Security Analytics

High-Density Storage Configuration Guide for Dell Hardware

Document Version: 1.3

15 Mar 2019

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE. SYMANTEC CORPORATION PRODUCTS, TECHNICAL SERVICES, AND ANY OTHER TECHNICAL DATA REFERENCED IN THIS DOCUMENT ARE SUBJECT TO U.S. EXPORT CONTROL AND SANCTIONS LAWS, REGULATIONS AND REQUIREMENTS, AND MAY BE SUBJECT TO EXPORT OR IMPORT REGULATIONS IN OTHER COUNTRIES. YOU AGREE TO COMPLY STRICTLY WITH THESE LAWS, REGULATIONS AND REQUIREMENTS, AND ACKNOWLEDGE THAT YOU HAVE THE RESPONSIBILITY TO OBTAIN ANY LICENSES, PERMITS OR OTHER APPROVALS THAT MAY BE REQUIRED IN ORDER TO EXPORT, RE-EXPORT, TRANSFER IN COUNTRY OR IMPORT AFTER DELIVERY TO YOU.

Americas:
Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

Rest of the World:
Symantec Limited
Ballycoolin Business Park
Blanchardstown, Dublin 15, Ireland

About This Document

This document contains instructions to connect a "head unit" (Security Analytics 10G-HD Forensic Appliance or Security Analytics SA-S500-30-FA Forensic Appliance) to 1–3 "storage arrays" (Dell® PowerVault® MD3860f High-Speed Fibre Channel Storage or NetApp® E5660 Storage Array with 4TB drives), connected either directly or through redundant Fibre Channel switches.

To configure NetApp E5660 storage arrays with 6TB drives using Security Analytics 7.2.3 or later, consult the Security Analytics Configuration Guide for E5660 300T Intelligent Storage Arrays (DOC10304 on support.symantec.com).

Consult the approved bills of material (BOMs) for the head units and storage arrays on the Security Analytics documentation page under Compatibility Lists. The quick-start guides for each hardware unit are under Getting Started Guides.

For assistance with the installation of this software:

- Symantec Support: support.symantec.com/en_US/contact-support.html
- Security Analytics Documentation: support.symantec.com/content/unifiedweb/en_US/Documentation.1145515.html

Table of Contents

1. Requirements 4
   1.1. Terminology 6
   1.2. Head Unit I/O Configuration 6
   1.3. Storage Array I/O Configuration 7
2. Supported Configurations 9
   2.1. Point-to-Point Connections 9
   2.2. Fibre Channel Switch Fabric 9
3. Prepare the Devices 11
   3.1. Set Up the Workstation 11
   3.2. Set Up the Storage Array 11
   3.3. Set Up the Head Unit 12
   3.4. Choose a Management Topology 13
   3.5. Set the IP Addresses 14
   3.6. Obtain the Host Port Identifiers for the Head Unit 18
4. Power Down the Devices 19
5. Establish Fibre Channel Connectivity 19
   5.1. With Point-to-Point Connections 19
   5.2. Through Fibre Channel Switches 19
6. Power On the Devices 20
7. Discover the Storage Arrays 21
   7.1. Add the Arrays 21
   7.2. Verify the Condition of the Physical Disks 23
   7.3. Enable Disk Encryption on the Enclosure 23
   7.4. Configure the Indexing Disk Groups 25
   7.5. Configure the Capture Drives 28
   7.6. Configure the Hot Spares 30
8. Map the Head Unit to the Storage Array .. 31
9. Verify Multipath Configuration 34
10. Reinstall Security Analytics Software 36
11. Next Steps 37

Appendix A: Disk-Group Configuration 38

Appendix B: Initial Head-Unit Configuration 39
- B.1. Establish a Connection to the Head Unit 39
- B.2. Configure the BIOS Settings 39
- B.3. Optional—Configure the iDRAC Interface 40
- B.4. Enable Disk Encryption on the Head Unit 41
- B.5. Configure the RAID Array 43

Appendix C: Troubleshooting Tools 46

Appendix D: Switch-Port Sizing 49

Appendix E: Supported Hardware Configurations 50
- E.1. One Head Unit, One Array 52
- E.2. One Head Unit, Two Arrays 54
- E.3. One Head Unit, Three Arrays 58
- E.4. Two Head Units, One Array Each 60
- E.5. Two Head Units, Two Arrays Each 62
- E.6. Two Head Units, Three Arrays Each 65
- E.7. Three Head Units, One Array Each 67
- E.8. Three Head Units, Two Arrays Each 69
- E.9. Three Head Units, Three Arrays Each 72

Changes to This Document

Version	Date	Change	Pages
1.3	15 Mar 2019	Update documentation links	
1.2	5 Feb 2018	Add SA-S500-30-FA hardware as a head unit	

1. Requirements

This installation requires the following:

- Security Analytics 10G-HD Forensic Appliance
  - Security Analytics SA-S500-30-FA Forensic Appliance
  - Dell PowerEdge R630 Rack Server with the configuration specified in the 10G-HD bill of materials (BOM) (DOC10076 on support.symantec.com):
    - Eight SED (2.5-inch) disk drive bays and 3 PCIe slots
    - Two Emulex LPe16002B Dual Port 16 Gb Fibre Channel Low Profile HBAs, including Short Wave Optical – LC SFP+ optics

IMPORTANT Ports for 16 Gb Fibre Channel connections require SFP+ transceivers that are designed for this data rate. SFP+ transceivers that support other data rates are incompatible.

- Symantec 240T Storage Array (no more than three per head unit):
  - NetApp E5660 Storage Array
  - Dell PowerVault MD3860f
- Modular Disk Storage Manager (MDSM) utility, included with the MD3860f

Note This document provides instructions to configure Dell MD3860f storage arrays, using MDSM. To configure NetApp E5660 storage arrays, consult the Security Analytics Configuration Guide for E5660 300T Intelligent Storage Arrays (DOC10304 on support.symantec.com).

- Optional—Fibre Channel switches: Brocade° 6505 (24 ports), Brocade 6510 (48 ports), or equivalent (must support WWN zoning):
  - For one or two storage arrays that are connected to the same head unit, Fibre Channel switches are optional, because the arrays can be connected directly to the head unit.
  - For three storage arrays connected to the same head unit, *redundant* Fibre Channel switches are mandatory.
    - Switch-Port Sizing—For each hardware unit, the following number of switch ports is required:
      - Head Unit—Two ports per switch
      - Storage Array—Four ports per switch
  - SFP+ Transceivers—For each switch port, one 16 Gb SFP+ transceiver is required

Note Go to Appendix D:: Switch-Port Sizing on page 49 for more information.

- Security Analytics ISO image, version 7.1.10 or later
- Symantec-provided license key
- Cat5 cable
- Windows° or Linux° workstation with one of the following browsers:
  - Apple° Safari° 9.1
  - Google° Chrome° 50
  - Microsoft Edge 25
  - Microsoft° Internet Explorer 11
  - Mozilla° Firefox° 38.8.0 ESR, 45.1.0 ESR, 46

1.1. Terminology

The following usage appears in this document:

- Head Unit—A 10G-HD or SA-S500-30-FA Forensics Appliance that writes to one or more storage arrays
- Storage Array—A Dell MD3860f High-Density Fibre Channel Array or NetApp E5660 Storage Array
- Management Workstation—A Windows or Linux workstation with Dell MDSM or NetApp SANtricity installed

1.2. Head Unit I/O Configuration

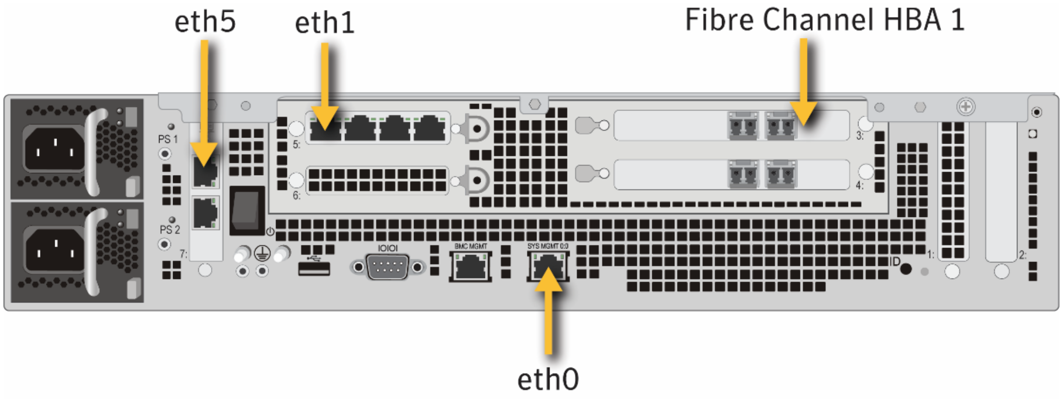


Figure 1: Symantec SA-S500-30-FA Forensic Appliance

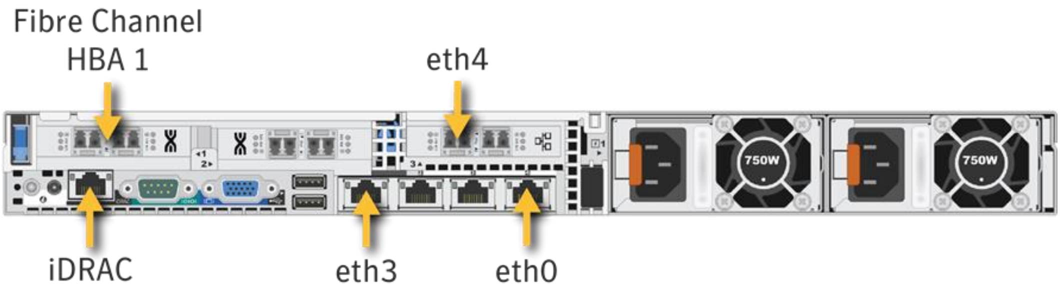


Figure 2: Symantec 10G-HD Forensic Appliance (Dell PowerEdge R630 Rack Server with Symantec BOM)

IMPORTANT The location of the management port on the Dell head unit is valid only after Security Analytics software has been installed. If you did not purchase your Dell head unit through Symantec, go to Appendix B:: Initial Head-Unit Configuration on page 39.

1.3. Storage Array I/O Configuration

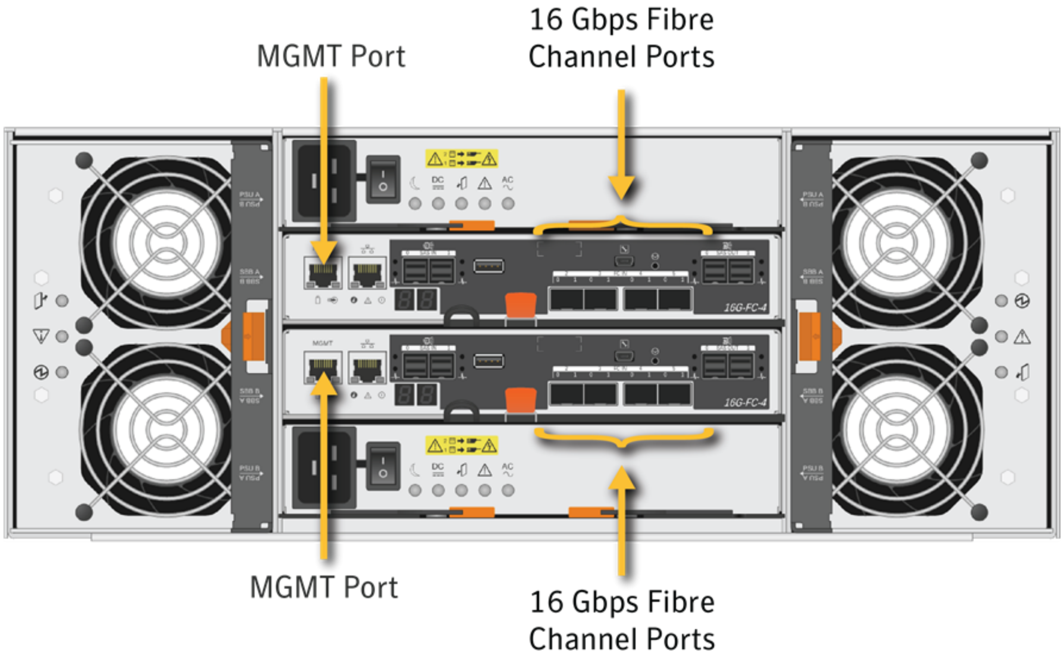


Figure 3: Symantec 240T Storage Array (Dell PowerVault MD3860f High-Density Fibre Channel Storage Array)

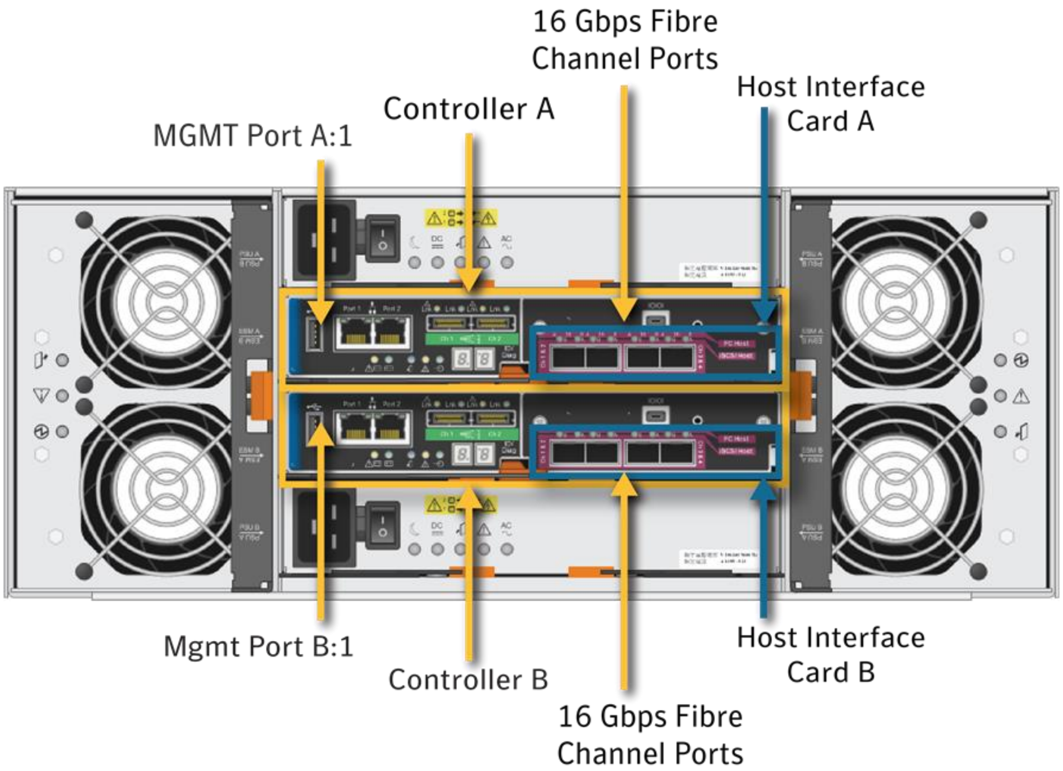


Figure 4: Symantec 240T Storage Array (NetApp° E5660 Storage System with 4TB Drives)

2. Supported Configurations

The illustrations below show supported head unit/storage array combinations and topologies. For detailed diagrams go to Appendix E: Supported Hardware Configurations on page 50.

Note Do not cable the head unit to the storage arrays or switches until indicated, later in these instructions.

2.1. Point-to-Point Connections

Security Analytics supports two types of point-to-point connections: one head unit plus one or two storage arrays.

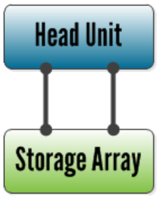


Figure 5: One Head Unit + One Storage Array

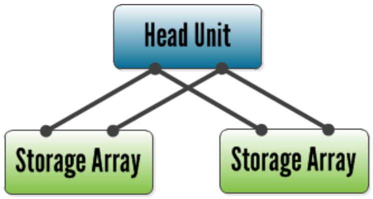


Figure 6: One Head Unit + Two Storage Arrays

2.2. Fibre Channel Switch Fabric

Security Analytics supports one head unit plus up to three storage arrays that are connected by redundant Fibre Channel switches.

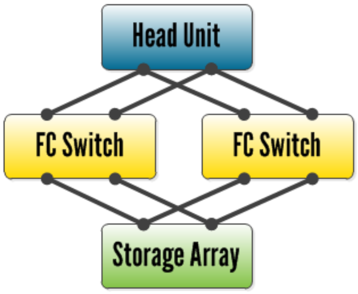


Figure 7: One Head Unit + One Storage Array

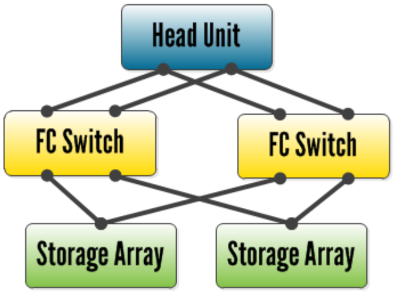


Figure 8: One Head Unit + Two Storage Arrays

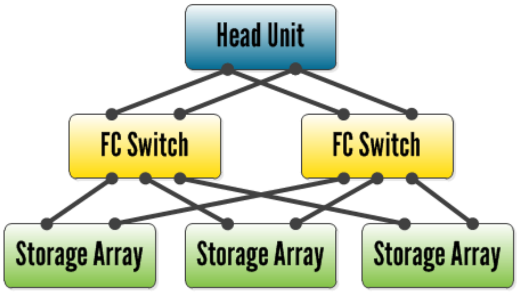


Figure 9: One Head Unit + Three Storage Arrays

IMPORTANT Although this high-density solution uses storage-area network (SAN) hardware, standard SAN topology cannot be used with Symantec Security Analytics. Under no circumstances should different head units write to the same storage array. Security Analytics's unique, proprietary file system requires that each head unit write to its own dedicated set of disks.

Shared Fibre Channel Switches

In the example below, the head units and their respective storage arrays are sharing the same redundant Fibre Channel switches, but the head units and their storage arrays can "see" only each other because of the switch zoning.

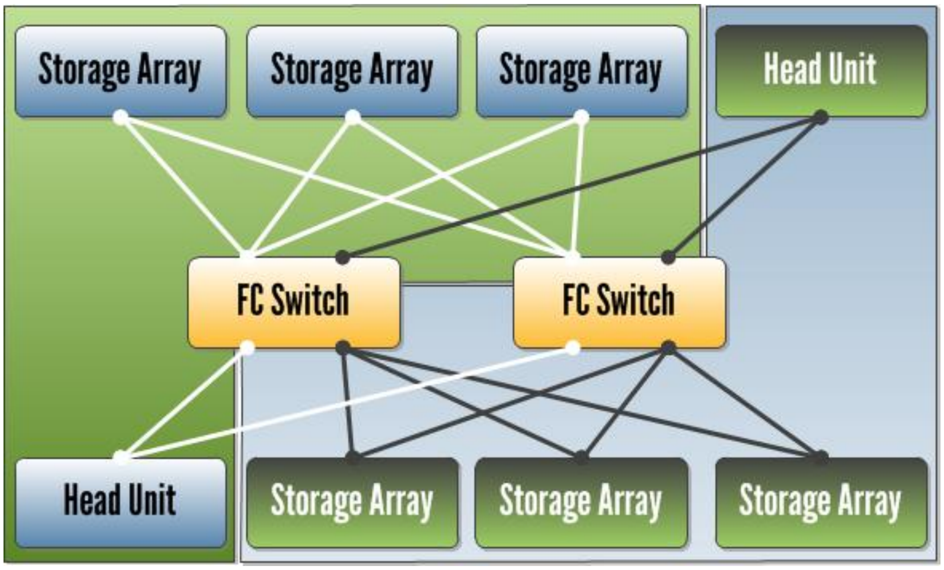


Figure 10: Two head units and their respective storage arrays, sharing redundant Fibre Channel switches.

Note For detailed diagrams go to Appendix E: Supported Hardware Configurations on page 50.

3. Prepare the Devices

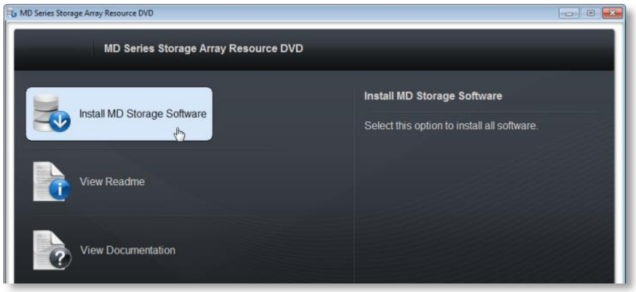
Perform these steps to prepare the management workstation, head unit, and storage array(s) for the configuration process.

3.1. Set Up the Workstation

Dell MDSM can be installed on a Windows or Linux workstation.

IMPORTANT You cannot install both Dell MDSM and NetApp SANtricity on the same workstation.

3.1.1. Insert the software installation DVD in the management workstation.


MD Series Storage Array Resource DVD
MD Series Storage Array Resource DVD
Install MD Storage Software
View Readme
View Documentation
Install MD Storage Software

Select this option to install all software.

Figure 11: MD Series Storage Array Resource DVD Splash Screen

3.1.2. Select Install MD Storage Software.

3.1.3. Under Core Software, select Management Station.

3.1.4. Follow the prompts to finish installing MDSM.

3.2. Set Up the Storage Array

No configuration should have been performed on the storage array, regardless of how it was obtained.

The *Quick-Start Guide* that was included with the Symantec-sourced storage array (Security Analytics Appliance Gen 6 and HD Quick-Start Guide; DOC10356 on support.symantec.com) instructs the user to perform a variety of tasks. At minimum, the following should be done before you begin:

3.2.1. Install the empty enclosure in the rack, preferably in the lowest position. The rack should support the weight of the fully populated storage array, which is 232.0 lb (105.2 kg).

3.2.2. Install all 60 disks in the drawers and verify that they are all seated properly.

3.2.3. Connect each of the enclosure's two power supplies to different 200V-to-240V input sources. Each power supply draws 7–10 amps.

IMPORTANT Do not power on the storage array until instructed, later in this procedure.

3.3. Set Up the Head Unit

Note If the R630-HD was not purchased through Symantec, go to Appendix B: Initial Head-Unit Configuration on page 39 and follow the instructions to configure the R630-HD.

Any 10G-HD forensic appliance that was ordered through Symantec should have the Blue Coat or Symantec branding on the bezel and also the following tasks performed at Dell prior to shipment:

- All eight internal hard drives configured as a single RAID 5 array
- Security Analytics Software 7.1.10 or later installed

IMPORTANT

- Security Analytics Software must be installed on the head unit prior to associating it with the storage arrays, because only versions 7.1.10 and later have the valid Light-Pulse Fibre Channel (LPFC) drivers for the storage array to detect the head unit.
- At this point in the procedure, the Security Analytics software is unaware of any indexing or capture drives; the head unit is therefore unable to perform capture or indexing; this is expected behavior.
- The Quick-Start Guide that was included in the box with the 10G-HD forensics appliance (Security Analytics Appliance Gen 6 and HD Quick-Start Guide; DOC10356 on support.symantec.com) instructs the user to configure the IP address and default gateway for eth0 and then to consult the Help Files to finish configuring the appliance. Any configuration that may exist on the appliance will be deleted by the process described in this installation guide. To save configuration settings, perform a manual backup using /etc/utils/solera-backup.sh.

Enable Disk Encryption on the Head Unit

Symantec strongly recommends that you enable disk encryption on both the head unit and the storage array.

- Instructions for enabling disk encryption on the storage array are provided later in this procedure.
- To enable disk encryption on the head unit, complete the instructions in *Enable Disk Encryption on the Head Unit* on page 41.

3.4. Choose a Management Topology

During the discovery and configuration of the storage array, you must use one of the two topologies to connect the management workstation to the management interfaces of the head unit and storage array:

Management Network

The management interfaces on the RAID controller modules and head unit are connected to the management workstation via a management network, as shown in Figure 12.

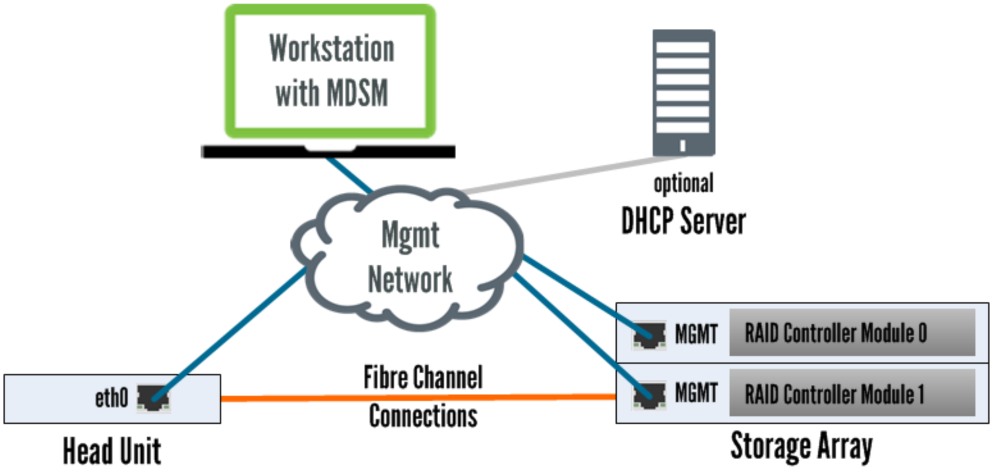


Figure 12: The workstation is connected to the management interfaces of the head unit and RAID controller modules over a management network. A DHCP server on the network is optional.

Direct Management

The workstation is directly connected to one MGMT interface of the storage array with a Cat5 cable, as shown in Figure 13.

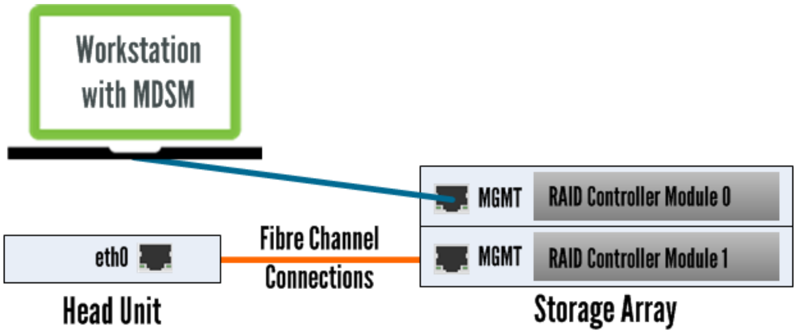


Figure 13: The workstation is connected to one the array's MGMT interfaces.

3.5. Set the IP Addresses

Use any of the following methods to configure the IP addresses for the MGMT interfaces on the storage array (RAID controller modules) and the head unit (eth0), according to the topology you chose in Step 3.4: Choose a Management Topology on page 13.

RAID Controller Modules

If a DHCP server is not available for 150 seconds, the MGMT interfaces on the RAID controller modules default to the following static IP addresses:

- Module 0—192.168.128.101
- Module 1—192.168.128.102

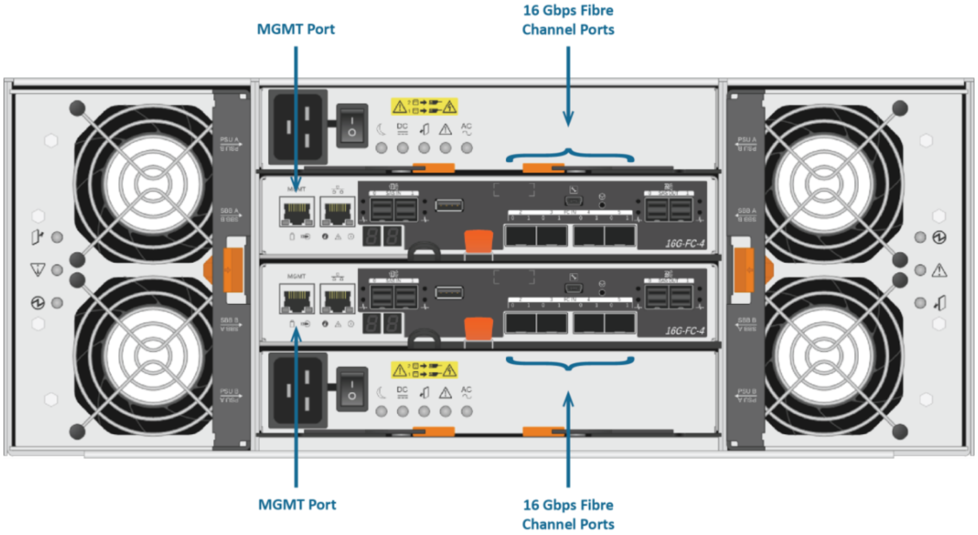


Figure 14: Symantec 240T Storage Array (Dell PowerVault MD3860f High-Density Fibre Channel Storage Array)

Follow these steps to change the MGMT interfaces on the RAID controller modules.

3.5.1. Configure the workstation IP for the 192.168.128.0/24 network, and then directly connect to one of the MGMT interfaces using a Cat5 cable.

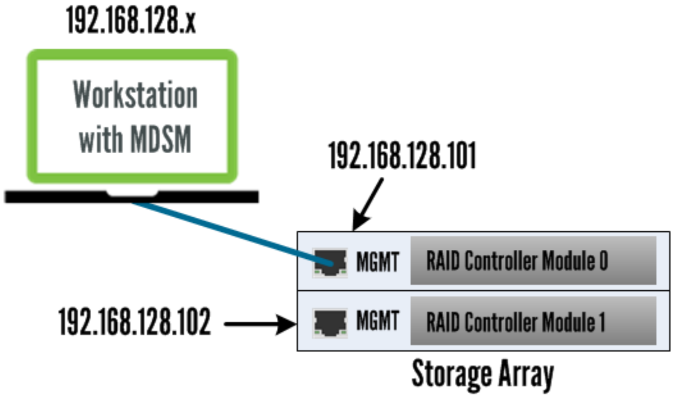
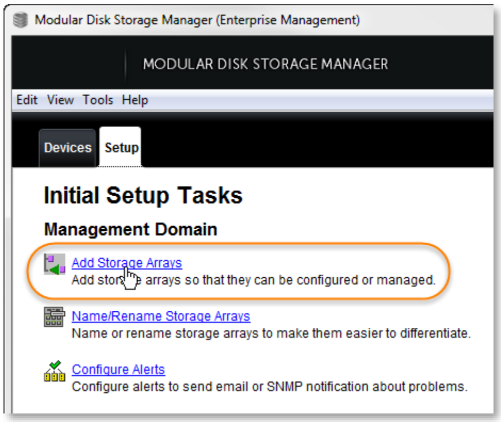


Figure 15: Connecting directly to the MGMT interface using a Cat5 cable

3.5.2. Power on the storage array and wait for it to finish booting.

3.5.3. Open the MDSM client on the management workstation.

3.5.4. On the Setup tab, select Add Storage Arrays.


Modular Disk Storage Manager (Enterprise Management)
MODULAR DISK STORAGE MANAGER
Edit View Tools Help
Devices
Setup

Initial Setup Tasks

Management Domain

Add Storage Arrays
Add storage arrays so that they can be configured or managed.

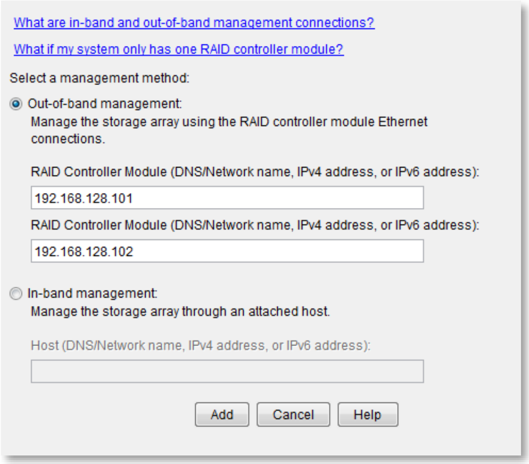
Name/Rename Storage Arrays
Name or rename storage arrays to make them easier to differentiate.

Configure Alerts
Configure alerts to send email or SNMP notification about problems.

Figure 16: Initial Setup Tasks—Add Storage Arrays

3.5.5. For *Select Addition Method*, select Manual and click OK.

3.5.6. On the *Add New Storage Array - Manual* dialog, for *Select a management method*, select Out-of-band management, input the RAID controller modules' static IP addresses in the spaces provided, and click Add.



What are in-band and out-of-band management connections?

What if my system only has one RAID controller module?

Select a management method:

● Out-of-band management:
Manage the storage array using the RAID controller module Ethernet connections.

RAID Controller Module (DNS/Network name, IPv4 address, or IPv6 address):
192.168.128.101

RAID Controller Module (DNS/Network name, IPv4 address, or IPv6 address):
192.168.128.102

○ In-band management:
Manage the storage array through an attached host.

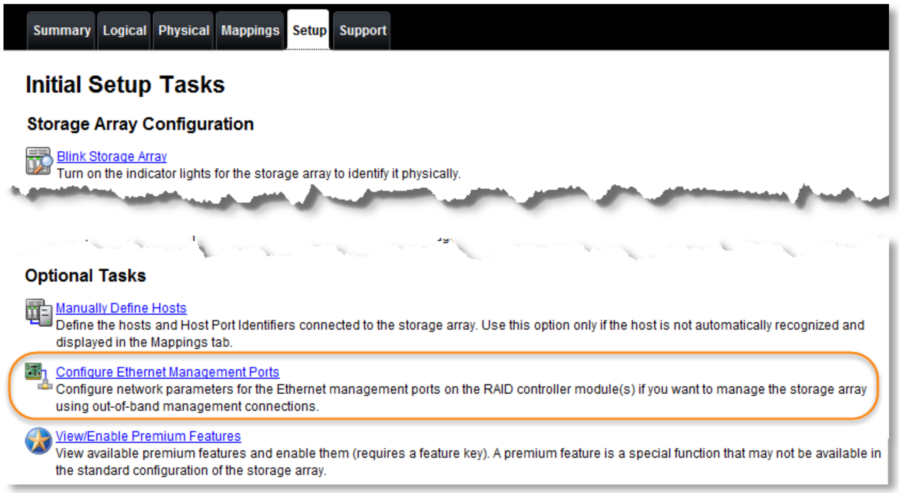
Host (DNS/Network name, IPv4 address, or IPv6 address):

Figure 17: Add the RAID controller modules using out-of-band management.

3.5.7. Click OK. On the *Storage Array Added* dialog click No. The storage array has been discovered.

3.5.8. To change the IP addresses, click Manage a Storage Array to open the *Array Management Window* for the array.

3.5.9. Click the Setup tab.



Initial Setup Tasks

Storage Array Configuration

Blink Storage Array
Turn on the indicator lights for the storage array to identify it physically.

Optional Tasks

Manually Define Hosts
Define the hosts and Host Port Identifiers connected to the storage array. Use this option only if the host is not automatically recognized and displayed in the Mappings tab.

Configure Ethernet Management Ports
Configure network parameters for the Ethernet management ports on the RAID controller module(s) if you want to manage the storage array using out-of-band management connections.

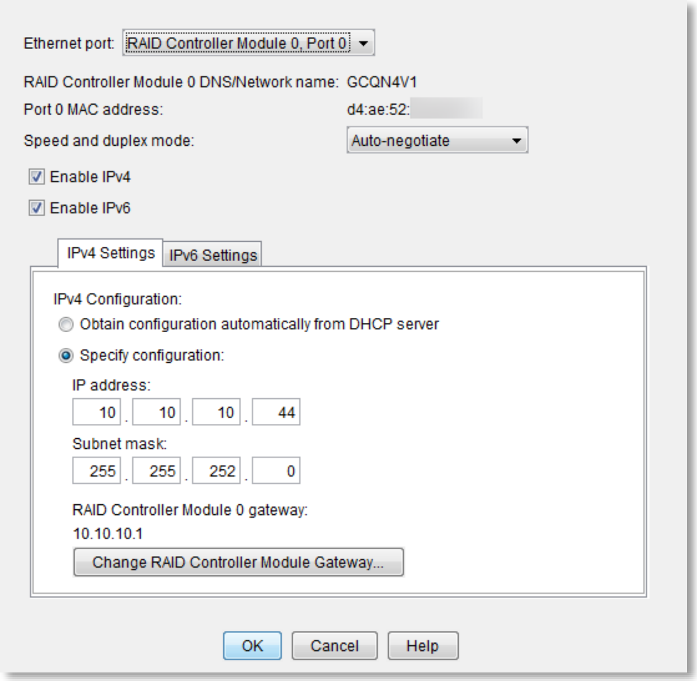
View/Enable Premium Features
View available premium features and enable them (requires a feature key). A premium feature is a special function that may not be available in the standard configuration of the storage array.

Figure 18: Ethernet management port configuration on the Setup tab

3.5.10. Under *Optional Tasks*, select Configure Ethernet Management Ports.

3.5.11. For Ethernet port, select RAID Controller Module 0, Port 0.

3.5.12. Assign an IP address in the management network to the MGMT port for the upper module (Module 0). As needed, change the gateway IP address.


Ethernet port: RAID Controller Module 0, Port 0

RAID Controller Module 0 DNS/Network name: GCQN4V1

Port 0 MAC address: d4:ae:52:[redacted]

Speed and duplex mode: Auto-negotiate

☑ Enable IPv4

☑ Enable IPv6

IPv4 Configuration:

○ Obtain configuration automatically from DHCP server

● Specify configuration:

IP address: 10 . 10 . 10 . 44

Subnet mask: 255 . 255 . 252 . 0

RAID Controller Module 0 gateway:
10.10.10.1

Figure 19: Manually setting the IP address for the RAID controller module MGMT port

3.5.13. For Ethernet port, select RAID Controller Module 1, Port 0 and repeat Steps 3.5.8 through 3.5.12.

3.5.14. Click OK.

Head Unit

By default, eth0 on the head unit has the static IP address 192.168.20.20.

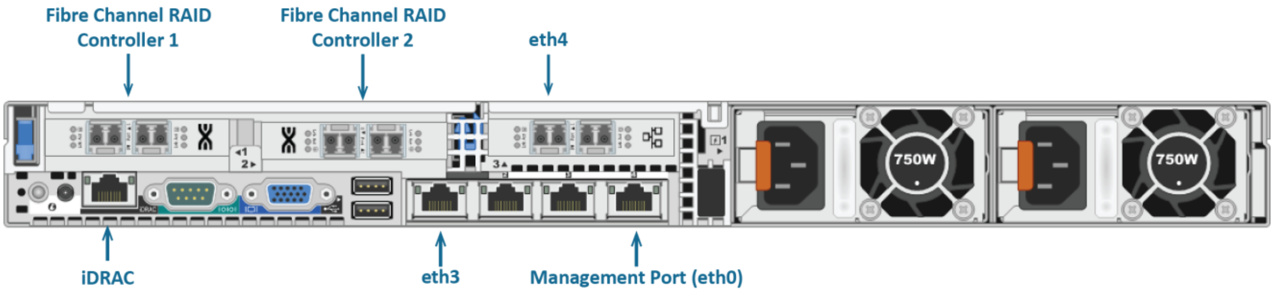

Fibre Channel RAID Controller 1
Fibre Channel RAID Controller 2
eth4
750W
750W
iDRAC
eth3
Management Port (eth0)

Figure 20: Symantec 10G-HD Forensic Appliance (Dell PowerEdge R630 Rack Server with Symantec BOM)

Note If the management port (eth0) does not have an IP address, go to Appendix B: Initial Head-Unit Configuration on page 39 and follow the instructions to configure the R630-HD.

3.5.15. Configure the workstation IP for the 192.168.20.0/24 network (for example, 192.168.20.111) and then directly connect to eth0 over SSH.

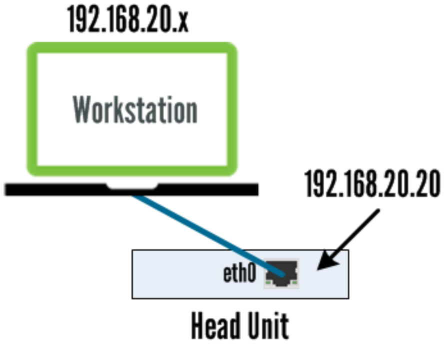


Figure 21: Connecting directly to eth0 over SSH

3.5.16. Log in using admin | Solera or root | <root_password>

3.5.17. Do one of the following:

- Enable DHCP:

```
[sudo] dhclient eth0
```

- Set a static IP address:

```
[sudo] ifconfig eth0 <ip_address> netmask <netmask>
[sudo] route add default gw <gateway>
```

Note An IP address that is set using sudo ifconfig does not persist after reboot.

3.6. Obtain the Host Port Identifiers for the Head Unit

Follow these instructions to get the host port identifiers (world-wide names [WWNs]) for the HBAs on the 10G-HD.

3.6.1. Connect to the head unit over SSH or the console and log in as root.

3.6.2. Get a list of Fibre Channel interfaces:

```
ls /sys/class/fc_host
```

The result will be similar to the following:

```
host12  host13  host14  host15
```

3.6.3. For each interface listed, get the host port identifier (MAC address):

```
cat /sys/class/fc_host/<hostNN>/device/fc_host/<hostNN>/port_name
```

Therefore:

```
[root ~]# cat /sys/class/fc_host/host12/device/fc_host/host12/port_name
0x10000090fafafa4a
[root ~]# cat /sys/class/fc_host/host13/device/fc_host/host13/port_name
0x10000090fafafa4b
[root ~]# cat /sys/class/fc_host/host14/device/fc_host/host14/port_name
0x10000090fafafac2
[root ~]# cat /sys/class/fc_host/host15/device/fc_host/host15/port_name
0x10000090fafafac3
```

The shaded digits identify the ports as Emulex LPe16002B Fibre Channel HBAs.

Note Write down the last 6–8 digits of each identifier with its corresponding head unit, for use later in the procedure.

4. Power Down the Devices

Verify that the management topology that you chose in Step 3.4: Choose a Management Topology on page 13 is configured properly, and then power down the head unit and the storage array. The workstation does not need to be powered down.

5. Establish Fibre Channel Connectivity

With all head units and storage arrays powered down, use the Fibre Channel cables that were included with the storage arrays (and the switches, if any) to connect the HBAs on the head units to the Fibre Channel ports on the RAID controller modules on the storage arrays.

5.1. With Point-to-Point Connections

5.1.1. Consult the diagrams in Appendix E: to see point-to-point connections for the following configurations:

- One Head Unit, One Array on page 52
- One Head Unit, Two Arrays on page 54

5.1.2. Go to Step 6: Power On the Devices on page 20.

5.2. Through Fibre Channel Switches

The specific method for configuring a Fibre Channel switch is beyond the scope of this document. Consult the manufacturer's instructions, and while configuring the switches, follow these guidelines:

- The Fibre Channel topology must be switched-fabric, not arbitrated loop.
- Use two switches for redundancy.
- Use the world-wide name (WWN) zoning method, such that the WWN of the devices are assigned to the zones instead of assigning switch ports to the zones.
- Each host port on a head unit must be in a different zone, and each HBA should be connected to both switches.
- Two or more head units may share a Fibre Channel switch, but only as long as none of the host ports are in the same zone.

- Consult Appendix E: to see diagrams and switch zones for these configurations.
    - Mandatory Switch-Fabric Connections:
        - One Head Unit, Three Arrays on page 58
        - Two Head Units, Three Arrays Each on page 65
        - Three Head Units, Three Arrays Each on page 72
    - All Other Connections:
        - One Head Unit, One Array on page 52
        - One Head Unit, Two Arrays on page 54
        - Two Head Units, One Array Each on page 60
        - Two Head Units, Two Arrays Each on page 62
        - Three Head Units, One Array Each on page 67
        - Three Head Units, Two Arrays Each on page 69

5.2.1. Continue to Step 6: Power On the Devices on page 20.

6. Power On the Devices

Power on all devices in the following order:

- Fibre Channel switches
- Storage array
- Head unit

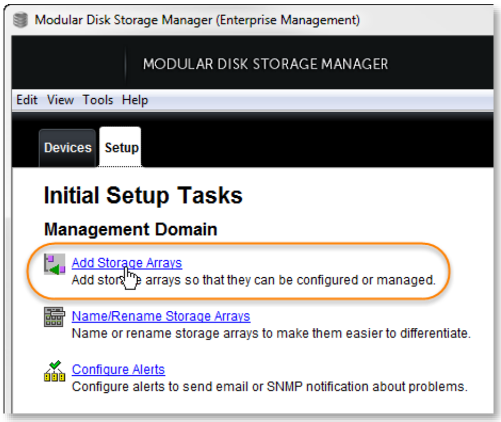
7. Discover the Storage Arrays

With all devices connected according to the management topology that you chose in Step 3.4: Choose a Management Topology on page 13, you are ready to discover the storage arrays.

7.1. Add the Arrays

7.1.1. Open MDSM on the management workstation.

7.1.2. On the Setup tab, select Add Storage Arrays.


Modular Disk Storage Manager (Enterprise Management)
MODULAR DISK STORAGE MANAGER
Edit View Tools Help
Devices
Setup

Initial Setup Tasks

Management Domain

Add Storage Arrays
Add storage arrays so that they can be configured or managed.

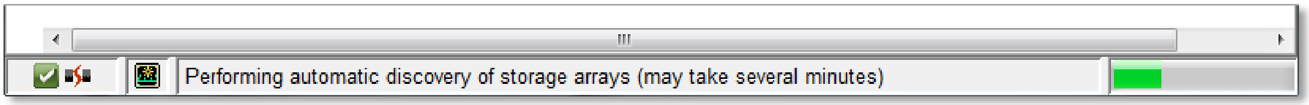
Name/Rename Storage Arrays
Name or rename storage arrays to make them easier to differentiate.

Configure Alerts
Configure alerts to send email or SNMP notification about problems.

Figure 22: Initial Setup Tasks—Add Storage Arrays

7.1.3. For *Select Addition Method*, select Automatic and click OK.

7.1.4. On the *Automatic Discovery* dialog, click OK. The bar at the bottom of the *Modular Disk Storage Management* window displays the discovery progress.

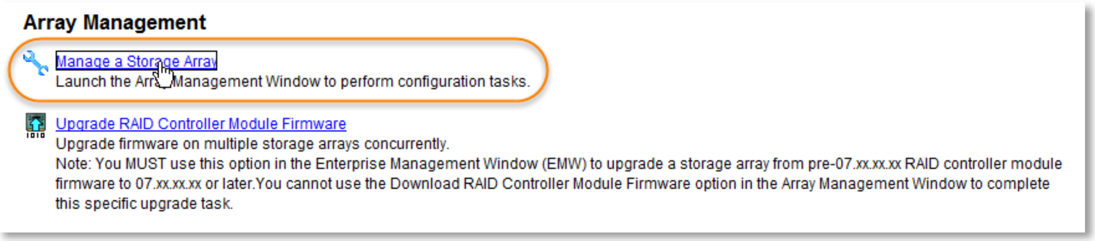


Performing automatic discovery of storage arrays (may take several minutes)

Figure 23: Automatic discovery in progress

7.1.5. When the discovery process has completed, return to the Setup tab.

7.1.6. Under *Array Management*, select Manage a Storage Array.



Array Management

Manage a Storage Array
Launch the Array Management Window to perform configuration tasks.

Upgrade RAID Controller Module Firmware
Upgrade firmware on multiple storage arrays concurrently.
Note: You MUST use this option in the Enterprise Management Window (EMW) to upgrade a storage array from pre-07.xx.xx.xx RAID controller module firmware to 07.xx.xx.xx or later.You cannot use the Download RAID Controller Module Firmware option in the Array Management Window to complete this specific upgrade task.

Figure 24: Launching the Array Management utility

7.1.7. On the *Select Storage Array* dialog, select the MD3860f entry and click OK. The *Array Management* utility is displayed.

7.1.8. When the *Disk Pool Automatic Configuration* wizard is displayed click No.

IMPORTANT Security Analytics does not support disk pools.

7.2. Verify the Condition of the Physical Disks

Before you begin to configure the storage array, you should verify that all of the disks are in good working order. Damaged disks cannot be encrypted, added to disk groups, or designated as hot spares.

7.2.1. In the *Array Management* utility click the Hardware tab. A graphical representation of the array is displayed.

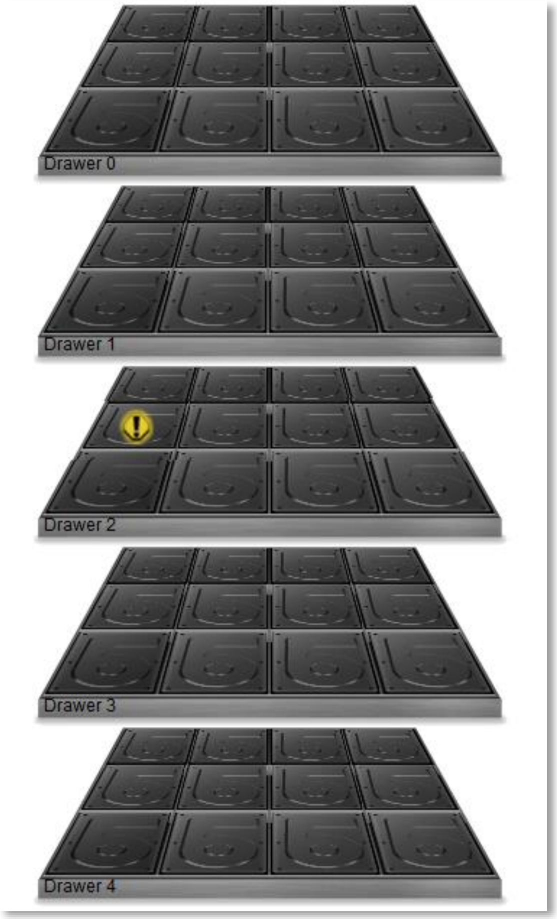


Figure 25: Representation of the Physical Disks

7.2.2. An alert icon identifies any damaged disks.

7.2.3. Replace all damaged disks before continuing this procedure.

IMPORTANT The virtual disk groups must all be the same size within the same function—for example, all of the disk groups that are designated for capture must have the same capacity. If you attempt to work around a damaged disk by creating a disk group that has one fewer disk than the other groups, Security Analytics will behave in unexpected ways, and performance will be severely degraded.

7.3. Enable Disk Encryption on the Enclosure

The Symantec-approved BOM specifies that all sixty physical disks be self-encrypting disks (SEDs), which means that the data cannot be retrieved from an encrypted disk that has been improperly removed from the enclosure. Once the disks are secured, only a RAID controller module with a valid key can decrypt the content on the disk.

If you desire to encrypt the disks on the array, follow these steps to create the physical disk security key:

7.3.1. In the Array Management utility, select Storage Array > Security > Physical Disk Security > Create Key.

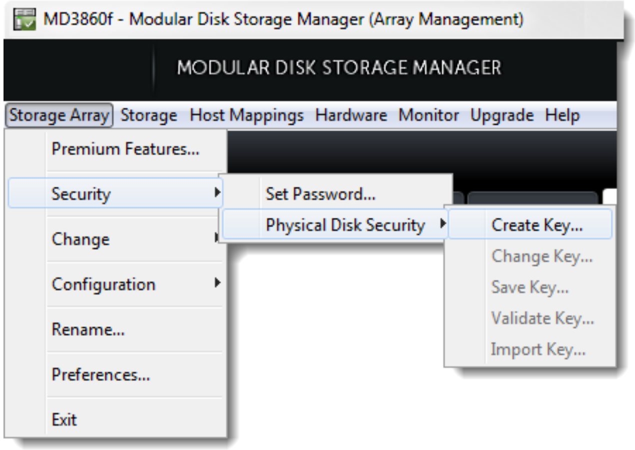


Figure 26: Creating the encryption key for the disks in the storage array.

IMPORTANT

- The **Security > Set Password** option creates a password to access the Array Management utility itself. Do not confuse the utility-access password with the pass phrase that you will provide below to protect copies of the security key.
- After the physical disk security key has been generated, the **Create Key** option will not be available again.

7.3.2. On the *Create Security Key* dialog, provide a user-friendly name for Security key identifier.

7.3.3. For File name, click Browse and specify a name for the security key file.

7.3.4. For Pass phrase, enter a password that complies with the requirements that are specified on the dialog.

7.3.5. Click Create Key. When the key has been generated by the RAID controller modules, the *Create Security Key Complete* dialog displays the Security key identifier and File name.

IMPORTANT Follow best key-maintenance practices such as recording the identifier, pass phrase, and key location, and by keeping a copy of that information in a separate location.

Note You can erase security-enabled physical disks to reuse the disks in another disk group or in another storage array. You will need to delete the group that the disk belongs to and then use the Secure Erase option. Consult the MDSM help files for more information.

7.4. Configure the Indexing Disk Groups

Follow these steps to create the physical and virtual indexing drives. Consult the table below to see which disks to add to the index groups.

	index0	index1
Number of Disks	5 disks	5 disks
RAID Level	RAID 5	RAID 5
Disk Group Capacity	14.533 TB	14.533 TB
Drawer,Slot Range	0,0 – 0,4	0,5 – 0,9

7.4.1. Select the Storage & Copy Services tab.

7.4.2. In the left pane, under *[Storage Array Name]*, right-click the Total Unconfigured Capacity item and select Create Disk Group.

7.4.3. On the *Introduction* page of the *Create Disk Groups* wizard click Next.

7.4.4. On the *Disk Group Name & Physical Disk Selection* page, provide a name for the indexing disk group, for example: index0

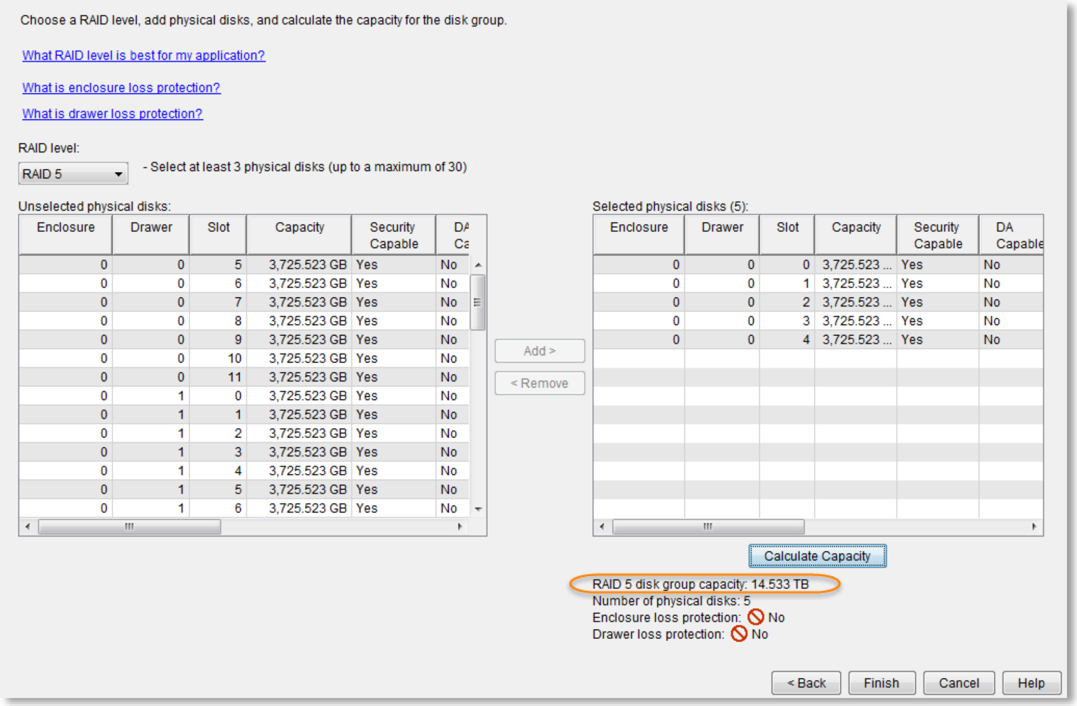
7.4.5. Select the Create a secure disk group check box. If this option is not available, and you want to create secure disk groups, return to Step 7.3: Enable Disk Encryption on page 23.

7.4.6. Select Manual for Physical Disk selection choices and click Next.

7.4.7. On the *Manual Physical Disk Selection* page, select RAID 5 for the RAID level.

7.4.8. In the *Unselected physical disks* list, press Ctrl while clicking on the disks for the index0 array. Click Add to move the disks to the *Selected physical disks* list.

7.4.9. Click Calculate Capacity and review the disk group capacity.



Choose a RAID level, add physical disks, and calculate the capacity for the disk group.

What RAID level is best for my application?

What is enclosure loss protection?

What is drawer loss protection?

RAID level: RAID 5 - Select at least 3 physical disks (up to a maximum of 30)

Unselected physical disks:

Enclosure	Drawer	Slot	Capacity	Security Capable	DA Ca
0	0	5	3,725.523 GB	Yes	No
0	0	6	3,725.523 GB	Yes	No
0	0	7	3,725.523 GB	Yes	No
0	0	8	3,725.523 GB	Yes	No
0	0	9	3,725.523 GB	Yes	No
0	0	10	3,725.523 GB	Yes	No
0	0	11	3,725.523 GB	Yes	No
0	1	0	3,725.523 GB	Yes	No
0	1	1	3,725.523 GB	Yes	No
0	1	2	3,725.523 GB	Yes	No
0	1	3	3,725.523 GB	Yes	No
0	1	4	3,725.523 GB	Yes	No
0	1	5	3,725.523 GB	Yes	No
0	1	6	3,725.523 GB	Yes	No

Selected physical disks (5):

Enclosure	Drawer	Slot	Capacity	Security Capable	DA Capable
0	0	0	3,725.523 ...	Yes	No
0	0	1	3,725.523 ...	Yes	No
0	0	2	3,725.523 ...	Yes	No
0	0	3	3,725.523 ...	Yes	No
0	0	4	3,725.523 ...	Yes	No

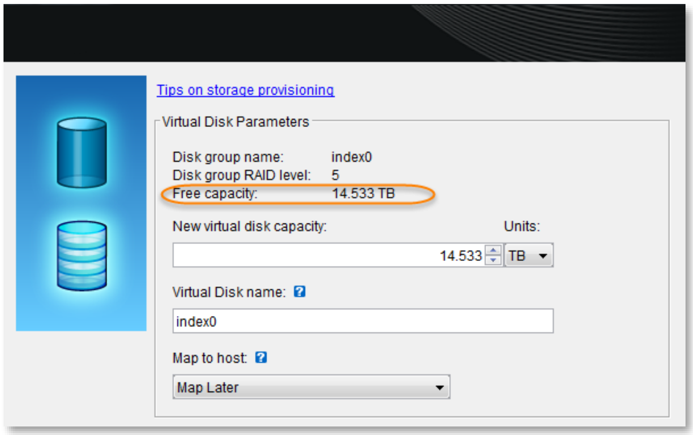
RAID 5 disk group capacity: 14.533 TB
Number of physical disks: 5
Enclosure loss protection: ⃠ No
Drawer loss protection: ⃠ No

Figure 27: Calculate the capacity of the disk group.

7.4.10. Click Finish. On the *Disk Group Created* dialog click Yes.

7.4.11. The *Create Virtual Disk: Specify Parameters* dialog is displayed.

7.4.12. For New virtual disk capacity select TB as the unit and then enter the Free capacity number in the space provided, or type `99999` and click the down arrow to auto-fill the correct amount.



Tips on storage provisioning

Virtual Disk Parameters

Disk group name: index0
Disk group RAID level: 5
Free capacity: 14.533 TB

New virtual disk capacity: 14.533 Units: TB

Virtual Disk name: index0

Map to host: Map Later

Figure 28: Specify the Free capacity of the virtual disk.

7.4.13. Provide a Virtual disk name. Recommended: Use the same name as the disk group.

7.4.14. For Map to host accept the default (Map Later) and click Finish.

7.4.15. For *Create Virtual Disk - Completed*, click OK. The new disk group is displayed in the left pane.

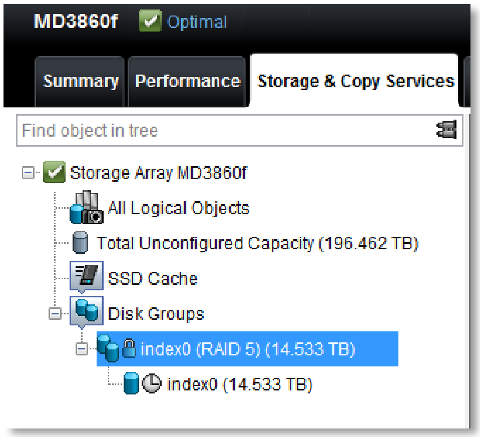
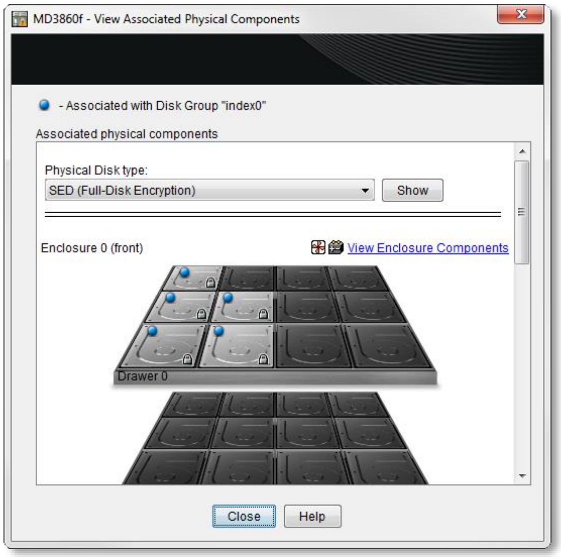


Figure 29: Index Disk Group Displayed

7.4.16. Right-click index0 (RAID 5) and select View Associated Physical Components.


MD3860f - View Associated Physical Components

- Associated with Disk Group "index0"

Associated physical components

Physical Disk type: SED (Full-Disk Encryption)

Figure 30: Physical components of index0, showing group membership and security status

7.4.17. A graphical representation of the disks is displayed. A blue dot marks the disks in index0, the lock icon shows that the disks have been secured, and the lighter gray color indicates that the disks have been assigned to a group.

7.4.18. Repeat Steps 7.4.2 through 7.4.15 for index1.

7.5. Configure the Capture Drives

Follow these steps to create the physical and virtual capture drives. Consult the table below to see how many disks to add to the capture groups.

	capture0	capture1	capture2	capture3
Number of Disks	12 disks	12 disks	12 disks	12 disks
RAID Level	RAID 5	RAID 5	RAID 5	RAID 5
Disk Group Capacity	39.966 TB	39.966 TB	39.966 TB	39.966 TB
Drawer,Slot Range	0,10 – 1,9	1,10 – 2,9	2,10 – 3,9	3,10 – 4,9

7.5.1. Right-click Total Unconfigured Capacity and select Create Disk Group.

7.5.2. On the *Introduction* page of the *Create Disk Groups* wizard click Next.

7.5.3. On the *Disk Group Name & Physical Disk Selection* page, provide a name for the indexing disk group, for example: capture0

7.5.4. Select the Create a secure disk group check box. If this option is not available, and you want to create secure disk groups, return to Step 7.3: Enable Disk Encryption on page 23.

7.5.5. Select Manual for Physical Disk selection choices and click Next.

7.5.6. On the *Manual Physical Disk Selection* page, select RAID 5 for the RAID level.

7.5.7. In the Unselected physical disks list, select the next disks and click Add.

7.5.8. Click Calculate Capacity and review the disk-group capacity number.

7.5.9. Click Finish. On the *Disk Group Created* dialog click Yes.

7.5.10. The *Create Virtual Disk: Specify Parameters* dialog is displayed.

7.5.11. For New virtual disk capacity select TB as the unit and then enter the Free Capacity number in the space provided.

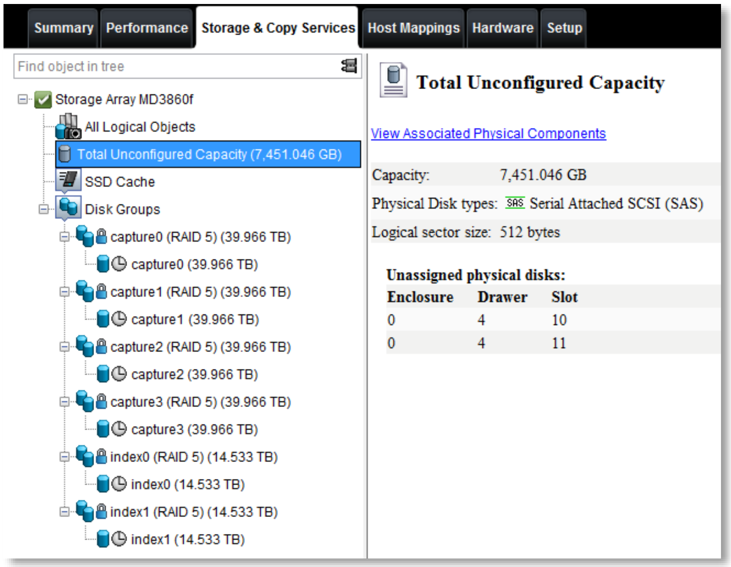
7.5.12. Provide a Virtual disk name. Recommended: Use the same name as the disk group.

7.5.13. For Map to host accept the default (Map Later) and click Finish.

7.5.14. For *Create Virtual Disk - Completed*, click OK. The new disk group is displayed in the left pane.

7.5.15. Repeat Steps 7.5.1 through 7.5.14 for the rest of the capture disk groups: capture1, capture2, and capture3.

7.5.16. After you have finished configuring all of the capture drives, click Total Unconfigured Capacity. Two disks should remain unassigned.


Summary
Performance
Storage & Copy Services
Host Mappings
Hardware
Setup
Find object in tree
Storage Array MD3860f
All Logical Objects
Total Unconfigured Capacity (7,451.046 GB)
SSD Cache
Disk Groups
capture0 (RAID 5) (39.966 TB)
capture0 (39.966 TB)
capture1 (RAID 5) (39.966 TB)
capture1 (39.966 TB)
capture2 (RAID 5) (39.966 TB)
capture2 (39.966 TB)
capture3 (RAID 5) (39.966 TB)
capture3 (39.966 TB)
index0 (RAID 5) (14.533 TB)
index0 (14.533 TB)
index1 (RAID 5) (14.533 TB)
index1 (14.533 TB)
Total Unconfigured Capacity
View Associated Physical Components

Capacity: 7,451.046 GB

Physical Disk types: SAS Serial Attached SCSI (SAS)

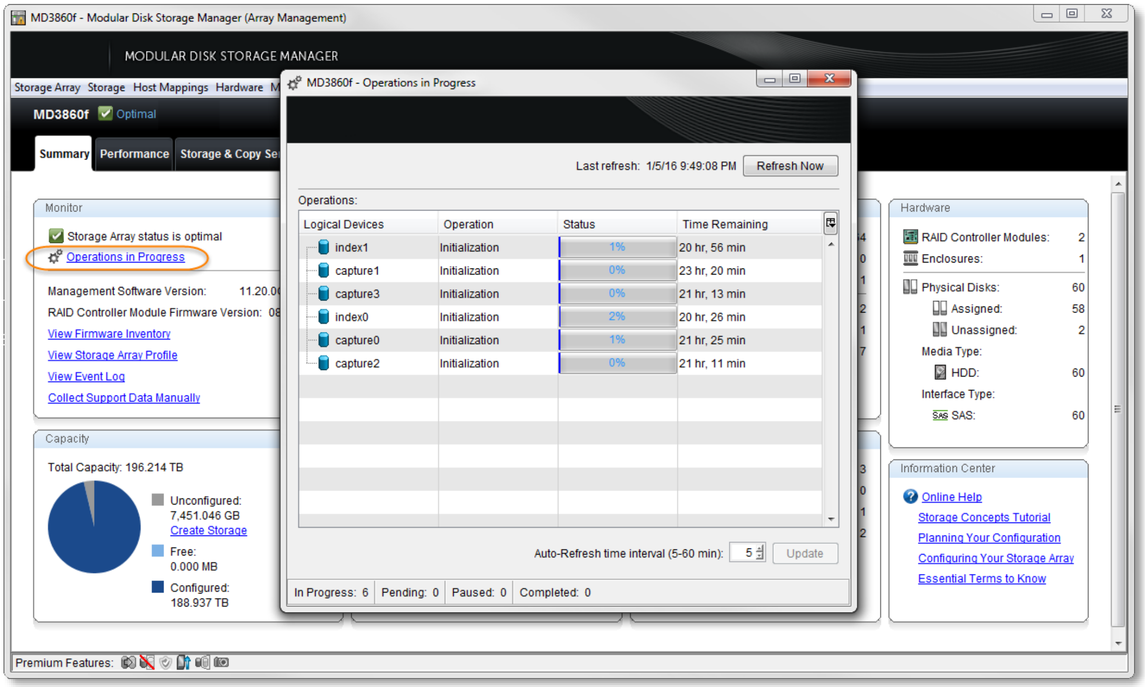
Logical sector size: 512 bytes

Unassigned physical disks:

Enclosure	Drawer	Slot
0	4	10
0	4	11

Figure 31: All Disk Groups Added

7.5.17. Click the Summary tab. Under *Monitor*, click Operations in Progress.


MD3860f - Modular Disk Storage Manager (Array Management)
MODULAR DISK STORAGE MANAGER
Storage Array
Storage
Host Mappings
Hardware
MD3860f
Optimal
Summary
Performance
Storage & Copy Se
Monitor
Capacity
Hardware
Information Center
Online Help
Storage Concepts Tutorial
Planning Your Configuration
Configuring Your Storage Array
Essential Terms to Know
Premium Features:
MD3860f - Operations in Progress
Refresh Now
Update

Storage Array status is optimal

Operations in Progress

Management Software Version: 11.20.0

RAID Controller Module Firmware Version: 08

View Firmware Inventory

View Storage Array Profile

View Event Log

Collect Support Data Manually

Total Capacity: 196.214 TB

Unconfigured: 7,451.046 GB

Create Storage

Free: 0.000 MB

Configured: 188.937 TB

RAID Controller Modules:	2
Enclosures:	1
Physical Disks:	60
Assigned:	58
Unassigned:	2
Media Type:	
HDD:	60
Interface Type:	
SAS:	60

Last refresh: 1/5/16 9:49:08 PM

Operations:

Logical Devices	Operation	Status	Time Remaining
index1	Initialization	1%	20 hr, 56 min
capture1	Initialization	0%	23 hr, 20 min
capture3	Initialization	0%	21 hr, 13 min
index0	Initialization	2%	20 hr, 26 min
capture0	Initialization	1%	21 hr, 25 min
capture2	Initialization	0%	21 hr, 11 min

Auto-Refresh time interval (5-60 min): 5

In Progress: 6 Pending: 0 Paused: 0 Completed: 0

Figure 32: Operations in Progress dialog, showing the initialization progress for each disk group

7.6. Configure the Hot Spares

Configure the remaining two disks as hot spares.

7.6.1. On the Storage & Copy Services tab, right-click the storage array and select Configuration > Hot Spare Coverage.

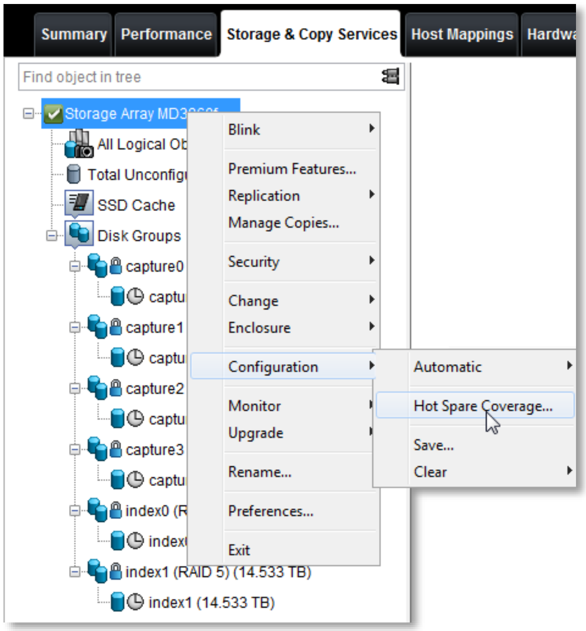
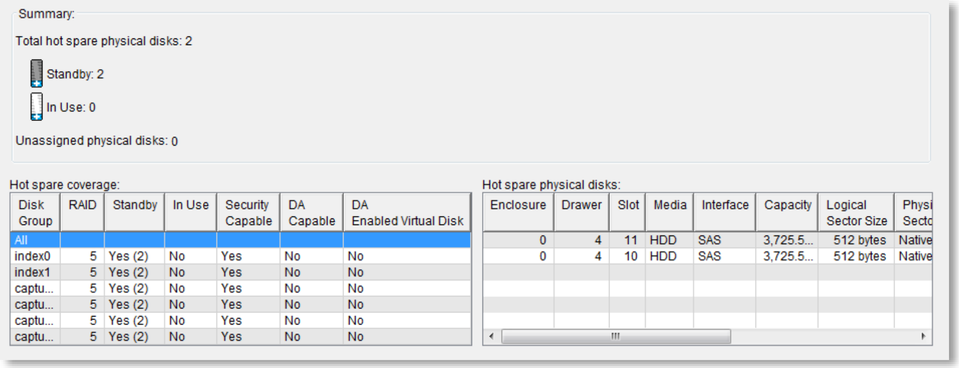


Figure 33: Configuring Hot Spare Coverage

7.6.2. On the *Hot Spare Physical Disk Options* dialog, select View/change current hot spare coverage and click OK.

7.6.3. On the *Hot Spare Coverage* dialog, click Assign.

7.6.4. On the *Assign Hot Spare* dialog, select the remaining two disks and click OK. The disks are displayed under *Hot spare physical disks*.



Summary:

Total hot spare physical disks: 2

Standby: 2

In Use: 0

Unassigned physical disks: 0

Hot spare coverage:

Disk Group	RAID	Standby	In Use	Security Capable	DA Capable	DA Enabled Virtual Disk
All						
index0	5	Yes (2)	No	Yes	No	No
index1	5	Yes (2)	No	Yes	No	No
captu...	5	Yes (2)	No	Yes	No	No
captu...	5	Yes (2)	No	Yes	No	No
captu...	5	Yes (2)	No	Yes	No	No
captu...	5	Yes (2)	No	Yes	No	No

Hot spare physical disks:

Enclosure	Drawer	Slot	Media	Interface	Capacity	Logical Sector Size	Physi Secto
0	4	11	HDD	SAS	3,725.5...	512 bytes	Native
0	4	10	HDD	SAS	3,725.5...	512 bytes	Native

Figure 34: Hot spare disks and the disk groups that they cover.

7.6.5. Click Close.

8. Map the Head Unit to the Storage Array

8.1.1. On the MDSM Array Management utility, click the Host Mappings tab.

8.1.2. Right-click Storage Array MD3860f in the left pane and select Define > Host.

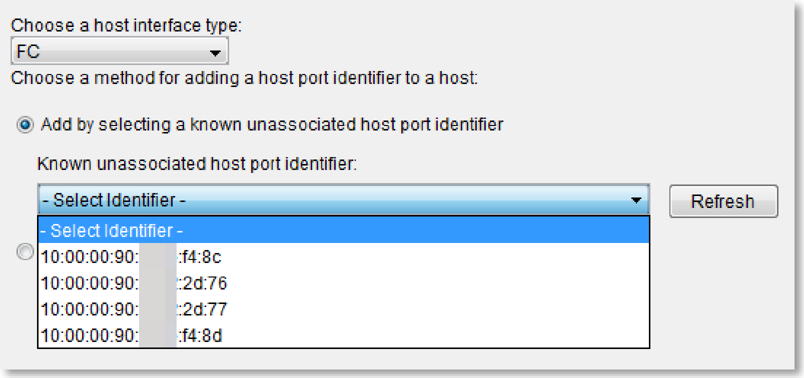
IMPORTANT Security Analytics does not support host groups.

8.1.3. Provide a Host name for the head unit.

8.1.4. Select No for Do you plan to use storage partitions on this storage array? and click Next.

8.1.5. Under Choose a host interface type select FC.

8.1.6. The list for Add by selecting a known unassociated host port identifier should contain exactly four host port identifiers. These are the same host port identifiers that you obtained in Step 3.6: Obtain the Host Port Identifiers for the Head Unit on page 18.



Choose a host interface type:
FC

Choose a method for adding a host port identifier to a host:

● Add by selecting a known unassociated host port identifier

Known unassociated host port identifier:
- Select Identifier -

○
- Select Identifier -
10:00:00:90:[redacted]:f4:8c
10:00:00:90:[redacted]:2d:76
10:00:00:90:[redacted]:2d:77
10:00:00:90:[redacted]:f4:8d

Figure 35: Unassociated Host Port Identifiers That the Storage Array Has Detected

IMPORTANT

- If there are more than four entries in the list, it is possible that the storage array has not been properly isolated from other head units that are sharing the Fibre Channel switches. Review the switch zoning to ensure that the storage array can detect only the host port identifiers for its head unit.
- If the host port identifiers for the head unit are not in the list, verify that the head unit and the storage array have full connectivity.

Note For ease of management, select the lowest number of a pair of identifiers first and the next number second, so that the aliases for the ports from the same HBA are in sequence.

8.1.7. For Alias provide a meaningful name such as port00 and click Add. The host port identifier and its alias are displayed under *Host port identifiers to be associated with the host*.

8.1.8. Repeat Steps 8.1.6 and 8.1.7 to associate the remaining three host port identifiers with the head unit (for example: port 01, port11, port10).

8.1.9. Click Next.

8.1.10. For Host type (operating system) select Linux and click Next.

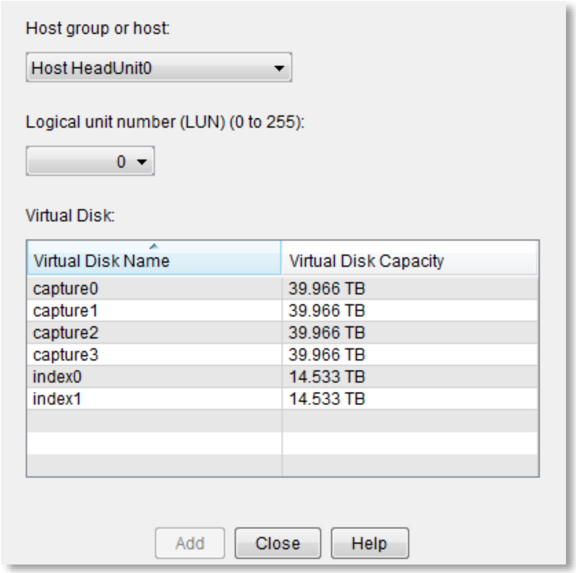
8.1.11. The *Current host definition* is displayed. Review the information and click Finish.

8.1.12. On the Creation Successful (Define Host) dialog click No.

8.1.13. The head unit is displayed under Default Group.

8.1.14. Right-click the head unit and select Manage Host Port Identifiers. On the dialog that is displayed, you can edit the host port identifiers that are associated with the head unit, should it be necessary. Click Close.

8.1.15. Right-click the head unit again and select Add LUN Mapping. The *Define Additional Mapping* dialog displays all of the virtual disk names, and the head unit's hostname should be displayed under Host group or host.



Host group or host: Host HeadUnit0

Logical unit number (LUN) (0 to 255): 0

Virtual Disk:

Virtual Disk Name	Virtual Disk Capacity
capture0	39.966 TB
capture1	39.966 TB
capture2	39.966 TB
capture3	39.966 TB
index0	14.533 TB
index1	14.533 TB

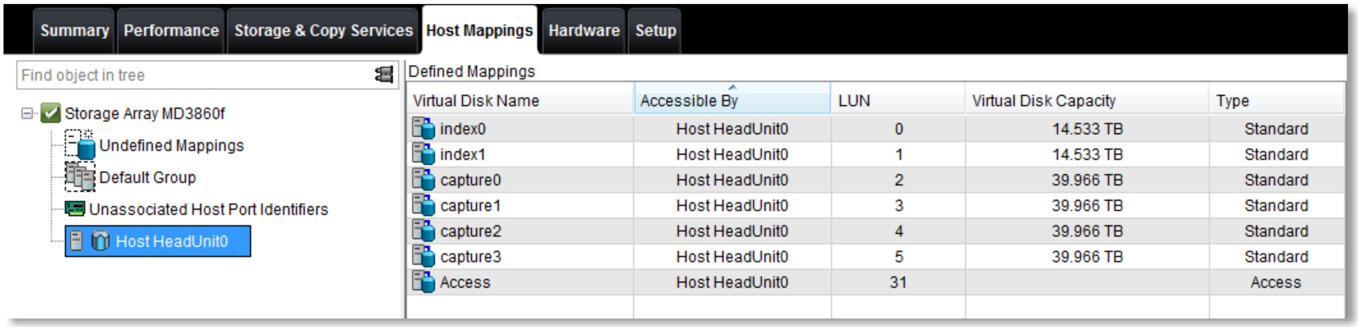
Figure 36: Logical Unit Number Assignation

8.1.16. Select the first indexing virtual disk (index0) and click Add. It is assigned the default logical unit number (LUN), which in this case should be 0.

8.1.17. Repeat Step 8.1.16 for the rest of the virtual disks and click Close. For ease of management, assign the LUNs as follows:

Virtual Disk	LUN
index0	0
index1	1
capture0	2
capture1	3
capture2	4
capture3	5

8.1.18. When you have finished assigning the LUNs, the head unit is displayed on the first level below the storage-array name. Click the head unit to see the virtual disks and LUNs.



Defined Mappings

Virtual Disk Name	Accessible By	LUN	Virtual Disk Capacity	Type
index0	Host HeadUnit0	0	14.533 TB	Standard
index1	Host HeadUnit0	1	14.533 TB	Standard
capture0	Host HeadUnit0	2	39.966 TB	Standard
capture1	Host HeadUnit0	3	39.966 TB	Standard
capture2	Host HeadUnit0	4	39.966 TB	Standard
capture3	Host HeadUnit0	5	39.966 TB	Standard
Access	Host HeadUnit0	31		Access

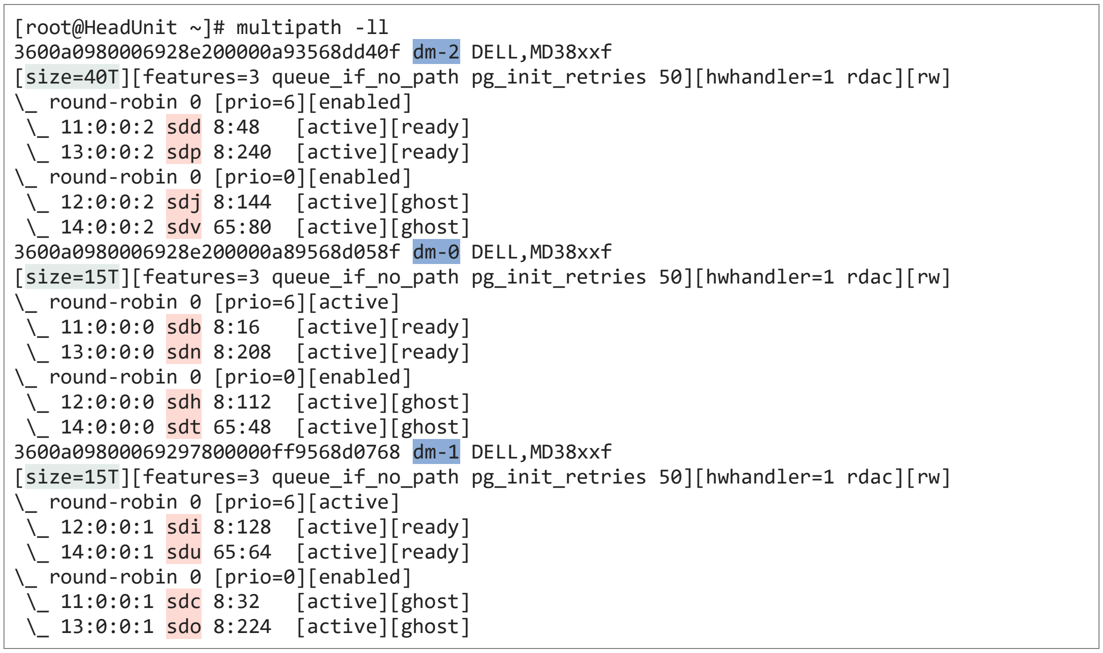
Figure 37: Completed Host Mappings

9. Verify Multipath Configuration

9.1.1. Using the command-line interface on the head unit, verify that multipath is set up:

```
[root@HeadUnit ~] multipath -ll
```

9.1.2. The readout is similar to the following when multipathd is successful:



```
[root@HeadUnit ~]# multipath -ll
3600a0980006928e200000a93568dd40f dm-2 DELL,MD38xxf
[size=40T][features=3 queue_if_no_path pg_init_retries 50][hwhandler=1 rdac][rw]
\_ round-robin 0 [prio=6][enabled]
 \_ 11:0:0:2 sdd 8:48   [active][ready]
 \_ 13:0:0:2 sdp 8:240  [active][ready]
\_ round-robin 0 [prio=0][enabled]
 \_ 12:0:0:2 sdj 8:144  [active][ghost]
 \_ 14:0:0:2 sdv 65:80  [active][ghost]
3600a0980006928e200000a89568d058f dm-0 DELL,MD38xxf
[size=15T][features=3 queue_if_no_path pg_init_retries 50][hwhandler=1 rdac][rw]
\_ round-robin 0 [prio=6][active]
 \_ 11:0:0:0 sdb 8:16   [active][ready]
 \_ 13:0:0:0 sdn 8:208  [active][ready]
\_ round-robin 0 [prio=0][enabled]
 \_ 12:0:0:0 sdh 8:112  [active][ghost]
 \_ 14:0:0:0 sdt 65:48  [active][ghost]
3600a09800069297800000ff9568d0768 dm-1 DELL,MD38xxf
[size=15T][features=3 queue_if_no_path pg_init_retries 50][hwhandler=1 rdac][rw]
\_ round-robin 0 [prio=6][active]
 \_ 12:0:0:1 sdi 8:128  [active][ready]
 \_ 14:0:0:1 sdu 65:64  [active][ready]
\_ round-robin 0 [prio=0][enabled]
 \_ 11:0:0:1 sdc 8:32   [active][ghost]
 \_ 13:0:0:1 sdo 8:224  [active][ghost]
```

Figure 38: A successful multipathd readout for a single array shows six DM volumes and their respective SD volumes.

9.1.3. For each array, you should see six DM volumes (two indexing and four capture) with their respective multipath SD volumes.

- Path States:
  - active | ready—Path is able to handle I/O requests.
  - shaky—Path is up but temporarily not available for normal operations.
  - faulty | failed—Path is unable to handle I/O requests.
  - ghost—Path is a passive path on an active/passive controller.
- DM Volume Size:

  Make a note of which DM volumes are index and which are capture

  - size=40T—Capture
  - size=15T—Index

9.1.4. If your readout does not look similar to Figure 38, restart the multipath daemon:

```
[root@HeadUnit ~] service multipathd restart
```

Note After you restart the multipath daemon, the order in which the volume numbers are displayed may change. This is expected behavior.

9.1.5. If the readout is similar to the following, you must wait until the disks have finished initializing before running multipathd again:

```
[root@HeadUnit ~]# multipath -ll
360080e500029f54000000427568d78d3 dm-0 ,
[size=15T][features=3 queue_if_no_path pg_init_retries 50][hwhandler=1 rdac][rw]
\_ round-robin 0 [prio=0][active]
\_ #:#:#:#  -   #:#   [failed][faulty]
\_ #:#:#:#  -   #:#   [active][faulty]
\_ round-robin 0 [prio=0][enabled]
\_ #:#:#:#  -   #:#   [active][faulty]
\_ #:#:#:#  -   #:#   [failed][faulty]
360080e500029f54000000430568d7b62 dm-5 ,
[size=40T][features=3 queue_if_no_path pg_init_retries 50][hwhandler=1 rdac][rw]
\_ round-robin 0 [prio=0][active]
\_ #:#:#:#  -   #:#   [failed][faulty]
\_ #:#:#:#  -   #:#   [active][faulty]
\_ round-robin 0 [prio=0][enabled]
\_ #:#:#:#  -   #:#   [active][faulty]
\_ #:#:#:#  -   #:#   [failed][faulty]
```

Figure 39: An unsuccessful multipathd readout indicates that the disks have not finished initializing.

Note As necessary, use the Troubleshooting Tools on page 46.

10. Reinstall Security Analytics Software

Now that the DM volumes are configured, the head unit is ready for a proper installation of Security Analytics that incorporates the indexing and capture drives. Use one of the following methods:

- Insert the USB key into the head unit, reboot, and then follow the conventional instructions on the console to install (not upgrade) Security Analytics software. This method overwrites all settings.
- Use the solera-reinstall script, which overwrites all settings except for the eth0 IP address and default gateway:

  ```
  cd /ds/upgrade
  mv Solera-7.1.10-99999-x86_64-DVD.iso Solera.iso
  /etc/utils/solera-reinstall.sh
  reboot
  ```

- Manually define the drives, which does not reinstall the software nor overwrite settings. Consult the multipathd readout to see which DMs are capture drives (x) and which are index (y).

  ```
  build-ds-capture dm-$x_1$ dm-$x_2$ dm-$x_3$ dm-$x_4$
  build-ds-index dm-$y_1$ dm-$y_2$
  reboot
  ```

  For example, a head unit that has three arrays attached will have 12 capture DMs and 6 index DMs:

  ```
  build-ds-capture dm-2 dm-3 dm-4 dm-5 dm-8 dm-9 dm-10 dm-11 dm-14 dm-15 dm-16
  dm-17
  build-ds-index dm-0 dm-1 dm-6 dm-7 dm-12 dm-13
  reboot
  ```

Note As soon as possible, upgrade to the latest version of Security Analytics.

11. Next Steps

After your Security Analytics appliance reboots, open the web UI, select Settings > Help > English, and click Initial Settings for help in licensing Security Analytics software.

For assistance with your appliance, contact:

- Symantec Support: support.symantec.com/en_US/contact-support.html
- Security Analytics Documentation: support.symantec.com/content/unifiedweb/en_US/Documentation.1145515.html

Appendix A: Disk-Group Configuration

Consult the table below for the disk-group configuration for a single storage array. If you have two or three storage arrays, configure each array exactly as specified in this table: all arrays should be identical.

	index0	index1	capture0	capture1	capture2	capture3	Hot Spares
Disks	5 disks	5 disks	12 disks	12 disks	12 disks	12 disks	2 disks
RAID Level	RAID 5	RAID 5	RAID 5	RAID 5	RAID 5	RAID 5	n/a
Parity Storage	8TB	8TB	16TB	16TB	16TB	16TB	n/a
Raw Space	16TB	16TB	48TB	48TB	48TB	48TB	8TB
Disk Group Capacity	14.533 TB	14.533 TB	39.966 TB	39.966 TB	39.966 TB	39.966 TB	7.45TB
Drawer,Slot Range	0,0 – 0,4	0,5 – 0,9	0,10 – 1,9	1,10 – 2,9	2,10 – 3,9	3,10 – 4,9	4,10 – 4,11

Appendix B: **Initial Head-Unit Configuration**

If your R630-HD was not purchased through Symantec, the head unit has not been properly configured. Follow these instructions to configure the R630-HD head unit with Security Analytics-specific settings.

B.1. Establish a Connection to the Head Unit

B.1.1 With the VGA cable, connect your monitor to the head unit.

B.1.2 Plug in the USB keyboard to the server.

B.2. Configure the BIOS Settings

B.2.1 Power on the head unit. While the head unit boots, watch for the following 8-bit menu items:

```
F2 = System Setup
Lifecycle Controller disabled
F11 = Boot Manager
F12 = PXE Boot
```

B.2.2 When these items are displayed, press F2 to enter the system setup. If you are prompted to install the Emulex BIOS drivers, press the S key to skip.

B.2.3 Click System BIOS and verify that these settings are configured as follows:

Page	Attribute	Value
Memory Settings	Memory Operating Mode	Optimizer Mode
Processor Settings	Virtualization Technology	Disabled
Serial Communication	Serial Port Address	Serial Device1=COM1,Serial Device 2=COM2
System Profile Settings	System Profile	Performance

B.2.4 Return to the main *System BIOS* page but do not exit.

B.2.5 On the main *System BIOS Settings* page click Boot Settings > BIOS Boot Settings > Hard-Disk Drive Sequence.

B.2.6 On the *Change Order* dialog, move the device that contains the Security Analytics ISO to the top of the boot-sequence list and click OK.

B.2.7 Press ESC until you return to the main *System BIOS Settings* page. Click Finish.

B.2.8 On the main *System Settings* page, click Finish to save and exit. The system reboots.

B.3. Optional—Configure the iDRAC Interface

The Integrated Dell Remote Access Control (iDRAC) interface is Dell’s version of the Intelligent Platform Management Interface (IPMI).

B.3.1 If you did not reboot the head unit in Step B.2.8, power on the head unit. While the head unit boots, watch for the following 8-bit menu items:

```
F2 = System Setup
Lifecycle Controller disabled
F11 = Boot Manager
F12 = PXE Boot
```

B.3.2 When these items are displayed, press F2 to enter the system setup. If you are prompted to install Emulex BIOS drivers, press the S key to skip.

B.3.3 From the System Setup Main Menu, select iDRAC Settings and configure the settings as follows:

Page	Attribute	Value
Network	Enable NIC	Enabled
	NIC Selection	Dedicated
	Failover Network	None
	Enable DHCP	[as desired]
	Enable IPv4 or IPv6	[as desired]
Lifecycle Controller	Collect System Inventory on Restart	Disabled
User Configuration	User Name	[as desired]
	Change Password	[as desired]

Note If you choose to enable DHCP for the iDRAC interface, it is recommended that you use the DHCP reservation feature of your DHCP server to statically map the MAC address of the iDRAC interface to an IP address.

B.3.4 Click Finish at the lower-right of the screen and follow the prompts to save and exit.

B.4. Enable Disk Encryption on the Head Unit

With disk encryption enabled, a hard drive that is physically removed from a head unit cannot be read unless the encryption key is provided.

IMPORTANT

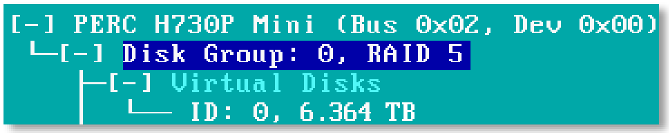
- Enabling disk encryption is optional but highly recommended.
- It is also possible to enable encryption on a virtual disk **after** it has been created.

B.4.1 If you did not reboot the system in Step B.2.8, reboot the system now. While the head unit boots, watch for the following 8-bit menu items:

```
F2 = System Setup
Lifecycle Controller disabled
F11 = Boot Manager
F12 = PXE Boot

Initializing Intel(R) Boot Agent GE v.1.5.73
PXE 2.1 Build 092 (WfM 2.0)



PowerEdge Expandable RAID Controller BIOS
Copyright (c) 2015 Avago Corporation
Press <Ctrl><R> to Run Configuration Utility
HA -0 (Bus 2 Dev 0) PERC H730P Mini
FW package: 25.3.0-0016
```

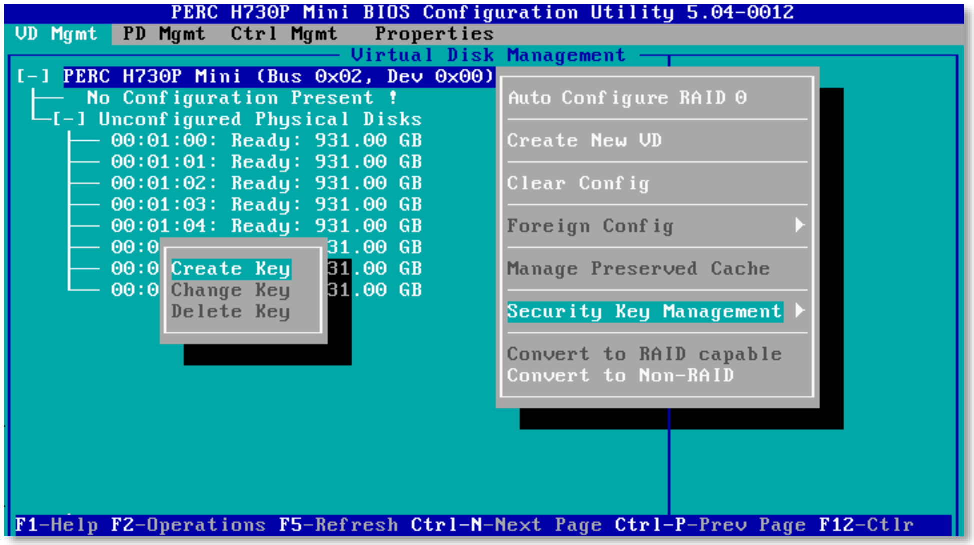
B.4.2 When you see this screen, press Ctrl+R to enter the RAID configuration utility. If you are prompted to install the Emulex BIOS drivers, press the S key to skip. The *Virtual Disk Management* screen is displayed.

B.4.3 Does Disk Group: 0, RAID 5 already exist?



```
[-] PERC H730P Mini (Bus 0x02, Dev 0x00)
 └─[-] Disk Group: 0, RAID 5
     ├─[-] Virtual Disks
     │   └── ID: 0, 6.364 TB
```

Yes — Select the disk group and press F2.	No — Select PERC H730P Mini and press F2.

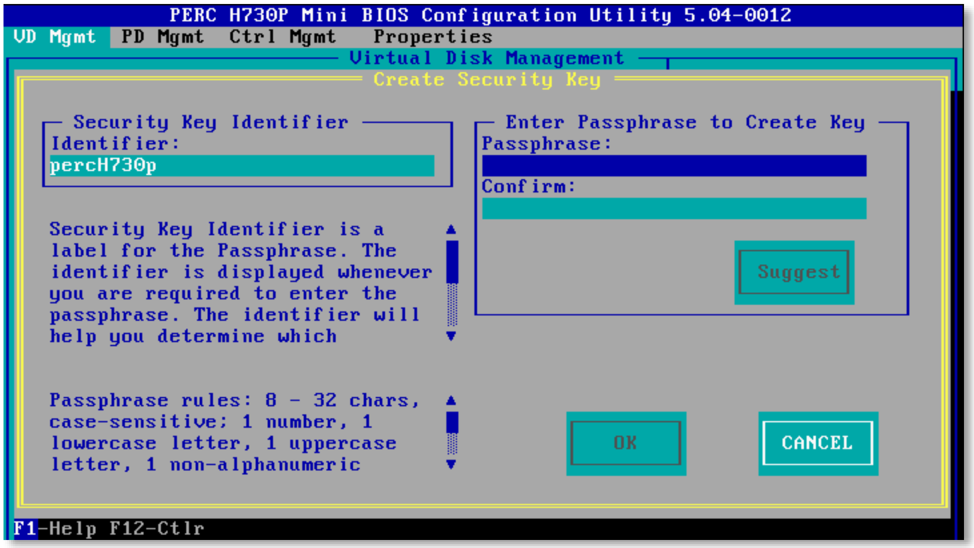


```
            PERC H730P Mini BIOS Configuration Utility 5.04-0012
VD Mgmt  PD Mgmt  Ctrl Mgmt   Properties
                            Virtual Disk Management
[-] PERC H730P Mini (Bus 0x02, Dev 0x00)   Auto Configure RAID 0
  ├── No Configuration Present !            Create New VD
  └[-] Unconfigured Physical Disks          Clear Config
      ├── 00:01:00: Ready: 931.00 GB        Foreign Config          ►
      ├── 00:01:01: Ready: 931.00 GB        Manage Preserved Cache
      ├── 00:01:02: Ready: 931.00 GB        Security Key Management ►
      ├── 00:01:03: Ready: 931.00 GB        Convert to RAID capable
      ├── 00:01:04: Ready: 931.00 GB        Convert to Non-RAID
      ├── 00:0                31.00 GB
      ├── 00:0 Create Key     31.00 GB
      └── 00:0 Change Key     31.00 GB
               Delete Key
F1-Help F2-Operations F5-Refresh Ctrl-N-Next Page Ctrl-P-Prev Page F12-Ctlr
```

Figure 40: Creating a Security Key

B.4.4 Select Security Key Management and press Enter.

B.4.5 Select Create Key and press Enter to open the *Create Security Key* dialog.



```
            PERC H730P Mini BIOS Configuration Utility 5.04-0012
VD Mgmt  PD Mgmt  Ctrl Mgmt   Properties
                            Virtual Disk Management
                              Create Security Key
  ┌ Security Key Identifier ──────┐   ┌ Enter Passphrase to Create Key ┐
  │Identifier:                    │   │Passphrase:                      │
  │percH730p                      │   │                                 │
  └───────────────────────────────┘   │Confirm:                         │
                                      │                                 │
  Security Key Identifier is a     ▲  │                      [Suggest]  │
  label for the Passphrase. The       └─────────────────────────────────┘
  identifier is displayed whenever
  you are required to enter the
  passphrase. The identifier will
  help you determine which         ▼

  Passphrase rules: 8 - 32 chars,  ▲
  case-sensitive; 1 number, 1               [  OK  ]     [CANCEL]
  lowercase letter, 1 uppercase
  letter, 1 non-alphanumeric       ▼
F1-Help F12-Ctlr
```

Figure 41: Specifying the Security Key Identifier and Passphrase

B.4.6 For the Security Key Identifier, specify a unique name for the security key.

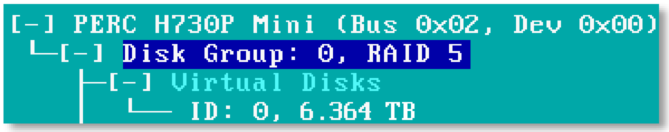
B.4.7 Enter the passphrase twice. The passphrase will be legible in both fields.

IMPORTANT

- There is no passphrase backup option when you create a security key on the R630-HD. If you lose the passphrase you will lose all encrypted data.
- Follow standard key-maintenance practices by manually recording the identifier and passphrase, and by keeping a copy of that information in a separate location.
- See KB article SLN164101 on Dell.com for more information.

B.4.8 Select OK and press Enter to return to the *Virtual Disk Management* screen.

B.4.9 Does Disk Group: 0, RAID 5 already exist?



```
[-] PERC H730P Mini (Bus 0x02, Dev 0x00)
 └─[-] Disk Group: 0, RAID 5
     ├─[-] Virtual Disks
     │    └── ID: 0, 6.364 TB
```

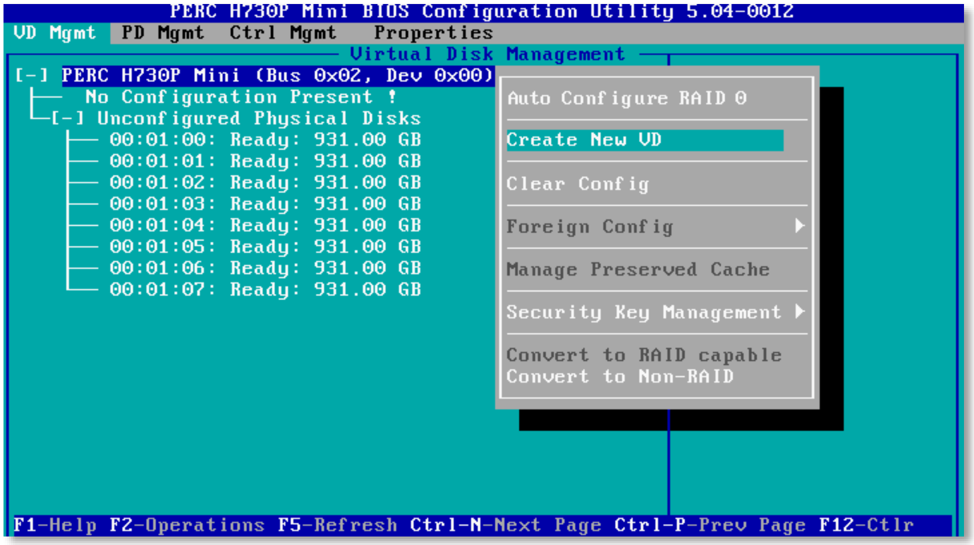
Yes — Return to *Step 3.4: Choose a Management Topology* on page 13 and continue the procedure.	No — Continue the procedure.

B.5. Configure the RAID Array

Follow these steps to configure the system array that comprises all of the disks on the head unit.

B.5.1 If you are not on the *Virtual Disk Management* screen, press F12.

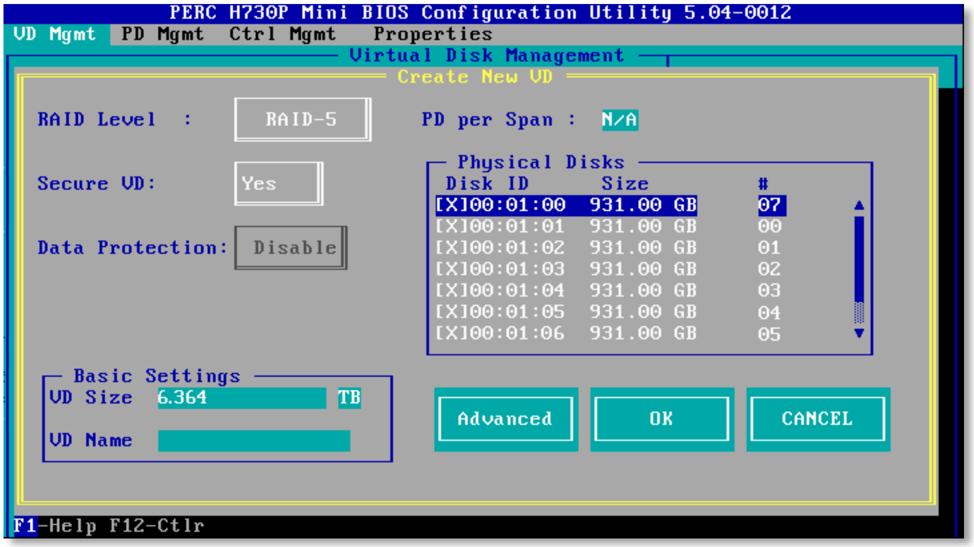
B.5.2 Select PERC H730P Mini and press F2.



```
                PERC H730P Mini BIOS Configuration Utility 5.04-0012
VD Mgmt  PD Mgmt  Ctrl Mgmt   Properties
                            Virtual Disk Management
[-] PERC H730P Mini (Bus 0x02, Dev 0x00)
 ├── No Configuration Present !
 └─[-] Unconfigured Physical Disks
     ├── 00:01:00: Ready: 931.00 GB
     ├── 00:01:01: Ready: 931.00 GB
     ├── 00:01:02: Ready: 931.00 GB
     ├── 00:01:03: Ready: 931.00 GB
     ├── 00:01:04: Ready: 931.00 GB
     ├── 00:01:05: Ready: 931.00 GB
     ├── 00:01:06: Ready: 931.00 GB
     └── 00:01:07: Ready: 931.00 GB
```

Figure 42: Selecting Create New VD

B.5.3 Select Create New VD and press Enter to open the *Create New VD* dialog.



```
PERC H730P Mini BIOS Configuration Utility 5.04-0012
VD Mgmt  PD Mgmt  Ctrl Mgmt   Properties
                    Virtual Disk Management
                        Create New VD

RAID Level   :    RAID-5          PD per Span :  N/A

Secure VD:        Yes             Physical Disks
                                   Disk ID       Size          #
                                  [X]00:01:00   931.00 GB     07
                                  [X]00:01:01   931.00 GB     00
Data Protection:  Disable         [X]00:01:02   931.00 GB     01
                                  [X]00:01:03   931.00 GB     02
                                  [X]00:01:04   931.00 GB     03
                                  [X]00:01:05   931.00 GB     04
                                  [X]00:01:06   931.00 GB     05

  Basic Settings
 VD Size   6.364          TB      Advanced     OK     CANCEL

 VD Name

F1-Help F12-Ctlr
```

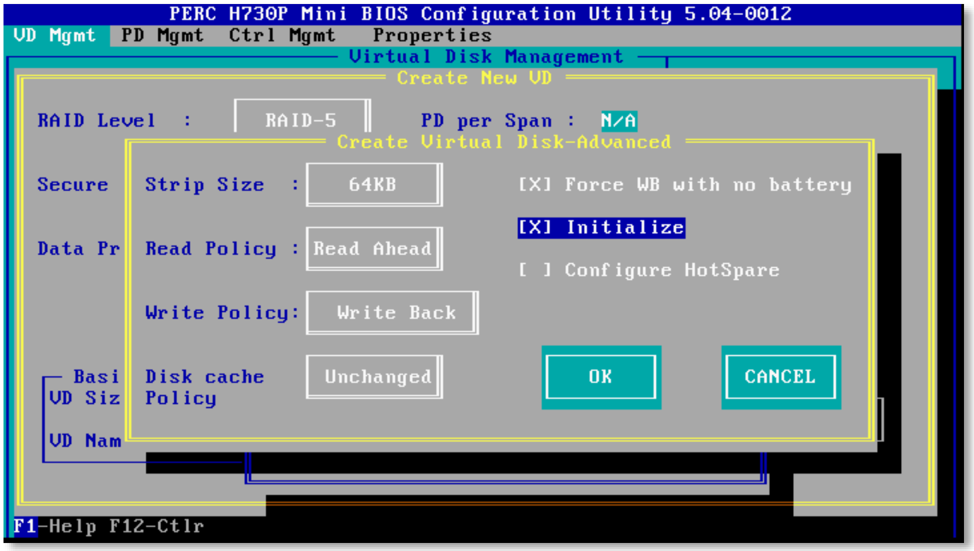
Figure 43: Selecting All Available Disks for the RAID-5 Virtual Disk

B.5.4 For RAID Level select RAID-5.

B.5.5 If available, for Secure VD select Yes.

B.5.6 Under Physical Disks use the arrow keys to highlight *every* Disk ID and press Enter to select.

B.5.7 Select Advanced and press Enter to open the *Create Virtual Disk—Advanced* dialog.



```
PERC H730P Mini BIOS Configuration Utility 5.04-0012
VD Mgmt  PD Mgmt  Ctrl Mgmt   Properties
                    Virtual Disk Management
                        Create New VD

RAID Level   :    RAID-5          PD per Span :  N/A
                    Create Virtual Disk-Advanced
Secure     Strip Size   :    64KB         [X] Force WB with no battery

Data Pr    Read Policy  :  Read Ahead     [X] Initialize

                                          [ ] Configure HotSpare
           Write Policy:    Write Back

  Basi     Disk cache      Unchanged          OK        CANCEL
 VD Siz    Policy

 VD Nam

F1-Help F12-Ctlr
```

Figure 44: Advanced Options for the Virtual Disk

B.5.8 Select the Force WB with no battery and Initialize options, and then select OK.

B.5.9 Select OK again.

B.5.10 Attach the Security Analytics ISO to the server (USB key or DVD drive).

B.5.11 Reboot the head unit by pressing the power button or by pressing `Ctrl+Alt+Delete`.

B.5.12 At the *Welcome* screen, select `Install Security Analytics` and press `Enter`. The installation begins.

B.5.13 When the *Complete* screen is displayed, remove the drive and press `Enter` to reboot.

B.5.14 Return to *Step 3.4: Choose a Management Topology* on page 13 and continue the procedure.

Appendix C: Troubleshooting Tools

Use the following tools to aid in troubleshooting the setup.

`multipath -v6`

Verbose output for multipath.

```
Feb 27 17:46:53 | Discover device /sys/block/ram0
Feb 27 17:46:53 | ram0: device node name blacklisted
Feb 27 17:46:53 | Discover device /sys/block/ram1
Feb 27 17:46:53 | ram1: device node name blacklisted
Feb 27 17:46:53 | Discover device /sys/block/ram2
Feb 27 17:46:53 | ram2: device node name blacklisted
Feb 27 17:46:53 | Discover device /sys/block/ram3
Feb 27 17:46:53 | ram3: device node name blacklisted
Feb 27 17:46:53 | Discover device /sys/block/ram4
Feb 27 17:46:53 | ram4: device node name blacklisted
....
Feb 27 17:46:53 | Discover device /sys/block/ram10
Feb 27 17:46:53 | ram10: device node name blacklisted
Feb 27 17:46:53 | Discover device /sys/block/ram11
Feb 27 17:46:53 | ram11: device node name blacklisted
Feb 27 17:46:53 | Discover device /sys/block/ram12
Feb 27 17:46:53 | ram12: device node name blacklisted
Feb 27 17:46:53 | Discover device /sys/block/ram13
Feb 27 17:46:53 | ram13: device node name blacklisted
Feb 27 17:46:53 | Discover device /sys/block/ram14
Feb 27 17:46:53 | ram14: device node name blacklisted
Feb 27 17:46:53 | Discover device /sys/block/ram15
Feb 27 17:46:53 | ram15: device node name blacklisted
Feb 27 17:46:53 | Discover device /sys/block/sda
Feb 27 17:46:53 | sda: device node name blacklisted
Feb 27 17:46:53 | Discover device /sys/block/sdb
Feb 27 17:46:53 | sdb: device node name blacklisted
Feb 27 17:46:53 | Discover device /sys/block/sdc
Feb 27 17:46:53 | sdc: device node name blacklisted
Feb 27 17:46:53 | Discover device /sys/block/sdd
Feb 27 17:46:53 | sdd: device node name blacklisted
Feb 27 17:46:53 | Discover device /sys/block/sde
Feb 27 17:46:53 | sde: device node name blacklisted
Feb 27 17:46:53 | Discover device /sys/block/sdf
Feb 27 17:46:53 | sdf: device node name blacklisted
Feb 27 17:46:53 | Discover device /sys/block/sdg
Feb 27 17:46:53 | sdg: device node name blacklisted
Feb 27 17:46:53 | Discover device /sys/block/sdh
Feb 27 17:46:53 | sdh: device node name blacklisted
Feb 27 17:46:53 | Discover device /sys/block/sdi
Feb 27 17:46:53 | sdi: device node name blacklisted
Feb 27 17:46:53 | Discover device /sys/block/sdj
Feb 27 17:46:53 | sdj: device node name blacklisted
Feb 27 17:46:53 | Discover device /sys/block/sdk
Feb 27 17:46:53 | sdk: device node name blacklisted
Feb 27 17:46:53 | Discover device /sys/block/sdl
Feb 27 17:46:53 | sdl: device node name blacklisted
Feb 27 17:46:53 | Discover device /sys/block/sdm
Feb 27 17:46:53 | sdm: device node name blacklisted
Feb 27 17:46:53 | Discovery status 0
===== no paths =====
Feb 27 17:46:53 | libdevmapper: ioctl/libdm-iface.c(1606): dm names   NF   [16384]
```

`fdisk -l`

Lists file-system partitions.

```
Disk /dev/sda: 6997.5 GB, 6997575467008 bytes
255 heads, 63 sectors/track, 850740 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Disk identifier: 0x00000000

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1               1      267350  2147483647+  ee  GPT

Disk /dev/sdb: 15979.5 GB, 15979518099456 bytes
255 heads, 63 sectors/track, 1942732 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Disk identifier: 0x00000000


Disk /dev/sdc: 15979.5 GB, 15979518099456 bytes
255 heads, 63 sectors/track, 1942732 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Disk identifier: 0x00000000


...


Disk /dev/sdh: 15979.5 GB, 15979518099456 bytes
255 heads, 63 sectors/track, 1942732 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Disk identifier: 0x00000000


Disk /dev/sdi: 15979.5 GB, 15979518099456 bytes
255 heads, 63 sectors/track, 1942732 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Disk identifier: 0x00000000


Disk /dev/sdj: 43943.6 GB, 43943674773504 bytes
255 heads, 63 sectors/track, 5342514 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Disk identifier: 0x00000000


Disk /dev/sdk: 43943.6 GB, 43943674773504 bytes
255 heads, 63 sectors/track, 5342514 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Disk identifier: 0x00000000


Disk /dev/sdl: 43943.6 GB, 43943674773504 bytes
255 heads, 63 sectors/track, 5342514 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Disk identifier: 0x00000000


Disk /dev/sdm: 43943.6 GB, 43943674773504 bytes
255 heads, 63 sectors/track, 5342514 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Disk identifier: 0x00000000
```

lsmod

Lists currently loaded modules.

```
Module                  Size  Used by
vfat                    9831  0
fat                    47903  1 vfat
usb_storage            35400  0
coretemp                4448  0
hwmon_vid               3068  0
i2c_i801                7942  0
i2c_core               16988  1 i2c_i801
nf_conntrack_ipv4       9777  1
nf_defrag_ipv4          1179  1 nf_conntrack_ipv4
xt_state                1135  1
nf_conntrack           47130  2 nf_conntrack_ipv4,xt_state
xt_tcpudp               2247  14
iptable_filter          1120  1
ip_tables               9499  1 iptable_filter
x_tables               12726  4 xt_state,xt_tcpudp,iptable_filter,ip_tables
autofs4                22476  2
ipmi_devintf            5478  0
ipmi_si                41131  0
ipmi_msghandler        31233  2 ipmi_devintf,ipmi_si
sunrpc                187609  1
ext4                  270778  1
jbd2                   49591  1 ext4
crc16                   1201  1 ext4
dm_mirror              13193  0
dm_region_hash          6688  1 dm_mirror
dm_log                  8296  2 dm_mirror,dm_region_hash
dm_multipath           15813  0
scsi_dh                 4649  1 dm_multipath
lpfc                  620163  0
scsi_transport_fc      40506  1 lpfc
tpm_tis                 8568  0
tpm                    11955  1 tpm_tis
tpm_bios                4801  1 tpm
rtc_cmos                8374  0
acpi_power_meter        9128  0
hwmon                   1233  2 coretemp,acpi_power_meter
button                  4079  0
megaraid_sas           73252  6
uhci_hcd               22363  0
ohci_hcd               21094  0
ehci_hcd               43037  0
```

Appendix D: **Switch-Port Sizing**

For each hardware unit, the following number of switch ports is required:

- Head Unit—Two ports per switch
- Storage Array—Four ports per switch
- SFP+ Transceivers—For each switch port, one 16 Gb SFP+ transceiver is required.

Consult the table below for hardware requirements:

Head Units	Arrays per HU	Ports per Switch	Total SFP+ Modules	Zones per Switch	Brocade Models	Link to Diagram
1	1*	6	12	2	6505, 6510	1 Head Unit : 1 Array
1	2*	10	20	2	6505, 6510	1 Head Unit : 2 Arrays
1	3	14	28	2	6505, 6510	1 Head Unit : 3 Arrays
2	1*	12	24	4	6505, 6510	2 Head Units : 1 Array Each
2	2*	20	40	4	6505, 6510	2 Head Units : 2 Arrays Each
2	3	28	56	4	6510	2 Head Units : 3 Arrays Each
3	1*	18	36	6	6505, 6510	3 Head Units : 1 Array Each
3	2*	30	60	6	6510	3 Head Units : 2 Arrays Each
3	3	42	84	6	6510	3 Head Units : 3 Arrays Each

* Using Fibre Channel switches for this number of arrays is optional.

Appendix E: Supported Hardware Configurations

Consult these sections to see the hardware combinations and configurations that are supported by Symantec Security Analytics. In the examples to follow, port numbers on HBAs are designated as shown in Figure 45:

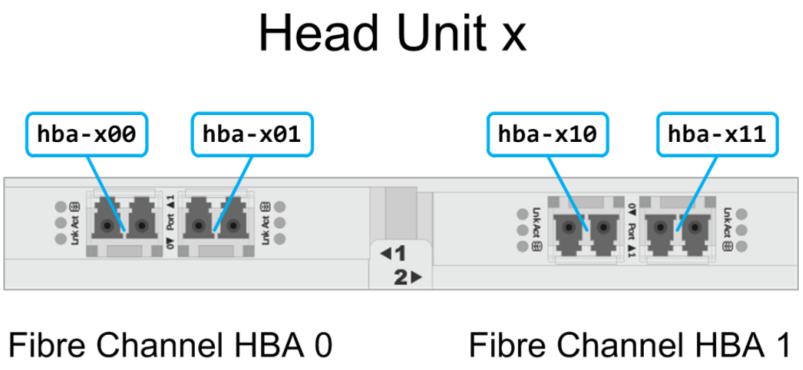


Figure 45: HBA Port-Designation Convention

example

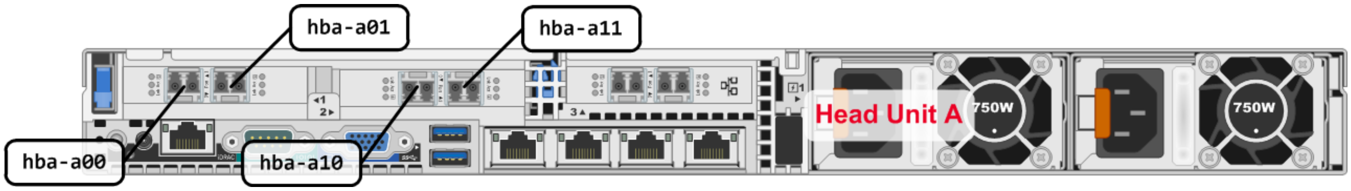


Figure 46: Port Designators for Head Unit A

For the ports on Storage Array n that is connected to Head Unit x, the designations are as follows:

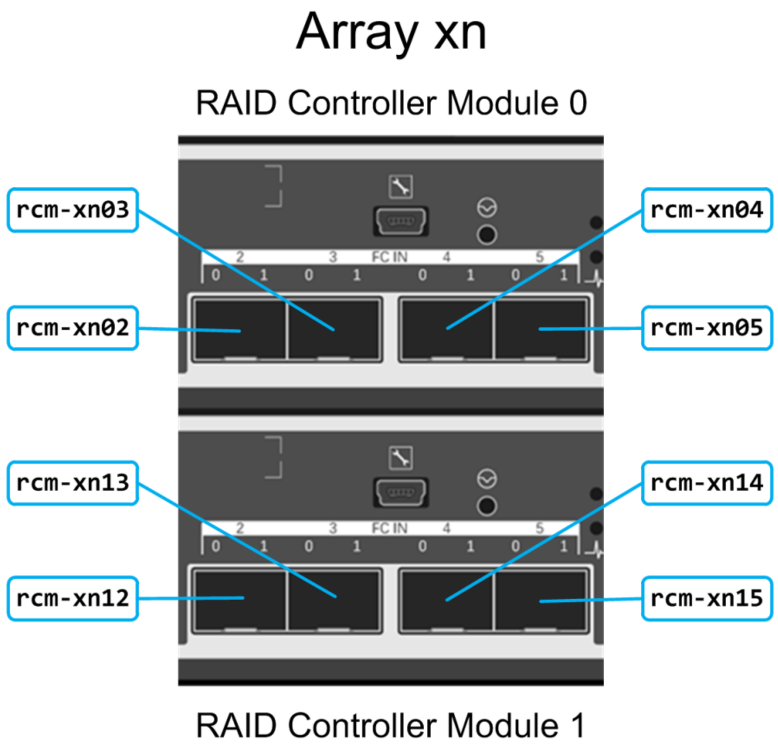


Figure 47: Storage Array Port-Designation Conventions

example

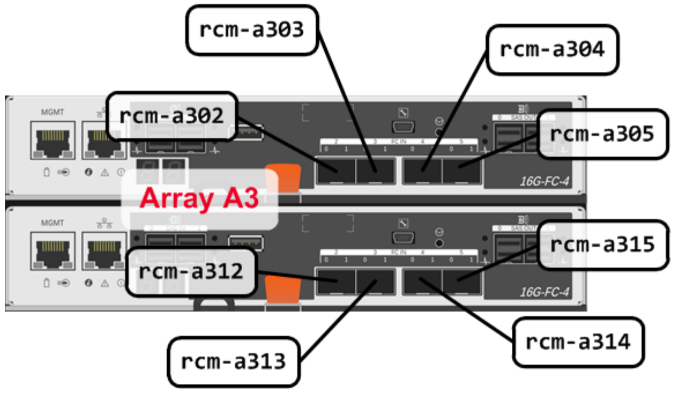


Figure 48: Port Designators for Array A3, connected to Head Unit A

E.1. One Head Unit, One Array

For one head unit with one array, you can use point-to-point connections or Fibre Channel switches.

1:1 — Point-to-Point

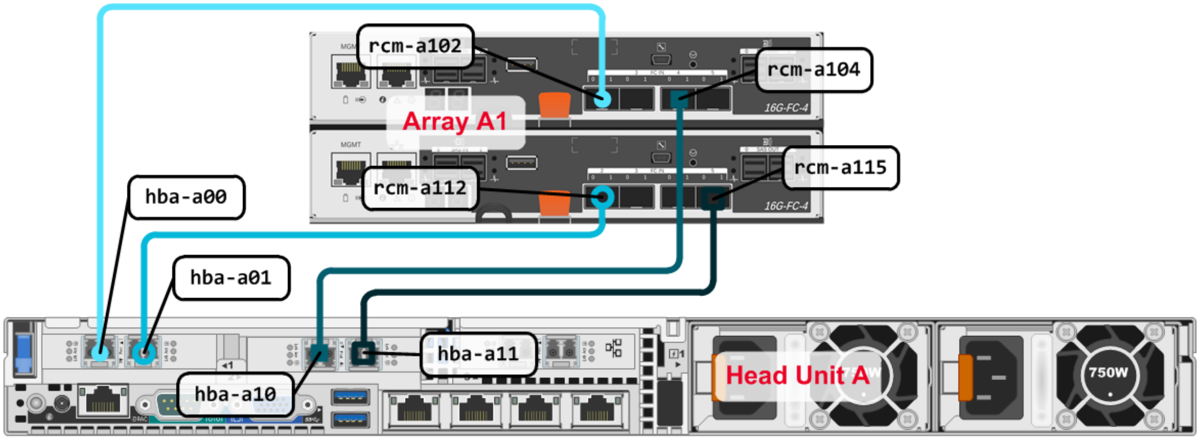


Figure 49: One Head Unit Connected to One Storage Array via Point-to-Point Connections

Note It is not important which of the four ports on the RAID controller modules is used as long as each HBA on the head unit is connected to both modules.

Consult this table for the connections shown in Figure 49.

Connector	HBA x	Array x1
⊔	hba-a00	rcm-a102
⊔	hba-a01	rcm-a112
⊔	hba-a10	rcm-a104
⊔	hba-a11	rcm-a115

1:1 — Fibre Channel Switches

When one head unit writes to only one array, connecting through Fibre Channel switches is optional.

Head Units	Total Arrays	Ports per Switch	Total SFP+	Total Switch Zones	Brocade Models
1	1	6	12	4	6505, 6510

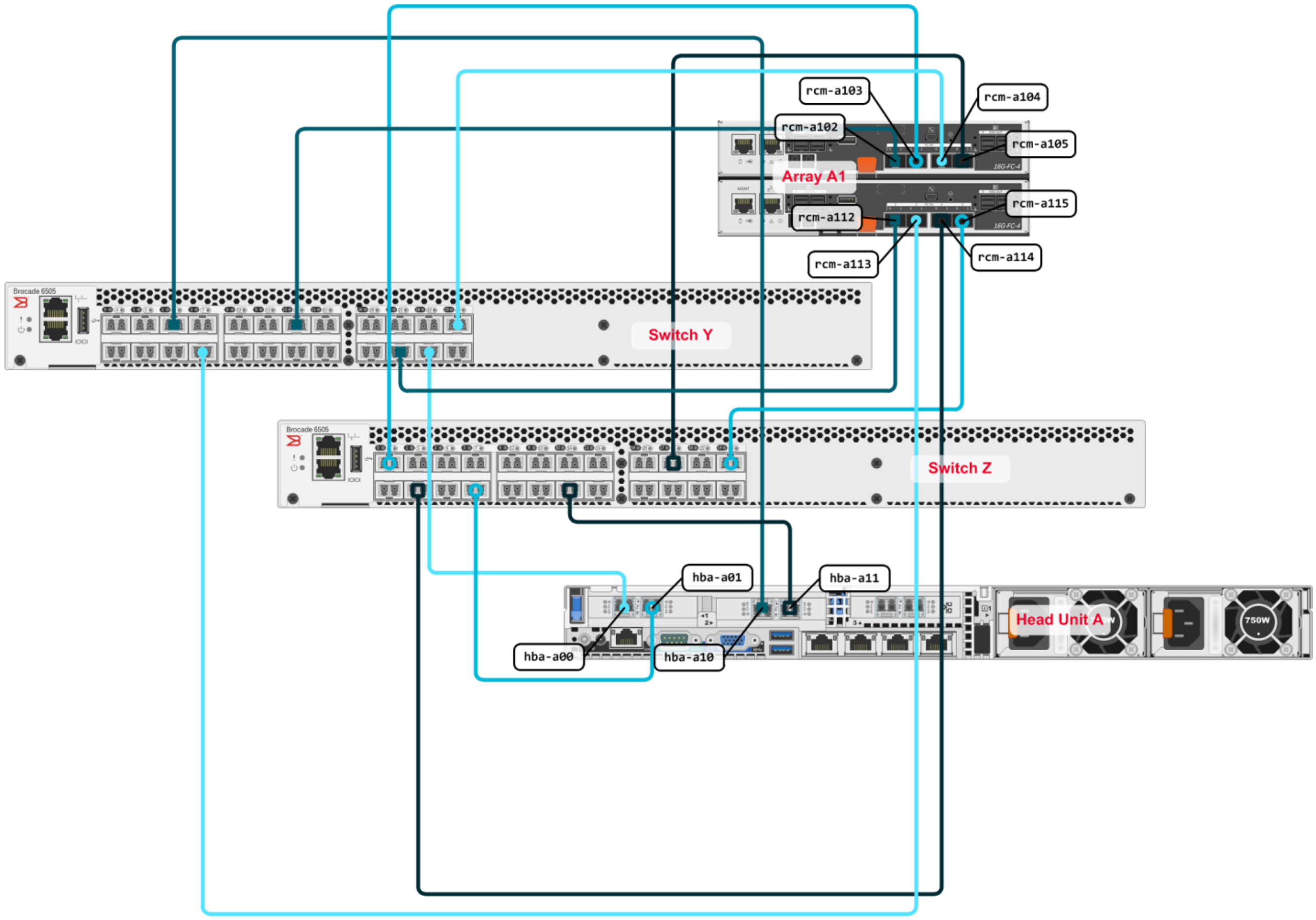


Figure 50: One Head Unit Connected to One Storage Array Through Redundant Brocade 6505 24-Port Fibre Channel Switches

Consult this table for the device ID assignments for the switch zones in Figure 50.

Switch	Zone	Connector	HBA x	Array x1
Y	1	⊔	hba-a00	rcm-a104 rcm-a113
Z	2	⊔	hba-a01	rcm-a103 rcm-a115
Y	3	⊔	hba-a10	rcm-a102 rcm-a112
Z	4	⊔	hba-a11	rcm-a105 rcm-a114

E.2. One Head Unit, Two Arrays

For one head unit with two arrays, use point-to-point connections or redundant Fibre Channel switches.

1:2 — Point-to-Point

IMPORTANT This cabling method is not redundant and therefore is vulnerable to failure.

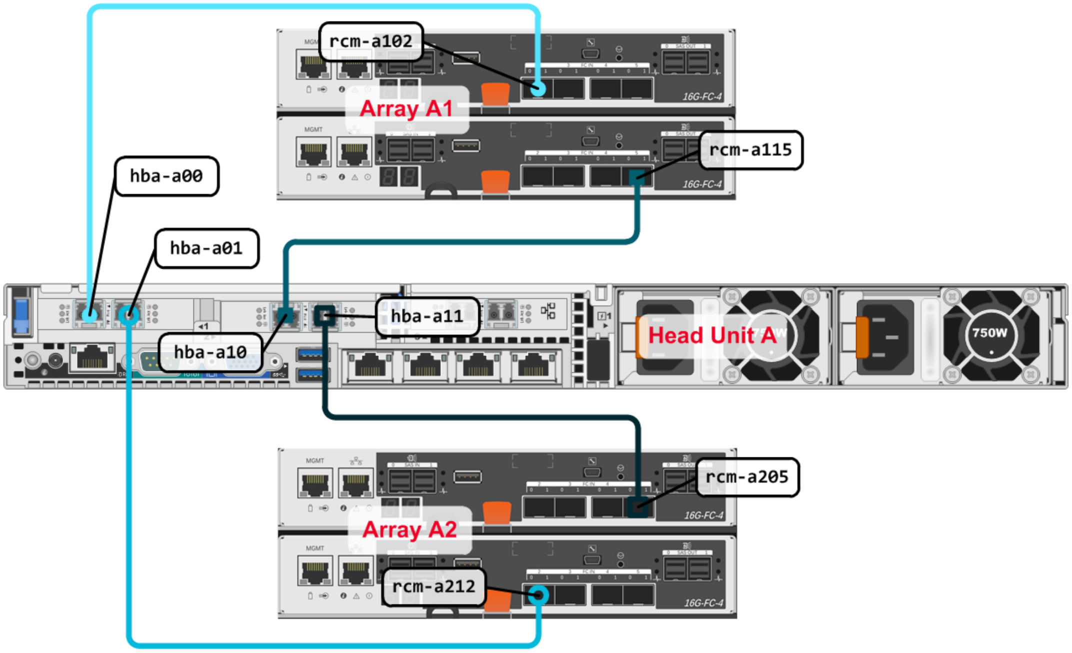
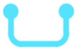
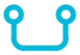
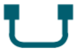
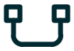


Figure 51: One Head Unit Connected to Two Storage Arrays via Point-to-Point Connections

Note It is not important which of the ports on the RAID controller modules is used as long as each HBA on the head unit is connected to both modules.

Consult this table for the connections in Figure 51.

Connector	HBA x	Array x1	Array x2
	hba-a00	rcm-a102	n/a
	hba-a01	n/a	rcm-a212
	hba-a10	rcm-a104	n/a
	hba-a11	n/a	rcm-a205

1:2 — Fibre Channel Switches

When one head unit writes to only two arrays, connecting through Fibre Channel switches is optional.

Head Units	Total Arrays	Ports per Switch	Total SFP+	Total Switch Zones	Brocade Models
1	2	10	20	4	6505, 6510

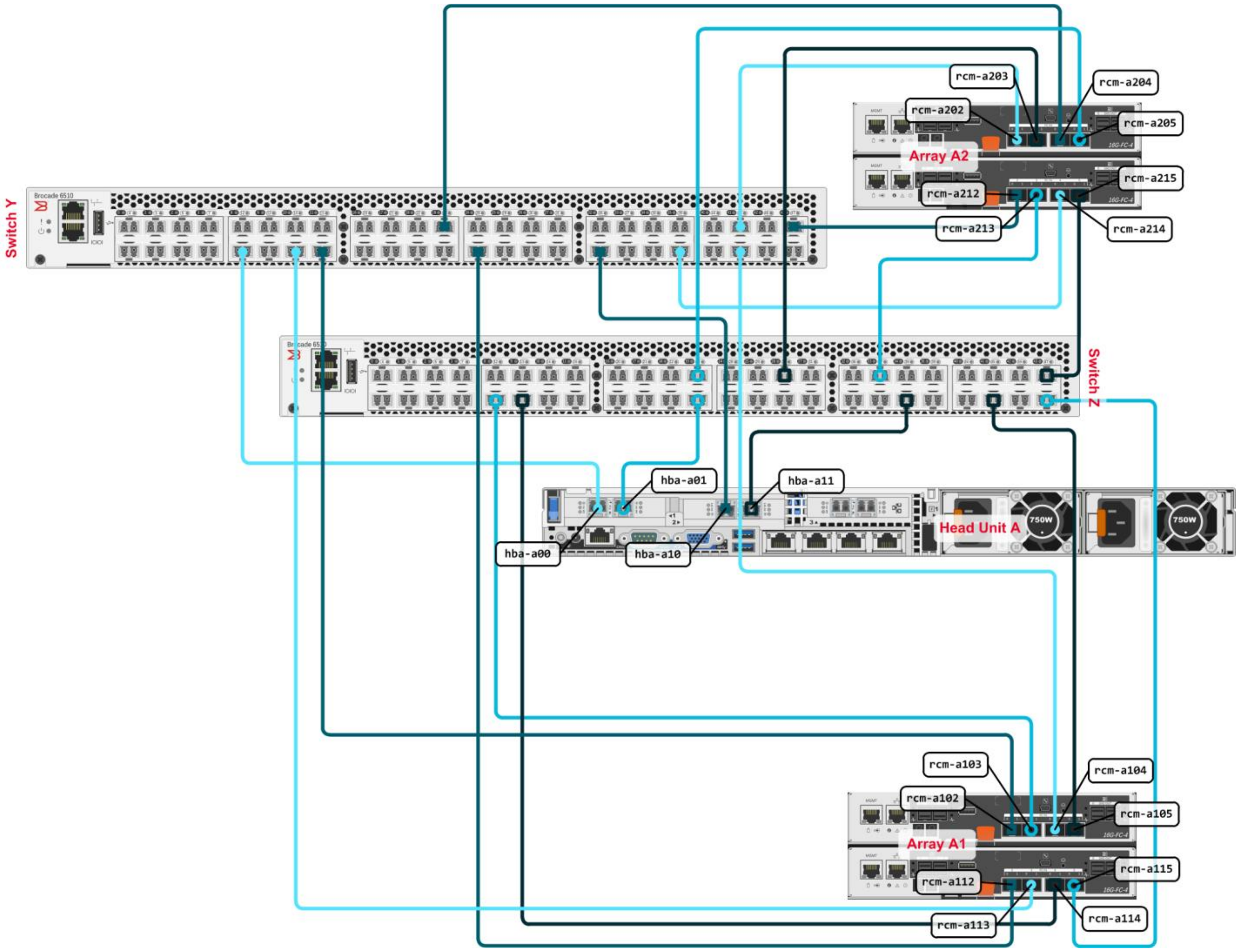
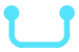
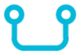
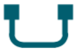
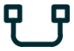


Figure 52: One Head Unit Connected to Two Storage Arrays, Through Redundant Brocade 6510 48-Port Fibre Channel Switches

Consult this table for the device ID assignments for the switch zones in Figure 52 on the previous page.

Switch	Zone	Connector	HBA x	Array x1	Array x2
Y	1		hba-a00	rcm-a104 rcm-a113	rcm-a202 rcm-a214
Z	2		hba-a01	rcm-a103 rcm-a115	rcm-a205 rcm-a213
Y	3		hba-a10	rcm-a102 rcm-a112	rcm-a204 rcm-a212
Z	4		hba-a11	rcm-a105 rcm-a114	rcm-a203 rcm-a215

E.3. One Head Unit, Three Arrays

When a head unit writes to three arrays, connecting through Fibre Channel switches is mandatory.

Head Units	Total Arrays	Ports per Switch	Total SFP+	Total Switch Zones	Brocade Models
1	3	14	28	4	6505, 6510

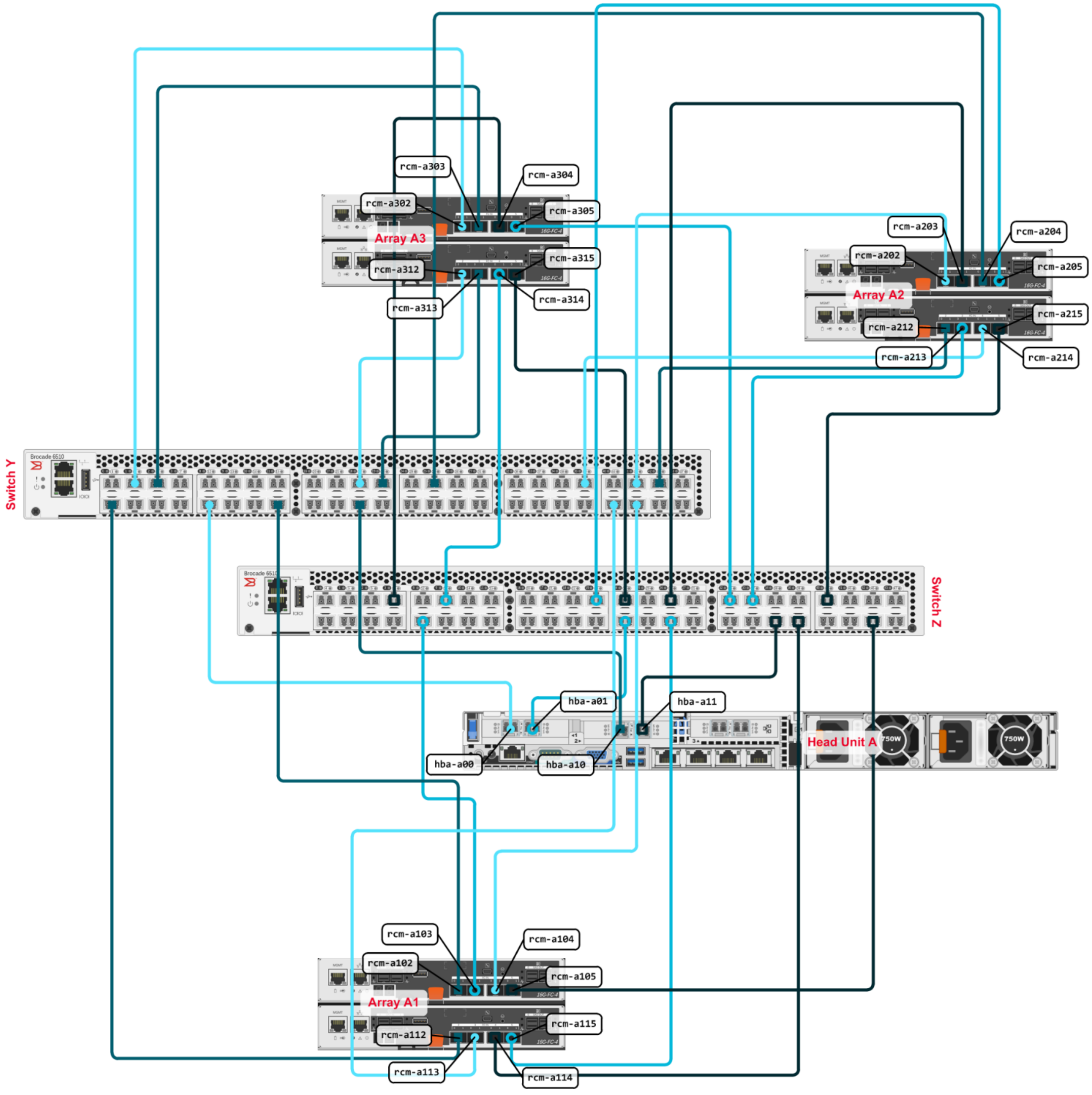
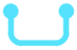
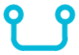
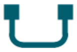
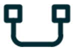


Figure 53: One Head Unit Connected to Three Storage Arrays, Through Redundant Brocade 6510 48-Port Fibre Channel Switches

Consult this table for the device ID assignments for the switch zones in Figure 53 on the previous page.

Switch	Zone	Connector	HBA x	Array x1	Array x2	Array x3
Y	1		hba-a00	rcm-a104 rcm-a113	rcm-a202 rcm-a214	rcm-a303 rcm-a312
Z	2		hba-a01	rcm-a103 rcm-a115	rcm-a205 rcm-a213	rcm-a305 rcm-a314
Y	3		hba-a10	rcm-a102 rcm-a112	rcm-a204 rcm-a212	rcm-a303 rcm-a313
Z	4		hba-a11	rcm-a105 rcm-a114	rcm-a203 rcm-a215	rcm-a304 rcm-a315

E.4. Two Head Units, One Array Each

Because each head unit writes to only one array, you can use the point-to-point connections shown in One Head Unit, One Array on page 52, instead of connecting to the arrays through Fibre Channel switches.

Head Units	Total Arrays	Ports per Switch	Total SFP+	Total Switch Zones	Brocade Models
2	2	12	24	4	6505, 6510

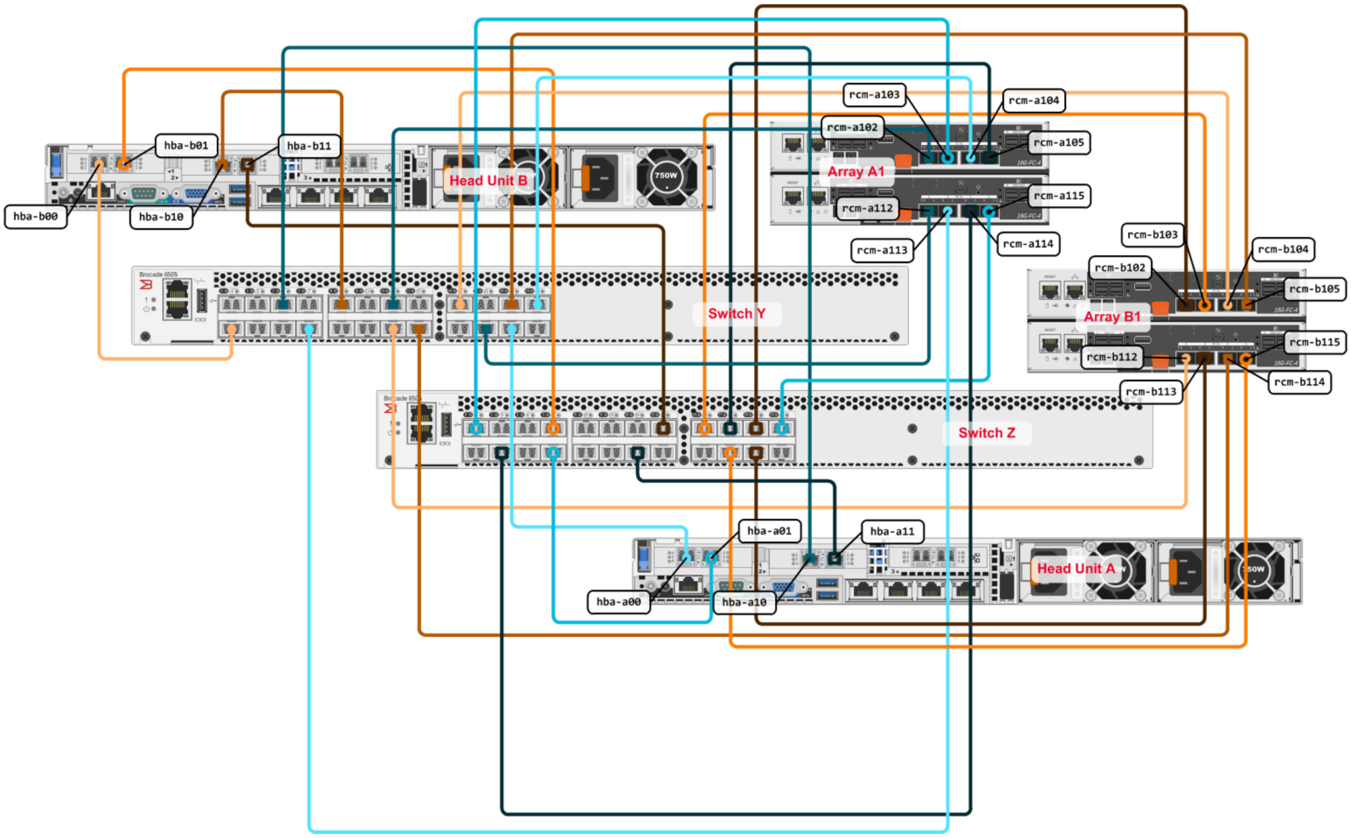
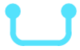
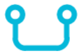
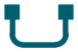
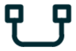
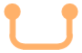
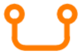
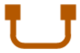
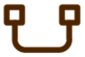


Figure 54: **Two Head Units Connected to One Storage Array Each, Through Redundant Brocade 6505 24-Port Fibre Channel Switches**

Consult this table for the device ID assignments for the switch zones in Figure 54 on the previous page.

Switch	Zone	Connector	HBA x	Array x1
Y	1		hba-a00	rcm-a104 rcm-a113
Z	2		hba-a01	rcm-a103 rcm-a115
Y	3		hba-a10	rcm-a102 rcm-a112
Z	4		hba-a11	rcm-a105 rcm-a114
Y	5		hba-b00	rcm-b104 rcm-b112
Z	6		hba-b01	rcm-b103 rcm-b115
Y	7		hba-b10	rcm-b105 rcm-b114
Z	8		hba-b11	rcm-b102 rcm-b113

E.5. Two Head Units, Two Arrays Each

Because each head unit writes to only two arrays, you can use the point-to-point connections shown in One Head Unit, Two Arrays on page 54, instead of connecting to the arrays through Fibre Channel switches.

Head Units	Total Arrays	Ports per Switch	Total SFP+	Total Switch Zones	Brocade Models
2	4	20	40	8	6505, 6510

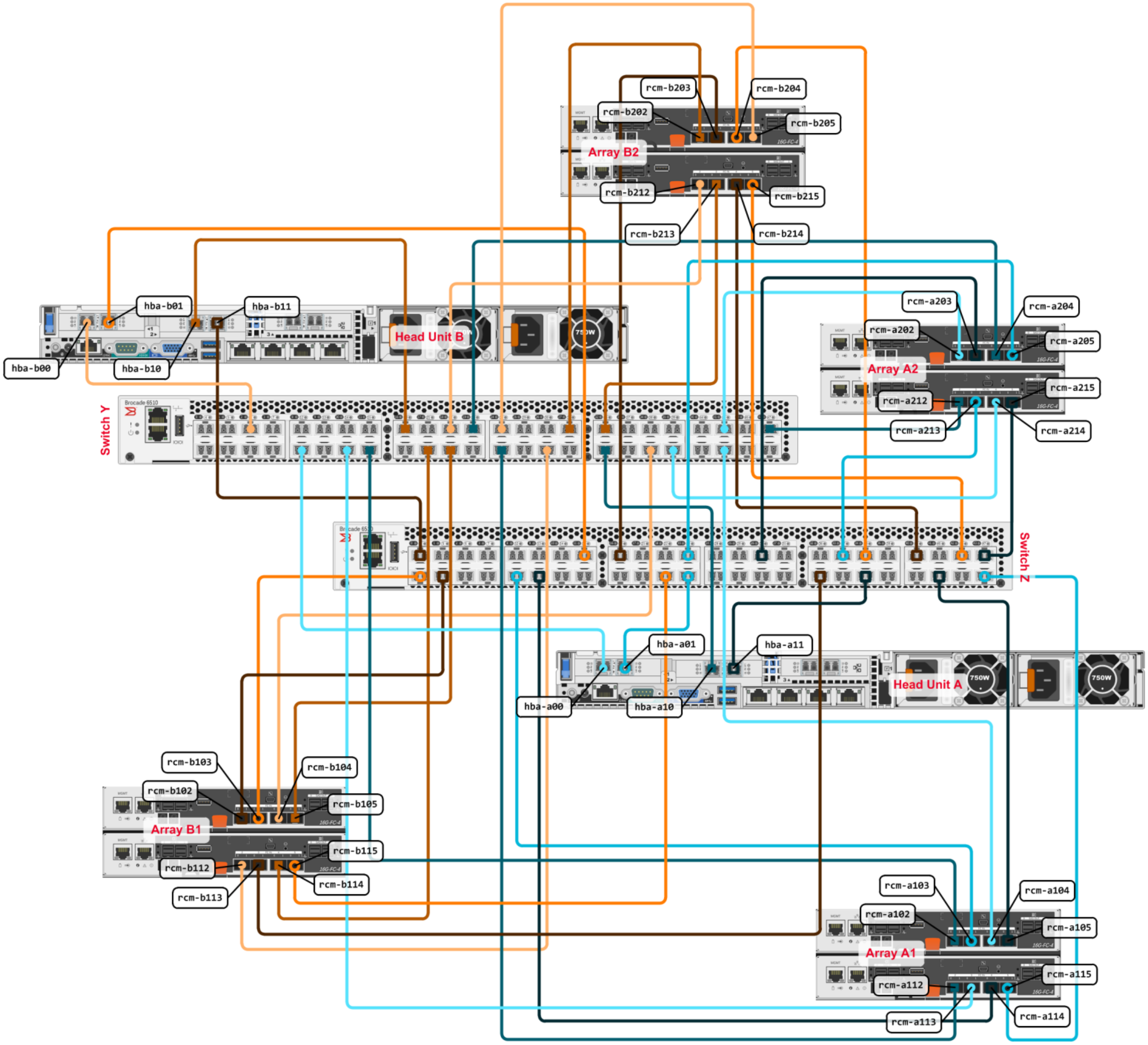


Figure 55: Two Head Units Connected to Two Storage Arrays Each, Through Redundant Brocade 6510 48-Port Fibre Channel Switches

Consult this table for the device ID assignments for the switch zones in Figure 55 on the previous page.

Switch	Zone	Connector	HBA x	Array x1	Array x2
Y	1	⊔	hba-a00	rcm-a104 rcm-a113	rcm-a202 rcm-a214
Z	2	⊔	hba-a01	rcm-a103 rcm-a115	rcm-a205 rcm-a213

Switch	Zone	Connector	HBA x	Array x1	Array x2
Y	3		hba-a10	rcm-a102 rcm-a112	rcm-a204 rcm-a212
Z	4		hba-a11	rcm-a105 rcm-a114	rcm-a203 rcm-a215
Y	5		hba-b00	rcm-b104 rcm-b112	rcm-b205 rcm-b212
Z	6		hba-b01	rcm-b103 rcm-b115	rcm-b204 rcm-b215
Y	7		hba-b10	rcm-b105 rcm-b114	rcm-b202 rcm-b213
Z	8		hba-b11	rcm-b102 rcm-b113	rcm-b203 rcm-b214

E.6. Two Head Units, Three Arrays Each

When a head unit writes to three arrays, connecting through Fibre Channel switches is mandatory.

Head Units	Total Arrays	Ports per Switch	Total SFP+	Total Switch Zones	Brocade Models
2	6	28	56	8	6510

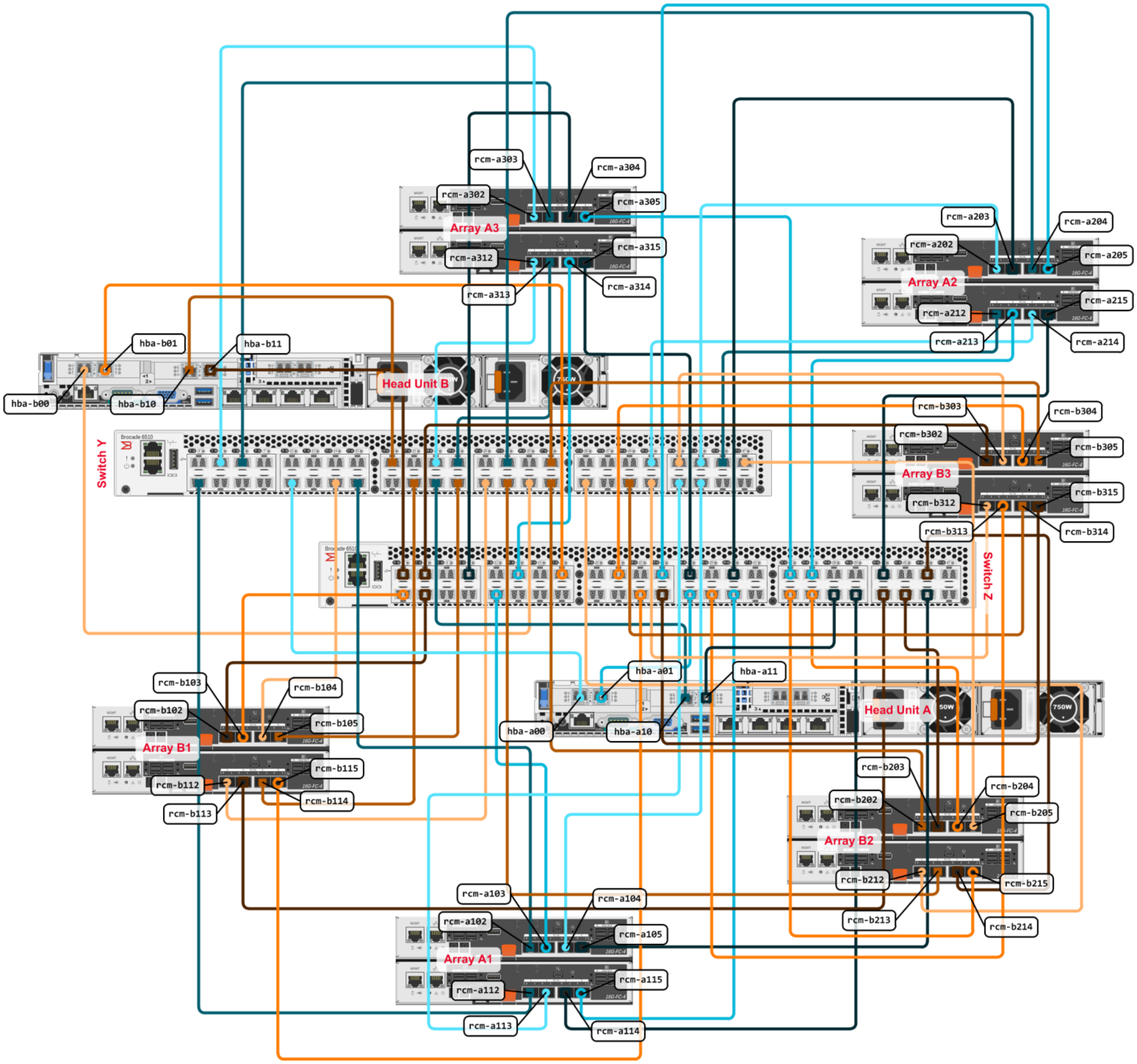
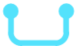
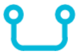
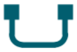
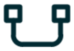
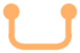
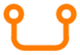
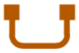
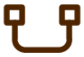


Figure 56: Two Head Units Connected to Three Storage Arrays Each, Through Redundant Brocade 6510 48-Port Fibre Channel Switches

Consult this table for the device ID assignments for the switch zones in Figure 56 on the previous page.

Switch	Zone	Connector	HBA x	Array x1	Array x2	Array x3
Y	1		hba-a00	rcm-a104 rcm-a113	rcm-a202 rcm-a214	rcm-a303 rcm-a312
Z	2		hba-a01	rcm-a103 rcm-a115	rcm-a205 rcm-a213	rcm-a305 rcm-a314
Y	3		hba-a10	rcm-a102 rcm-a112	rcm-a204 rcm-a212	rcm-a303 rcm-a313
Z	4		hba-a11	rcm-a105 rcm-a114	rcm-a203 rcm-a215	rcm-a304 rcm-a315
Y	5		hba-b00	rcm-b104 rcm-b112	rcm-b205 rcm-b212	rcm-b312 rcm-b303
Z	6		hba-b01	rcm-b103 rcm-b115	rcm-b204 rcm-b215	rcm-b304 rcm-b313
Y	7		hba-b10	rcm-b105 rcm-b114	rcm-b202 rcm-b213	rcm-b305 rcm-b314
Z	8		hba-b11	rcm-b102 rcm-b113	rcm-b203 rcm-b214	rcm-b302 rcm-b315

E.7. Three Head Units, One Array Each

Because each head unit writes to only one array, you can use the point-to-point connections shown in One Head Unit, One Array on page 52, instead of connecting to the arrays through Fibre Channel switches.

Head Units	Total Arrays	Ports per Switch	Total SFP+	Total Switch Zones	Brocade Models
3	3	18	36	12	6505, 6510

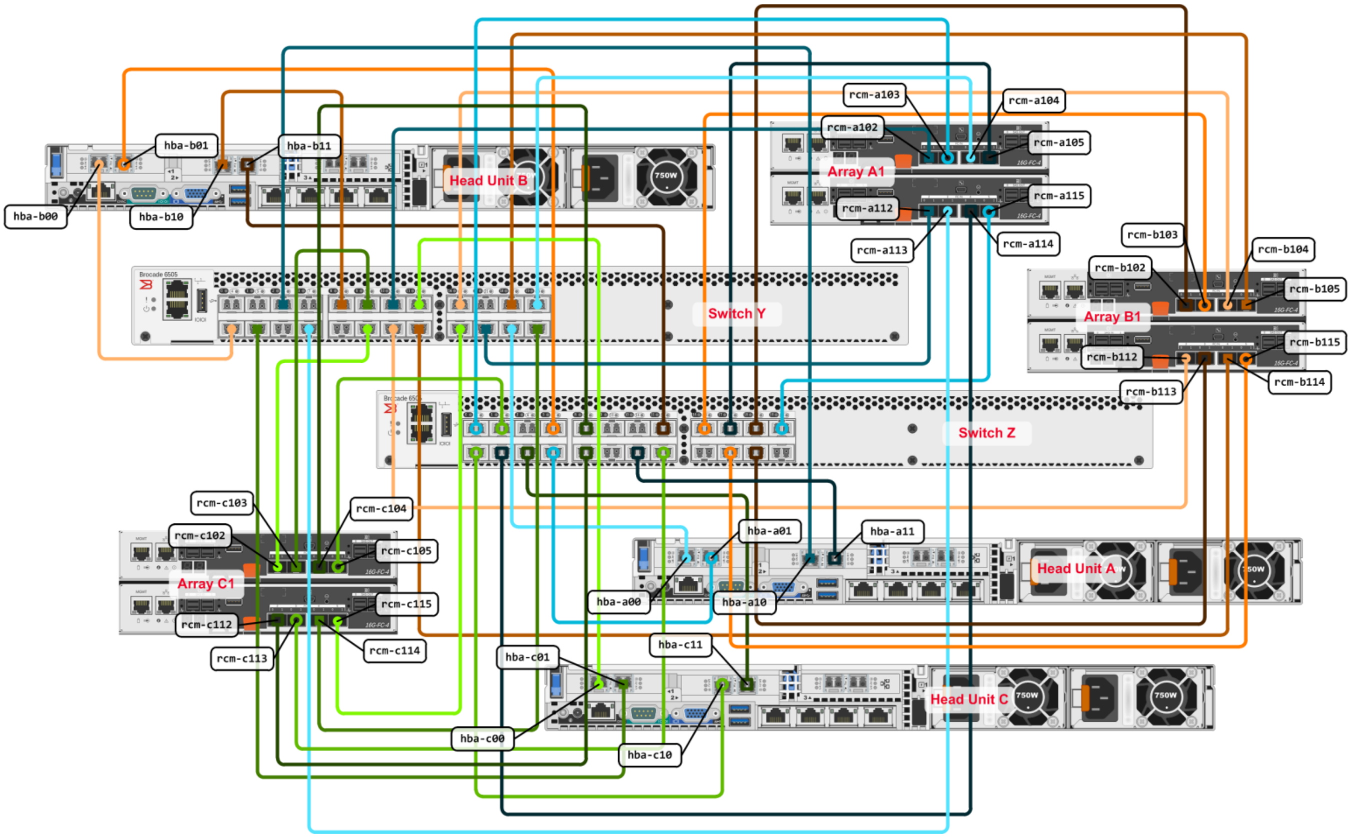
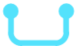
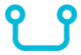
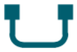
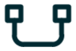
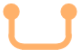
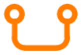
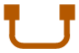
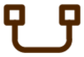
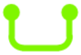
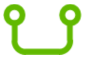
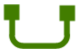
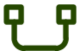


Figure 57: Three Head Units Connected to One Storage Array Each, Through Redundant Brocade 6505 24-Port Fibre Channel Switches

Consult this table for the device ID assignments for the switch zones in Figure 57 on the previous page.

Switch	Zone	Connector	HBA x	Array x1
Y	1		hba-a00	rcm-a104 rcm-a113
Z	2		hba-a01	rcm-a103 rcm-a115
Y	3		hba-a10	rcm-a102 rcm-a112
Z	4		hba-a11	rcm-a105 rcm-a114
Y	5		hba-b00	rcm-b104 rcm-b112
Z	6		hba-b01	rcm-b103 rcm-b115
Y	7		hba-b10	rcm-b105 rcm-b114
Z	8		hba-b11	rcm-b102 rcm-b113
Y	9		hba-c00	rcm-c102 rcm-c115
Z	10		hba-c01	rcm-c105 rcm-c113
Y	11		hba-c10	rcm-c103 rcm-c114
Z	12		hba-c11	rcm-c104 rcm-c112

E.8. Three Head Units, Two Arrays Each

Because each head unit writes to only two arrays, you can use the point-to-point connections shown in One Head Unit, Two Arrays on page 54, instead of connecting to the arrays through Fibre Channel switches.

Head Units	Total Arrays	Ports per Switch	Total SFP+	Total Switch Zones	Brocade Models
3	6	30	60	12	6510

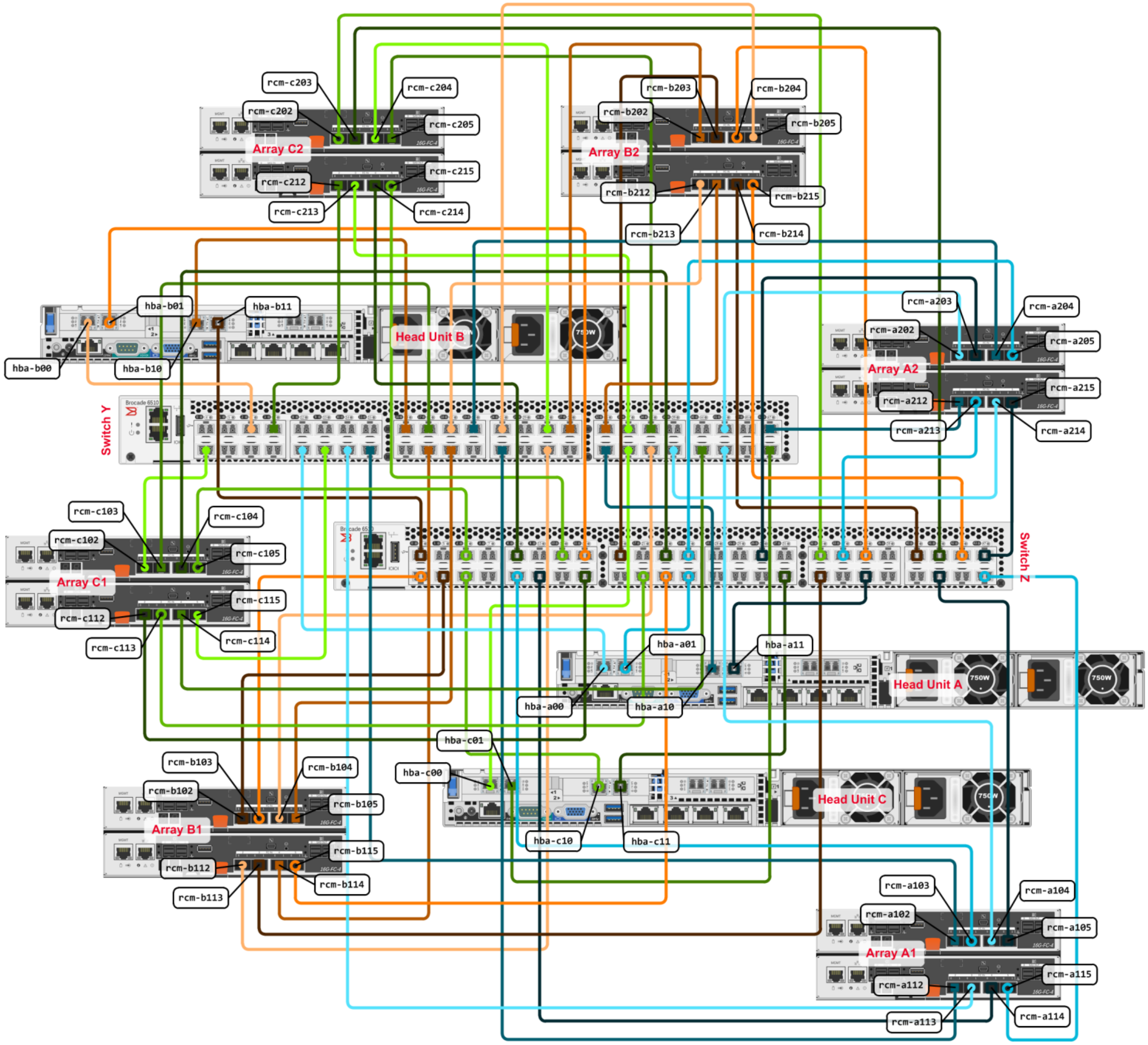


Figure 58: **Three Head Units Connected to Two Storage Arrays Each, Through Redundant Brocade 6510 48-Port Fibre Channel Switches**

Consult this table for the device ID assignments for the switch zones in Figure 58 on the previous page.

Switch	Zone	Connector	HBA x	Array x1	Array x2
Y	1	●⊔●	hba-a00	rcm-a104 rcm-a113	rcm-a202 rcm-a214
Z	2	○⊔○	hba-a01	rcm-a103 rcm-a115	rcm-a205 rcm-a213

Switch	Zone	Connector	HBA x	Array x1	Array x2
Y	3		hba-a10	rcm-a102 rcm-a112	rcm-a204 rcm-a212
Z	4		hba-a11	rcm-a105 rcm-a114	rcm-a203 rcm-a215
Y	5		hba-b00	rcm-b104 rcm-b112	rcm-b205 rcm-b212
Z	6		hba-b01	rcm-b103 rcm-b115	rcm-b204 rcm-b215
Y	7		hba-b10	rcm-b105 rcm-b114	rcm-b202 rcm-b213
Z	8		hba-b11	rcm-b102 rcm-b113	rcm-b203 rcm-b214
Y	9		hba-c00	rcm-c102 rcm-c115	rcm-c204 rcm-c213
Z	10		hba-c01	rcm-c105 rcm-c113	rcm-c202 rcm-c215
Y	11		hba-c10	rcm-c103 rcm-c114	rcm-c205 rcm-c212
Z	12		hba-c11	rcm-c104 rcm-c112	rcm-c203 rcm-c214

E.9. Three Head Units, Three Arrays Each

When a head unit writes to three arrays, connecting through Fibre Channel switches is mandatory.

Head Units	Total Arrays	Ports per Switch	Total SFP+	Total Switch Zones	Brocade Models
3	9	42	84	12	6510

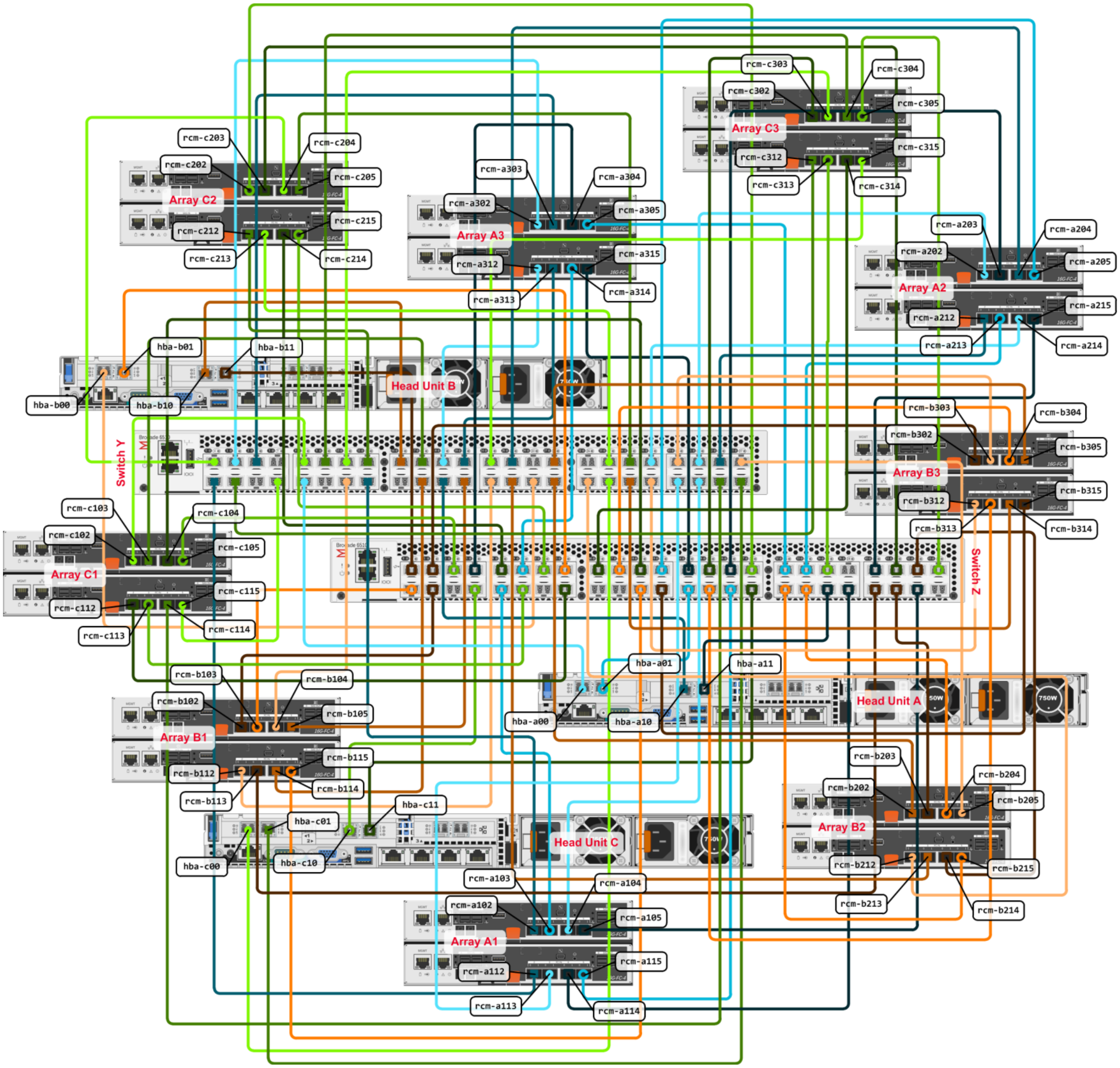


Figure 59: Three Head Units Connected to Three Storage Arrays Each, Through Redundant Brocade 6510 48-Port Fibre Channel Switches

Consult this table for the device ID assignments for the switch zones in Figure 59 on the previous page.

Switch	Zone	Connector	HBA x	Array x1	Array x2	Array x3
Y	1		hba-a00	rcm-a104 rcm-a113	rcm-a202 rcm-a214	rcm-a303 rcm-a312
Z	2		hba-a01	rcm-a103 rcm-a115	rcm-a205 rcm-a213	rcm-a305 rcm-a314
Y	3		hba-a10	rcm-a102 rcm-a112	rcm-a204 rcm-a212	rcm-a303 rcm-a313
Z	4		hba-a11	rcm-a105 rcm-a114	rcm-a203 rcm-a215	rcm-a304 rcm-a315
Y	5		hba-b00	rcm-b104 rcm-b112	rcm-b205 rcm-b212	rcm-b312 rcm-b303
Z	6		hba-b01	rcm-b103 rcm-b115	rcm-b204 rcm-b215	rcm-b304 rcm-b313
Y	7		hba-b10	rcm-b105 rcm-b114	rcm-b202 rcm-b213	rcm-b305 rcm-b314
Z	8		hba-b11	rcm-b102 rcm-b113	rcm-b203 rcm-b214	rcm-b302 rcm-b315
Y	9		hba-c00	rcm-c102 rcm-c115	rcm-c204 rcm-c213	rcm-c303 rcm-c315
Z	10		hba-c01	rcm-c105 rcm-c113	rcm-c202 rcm-c215	rcm-c305 rcm-c313
Y	11		hba-c10	rcm-c103 rcm-c114	rcm-c205 rcm-c212	rcm-c305 rcm-c313
Z	12		hba-c11	rcm-c104 rcm-c112	rcm-c203 rcm-c214	rcm-c302 rcm-c314