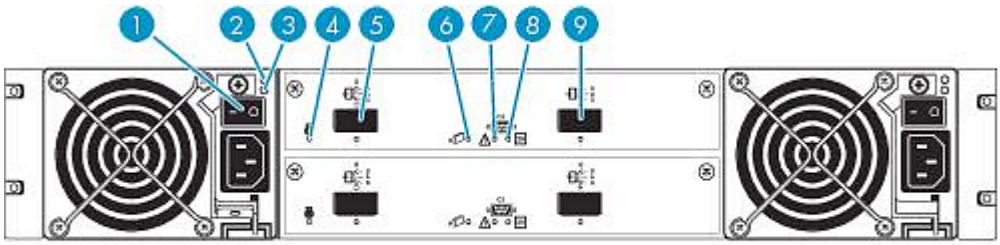


Item	Description	Status
1	Power switch[1]	Toggle, where O is Off.
2	AC Power Good LED	Green = AC power is on and input voltage is normal. Off = AC power is off or input voltage is below the minimum threshold.
3	DC-Fan Fault/ Service Required LED	Yellow = DC output voltage is out of range or a fan is operating below the minimum required RPM. Off = DC output voltage is normal.
4	FC link status (L) LED	Green = The port link is connected. Off = The port is empty or the link is down.

Item	Description	Status
5	FC link speed (S) LED	Green = The data transfer rate is 4 Gbps. Off = The data transfer rate is 2 Gbps.
6	Unit locator LED	Blinking white = RAID controller is selected (for identification purposes only). Off = Not active.
7	OK to remove LED	Blue = The RAID controller can be removed. Off = The RAID controller is not prepared for removal.
8	Fault/Service required LED	Yellow = A fault has been detected or a service action is required. Blinking yellow = A hardware-controlled power on or a cache flush or restore error occurred.
9	Power On/OK LED	Green = RAID controller is operating normally. Off = RAID controller is not OK.
10	Cache status LED	Green = Cache is dirty (contains unwritten data) and operation is normal. Blinking green (1 Hz) = A Compact Flash flush is in progress. Blinking green (10 Hz) = A cache self-refresh is in progress. Valid data will remain until supercaps have drained, approximately 15 minutes. Off = Cache is clean (contains no unwritten data).
11	Fibre Channel port activity LED	Blinking green = At least one FC port has I/O activity. Off = The FC ports have no I/O activity.
12	Ethernet link status LED	Green = The Ethernet link is up. Off = The Ethernet port is not connected or the link is down.
13	Ethernet activity LED	Blinking green = The Ethernet link has I/O activity. Off = The Ethernet link has no I/O activity.
14	SAS port status LED	Green = The port link is connected. Off = The port is empty or the link is down.

[1] Some power supply models do not have a power switch. In this case, power down the enclosure by unplugging the power cords from the enclosure.

Capacity Enclosure



11738

Item	Description	Status
1	Power switch[1]	Toggle, where O is Off.
2	AC Power Good LED	Green = AC power is on and input voltage is normal. Off = AC power is off or input voltage is below the minimum threshold.

Item	Description	Status
3	DC-Fan Fault/ Service Required LED	Yellow = DC output voltage is out of range or a fan is operating below the minimum required RPM. Off = DC output voltage is normal.
4	Unit locator LED	Blinking white = Expansion controller is selected (for identification purposes only). Off = Not active.
5	SAS port 0, input port, status LED	Green = The port link is connected. Off = The port is empty or the link is down.
6	OK to remove LED	Blue = Not implemented.
7	Fault/Service required LED	Yellow = A fault has been detected or a service action is required. Blinking yellow = A hardware-controlled power on or a cache flush or restore error occurred.
8	Power On/OK LED	Green = Expansion controller is operating normally. Off = Expansion controller is not OK.
9	SAS port 1, output port, status LED	Green = The port link is connected. Off = The port is empty or the link is down.

[1] Some power supply models do not have a power switch. In this case, power down the enclosure by unplugging the power cords from the enclosure.

14 Component Replacement

This section provides detailed instructions for replacing customer-replaceable VLS components. See Customer Self Repair for details.

CAUTION: Always replace components with the same make, size, and type of component. Changing the hardware configuration voids the warranty.

Safety Considerations

Before performing component replacement procedures, review all the safety information in this guide.

Preventing Electrostatic Discharge

To prevent damaging the system, be aware of the precautions you need to follow when setting up the system or handling parts. A discharge of static electricity from a finger or other conductor may damage static-sensitive devices or micro circuitry. This type of damage may reduce the life expectancy of the device. Proper packaging and grounding techniques are necessary precautions to prevent damage.

To prevent electrostatic damage:

- Avoid hand contact by transporting and storing products in static-safe containers, such as conductive tubes, bags, or boxes.
- Keep electrostatic-sensitive parts in their containers until they arrive at static-free workstations.
- Cover workstations with approved static-dissipating material. Use a wrist strap connected to the work surface and properly grounded (earthed) tools and equipment.
- Keep work area free of non-conductive materials, such as ordinary plastic assembly aids and foam packing.
- Place parts on a grounded surface before removing them from their containers.
- Always be properly grounded when touching a static-sensitive component or assembly.
- Avoid touching pins, leads, or circuitry.

Grounding Methods to Prevent Electrostatic Damage

There are several methods for grounding. Use one or more of the following methods when handling or installing electrostatic-sensitive parts:

- Use a wrist strap connected by a ground cord to a grounded workstation or computer chassis. Wrist straps are flexible straps with a minimum of 1 megaohm ± 10 percent resistance in the ground cords. To provide proper ground, wear the strap snug against the skin.
- Use heel straps, toe straps, or boot straps at standing workstations. Wear the straps on both feet when standing on conductive floors or dissipating floor mats.
- Use conductive field service tools.
- Use a portable field service kit with a folding static-dissipating work mat.

If you do not have any of the suggested equipment for proper grounding, have an authorized reseller install the part. For more information on static electricity, or assistance with product installation, contact your authorized reseller.

Warnings and Cautions

Before removing the node access panel, be sure that you understand the following warnings and cautions.

⚠ **WARNING!** To reduce the risk of electric shock or damage to the equipment:

- Do not disable the AC power cord grounding plug. The grounding plug is an important safety feature.
- Plug the power cord into a grounded (earthed) electrical outlet that is easily accessible at all times.
- Unplug the power cord from each power supply to disconnect power to the equipment.

WARNING! To reduce the risk of personal injury from hot surfaces, allow the drives and the internal system components to cool before touching them.

⚠ **CAUTION:** Do not operate the node for long periods without the access panel. Operating the node without the access panel results in improper airflow and improper cooling that can lead to thermal damage.

Preparation Procedures

To access some components and perform certain replacement procedures, you must perform one or more of the following procedures:

- Extend the node from the rack. See Extending a VLS Node from the Rack.

  If you are performing service procedures in an HP, Compaq branded, telco, or third-party rack cabinet, use the locking feature of the rack rails to support the node and gain access to internal components.

  For more information about telco rack solutions, see the RackSolutions.com web site (http://www.racksolutions.com/hp).
- If you must remove a non-hot-plug component from the node, power off the system. See Powering Off the System.
- Remove the node from the rack. See Removing a VLS Node from the Rack.
- Remove the node access panel. See Removing the VLS Node Access Panel.

  If you must remove a component located inside the node, remove the access panel.

Extending a VLS Node from the Rack

⚠ **WARNING!** To reduce the risk of personal injury or equipment damage, be sure that the rack is adequately stabilized before extending a node from the rack.

WARNING! Be careful when pressing the rail-release levers and sliding the component into or out of the rack. The sliding rails could pinch your fingertips.

To extend a node from the rack:

1. Loosen the thumbscrews that secure the node faceplate to the front of the rack.
2. Extend the node on the rack rails until the node rail-release latches engage.
3. After performing the replacement procedure, slide the node back into the rack:
   a. Press the node rail-release latches and slide the node fully into the rack.
   b. Secure the node by tightening the thumbscrews.

Removing a VLS Node from the Rack

To remove the node from a rack:

1. Power off the node. See Powering Off the System.
2. Disconnect the cabling.
3. Extend the node from the rack. See Extending a VLS Node from the Rack.
4. Remove the node from the rack. For more information, refer to the documentation that ships with the rack mounting option.
5. Place the node on a sturdy, level surface.

Removing the VLS Node Access Panel

⚠ **WARNING!** Pressing the Power on/Standby button sets the node to the standby position, which removes power from most areas of the node. However, portions of the power supply and some internal circuitry remain active until the AC power cord is removed.

WARNING! To reduce the risk of personal injury from hot surfaces, allow the internal system components to cool before touching them.

⚠ **CAUTION:** Do not operate the node for long periods without the access panel. Operating the node without the access panel results in improper airflow and improper cooling that can lead to thermal damage.

CAUTION: Electrostatic discharge can damage electronic components. Properly ground yourself before beginning any installation procedure.

1. Power off the node. See Powering Off the System.
2. Extend the node from the rack. See Extending a VLS Node from the Rack.
3. Lift up on the hood latch handle which slides the panel toward the rear of the unit.
4. Lift up the panel to remove it.

Installing the VLS Node Access Panel

1. Set the access panel on top of the node about 0.2 inch from the opening with the hood latch open.
2. Engage the anchoring pin with the corresponding hole in the latch.
3. Push down on the hood latch.
4. Slide the access panel into the closed position.

VLS Node Component Replacement

Hard Drive

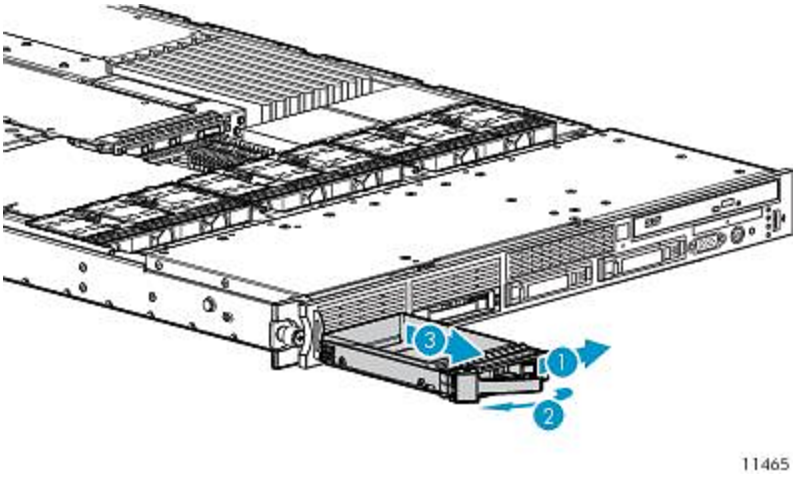
⚠ **CAUTION:** To prevent improper cooling and thermal damage, do not operate the node unless all bays are populated with either a component or a blank.

NOTE: The node contains one of several possible hard drives. The replacement hard drive must be the same or greater capacity as the original hard drive; see the label on the front of the original hard drive for the correct supported replacement capacity and part number.

1. Press the drive latch release button (1).

2. Pull the hard drive (3) out of the node by the latch handle (2).

Figure 27 Removing a Node Hard Drive



To replace the component, pull out the latch handle (2) out as far as it can go and slide the drive into the bay until the latch mechanism engages the chassis. Then, firmly push in the latch handle to lock the drive in the drive bay.

Figure 28 Preparing the Node Hard Drive

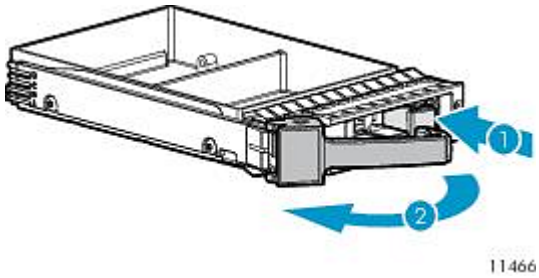
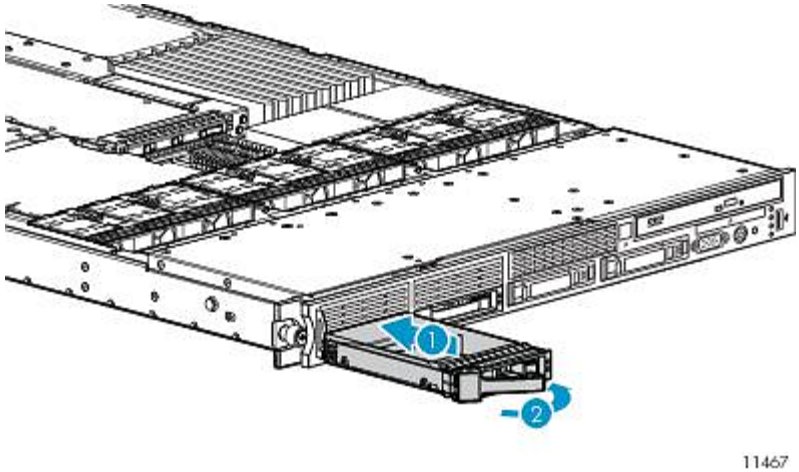


Figure 29 Installing the Node Hard Drive



NOTE: The replacement drive is automatically configured to RAID 1; no administrator action is required.

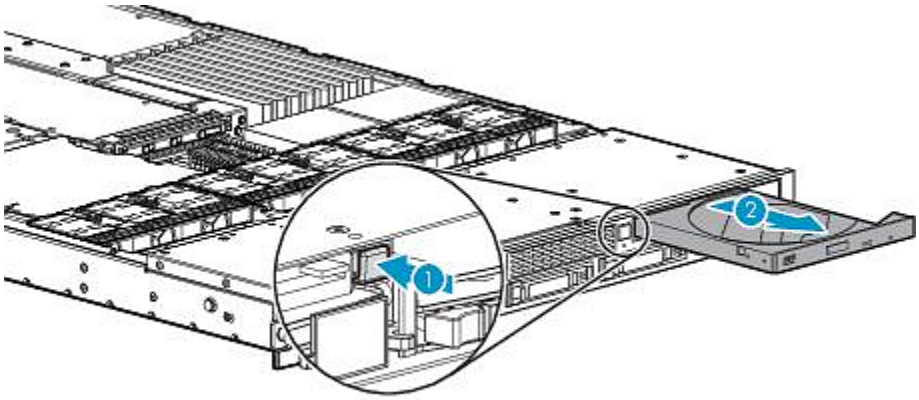
DVD-CD Drive

CAUTION: To prevent improper cooling and thermal damage, do not operate the node unless all bays are populated with either a component or a blank.

1. Power off the node.

   NOTE: The ejector button for the CD-ROM drive is recessed to prevent accidental ejection; it may be helpful to use a small, flat, blunt object, such as a key or pen, to push the ejector button.

2. Press the ejector button in firmly until the DVD-CD drive ejects (1).

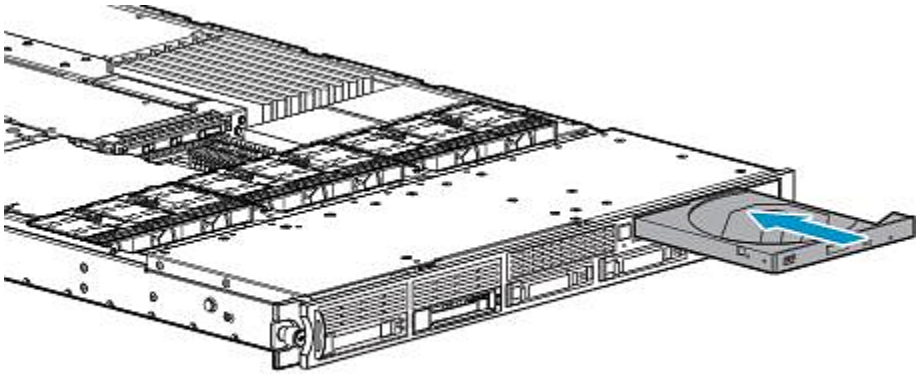


11468

3. Pull the DVD-CD drive out of the node (2).

To replace the component:

1. Carefully align the connector on the rear of the drive with the connector on the DVD-CD drive interface board.
2. Slide the drive into the bay until it clicks.



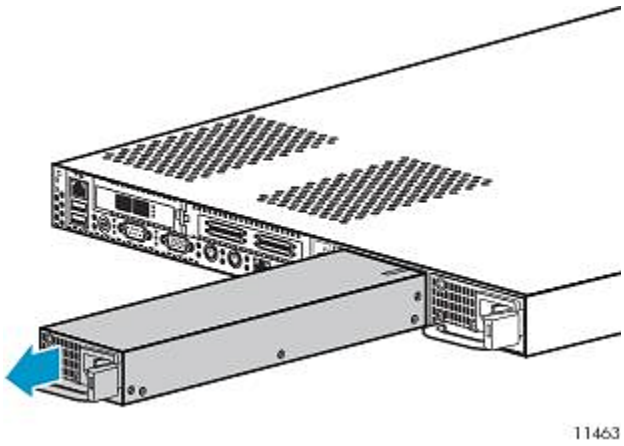
11469

Power Supply

CAUTION: To prevent improper cooling and thermal damage, do not operate the node unless all bays are populated with either a component or a blank.

1. Disconnect the power cord from the power supply.

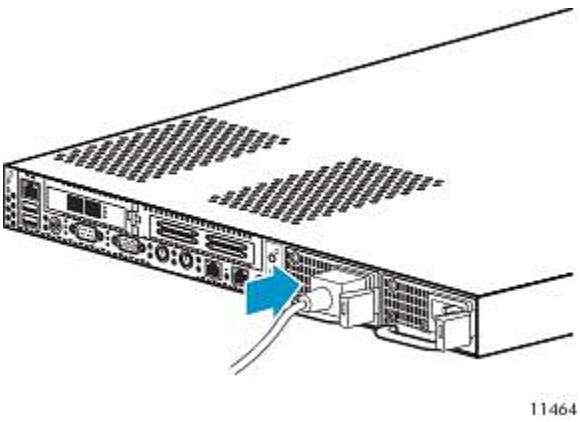
2. Press the power supply release lever (1), and then pull the power supply from the node.



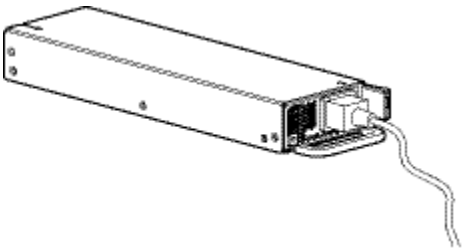
To replace the component:

WARNING! To reduce the risk of electric shock or damage to the equipment, do not connect the power cord to the power supply until the power supply is installed.

1. Remove the protective cover from the connector pins on the power supply.
2. Slide the power supply into the bay until it clicks.



3. Use the strain relief clip to secure the power cord.

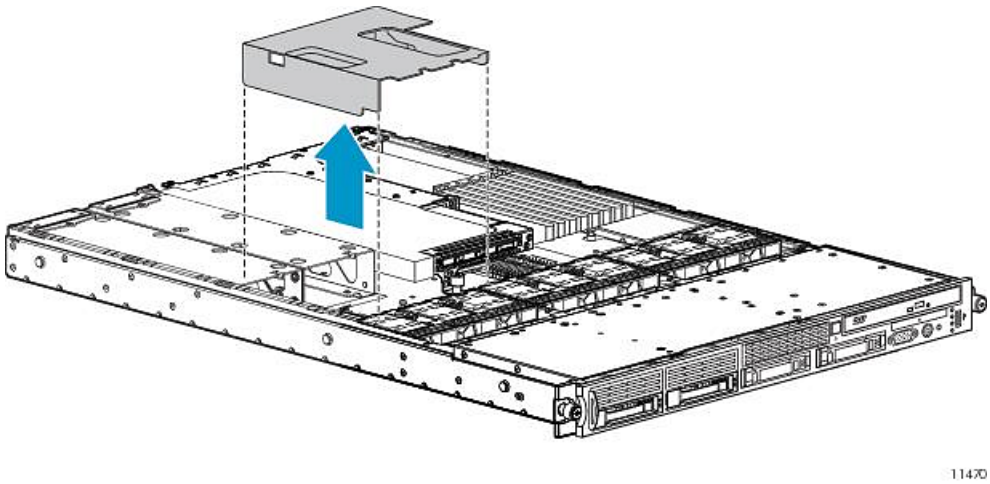


4. Connect the power cord to the power supply.
5. Be sure that the power supply LED is green.
6. Be sure that the front panel external health LED is green.

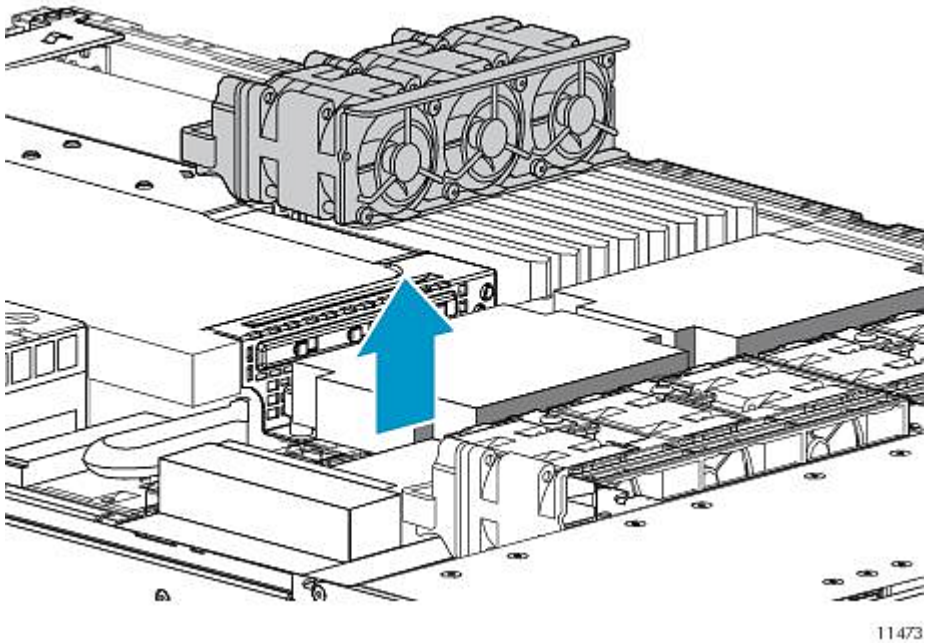
Fan Module

CAUTION: Do not operate the node for long periods without the access panel. Operating the node without the access panel results in improper airflow and improper cooling that can lead to thermal damage.

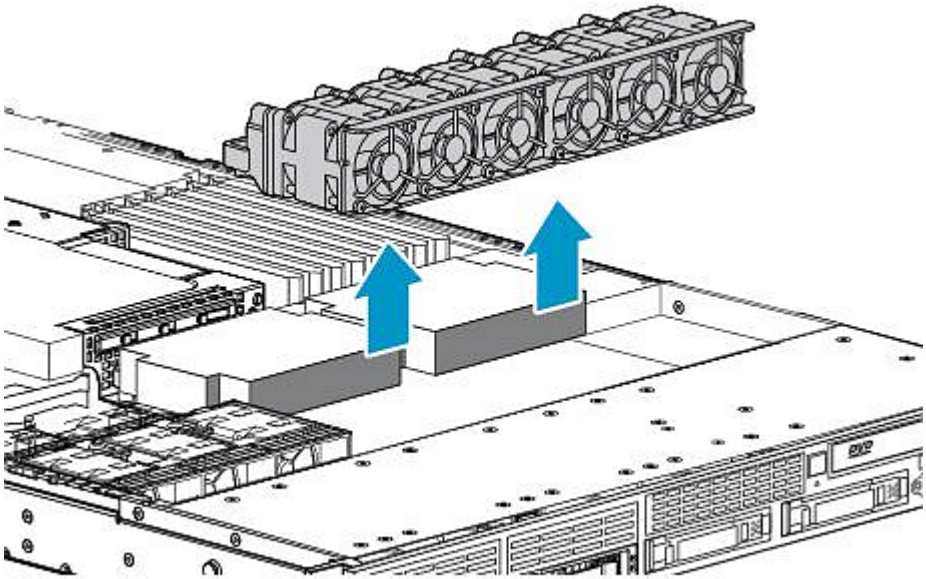
1. Power off the node.
2. Extend or remove the node from the rack. See Extending a VLS Node from the Rack or Removing a VLS Node from the Rack.
3. Remove the access panel.
4. To remove fan module 1:
   a. Remove the power supply air baffle.



   b. Remove fan module 1.



5. To remove fan module 2 or 3:
   a. Remove the power supply air baffle.
   b. Remove fan module 2 or 3.



To replace the component, reverse the removal procedure.

IMPORTANT: After installing the fan module, firmly press the top of the module connectors to ensure the connectors are seated properly.

FBDIMM

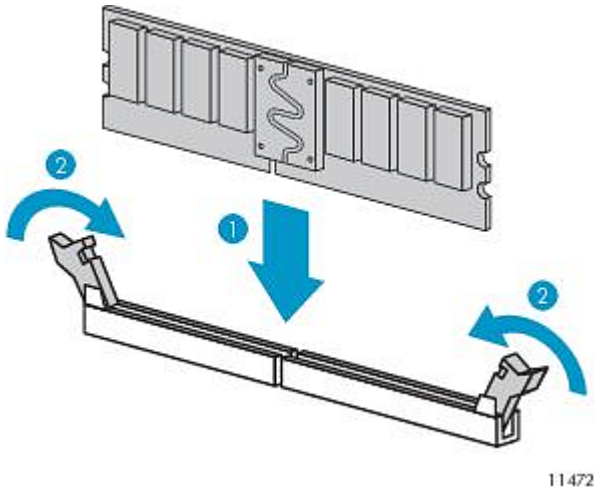
1. Power off the node.
2. Extend or remove the node from the rack. See Extending a VLS Node from the Rack or Removing a VLS Node from the Rack.
3. Remove the access panel.
4. Open the FBDIMM slot latches.
5. Remove the FBDIMM.

CAUTION: Use only Compaq branded or HP FBDIMMs. FBDIMMs from other sources may adversely affect data integrity.

To replace the component, reverse the removal procedure.

NOTE: FBDIMMs do not seat fully if turned the wrong way.

When replacing a FBDIMM, align the FBDIMM with the slot and insert the FBDIMM firmly (1), pressing down until the FBDIMM snaps into place. When fully seated, the FBDIMM slot latches (2) lock into place.



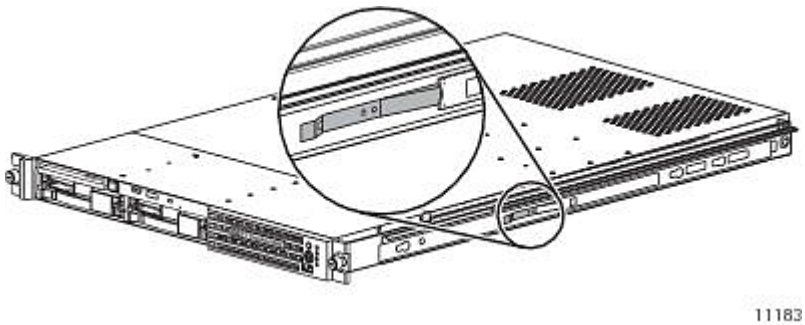
Replacing a Primary Node

CAUTION: Each VLS node weighs 17.9 kg (39.5 lb) full. At least two people are required to lift and move each node.

To replace a primary node:

1. Remove the existing node from the rack:
   a. Power off the system. See Powering Off the System.
   b. From the back of the node, make a note of all cable connections then disconnect the cables.
   c. From the front of the node, loosen the captive thumbscrews until the thumbscrews are free of the rack.
   d. Pull the node out from the rack until it stops.
   e. Squeeze the release brackets (see Figure 30 (page 222)), then pull the node free from the rails.

Figure 30 Rail Release Bracket



2. Install the new node into the rack. See Installing the VLS Node into a Rack.
3. Reconnect the cables to the new node exactly as they were connected to the previous node.
4. Configure the node:

a. On the primary node, connect to the serial port or use the keyboard and mouse ports to connect to a console.
b. Power on the primary node.

   After several minutes, a menu will appear on your monitor asking whether the node is a primary (master, m) or secondary (slave, s) node.
c. Enter `m`. The node will then run cable checks and configuration checks.
d. After the checks are complete the node will reboot automatically. Wait for the primary node to fully boot.

   Rebooting is complete when you receive the "Initializing node#" and then "Initializing for node# completed." messages in the systems notifications (if you have DHCP enabled) of Command View VLS or when you see the login prompt on the terminal.

5. The warm failover feature will now automatically restore the original configuration and licenses.

Replacing a Secondary Node

CAUTION: Each VLS node weighs 17.9 kg (39.5 lb) full. At least two people are required to lift and move each node.

To replace a secondary node:

1. Remove the existing node from the rack:
   a. Power off the system. See Powering Off the System.
   b. From the back of the node, make a note of all cable connections then disconnect the cables.
   c. From the front of the node, loosen the captive thumbscrews until the thumbscrews are free of the rack.
   d. Pull the node out from the rack until it stops.
   e. Squeeze the release brackets (see Figure 30 (page 222)), then pull the node free from the rails.
2. Install the new node into the rack. See Installing the VLS Node into a Rack.
3. Reconnect the cables to the new node exactly as they were connected to the previous node.
4. Configure the node. See Configuring the Secondary Nodes.
5. Reboot the system. See Rebooting the System.

Replacing All VLS9000 Nodes with VLS9200 Nodes

Prior to the node replacement:

1. The VLS9000 system must be running firmware version 6.1.0. If your system is not on 6.1.0, follow the procedure in the *HP Virtual Library System Firmware Version 6.1.0 Release Notes* to upgrade.
2. Schedule sufficient time for the node replacement. The time needed depends on the number of nodes and the wiring; assume a minimum of 30 minutes per node and an additional two hours for configuration.
3. Stop any in-process backups and restores, and disable the VLS in the backup applications to suspend operations during the node replacement.
4. Create a firmware version 6.1.0 Quick Restore DVD. Having one DVD for each node will speed up the Quick Restore process.

To replace the nodes:

1. Attach rails to all of the replacement VLS9200 nodes; see the instructions in the rail kit.
2. As a best practice, save the configuration on the live VLS system.
3. Shut down all VLS nodes. You will start the replacements with the master node.

4. Disconnect all power cords from the node.
5. From the back of the node, make a note of all cable connections then disconnect the cables.
6. Remove the node from the front of the chassis. See "Replacing a Primary Node" (page 222) for details.
7. Install the replacement VLS9200 node into the rack.
8. Reconnect the cables to the new node.

   The VLS9200 master node does not need the USB dongle. The Ethernet switch cables should now connect to NIC ports 3 and 4.
9. Reconnect the power cords to the node.
10. Power up the node.
11. Insert the Quick Restore DVD into the drive and start the Quick Restore process. When the Quick Restore is complete, the node will automatically reboot.
12. Repeat Step 4 through Step 11 for all secondary nodes.
13. When the master node comes up after the reboot, configure it as you would configure a new VLS installation. See "Configuring the Primary Node 0" (page 44) for details. The node will reboot after the configuration is set.
14. After the master node comes up after the reboot, configure each secondary node as you would configure a new VLS installation. See "Configuring the Secondary Nodes" (page 44) for details.
15. Log into Command View VLS to ensure that all secondary nodes have come up. (It does not matter if they show a degraded state.)
16. Install the hp_6.1.0_reboot_3053 patch to the system; this will adjust the new backend Ethernet configuration on each node. See the *HP Virtual Library System hp_6.1.0_reboot_3053 Patch Release Notes* for details.
17. After the automatic reboot from the patch, log back into Command View VLS.
18. If any of the secondary nodes show a degraded state, run the **Clear All Faults** task on the **Chassis** screen.

    All nodes should now be up and in the green Good state.

Fibre Channel Switch Replacement

To replace a Fibre Channel Switch:

1. Power off the switch.
2. Make a note of all cable connections to the switch then disconnect the cables.
3. Remove the 1U cover plate for the switch from the front of the rack.
4. Remove the four bolts from the rail flanges on the rear rack uprights using a #2 Phillips screwdriver.
5. Loosen the two nuts securing the rail ends to the adjustable mounting flanges, which are mounted on the front rack uprights, using a 7/16 inch wrench.
6. Slide the switch out the rear of the rack.

△ **CAUTION:** Make sure the switch is supported below, either by equipment mounted in the next rack slot or with your hand, before sliding the switch off the adjustable mounting flanges that support it.

7. Disconnect the AC power cables from the back of the switch.
8. Remove the rack rails from the switch.
9. Install the rack rails on the new switch and then mount the switch in the rack. See Installing the Fibre Channel Switch 8/24q into a Rack.
10. Reconnect all cables to the new switch exactly as they were connected to the failed switch.
11. Re-install the 1U cover plate for the switch to the front of the rack.

12. Power on the new switch.

Fibre Channel Transceiver Replacement

To replace a Fibre Channel transceiver

1. Power off the system. See Powering Off the System.
2. Disconnect the Fibre Channel cable by squeezing the end of the cable connector.

   If removing more than one cable, make sure that they are labeled before removing them. The cables are fragile; use care when handling them.

CAUTION: Mishandling Fibre Channel cables can degrade performance. Do not twist, fold, pinch, or step on cables. Do not bend the cables tighter than a 2-inch radius.

3. Some models of transceivers are held in place by a small wire bail actuator; pull down on the top of the bail and rotate it in the downward direction.
4. Grasp the transceiver between your thumb and index finger, and carefully remove it from the Fibre Channel port.
5. Insert a new transceiver in the Fibre Channel port and gently push in the transceiver until it clicks in place.

   NOTE: A transceiver fits only one way in the port. If the transceiver does not install under gentle pressure, pull it out of the port, turn it over, and re-insert it.

6. Plug the Fibre Channel cable into the duplex jack at the end of the transceiver.
7. Power on the system. See Powering on the VLS System.

Ethernet Switch Replacement

To replace an Ethernet Switch:

1. Power off the switch.
2. Make a note of all cable connections to the switch then disconnect the cables.
3. From the front of the switch, loosen the captive thumbscrews until the thumbscrews are free of the rack.
4. Remove the switch from the rack.
5. Install the new switch into the rack. See "Installing the 100 Mb Ethernet Switch 2510-24 into a Rack" (page 35) or "Installing the Ethernet Switch 6600–24G into a Rack" (page 31).
6. Reconnect all cables to the new switch exactly as they were connected to the failed switch.
7. Power on the new switch.

VLS9200 Disk Array Component Replacement

This section describes the processes for replacing the hard drive, power module, and RAID or expansion controller components of the VLS disk array enclosures.

Hard Drive

CAUTION: Before removing a hard drive from the disk array, ensure that a replacement hard drive is immediately available. Removing a hard drive causes a significant change in the airflow within the disk array, and the disk array could overheat if a replacement hard drive is not installed within a relatively short time.

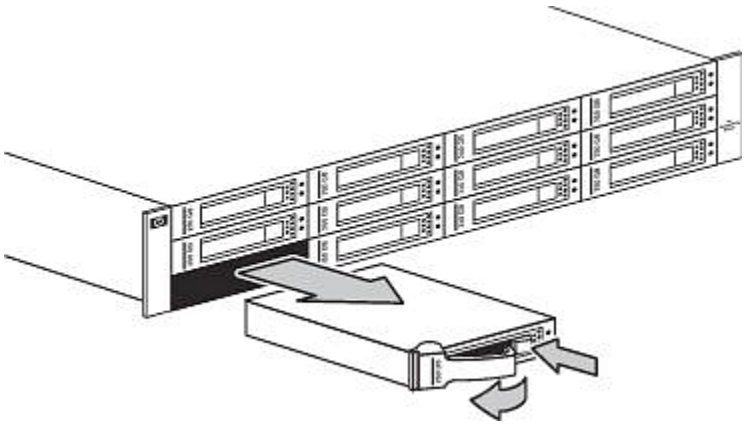
Be careful when replacing a drive. The drives in the disk array are fragile.

1. Press the drive latch release button.

2. Pull the drive out of the disk array by its latch handle about 3 cm (1 inch) so that it is disconnected from the backplane connector.

CAUTION: A drive with a rapidly spinning disk can be difficult to hold securely. To decrease the chance of dropping the drive, do not remove it completely from the disk array until the disk has stopped rotating. This usually takes a few seconds.

3. When the disk is no longer spinning, remove the drive from the disk array.



To replace the component:

1. Pull out the latch handle on the drive as far as it can go.
2. Slide the replacement drive into the bay until it can go no further. About 1 cm (0.5 inch) of the drive protrudes from the bay.
3. Push the release lever all the way in. This action installs the drive completely in the bay and seats it firmly against the connector in the disk array.
4. Firmly close the latch handle to lock the drive in the drive bay.
5. Observe the drive status LEDs to confirm that the replacement drive is functioning correctly. See Front Panel LEDs.

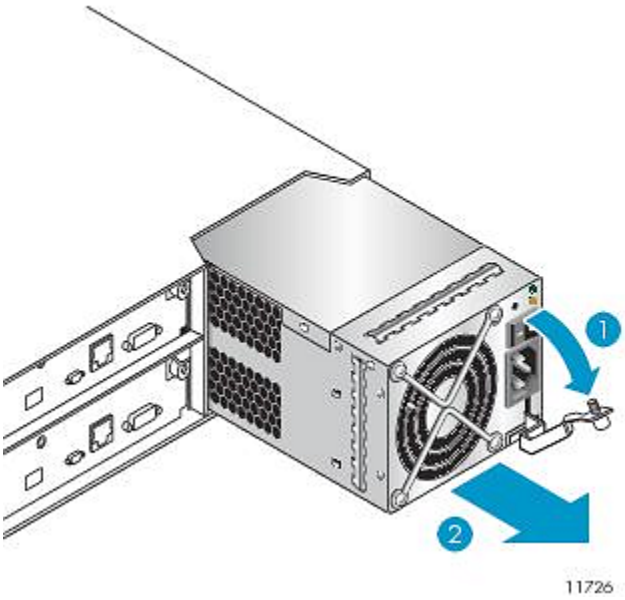
Power Module

CAUTION: Before removing a power module from the disk array enclosure, ensure that a replacement power module is immediately available. Removing a power module causes a significant change in the airflow within the disk array enclosure, and the disk array enclosure could overheat if a replacement power module is not installed within two minutes.

NOTE: When a power supply fails, the fans of the power module continue to operate because they draw power from the power bus located on the midplane.

1. If the defective power module has a power switch, set it the Off position.
2. Disconnect the AC power cord from the defective power module.
3. Turn the thumbscrew at the top of the latch counterclockwise until the thumbscrew is disengaged from the power module.

   Do not remove the thumbscrew from the latch.



4. Rotate the latch downward to about 45 degrees, supplying leverage to disconnect the power module from the internal connector.
5. Use the latch to pull the power module out of the chassis.

NOTE: Do not lift the power module by the latch. This could break the latch. Hold the power module by the metal casing.

6. Position the new power module so that AC connector and power switch are on the right side, and slide the power module into the power module slot as far as it will go.
7. Rotate the latch upward so that it is flush against the power module to ensure that the connector on the power module engages the connector inside the chassis.
8. Turn the thumbscrew at the top of the power module latch clockwise until it is finger-tight to secure the latch to the power module.
9. Connect the AC power cord.
10. If the new power module has a power switch, set it to the On position.
11. Confirm that the AC Power Good LED on the replacement power supply is illuminated green. See Rear Panel LEDs and Buttons.
12. Confirm that the DC-Fan fault/service required LED on the replacement power supply is off.

RAID or Expansion Controller

There are two controllers in each VLS disk array enclosure: either two RAID controllers or two expansion controllers. Both controllers in a disk array enclosure operate during normal disk array operation. If one of the controllers fails, the other controller takes over operation of the storage system until you install a new controller. A controller can be hot-swapped, which means you can replace one controller without halting I/O to the storage system or powering it off, as long the other controller is operational.

IMPORTANT: RAID controllers should only be replaced while the array is powered up to ensure that the array will copy configuration data from the surviving controller into the newly added controller.

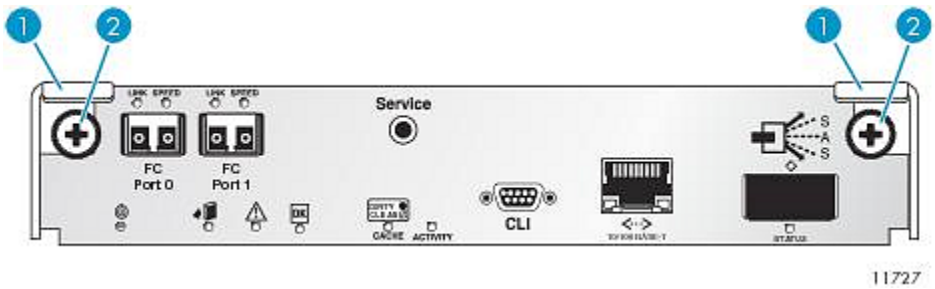
CAUTION: When removing a controller, allow 60 seconds for the failover to complete before fully inserting a replacement. When you remove a controller with the disk array enclosure powered on, install a replacement controller or a blank within two minutes. Otherwise, the disk array enclosure might overheat.

NOTE: A damaged midplane may appear as though a controller has failed. If you replace a controller and it does not remedy the original fault, replace the whole disk array enclosure.

To replace a RAID controller or expansion controller:

1. Disconnect all cables attached to the controller in this order:
   - For a RAID controller:
     1. Fibre Channel port 0
     2. SAS output port
     3. Ethernet port
   - For an expansion controller:
     1. SAS port 0, input port
     2. SAS port 1, output port
2. Turn the thumbscrew on each latch counterclockwise until the screw disengages from the controller.

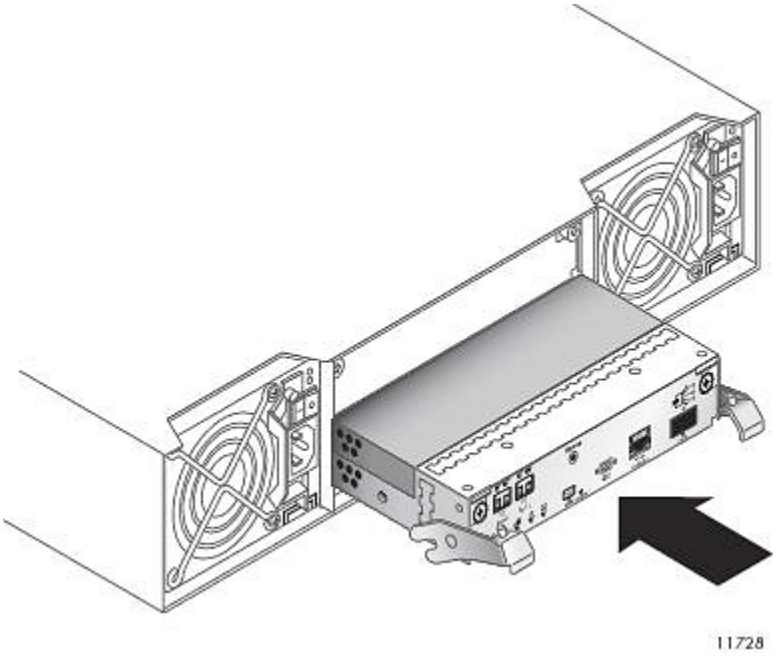
   Do not remove the screw from the handle.



Item	Description
1	Latches
2	Thumbscrews

3. Press both latches downward to disconnect the module from the midplane.
4. Pull outward on the latches to slide the controller out of the disk array enclosure.
5. Loosen the thumbscrews on the latches of the new controller and press the latches downward.
6. Position the controller with the latches toward the top and slide the controller into a slot as far as it will go.

CAUTION: When replacing a controller, ensure that less than 10 seconds elapse between inserting the controller into a slot and fully latching it in place. Failing to do so might cause the controller to fail. If it is not latched within 10 seconds, remove the controller from the slot and repeat the process.



7. Press the latches upward until they are flush with the top edge of the controller, then turn the thumbscrew on each latch clockwise until they are finger-tight.

   The controller begins initializing.

   The Power On/OK LED illuminates green when the controller completes initializing and is online.

8. Connect the disconnected cables to the new controller in reverse order of Step 1.
9. If you are replacing a RAID controller, restore the failed path:
   a. In Command View VLS, access the System tab.
   b. Select **Storage LUNs** from the navigation tree.
   c. Select **View** to display the storage LUN details.
   d. Select **Fix Primary Paths** from the task bar to display the **Fix Primary Paths Wizard**.
   e. Select **Apply** to set all paths back to their primary paths.

NOTE: Upgrade of the firmware for the RAID controller's components is automatically provided by the operational controller and will occur within the first 10 minutes of power on. Upgrade of the firmware on the expansion controller is not automatic; schedule a VLS restart if an upgrade is needed. To check the current expansion controller firmware, use Command View VLS to review the enclosure information on the System tab. For the enclosure repaired, compare the firmware version on Disk Adapter 0 and Disk Adapter 1 and confirm they are the same. If the replacement controller has a lower firmware version, HP recommends a VLS reboot at the earliest opportunity. Earlier versions of the expansion controller firmware are supported by the current RAID controller firmware.

15 Disaster Recovery

This section details the VLS disaster recovery procedures. It includes recovering from operating system failures, disk array failures, and node failures.

Recovering from Operating System Failure

Re-install the operating system if it becomes corrupted or is lost as a result of node RAID volume failure.

CAUTION: Only install the VLS operating system on the node hard drives. Installing any other operating system on the node hard drives voids the warranty.

NOTE: The VLS operating system contains all the hardware device drivers, firmware, and utilities required to operate the VLS.

To re-install the operating system:

1. Connect a keyboard to the keyboard connector.
2. Connect a monitor to the video connector.
3. Insert the VLS Quick Restore CD into the CD-ROM or DVD-CD drive.

   The VLS Quick Restore CD auto starts.
4. Press **R** on the keyboard to start the re-installation.

   The re-installation takes 30 minutes or less to complete. The screen may freeze during the last 10 minutes of the re-installation. This is normal.

   The VLS Quick Restore CD is ejected and the system reboots when the re-installation is complete.
5. Restore the VLS.

   The warm failover process automatically restores the node to its previous configuration including the serial numbers, front-end Fibre Channel WWPNs, virtual device configuration, and licenses. No reconfiguration is required. See Restoring the System by Warm Failover.

   If the warm failover process does not restore the system, you can manually restore using a configuration file. See Manually Restoring the System.

   If you are restoring a primary node:

   a. Power up the secondary nodes once the primary node fully reboots.
   b. Set it as the master node in Command View VLS. See Configuring the Primary Node 0. (The final step of setting the IP address and other public network configurations is not necessary.)
   c. Re-enter the IP addresses of the secondary nodes. See Setting the Network Settings using Command View VLS.

NOTE:
If you have the iLO Advanced license installed, you can Quick Restore your system using the Virtual Media feature; see the iLO user guide for details.

Restoring the System with Warm Failover

After any configuration or license change, the VLS automatically saves (within one hour) the updated configuration and licenses to a hidden virtual cartridge stored on the back-end disk arrays. When you replace the node or node hard drives, or re-install the operating system, the VLS uses this information to automatically restore the system to a configuration identical to what it had before. This automated process eliminates the need to manually restore the configuration.

Manually Restoring the System

After re-installing the operating system, the warm failover feature restores the licenses and configuration settings. However, if the warm failover does not occur (for example, due to a corrupt or missing file), the VLS virtual library configuration and network settings can be quickly restored from the configuration file created by performing a Save Configuration. See Restoring the Configuration from a Configuration File.

If a configuration file was not created, you must reconfigure the network settings and rebuild the virtual library and virtual drive configurations. The cartridge configurations, however, do not have to be rebuilt, as they are stored on the disk arrays. See Manually Rebuilding the Virtual Library Configuration.

In either case, begin by re-installing the licenses.

Re-installing the VLS Licenses

If one or more capacity bundles (or existing disk arrays), deduplication licenses, and/or replication licenses were added to the VLS, you must re-install the VLS licenses.

To re-install the VLS licenses:

1. Locate the emails containing the license keys.

   Your VLS license keys were emailed to you when you originally requested them. If you no longer have these emails, contact HP technical support to obtain new license keys.
2. Log into Command View VLS.
3. Follow the Installing Additional Licenses procedure beginning with Step 9.

Restoring the Configuration from a Configuration File

Restoring the virtual library configuration from the configuration file restores the virtual library and virtual drive configurations, and administrative and network settings (including the VLS serial number and persistent Fibre Channel port WWPNs).

NOTE: Configuration files are not backwards compatible with earlier firmware versions. For example, a configuration file created on a system running firmware version 6.0 will not work on the system at firmware version 3.4. Make sure your system is at the version that created the configuration file before restoring the configuration.

To restore the virtual library and network settings from the configuration file:

1. Set the network settings so you can open a Command View VLS session. See Setting the Network Settings.
2. Add all secondary nodes using the Add Node Wizard. For each secondary node:
   a. In Command View VLS, select the **System** tab.
   b. Select **Nodes** from the navigation tree.
   c. Select **Add Node** from the task bar in the main window. This will bring up the **Add Node Wizard**.
   d. Verify that the node name in the **Node Name** field is the next available number that you configured previously. For example, the primary node, previously configured as Node 0, is identified as Node 0 in the list of nodes on the navigation tree. The first secondary node added should be Node 1. The next secondary node added should be Node 2.
   e. Select **Finish** to add the node.
3. Select **Chassis** in the navigation tree.
4. Click **Restore Config** under **Maintenance Tasks**. The Restore Config window opens.
5. Click **Browse**.
6. Locate and select the desired configuration file.
7. Click **Open**.

8. Click **Next Step**. A message displays indicating that the file was uploaded successfully.
9. Click **Next** to start loading the configuration file.

   After the configuration file is loaded, the system automatically applies the configuration and reboots.

Manually Rebuilding the Virtual Library Configuration

If you are unable to manually restore the system from the configuration file, you must manually reconfigure the network settings and rebuild the virtual library configuration:

1. Set the network settings so you can open a Command View VLS session. See Setting the Network Settings.
2. Rebuild the virtual library and virtual drive configurations and re-enter your other configuration settings, such as the notification alert settings. See Configuration, Management, and Monitoring.

NOTE: If the node system board was ever changed and the virtual library configuration and network settings were not saved to a configuration file, the persistent VLS serial number and Fibre Channel port WWPNs are lost and cannot be recovered. The VLS firmware will automatically generate a new VLS serial number and new Fibre Channel port WWPNs based on the node system board's MAC address.

If this occurs, any capacity licenses installed on the VLS will no longer work, as they only work with the VLS serial number for which they were issued. You can obtain new capacity licenses from HP technical support using the new VLS serial number. You will also need to reconfigure your SAN to reflect the new Fibre Channel port WWPNs.

Recovering from a VLS Disk Array RAID Volume Failure

If three or more hard drives have failed in a single VLS9000 disk array enclosure, a disk array RAID volume failure has occurred. Each disk array enclosure is configured as one RAID6 volume. A disk array enclosure RAID volume failure will corrupt all the data stored on the VLS storage pool using that RAID volume, making it unrecoverable.

NOTE: Only perform this procedure if a RAID volume failure has actually occurred. Other factors can result in a false RAID volume failure being reported, such as a disk array enclosure being powered down or the disk array enclosure external cabling being disconnected at either end.

To recover from a disk array enclosure RAID volume failure:

1. Repair the failed RAID volume (for example, replace the failed hard drives in the RAID volume). See Hard Drive.
2. Erase all the virtual media from the disk array enclosures and rebuild all the RAID volumes on the storage pool affected:
   a. Select **Storage Pools** in the navigation tree, then select the storage pool that needs recovery.
   b. Click **Rebuild Storage Pool** in the task bar.
   c. Click **Rebuild**.
   d. Click **Yes** to confirm.
3. Recreate the cartridges that existed on the VLS storage pool.

   VLS cartridge configurations are stored on the disk arrays and have been erased.

Recovering from a Node RAID Volume Failure

To recover from a node RAID volume failure, which occurs when both node hard drives fail:

1. When restoring a primary node, power down all of the secondary nodes.
2. Replace the failed node hard drives.

3. Install the operating system on the new hard drives and restore the VLS. See Recovering from Operating System Failure.

Recovering from a Primary Node Failure using a Cold Spare Primary Node

On a multi-node VLS, the primary node maintains the configuration for the entire VLS library. In the unlikely event of a primary node failure, the VLS library would be unavailable until the node is replaced or repaired. To avoid extended downtime, you can configure an additional node as a "cold failover" node with all the same attributes as the primary. If the primary node fails, deploy the spare primary node in place of the failed primary node to bring the entire VLS library back online quickly.

Install the spare primary node into the rack directly above the primary node.

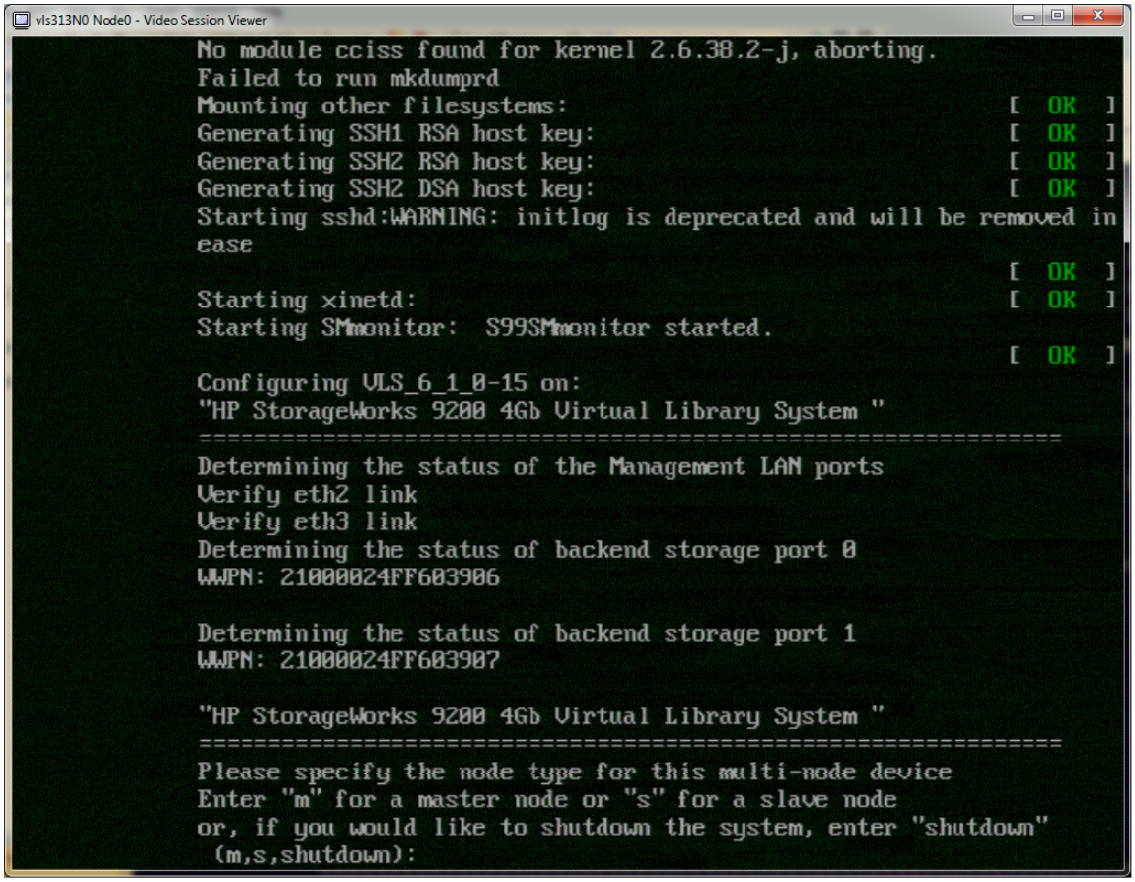
To deploy the spare primary node:

1. Shut down all nodes on the VLS.

   Because the original primary node has failed, he secondary nodes should be shut down from the command line of each node. Log in to the administrator account on each secondary node using the serial port or keyboard and mouse. At the prompt, enter `shutdownNode`.

2. Cable the spare primary node exactly as the original primary node was cabled:
   a. Move all Fibre Channel cables from the original primary node ports to the corresponding spare primary node ports.
   b. Move all Ethernet cables including the USB Ethernet adapter from the original primary node ports to the corresponding spare primary node ports.
   c. Connect to the serial port or use the keyboard and mouse ports to connect to the console of the spare primary node.
3. Power on the spare primary node.

   The node will run cable checks and configuration checks. After several minutes, a menu will appear on your monitor asking whether the node is a primary (master, m) or secondary (slave, s) node.



4. Record the backend Fibre Channel WWPN from the console and configure them for the automigration tape libraries.

   The Fibre Channel host port WWPNs on the spare primary node will be set to the same as the original primary node when the VLS configuration is restored.

   The Fibre Channel storage port WWPNs are not set to the same as the original primary node when the VLS configuration is restored, so the Fibre Channel storage port WWPNs must be added to the EVA storage presentation and any configured automigration tape library storage presentations.

5. Enter `m`.

   The node will then run cable checks and configuration checks. After the checks are complete the node will reboot automatically. Wait for the node to fully boot.

   The new primary node will reboot once more after it has retrieved the old configuration from the backend storage. Wait until the new primary node boots up with the correct hostname and configuration.

6. Log into Command View VLS and check:
   - VLS identity
   - Chassis general information
   - General information for the primary node such as name, serial number, memory, Ethernet, etc.
   - Fibre Channel configuration for the primary node (host ports and storage ports)
   - Virtual library configuration
   - Storage pool general information
   - EVA storage LUNs

- Cartridges configured
- Automigration configuration
- Host LUN mapping configuration

7. Power up all secondary nodes. The boot up can take 10 to 20 minutes.
8. Verify all secondary nodes.

   At this point, your VLS system is up and in working order. Do not connect the old primary node to the VLS because its configuration will be out of sync with the system.
9. Repair the old primary node and then Quick Restore it; do not configure the node after the Quick Restore. Power down the old node and keep it as the cold spare.

NOTE: If your primary node failed within an hour of making a configuration change, your most recent change may not be reinstated on the spare node. Check your configuration settings and reconfigure as needed.

16 Support and Other Resources

Related Information

Documents

HP provides the following documentation to support this product:

- HP Virtual Library System release notes
- *HP VLS Solutions Guide*
- *HP VLS9000 Virtual Library System User Guide*
- HP Virtual Library System installation posters

See the media kit provided with the VLS and our website for related documentation.

Websites

- HP website:
  http://www.hp.com
- HP VLS Support:
  http://hp.com/support/vls
- HP VLS Manuals:
  http://www.hp.com/support/vls/manuals
- HP Storage Sizer:
  http://www.hp.com/go/storageworks/sizer
- HP Enterprise Backup Solutions Overview and Features:
  http://www.hp.com/go/ebs
- HP Data Storage:
  http://www.hp.com/go/storage
- HP Drivers and Software:
  http://www.hp.com/support/downloads
- HP Partner Locator:
  http://www.hp.com/service_locator

Document Conventions and Symbols

Table 30 Document Conventions

Convention	Element
Blue text: Table 30 (page 236)	Cross-reference links and e-mail addresses
Blue, underlined text: http://www.hp.com	Web site addresses
Bold text	• Keys that are pressed • Text typed into a GUI element, such as a box • GUI elements that are clicked or selected, such as menu and list items, buttons, tabs, and check boxes
Italic text	Text emphasis

Table 30 Document Conventions *(continued)*

Convention	Element
`Monospace` text	• File and directory names • System output • Code • Commands, their arguments, and argument values
`Monospace, italic` text	• Code variables • Command variables
`Monospace, bold` text	Emphasized monospace text

WARNING! Indicates that failure to follow directions could result in bodily harm or death.

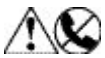
CAUTION: Indicates that failure to follow directions could result in damage to equipment or data.

NOTE: Provides additional information.

The following equipment symbols may be found on hardware to which this guide pertains. They have the following meanings:

WARNING!  These symbols, which mark an enclosed surface or area of the equipment, indicate the presence of electrical shock hazards. The enclosed area contains no operator serviceable parts.

WARNING: To reduce the risk of injury from electrical shock hazards, do not open this enclosure.

WARNING!  These symbols, which mark an RJ-45 receptacle, indicate a network interface connection.

WARNING: To reduce the risk of electrical shock, fire, or damage to the equipment, do not plug telephone or telecommunications connectors into this receptacle.

WARNING!  These symbols, which mark a surface or area of the equipment, indicate the presence of a hot surface or hot component. Contact with this surface could result in injury.

WARNING: To reduce the risk of injury from a hot component, allow the surface to cool before touching.

WARNING!  Power supplies or systems marked with these symbols indicate the presence of multiple sources of power.

WARNING: To reduce the risk of personal injury from electrical shock, remove all power cords to completely disconnect power from the power supplies and systems.

WARNING!  Any product or assembly marked with these symbols indicates that the component exceeds the recommended weight for one individual to handle safely.

WARNING: To reduce the risk of personal injury or damage to the equipment, observe local occupational health and safety requirements and guidelines for manually handling material.

Rack Stability

Rack stability protects personnel and equipment.

⚠ **WARNING!** To reduce the risk of personal injury or damage to equipment:

- Extend leveling jacks to the floor.
- Ensure that the full weight of the rack rests on the leveling jacks.
- Install stabilizing feet on the rack.
- In multiple-rack installations, fasten racks together securely.
- Extend only one rack component at a time. Racks can become unstable if more than one component is extended.

Contacting HP

Before you Contact HP

Be sure to have the following information available before calling HP:

- Technical support registration number (if applicable)
- Product serial numbers
- Product model names and numbers
- Applicable error messages
- Operating system type and revision level
- Detailed, specific questions

HP Contact Information

For the name of the nearest HP authorized reseller:

- See the Contact HP worldwide (in English) webpage (http://welcome.hp.com/country/us/en/wwcontact_us.html).
- In the United States, call 1-800-345-1518.
- In Canada, call 1-800-263-5868.

For HP technical support:

- In the United States, for contact options see the Contact HP United States webpage (http://welcome.hp.com/country/us/en/contact_us.html). To contact HP by phone:
  - Call 1-800-HP-INVENT (1-800-474-6836). This service is available 24 hours a day, 7 days a week. For continuous quality improvement, calls may be recorded or monitored.
  - If you have purchased a Care Pack (service upgrade), call 1-800-633-3600. For more information about Care Packs, refer to the HP website (http://www.hp.com/hps).
- In other locations, see the Contact HP worldwide (in English) webpage (http://welcome.hp.com/country/us/en/wwcontact.html).

Subscription Service

HP strongly recommends that customers register online using the Subscriber's choice web site: http://www.hp.com/go/e-updates.

Subscribing to this service provides you with e-mail updates on the latest product enhancements, newest driver versions, and firmware documentation updates as well as instant access to numerous other product resources.

After subscribing, locate your products by selecting **Business support** and then **Storage** under Product Category.

Customer Self Repair

HP customer self repair (CSR) programs allow you to repair your Storage product. If a CSR part needs replacing, HP ships the part directly to you so that you can install it at your convenience. Some parts do not qualify for CSR. Your HP-authorized service provider will determine whether a repair can be accomplished by CSR.

For more information about CSR, contact your local service provider. For North America, see the CSR website:

http://www.hp.com/go/selfrepair

HP Insight Remote Support Software

HP strongly recommends that you install HP Insight Remote Support software to complete the installation or upgrade of your product and to enable enhanced delivery of your HP Warranty, HP Care Pack Service or HP contractual support agreement. HP Insight Remote Support supplements your monitoring, 24x7 to ensure maximum system availability by providing intelligent event diagnosis, and automatic, secure submission of hardware event notifications to HP, which will initiate a fast and accurate resolution, based on your product's service level. Notifications may be sent to your authorized HP Channel Partner for on-site service, if configured and available in your country. The software is available in two variants:

- HP Insight Remote Support Standard: This software supports server and storage devices and is optimized for environments with 1-50 servers. Ideal for customers who can benefit from proactive notification, but do not need proactive service delivery and integration with a management platform.
- HP Insight Remote Support Advanced: This software provides comprehensive remote monitoring and proactive service support for nearly all HP servers, storage, network, and SAN environments, plus selected non-HP servers that have a support obligation with HP. It is integrated with HP Systems Insight Manager. A dedicated server is recommended to host both HP Systems Insight Manager and HP Insight Remote Support Advanced.

Details for both versions are available at:

http://www.hp.com/go/insightremotesupport

To download the software for free, go to Software Depot:

http://www.software.hp.com

Select **Insight Remote Support** from the menu on the right.

17 Documentation feedback

HP is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (**docsfeedback@hp.com**). Include the document title and part number, version number, or the URL when submitting your feedback.

A Troubleshooting

This appendix lists iLO troubleshooting features, and also describes some common issues you may encounter while configuring or using the VLS including automigration/replication and deduplication issues.

Using iLO

The VLS supports many of the features of iLO 2 Standard (non-licensed). If you are troubleshooting the VLS, especially if the system is down, you may find these features helpful:

- Power on the VLS.
- Power off the VLS. (Under normal conditions, you should use Command View VLS to power off the system.)
- Determine if the master node is powered on or off.
- Turn on or off the UID LED.
- Check the "Integrated Management Log" to see past node hardware failures.
- Check the hardware health and basic hardware configuration if the VLS is down or you have reason to suspect the reporting is incorrect.
- Check the master node's Serial Number, Product ID, BIOS firmware version, and iLO firmware version.

There are many other useful iLO features; see your iLO user guide for details.

VLS Common Issues

Symptom	Possible causes	Solution
Some of the virtual devices are not detected by the operating system when it scans the SAN for new hardware.	There are more LUNs on the FC host ports than the operating system is configured to see. Once the maximum number of LUNs on a device is detected, the operating system stops looking for more LUNs. In the case of the VLS, the operating system considers each FC host port to be one device. So, if the maximum number of LUNs an operating system is configured to see is eight, the operating system will only see LUN0, LUN1, ..., LUN7 and will not see LUN8, LUN9, ..., and up on each FC host port. By default Windows and HP-UX hosts can see a maximum of 8 LUNs per FC host port.	Increase the maximum number of LUNs per device the operating system is configured to see. To change the maximum LUN per device setting: • For Microsoft Windows—See http://support.microsoft.com/default.aspx?scid=kb%3ben-us%3b310072. • For HP-UX—The value can only be changed for HP-UX versions 11.31 and later. Increase the number of LUNs per bus on the HP-UX server by entering `# scsimgr set_attr -a max_lunid=32`. You can view the connected IO by entering `# ioscan -m lun`. You cannot create legacy DSFs for LUN IDs above 7; use persistent device special files instead. See the HP-UX documentation for more information. • For other operating systems—See the operating system web site.
		Use the VLS's LUN masking feature to restrict the number of virtual devices the host sees on the VLS FC host ports, so it only sees the virtual devices it needs to see. Then, use the VLS's LUN mapping feature to assign LUNs to the

Symptom	Possible causes	Solution
		virtual devices the host can see, such that the virtual device LUN numbers include a LUN0 and no gaps in the LUN numbering. See LUN Masking and LUN Mapping for instructions.
	There is a gap in the LUN numbering on the FC host port. Most operating systems will stop looking for virtual devices on an FC host port once a gap in the LUN numbering is detected. For example, if LUN0, LUN1, and LUN3 are mapped to an FC host port, the operating system will see LUN0 and LUN1. When it does not find a LUN2, it will assume there are no more LUNs on the port and stop looking.	Remove the gap in the LUN numbering by editing the host's LUN mapping (see LUN Mapping), or if a virtual device has been destroyed on the VLS, creating a gap in the LUN numbering, restart the VLS device emulations. The VLS firmware will reassign LUNs to the virtual devices as necessary to remove any gaps in the LUN numbering. See Restarting VLS Device Emulations.
The virtual tape drive devices either disappear or move to a different operating system path name (\\.\Tape0) on a Windows host node - but the Windows Device Manager still shows these virtual tape drive devices as being enabled and at the original BusNumber/TargetID/LUN Location.	There are two levels of logical device binding in the Windows OS. At the first level of logical device binding, the FC HBA binds the FC WWPN and FC LUN (Fibre Channel layer devices) to a SCSI Bus Number, SCSI Target ID, and SCSI LUN (SCSI layer device). At the second level, the Windows Removable Storage Manager (RSM) will bind the SCSI Bus Number, SCSI Target ID, and SCSI LUN (SCSI layer device) to an OS \\.\Tape# path name. Only tape drives are subject to this second binding level. **NOTE:** If you have built and connected Windows nodes before installing the VLS system, the Windows tape device paths can break, change, or disappear when RSM is run. (Windows runs RSM by default.) When RSM initially discovers any removable storage device, such as a tape drive, it will make an entry in NtmsData database. Once a tape drive is listed in this NtmsData database, the Windows OS can potentially either break the second level OS path name bind or re-bind it to a different OS path name, even with RSM in a "Disabled" state.	Delete the Windows NtmsData database and put the RSM into the Disabled state using the following procedure : 1. Disconnect the Windows node from the SAN (label and unplug all FC cables). 2. Delete all files and folders under the "./system32/NtmsData" folder (location of the system32 folder varies between Windows versions). 3. In the Microsoft Computer Management window, enable and start the RSM. 4. Bring up the Removable Storage utility in the Microsoft Computer Management window. 5. Verify there are no Tape or Library devices listed (other than the direct attached devices such as the CD-ROM drive). 6. Stop and Disable the RSM service in the Microsoft Computer Management window. 7. Reconnect the Windows node to the SAN (plug all FC cables back in to the original HBA Ports). 8. Repeat this process on all Windows backup server nodes.
The VLS cartridge barcode numbers displayed on Veritas Netbackup do not match the actual VLS cartridge barcode numbers.	Netbackup has a 6 character barcode limit. Only 6 characters of the actual VLS cartridge barcode numbers will be displayed.	See the Netbackup web site to determine if the six character limit can be changed. If the shortening of the cartridge barcode numbers removes characters from the barcode numbers, making them no longer unique, the barcode numbers cannot be used with Netbackup. You must create new cartridges with no more than six character barcode numbers.
Netbackup on HP-UX cannot build a device file for a VLS library.	Netbackup on HP-UX cannot see virtual devices on a VLS.	Manually create the device file for the virtual library. See the Veritas Netbackup manual.

Symptom	Possible causes	Solution
Netbackup does not display the cartridge barcodes for Autoloader library emulations on the VLS.	Real autoloader libraries do not support barcodes.	This is normal and will not cause problems.
HP Data Protector 5.1 does not display the VLS cartridge barcodes.	By default, the barcode reader support is turned off in Data Protector 5.1.	To turn on barcode reader support in Data Protector: 1. Click **Device & Media**. 2. Right-click the VLS library name and select **Properties**. 3. Click the **Control** tab. 4. Click the **Barcode reader support** box to select it.
VLS performance is being reduced by test unit ready (TURs) from a Windows host with access to the VLS.	The Removable Storage Manager or Removable Storage program on a Windows host is submitting TURs to the VLS.	Stop the Removable Storage Manager or Removable Storage program, and set the startup type to Disabled on the Windows host using the Services utility located under Control Panel > Administrative Tools.
VLS performance is being reduced by frequent tape drive polling.	Windows Removable Storage Manager service (RSM) polls tape drives on a frequent basis—every three seconds in Microsoft Windows 2000, and every second in Windows Server 2003. Windows' built-in backup software (NTBACKUP) relies on the RSM polling to detect media changes in the tape drive. In SAN configurations, this RSM polling can have a significant negative impact on tape drive performance. For SAN configurations, HP strongly recommends disabling RSM polling.	Refer to the Microsoft website at: http://support.microsoft.com/default.aspx?scid=kb;en-us;842411 or complete the following steps to disable RSM polling: 1. Install the 1.0.4.0 or later driver. 2. Disable device polling in the system registry. • Establish a CLI session. • Log into the system as **`Administrator`**. • Run **`RegEdit`** and navigate to the following registry: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\[p... • To disable RSM polling, edit the `AutoRun` value found in this key. A value of `0` (zero) indicates that polling is disabled; a value of `1` indicates that polling is enabled. 3. After completing steps 1 and 2, reboot the affected system. 4. Repeat this procedure for every server visible to tape drives. **IMPORTANT:** Adding or removing tape drives may cause an older driver .inf file to be reread, which can re-enable RSM polling. If tape drives are added or removed, check the registry for proper configuration. If necessary, repeat step 2 and 3 above. To disable polling in the HP SDLT driver (v3.0.2.0 or later): 1. Open the Device Manager on the server connected to the tape drive. 2. Double-click an SDLT tape drive. 3. Click the DLT tab.

Symptom	Possible causes	Solution
		4. Check `Increase performance by disabling support for Microsoft Backup Utility.` 5. Repeat this procedure for each server visible to each SDLT tape drive.
At reboot, there are spurious critical FC port failures reported as notification alerts, usually on every port. Later, Info notification alerts for each FC host port are generated, indicating the FC ports are operating normally.	This is expected behavior and does not indicate a problem.	None
The Identity tab of Command View VLS reports Total Usable Capacity of 0 GB, even though there are working disk arrays available to the VLS system.	Whenever the VLS detects more arrays than there are correctly installed licenses, the VLS system will disable ALL array storage and report 0 GB of Total Usable Capacity.	In Command View VLS, go to the License Summary screen (**System** > **Chassis** (on the navigation tree) > **Licensing**. The screen lists all of the licenses currently on the system. The summary at the top indicates the number of LTUs on the system and how many are licensed. Install additional licenses as needed.
After replacing drive 0 in a node, the system will not boot.	A blank drive was installed in drive bay 0.	If a blank drive is installed in drive bay 0, the system will not boot. To remedy this, switch the drive located in bay 0 with the drive located in bay 1.
When oversubscription is enabled and you create enough cartridges in a storage pool to put your free storage capacity below the threshold, the pool may reach critical status. If you then disable oversubscription, your storage pool will remain in critical status and will not return to good status—even after reboot.	When you disable oversubscription, the system does not monitor the storage pool's capacity, even to check that it is no longer at a critical level. The status will not change.	Re-enable oversubscription, set the alert threshold so that the storage pool is within the capacity threshold, then wait for the pool to return to good (green) status. Disable oversubscription and the storage pool will maintain good status.

Automigration and Replication Issues

Although automigration is configured and managed through the Automigration/Replication tab on Command View VLS, errors and events are reported through the usual notification alerts. See Notification Alerts.

IMPORTANT: If a destination library is directly connected to the VLS (`LOOP` mode), and you disconnect the destination library to change its connection to be via a SAN (`FABRIC` mode), you will need to reboot the VLS in order for this change to work. If you do not reboot, the destination library will be marked as `FAILED` after you disconnect and reconnect it.

NOTE: The "mirror_broken" state can occur when there is not enough room on the virtual tape to create the copy, there are no available slots to create the copy, the library cannot read the header of the physical tape, the library cannot determine that a tape without a header is blank, or the library cannot successfully write the header to the virtual tape.

For more help with automigration and replication issues:

- "Monitoring Destination Library Status" (page 65)
- "Replacing a Library" (page 73)

Deduplication Issues

Symptom	Possible causes	Solution
The VLS is not deduplicating the backup jobs.	The VLS does not free up storage on a cartridge until: • At least two full backups of the same policy exist on different cartridges • The delta-differencer has processed all of the backup sets on the cartridge • The cartridge is physically full	Consider using cartridges that are smaller than the sum of your daily backup jobs so the cartridges deduplicate sooner.
The deduplication compression ratio is low.	The compression ratio depends on the amount of data changed between the backup sets. In addition, not all data is deduplicated. For example, files less than 32 KB in size and backup sets less than 1 MB are ignored. If your data sets do not change significantly between backups, or if they contain many small files, the compression ratio may be low. This is expected behavior and does not indicate a problem.	None
The deduplication compression ratio was fine, but suddenly went down significantly.	After 50 versions of a backup set have been deduplicated, the VLS automatically restarts the deduplication process as though starting from scratch. As a result, the compression ratio will drop.	In time, the ratio will improve as more backup sets are deduplicated.
The restore performance is degrading.	The restore performance will continue to degrade as you restore older and older versions of a backup.	After 50 versions of a backup set have been deduplicated, the VLS automatically restarts the deduplication process as though from scratch. The restore performance will then improve because the restore versions are more recent.

B Specifications

This section provides the basic VLS node, Fibre Channel switch, Ethernet switch, and disk array enclosures specifications.

For a complete list of specifications, see the HP QuickSpecs for each product.

VLS9000Node

Item	Specification
Height	4.3 cm (1.70 in)
Depth	69.2 cm (27.3 in)
Width	42.6 cm (16.8 in)
Weight (fully loaded	17.9 kg (39.5 lb)
Weight (no drives installed)	14.1 kg (31.0 lb)
Rated input voltage	100 VAC to 240 VAC
Rated input frequency	50 Hz to 60 Hz
Rated input current	7.1 A (120 VAC); 3.5 A (240 VAC)
Rated input power	852 W
BTUs per hour	2910 (120 VAC); 2870 (240 VAC)
Rated steady-state power	700 W
SATA hard drive	60 GB capacity 7,200 rpm rotational speed
Power supply	700 W
DVD-CD drive	8x/24x IDE
Memory	4 x 1024 MB DDR2 SRAM ECC
Processor	2 xPentium® quad-core Xeon™ processor (2.0 GHz)

VLS9200 Node

Item	Specification
Physical	
Dimensions (HxWxD)	4.32 x 42.62 x 69.22 cm (1.70 x 16.78 x 27.25 in)
Weight (maximum: two processors, two power supplies, eight hard drives)	15.97 kg (35.20 lb)
Weight (minimum: one processor, one power supply, no hard drives)	14.51 kg (32.00 lb)
Weight (no drives installed)	14.06 kg (31.00 lb)
Power Consumption	250 W
Processor and memory	
Number of processors	2
Processors supported	Intel® Xeon® 5600 series

Item	Specification
Cache	12 GB L3
Memory type	DDR3 RDIMM
Standard memory	DDR3
Maximum memory	Up to 192 GB
Memory slots	18 DIMM
Storage	
Storage type	Hot-plug SFF SATA
Maximum internal storage	4 TB
Maximum internal drive bays	8
Expansion slots	2 PCIe x8 Gen 2 mezzanine
Storage controller	Smart Array P410i Controller

VLS9200 High Performance Node

Specification	Value
Physical	
Dimensions (HxWxD)	8.59 x 44.55 x 69.22 cm (3.38 x 17.54 x 27.25 in)
Weight (maximum: all hard drives, power supply, and processor installed)	27.27 kg (60.00 lb)
Weight (minimum: one hard drive, power supply, and processor installed)	21.45 kg (47.18 lb)
Processor and memory	
Number of processors	2
Processors supported	Intel® Xeon® 5600 series
Cache	8 MB L3
Memory type	DDR3 RDIMM
Standard memory	DDR3
Maximum memory	192 GB
Memory slots	18 DIMM
Storage	
Maximum internal storage	4 TB
Maximum internal drive bays	8
Expansion slots	6 PCIe x8 Gen 2 mezzanine
Storage controller	Smart Array P410i Controller

VLS9000 Disk Array Enclosure

Item	Specification
Dimensions	59.7 x 44.7 x 8.8 cm (23.5 x 17.6 x 3.5 in)
Weight	• Controller enclosure (with drives): 33.6 kg (74 lb) • Expansion enclosure (with drives): 31.3 kg (69 lb)
Input frequency	50/60 Hz
Input voltage	208 to 264 VAC

Input current requirement	• Controller enclosure:
	  ◦ Spin up: 2.7 A at 220 V, 60 Hz
	  ◦ Operating: 1.7 A at 220 V, 60 Hz
	• Expansion enclosure:
	  ◦ Spin up: 2.2 A at 220 V, 60 Hz
	  ◦ Operating: 1.2 A at 220 V, 60 Hz

Steady-state maximum input power	• Controller enclosure: 377 W (operating) • Expansion enclosure: 271 W (operating)
Heat dissipation	• Controller enclosure: 1286 BTU (operating) • Expansion enclosure: 925 BTU (operating)

VLS9200 Disk Array Enclosure

Item	Specification
Processor	Intel®Xeon® Processor E5640 (2.66 GHz, 12MB L3 Cache, 80 Watts, DDR3-1066, HT Turbo 1/1/2/2)
Cache Memory	12MB (1 x 12MB) Level 3 cache
Chipset	Intel® 5520 Chipset
Network Controller	Two HP NC382i Dual Port Multifunction Gigabit Server Adapters (four ports total) with TCP/IP Offload Engine, including support for Accelerated iSCSI
Server Power Cords	All Standard Model (BTO) servers ship with a high voltage server to PDU power cord. Localized cables may be included with geographic specific models in other world regions.
System Fans	4 fan modules, fan redundancy standard with all modules

Fibre Channel Switch 4/10q

Item	Specification
Fibre Channel ports	20 universal device ports, 4 stacking (ISL) ports (10 Gbps Fibre Channel, upgradeable to 20 Gbps)
Performance	• 8 Gbps line speed, full duplex • 10 Gbps and 20 Gbps stacking (ISL) port line speed, full duplex
Switch core	Non-blocking
Fabric latency	<0.2µ sec., cut-through routing
Maximum frame size	2148 bytes (2112 byte payload)
Classes of service	Class 2, Class 3, Class F (inter-switch frames) connectionless Fibre Channel protocol support
Port types	• 8 Gbps: FL_Port, F_Port, and E_Port; G_Port, GL_port (auto-configuring), Transparent Router (TR) • 10/20 Gbps: E_Port and F_Port; G_Port (auto-configuring)
Data traffic types	Fabric switches support unicast and broadcast
Media types	8 Gbps Small Form-Factor Pluggable Plus (SFP+) optical transceivers
Laser	Distance using short-wave 8 Gbps optical transceivers at 2 Gbps, 4 Gbps, and 8 Gbps connection speed: • 8 Gbps: OM3 fiber: 150 m, OM2 fiber: 50 m • 4 Gbps: OM3 fiber: 270 m, OM2 fiber: 150 m • 2 Gbps: OM3 fiber: 500 m, OM2 fiber: 300 m Distance using short-wave 4 Gbps optical transceivers at 2 Gbps and 4 Gbps connection speed: • 4 Gbps: OM3 fiber: 270 m, OM2 fiber: 150 m • 2 Gbps: OM3 fiber: 500 m, OM2 fiber: 300 m
Fabric services	• Simple name server • Hardware based zoning • Registered State Change Notification (RSCN) • I/O StreamGuard™ • Multi-chassis in-order delivery • Automatic path selection • FDMI support
Management access	10/100 Ethernet Base T (RJ-45), serial port (RS-232 with DB9), in-band (Fibre Channel)
Diagnostics	Power-on self test POST
Front-to-back airflow	RoHS compliant
Dimensions	
Height	1U, 1.7 in (4.32 cm)
Depth	18.75 in (47.6 cm)
Width	17 in (43.2 cm)
Weight	18 lb (8.16 kg)
Environmental	

Item	Specification
Temperature	• Operating: 41° to 104° F (5° to 40° C) • Non-operating: 4° to 158° F (20° to 70° C)
Humidity	• Operating: 10% to 90% non-condensing • Non-operating: 10% to 95% , non condensing
Altitude	• Operating: 0 to 10,000 ft. • Non-operating: 0 to 50,000 ft.
Shock	• Operating: 4 G, 11 ms, 20 repetitions • Non-operating: 30 G, 13 ms, trapezoidal
Vibration	• Operating: 5-500 Hz, random, 0.2 G • Non-operating: 2-200 Hz, random, 0.5 G
Power consumption	
Supported power range	100 to 240 VAC (operational)
Frequency	50 to 60 Hz
Heat output	80 watts nominal; 90 watts typical maximum

Fibre Channel Switch 4/16q

Item	Specification
Dimensions	17 x 20 x 1.70 in. (43.2 x 50.8 x 4.32 cm) 1U height
Weight	15 lbs. (6.80 kg) fully loaded
Ports per chassis	16 Fibre Channel 4 GB / 2 GB / 1 GB ports (upgradeable in 4-port increments, full-duplex, auto-negotiating for compatibility with existing 2Gb and 1Gb devices), 4 Fibre Channel 10 GB XPAK MSA-compliant ports (full-duplex), 1 Ethernet 10/100 BaseT with RJ45 port
Multi switch fabrics	• Supports all topologies, including: stack, cascade, cascaded loop, and mesh with E_Port • Supports multiple links between switches • In-order delivery of frames in all Multi-switch and multi-link configurations • Adaptive Trunking and Intelligent Path Selection on all 10Gb ports
Fabric port types	All ports can assume the following states: • F_port: Fabric • FL_port: Fabric loop (public loop) • E_port: Switch-to-switch • Ports are auto-discovering, self-configuring

Item	Specification
Media type	• Hot-pluggable, industry-standard SFPs (Small Form Pluggable) for 4Gb ports • Hot-pluggable, industry-standard XPAK optics or copper stacking cables for 10Gb ports
Supported SFP types	• Shortwave (optical) • Longwave (optical)
Media transmission ranges (@ 2 GB speeds)	Optical • Shortwave: 500 m (1,640 ft.) • Longwave: 10 km (6.2 mi.)
Cable types	50/62.5 micron multimode fiber optic 9 micron single-mode fiber optic
Fabric latency	• Less than 0.4 µs (best case, no contention) • Cut-through routing
Fabric point-to-point bandwidth	• 848MB/s Full-Duplex on 4 GB ports • 2400+ MB/s Full-Duplex on 10 GB ports
Fabric aggregate bandwidth	• Single chassis: Up to 144 Gbps (full-duplex) end-to-end • Non-blocking architecture
Maximum frame sizes	2148 bytes (2112 byte payload)
Per-port buffering	• ASIC-embedded memory (non-shared) • Each port has a guaranteed 16-credit zero wait state buffer for full performance up to 10km @ 2 GB and 2.5km @ 10 GB
Management processor	Pentium class
Management methods	SNMP, Telnet, GS-3

Item	Specification
Access methods	• In-band • Ethernet 10/100 BaseT with RJ45 • RS-232 serial port with DB9
Diagnostics	• Power-up self-test of all functionality except media modules • Field-selectable full self-test including media modules

Fabric services	• Simple name server
	• Fabric zoning
	  ◦ Hardware-based - Access Control List (port)
	  ◦ Name Server (WWN)
	  ◦ Orphan Zoning
	  ◦ All zoning assigned on per-node basis, even across Multi-stage fabrics
	• Registered State Change Notification (RSCN)
	• I/O StreamGuard™
	• Multi-chassis in-order delivery
	• Automatic path selection in Multi-stage configurations
	• FDMI device support

Voltage	100/240 VAC
Current	1.0 A at 100-120 VAC; 0.5 A at 200-240 VAC
Power	100W maximum (with full-optics configuration)
Frequency	50/60 Hz

Ethernet Switch 2510–24 Specifications

Item	Specification
Dimensions	9.3 x 17.42 x 1.73 in. (23.62 x 44.25 x 4.39 cm) 1U height
Weight	4.9 lb (2.2 kg) fully loaded
Ports	24 RJ-45 10/100 ports (IEEE 802.3 Type 10Base-T, IEEE 802.3u Type 100Base-TX); 1 RJ—45 serial console port; 2 dual-personality ports, each of which can be used as either an RJ-45 10/100/1000 port or an open mini-GBIC slot (for use with mini-GBIC transceivers)
Processor	MIPS, 264 MHz
Flash capacity	8 MB
RAM/ROM capacity	64 MB
Packet buffer size	384 KB
Latency (100 Mb)	< 4.9 µs (64-byte packets)
Latency (1000 Mb)	< 2.6 µs (64-byte packets)
Throughput	6.5 million pps (64-byte packets)
Switching capacity	8.8 Gbps
MAC address table size	8000 entries

Item	Specification
Maximum heat dissipation	68 BTU/hr
Voltage	100-127 VAC/200-240 VAC
Current	0.75 A /0.4 A
Power	20 W
Frequency	50/60 Hz

Ethernet Switch 2810–24G

Item	Specification
Dimensions	12.7 x 17.4 x 1.7 in. (32.26 x 44.2 x 4.32 cm) 1U height
Weight	7.21 lb (3.27 kg) fully loaded
Ports	20 auto-sensing 10/100/1000 ports (IEEE 802.3 Type 10Base-T, IEEE 802.3u Type 100Base-TX, IEEE 802.3ab Type 1000Base-T); 1 RJ–45 serial console port; 4 dual-personality ports, each of which can be used as either an RJ-45 10/100/1000 port or an open mini-GBIC slot (for use with mini-GBIC transceivers)
Processor	MIPS, 264 MHz
Flash capacity	16 MB
SDRAM	64 MB
Packet buffer size	0.75 MB
Latency	< 5.6 μs (FIFO 64-byte packets)
Throughput	up to 35.7 million pps (64-byte packets)
Switching capacity	48 Gbps
MAC address table size	8000 entries
Maximum heat dissipation	164 BTU/hr
Voltage	100-127 VAC/200-240 VAC
Current	1.25 A /0.75 A
Power	60 W
Frequency	50/60 Hz

Ethernet Switch 6600–24G

Item	Specification
Dimensions	21.5 x 17.4 x 1.7 in. (54.61 x 44.2 x 4.32 cm) 1U height
Weight	17.2 lb (7.8 kg) fully loaded
Ports	20 auto-sensing 10/100/1000 ports (IEEE 802.3 Type 10Base-T, IEEE 802.3u Type 100Base-TX, IEEE 802.3ab Type 1000Base-T); 1 RJ–45 serial console port; 4 dual-personality ports, each of which can be used as either an RJ-45 10/100/1000 port or an open mini-GBIC slot (for use with mini-GBIC transceivers)
Memory and Processor	Freescale PowerPC 8540 @ 666 MHz, 4 MB flash, 256 MB compact flash, 256 MB DDR SDRAM; packet buffer size: 36 MB QDR SDRAM total (18 MB for 1 GbE/10-GbE ports)

Item	Specification
1000 Mb Latency	< 3.4 µs (FIFO 64-byte packets)
10 Gbps Latency	< 2.4 µs (FIFO 64-byte packets)
Throughput	up to 75.7 million pps (64-byte packets)
Routing/Switching capacity	101.8 Gbps
Switch fabric speed	105.6 Gbps
Routing table size	10000 entries
MAC address table size	64000 entries
Maximum heat dissipation	697 BTU/hr (735.33 kJ/hr)
Voltage	100-120/200-240 VAC
Idle power	167.6 W
Maximum power rating	204.3 W
Frequency	50/60 Hz

Environmental

	Operating	Non-operating	Shipping
Temperature [1]	10°C to 35°C (50°F to 95°F)	-40°C to 66°C (-40°F to 150°F)	-40°C to 66°C (-40°F to 150°F)
Relative humidity (noncondensing) [2]	40% to 60%	10% to 95%	5% to 95%
Altitude	-1000 ft to 10,000 ft	-1000 ft to 10,000 ft	-1000 ft to 40,000 ft
Vibration	5-1000-5 Hz, 0.25 g, sinusoidal, 1 Octave/min., 3-axis	5-1000-5 Hz, 1.0 g, sinusoidal, 1 Octave/min., 3-axis	5-1000-5 Hz, 2.0 g, sinusoidal, 1 Octave/min., 3-axis
Shock	5 g, every 11 ms, 1/2 sine pulse, 3 axis	25 g, every 11 ms, 1/2 sine pulse, 3 axis	30 g, every 11 ms, 1/2 sine pulse, 3 axis

[1] All temperature ratings shown are for sea level. An altitude derating of 1°C per 300 m (1.8°F per 1,000 ft) to 3048 m (10,000 ft) is applicable. No direct sunlight allowed.

[2] Storage maximum humidity of 95% is based on a maximum temperature of 45°C (113°F). Altitude maximum for storage corresponds to a pressure minimum of 70 KPa.

C Regulatory Information

For the purpose of regulatory compliance certifications and identification, this product has been assigned a unique regulatory model number. The regulatory model number can be found on the product nameplate label, along with all required approval markings and information. When requesting compliance information for this product, always refer to this regulatory model number. The regulatory model number is not the marketing name or model number of the product.

Product specific information:

HP VLS9000 Virtual Library System.

Regulatory model number: FCLSE0701

FCC and CISPR classification: Class A

For important safety, environmental, and regulatory information, see *Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products*, available at http://www.hp.com/support/Safety-Compliance-EnterpriseProducts.

These products contain laser components. See the Class 1 laser statement in the document listed above.

Turkey RoHS material content declaration

Türkiye Cumhuriyeti: EEE Yönetmeliğine Uygundur

Ukraine RoHS material content declaration

Обладнання відповідає вимогам Технічного регламенту щодо обмеження використання деяких небезпечних речовин в електричному та електронному обладнанні, затвердженого постановою Кабінету Міністрів України від 3 грудня 2008 № 1057

Warranty information

HP ProLiant and X86 Servers and Options

http://www.hp.com/support/ProLiantServers-Warranties

HP Enterprise Servers

http://www.hp.com/support/EnterpriseServers-Warranties

HP Storage Products

http://www.hp.com/support/Storage-Warranties

HP Networking Products

http://www.hp.com/support/Networking-Warranties

Glossary

This glossary defines terms used in this guide or related to this product and is not a comprehensive glossary of computer terms.

A

Accelerated deduplication A method of deduplication that uses object-level differencing technology. *See also* deduplication..

appliance An intelligent device programmed to perform a single well-defined function.

Appliances differ from general-purpose computers in that their software is normally customized for the function they perform, pre-loaded by a vendor, and not alterable by the user.

array A synonym of storage array, storage system, and virtual array. A group of disks in one or more disk enclosures combined with controller software that presents disk storage capacity as one or more virtual disks.

automigration The process in which the virtual tape library acts as a tape copy engine that transfers data from virtual cartridges on disk to a physical tape library connected to the virtual tape device.

B

backup application An application used to create, manage, and monitor backups.

bandwidth Also known as data transfer rate. The amount of data that can be carried from one point to another in a given time period.

A real communications path usually consists of a succession of links, each with its own bandwidth. If one of these is much slower than the rest, it is said to be a bandwidth bottleneck.

C

cartridge 1) A removable storage module that contains magnetic or optical disks, magnetic tape, or memory chips.

(2) Software emulation of the behavior and contents of a physical tape cartridge on alternate media, such as disk, is called a virtual tape or virtual media.

See also virtual tape..

chassis A metal box that houses computer hardware.

CLI Command-line interface. An interface comprised of various commands which are used to control operating system responses.

D

data backup The activity of copying files or databases so that they will be preserved in case of equipment failure or other catastrophe. The retrieval of files you backed up is called restoring files.

data compression A software or hardware process that shrinks data files so that they occupy less storage space, and can be transmitted faster and easier. Data is encoded so it takes up less storage space and less bandwidth for transmission.

data migration The process of moving data from one storage device to another, such as migrating data from virtual media to physical media.

data restore To recover data files stored on virtual or physical media.

data retention period The length of time data is retained (stored) on virtual or physical media.

data striping The storing of sequential blocks of incoming data on all the different disk drives in a virtual disk. This method of writing data increases virtual disk throughput because multiple disks are working simultaneously, retrieving and storing data. RAID 0, 3, 5, 6, 10, and 50 use striping.

deduplication The process of eliminating duplicate data from the backups on a virtual cartridge to reduce the amount of disk space required.

disk array Two or more hard drives combined as a single logical unit for increased capacity, speed, and fault-tolerant operation. Disk arrays are logically grouped into a storage pool.

disk mirroring Also known as *data mirroring*.

disk striping The process of dividing a body of data into blocks and spreading the data blocks across several partitions on several disks.

disk-to-disk backup The backing up data on disks rather than on tape. Disk-to-disk backup systems provide a very fast single file restore capability compared with disk-to-tape backup.

disk-to-disk-to-tape backup

The process of archiving in which data is initially copied to backup storage on a disk-based storage system, such as a VLS, and then periodically copied again to a tape storage system.

dual port virtual devices Virtual devices (for example, the two host or device ports on each FC card in the node) with connectivity to two ports so that the device can be connected to more than one input or output.

dynamic disk filesystem A finely-tuned filesystem developed to handle large block I/O typical of a streaming backup and restore environment. This filesystem is optimized for sequential access and very large file sizes.

E

echo copy A software feature within automigration that automatically synchronizes the physical cartridges to matching virtual cartridges (with the same barcodes) based on user-defined policies, and is totally transparent to the backup application. (Echo copy is similar to mirror copy.)

extent The minimum amount of disk space allocated for writing by the VLS dynamic disk filesystem. A smaller extent reduces wasted disk space, but decreases restore performance. The VLS extent size is 32MB.
See also data restore..

F

failover protection A backup operational mode in which the functions of a system component (such as a hard drive or power supply) are assumed by secondary system components when the primary component becomes unavailable through either failure or scheduled down time.

fault tolerance The capacity to cope with internal hardware problems without interrupting the system's data availability, often by using backup systems brought online when a failure is detected. Many systems provide fault tolerance by using RAID architecture to give protection against loss of data when a single disk drive fails. Using RAID 1, 3, 5, 6, 10, or 50 techniques, the RAID controller can reconstruct data from a failed disk drive and write it to a spare or replacement disk drive.

Fibre Channel A data transfer architecture designed for mass storage devices and other peripheral devices that require high bandwidth.

file A VLS file is a virtual cartridge.

Firesafe The holding area for virtual media that is not assigned to a virtual library. Data cannot be restored from virtual media located in the Firesafe until the media is moved into a library.

H

hot plug The ability to add and remove devices to an appliance while the appliance is running and have the operating system automatically recognize the change.

I

iLO Integrated Lights-Out.

infrastructure The physical hardware used to interconnect computers. Infrastructure also includes the software used to send, receive, and manage the signals that are transmitted.

initiator A media (host) server that runs the backup/restore application that passes commands and data between the network and the VLS.

inputs/outputs per second A performance measurement for a host-attached storage device or RAID controller.

L

library A storage device that handles multiple units of media and provides one or more drives for reading and writing them, such as a physical tape library and virtual tape library. Software emulation of a physical tape library is called a virtual tape library.
See also virtual tape library..

logical unit number (LUN) An address used in the SCSI protocol to access a device within a target. In the case of the VLS, a LUN is assigned to each virtual library and tape drive.

LUN mapping A mechanism of changing the LUN assignments for a specific host.

LUN masking An authorization process that makes a LUN available to some hosts and unavailable to other hosts.

M

mean time until data loss (MTDL) The average time until a component failure can be expected to cause data loss. This includes the consideration that RAID redundancy can protect against data loss from the failure of a single component.

media access control (MAC) address A low-level unique hardware identifier for every Ethernet port in the world that is physically stored inside a network card or similar network interface. MAC addresses are assigned by the IEEE.

media server A computer whose purpose is to move or copy data from one location to another, such as from network clients to tape cartridges in a library.

metadata The data in the first sectors of a disk drive that the system uses to identify virtual disk members.

mirroring The act of creating an exact copy or image of data.

N

node A server that contains the hardware and firmware required to run a virtual library system. This refers to a hardware assembly containing a power supply, cooling fans, motherboard, expansion boards, and internal hard drives to support the VLS system.

O

oversubscription A condition that exists when more virtual media storage is configured on a VLS than there is physical storage available.

Because the VLS dynamically allocates storage space as user data is written, the VLS allows you to allocate more storage for virtual media than is physically available.

P

port mapping A mechanism of assigning a LUN (virtual device), such as a virtual library or tape drive, to a specific FC host port. Port mapping allows you to load-balance the LUNs among the FC host ports to maximize bandwidth.

At this time, you must manually load-balance the virtual tape drives in a VLS.

primary node A computer (node) that provides primary administrating and control for backup and restore operations on a server cluster and provides communication and control for all secondary servers on the system.

R

RAID A RAID volume consists of more than one drive, but appears to the operating system to be a single logical disk. RAID improves performance by disk striping, which involves partitioning each drive's storage space into units. By placing data on multiple disks, I/O operations can overlap in a balanced way, improving performance.

RAID1-level data storage A RAID that consists of at least two drives that use mirroring (100 percent duplication of the storage of data). There is no striping. Read performance is improved since either disk can be read at the same time. Write performance is the same as for single disk storage.

RAID5-level data storage A RAID that provides data striping at the byte level and also stripe error correction information. RAID5 configurations can tolerate one drive failure. Even with a failed drive, the data in a RAID5 volume can still be accessed normally.

RAID6-level data storage A RAID that provides data striping at the byte level and also stripe error correction information. RAID6 configurations can tolerate two drive failures. Even with two failed drives, the data in a RAID6 volume can still be accessed normally. RAID6 read performance is similar to RAID5, since all drives can service read operations, but the write performance is lower than that of RAID5 because the parity data must be updated on multiple drives.

redundancy In a redundant system, if you lose part of the system, it can continue to operate. For example, if you have two power supplies with one that takes over if the other one dies, that's redundancy.

replication The process of writing data to virtual tape, and after the backups are complete, writing the data to another virtual tape, known as the replication target, over the LAN/WAN. Similar to automigration.

S

SAN Storage area network. A network of storage devices available to one or more servers.

SATA Serial Advanced Technology Attachment.

SCSI Small Computer Systems Interface. A standard, intelligent parallel interface for attaching peripheral devices to computers, based on a device-independent protocol.

secondary node A computer (node) that provides secondary administrating and control for backup and restore operations on a server cluster, and provides additional storage and multi-pathing capabilities on the system.

SMI-S Allows control of the virtual tape library by a connected destination library for the purpose of implementing automigration. SMI-S support allows applications attached to the VLS to detect the virtual library configuration and to allow some users to change the state of the VLS.

SNMP Simple Network Management Protocol. A widely used network monitoring and control protocol. Data is passed from SNMP agents, which are hardware and/or software processes reporting activity in each network device (hub, router, bridge, and so on) to the workstation console used to oversee the network. The agents return information contained in a MIB (Management Information Base), which is a data structure that defines what is obtainable from the device and what can be controlled (turned off, on, and so on).

SSL certificate Secure Sockets Layer certificate. A protocol designed to enable applications to transmit information back and forth securely. Applications that use this protocol inherently know how to give and receive encryption keys with other applications, as well as how to encrypt and decrypt data sent between the two.

Some applications that are configured to run SSL include web browsers like Internet Explorer and Netscape, mail programs like GroupWise, Outlook, and Outlook Express, FTP (file transfer protocol) programs, etc. These programs are automatically able to receive SSL connections.

To send an SSL connection, however, or to open a secure connection, your application must first have an encryption key assigned to it by a Certification Authority. Once it has a unique key of its own, you can establish a secure connection with every other application that can "speak" the SSL protocol.

storage pool Multiple disk arrays logically grouped together from which the dynamic disk filesystem allocates storage. The disk arrays in a VLS are automatically configured into one storage array.

T

tape drive (1) A device that reads data from and writes data onto tape.

(2) A software emulation of a tape drive is called a virtual tape drive.

V

virtual tape A disk drive buffer that emulates one physical tape to the host system and appears to the host backup application as a physical tape. The same application used to back up to tape is used, but the data is stored on disk. Also known as a *piece of virtual media* or a *VLS cartridge*.

Data can be written to and read from the virtual tape, and the virtual tape can be migrated to physical tape.

virtual tape drive An emulation of a physical transport in a virtual tape library that looks like a physical tape transport to the host backup application. The data written to the virtual tape drive is really being written to disk.
See also virtual tape library..

virtual tape library A disk drive buffer containing virtual tape and virtual tape drives.
See also virtual tape drive..

W

WWNN World wide node name. A globally unique 64-bit identifier assigned to each Fibre Channel node.

WWNN World wide node name. A globally unique 64-bit identifier assigned to each Fibre Channel node process.

WWPN World wide port name. A unique 64-bit address used in a FC storage network to identify each device in a FC network.

Index

D

E

F

G

H

I

L

M

N

O

T