Dell EMC Host Connectivity Guide for HP-UX

P/N 300-000-614
REV 46
PUBLISHED SEPTEMBER 2018
# Preface

Dell EMC Host Connectivity Guide for HP-UX

---

## Part 1 VMAX and Symmetrix Connectivity with HP 9000 and Integrity Itanium

### Chapter 1 PowerMax and VMAX Environments

- Hardware connectivity
- Minimum Dell EMC PowerMAX OS, HYPERMAX OS and Enginuity requirements
- Boot device support
- Common serial number
- Logical devices
- Allocating/deallocating devices and LUNs
- VMAX and Symmetrix models
- VMAX and PowerMax configuration for HP-UX 11i v3.0
- Required director bit settings for HP-UX 11iv3 (HP-UX 11.31) initiators
- SPC-2 DMX, VMAX 20K/VMAX, VMAX 10K (Systems with SN xxx959xxxx), and VMAXe director flag
- VMAX 400K, VMAX 200K, VMAX 100K, VMAX 40K, VMAX 20K/VMAX, VMAX 10K (Systems with SN xxx959xxxx), VMAXe, and Symmetrix DMX minimum microcode requirements for HP-UX 11iv3 (11.31)
- VMAX and DMX os07 director flags
- VMAX and DMX minimum microcode requirements for os07 director configuration flag support

### Chapter 2 Virtual Provisioning on VMAX and Symmetrix Systems

- Symmetrix Virtual Provisioning
- Terminology
- Thin device
- Implementation considerations
- Over-subscribed thin pools
- Thin-hostile environments
- Pre-provisioning with thin devices in a thin hostile environment
- Host boot/root/swap/dump devices positioned on Symmetrix VP (tdev) devices
- Cluster configuration
- Symmetrix Virtual Provisioning in the HP-UX environment
- HP-UX Virtual Provisioning support
- Precaution considerations
- Unbound thin devices

### Chapter 3 Dell EMC VPLEX

- VPLEX overview
- VPLEX documentation
- Prerequisites
- Veritas DMP settings with VPLEX
- Provisioning and exporting storage
- VPLEX with GeoSynchrony v4.x
- VPLEX with GeoSynchrony v5.x
- Storage volumes
- Claiming and naming storage volumes
# Contents

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>System partitions</td>
<td>87</td>
</tr>
<tr>
<td>Configuring HP-UX to recognize VPLEX volumes</td>
<td>59</td>
</tr>
<tr>
<td>Volume Manager recommended settings</td>
<td>60</td>
</tr>
<tr>
<td>Front-end paths</td>
<td>57</td>
</tr>
<tr>
<td>Exporting virtual volumes to hosts</td>
<td>54</td>
</tr>
<tr>
<td>Initiators</td>
<td>58</td>
</tr>
<tr>
<td>Configuring HP-UX to recognize VPLEX volumes</td>
<td>59</td>
</tr>
<tr>
<td>Volume Manager recommended settings</td>
<td>60</td>
</tr>
<tr>
<td>Host connectivity</td>
<td>53</td>
</tr>
<tr>
<td>Required storage system setup</td>
<td>51</td>
</tr>
<tr>
<td>Required Symmetrix FA bit settings</td>
<td>52</td>
</tr>
<tr>
<td>Supported storage arrays</td>
<td>52</td>
</tr>
<tr>
<td>Initiator settings on back-end arrays</td>
<td>58</td>
</tr>
<tr>
<td>Viewing the World Wide Name for an HBA port</td>
<td>57</td>
</tr>
<tr>
<td>VPLEX ports</td>
<td>58</td>
</tr>
<tr>
<td>Initiators</td>
<td>58</td>
</tr>
<tr>
<td>Configuring HP-UX to recognize VPLEX volumes</td>
<td>59</td>
</tr>
<tr>
<td>Volume Manager recommended settings</td>
<td>60</td>
</tr>
<tr>
<td>Chapter 4 Fibre Channel Environment</td>
<td></td>
</tr>
<tr>
<td>Addressing</td>
<td>62</td>
</tr>
<tr>
<td>Fabric configuration</td>
<td>62</td>
</tr>
<tr>
<td>HBA</td>
<td>63</td>
</tr>
<tr>
<td>Switch</td>
<td>63</td>
</tr>
<tr>
<td>Incorporating VMAX or Symmetrix/Fibre Channel</td>
<td>64</td>
</tr>
<tr>
<td>HP hardware device mapping</td>
<td>65</td>
</tr>
<tr>
<td>Addressing VMAX or Symmetrix devices</td>
<td>68</td>
</tr>
<tr>
<td>Arbitrated loop addressing</td>
<td>68</td>
</tr>
<tr>
<td>Fabric addressing</td>
<td>68</td>
</tr>
<tr>
<td>SCSI-3 FCP addressing</td>
<td>69</td>
</tr>
<tr>
<td>Chapter 5 Host Environment</td>
<td></td>
</tr>
<tr>
<td>HP-UX OS support</td>
<td>72</td>
</tr>
<tr>
<td>HP-UX 10.20 on PA-Risc</td>
<td>72</td>
</tr>
<tr>
<td>HP-UX 11.00</td>
<td>72</td>
</tr>
<tr>
<td>HP-UX 11i v1</td>
<td>72</td>
</tr>
<tr>
<td>HP-UX 11i v2</td>
<td>72</td>
</tr>
<tr>
<td>HP-UX 11i v2 September 2004 (and later)</td>
<td>72</td>
</tr>
<tr>
<td>HP-UX 11i v3.0</td>
<td>74</td>
</tr>
<tr>
<td>HP-UX bundled applications</td>
<td>76</td>
</tr>
<tr>
<td>HP-UX patches and support</td>
<td>77</td>
</tr>
<tr>
<td>Useful HP-UX 11x utilities and functions</td>
<td>78</td>
</tr>
<tr>
<td>Maximum LUN and file system sizes</td>
<td>79</td>
</tr>
<tr>
<td>Recognizing new devices and LUNs</td>
<td>80</td>
</tr>
<tr>
<td>Adding devices on line</td>
<td>81</td>
</tr>
<tr>
<td>External boot from a VMAX or Symmetrix device</td>
<td>82</td>
</tr>
<tr>
<td>Fresh install</td>
<td>82</td>
</tr>
<tr>
<td>Mirroring an internal OS to an external device</td>
<td>83</td>
</tr>
<tr>
<td>Migrating an internal OS to an external device</td>
<td>84</td>
</tr>
<tr>
<td>Migrating root volume group</td>
<td>86</td>
</tr>
<tr>
<td>System partitions</td>
<td>87</td>
</tr>
</tbody>
</table>
Contents

nPartitions ........................................................................................................ 87
vPartitions ........................................................................................................ 88
Integrity Virtual Machines .............................................................................. 88
Volume managers ........................................................................................... 90
LVM guide ...................................................................................................... 90
LVM commands ............................................................................................ 95
VxVM ............................................................................................................. 96
VxVM commands ........................................................................................... 98
I/O time-out parameters ................................................................................... 99
HP LVM physical volume time-out (PVtimeout)............................................. 99
HP LVM logical volume time-out (LVtimeout) .............................................. 100
Veritas VxVM powerfail time-out (pfto) ...................................................... 103
Recommended I/O time-out values ............................................................... 104
Cluster ............................................................................................................ 105
Cluster overview ........................................................................................... 105
HA cluster ...................................................................................................... 106
Cluster services ............................................................................................. 106
Configuring and managing MC/ServiceGuard ............................................. 107
Failover/failback policies ............................................................................. 108
ServiceGuard Manager ................................................................................. 109
Cluster quorum ............................................................................................. 109
Mirroring ........................................................................................................ 110
Clustering in partitioned environments ......................................................... 110
Mixed OS cluster ........................................................................................... 110
ServiceGuard Storage Management Suite ............................................... 111
Creating the disk groups ............................................................................ 114
Creating the disk group cluster packages .................................................... 114
Symmetrix configuration ............................................................................. 115
VMAX and Symmetrix boot device in an HA environment ......................... 117

Part 2  Unity and VNX series, CLARiiON Connectivity

Chapter 6  HP-UX Hosts and VNX Series and CLARiiON Systems

HP-UX in a VNX series and CLARiiON environment .................................... 124
Host connectivity ........................................................................................... 124
Boot support .................................................................................................. 124
Logical device support .................................................................................. 124
Storage component overview ...................................................................... 125
Required storage system setup .................................................................... 125
VNX series and CLARiiON configuration for HP-UX hosts ......................... 126
VNX series and CLARiiON SPs and LUNs ................................................... 126
HP-UX initiator settings ................................................................................. 126
Enable VNX series and CLARiiON write cache ......................................... 127
Registering HP-UX initiator connections ..................................................... 127
Making LUNs available to HP-UX ............................................................... 128
Configuration requirements for VNX series and CLARiiON support with 11iv3 130
Prerequisites ................................................................................................ 130
System configuration .................................................................................... 131
External boot from VNX series and CLARiiON ........................................... 137
General guidelines ......................................................................................... 137
Firmware requirements ................................................................................ 137
Mirroring the HP-UX operating system and boot to VNX series and CLARiiON138
Configuring VNX series and CLARiiON for new HP-UX installation and boot138
HP-UX System Administration Manager (SAM) ........................................... 141
Contents

Logical Volume Manager (LVM) .............................................................. 144
Creating volume groups on LUNs ......................................................... 144
What next? ......................................................................................... 147
Veritas Volume Manager (VxVM) .......................................................... 148
MC/ServiceGuard .............................................................................. 149

Chapter 7  Virtual Provisioning on VNX Series and CLARiiON Systems

Virtual Provisioning on VNX series and CLARiiON systems .................. 152
Terminology ....................................................................................... 153
Thin pools ......................................................................................... 155
Thin pool capacity ............................................................................ 157
Thin LUNs ......................................................................................... 159
Attributes ......................................................................................... 160
Architecture and features ................................................................. 161
Using thin LUNs with applications .................................................... 162
HP-UX Virtual Provisioning support ................................................... 163
Precaution considerations ............................................................... 163

Chapter 8  HP-UX Hosts and Unity Series

HP-UX in a Unity environment ............................................................ 168
Host connectivity ............................................................................... 168
Boot support .................................................................................... 168
Storage management overview ........................................................ 168
Required storage system setup ......................................................... 169
Unity series configuration for HP-UX hosts ........................................ 170
Unity series storage processors and LUNs ........................................ 170
Enable Unity series write cache ....................................................... 170
Making LUNs available to HP-UX .................................................... 171
Configuration requirements for Unity series support ......................... 172
Prerequisites and restrictions ............................................................ 172
Configuring an external boot of HP-UX hosts .................................... 173
General guidelines ........................................................................... 173
Configuring Unity series for new HP-UX installation and boot .......... 173

Part 3  Best Practices

Chapter 9  Using Dell EMC TimeFinder in an HP-UX Environment

TimeFinder in HP-UX environments ................................................... 178
BCV operations ................................................................................ 178
Basic procedures for HP-UX ............................................................ 179
HP-UX clusters ............................................................................... 183
File system issues ............................................................................ 197

Chapter 10  SRDF and MirrorView Remote Boot

Remote boot ....................................................................................... 200

Chapter 11  OS Upgrade from HP-UX 11.23 to HP-UX 11.31

Upgrade from HP-UX 11.23 to HP-UX 11.31 ....................................... 204
Flags ............................................................................................... 204
Support ............................................................................................ 204
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pre-OS upgrade checklist</td>
<td>205</td>
</tr>
<tr>
<td>OS upgrade</td>
<td>205</td>
</tr>
<tr>
<td>Part 4 Appendices</td>
<td></td>
</tr>
<tr>
<td>Appendix A Migrating from SCSI Connections to Fibre Channel</td>
<td></td>
</tr>
<tr>
<td>Introduction</td>
<td>210</td>
</tr>
<tr>
<td>Running inquiry</td>
<td>211</td>
</tr>
<tr>
<td>Connecting to the Dell EMC FTP server</td>
<td>211</td>
</tr>
<tr>
<td>Migrating in the HP LVM environment</td>
<td>213</td>
</tr>
<tr>
<td>Moving ‘rootvg’ on HP LVM</td>
<td>214</td>
</tr>
<tr>
<td>Running the Dell EMC migration script</td>
<td>215</td>
</tr>
<tr>
<td>Usage</td>
<td>215</td>
</tr>
<tr>
<td>Limitations</td>
<td>215</td>
</tr>
<tr>
<td>Procedure</td>
<td>215</td>
</tr>
<tr>
<td>Appendix B Setting Up Cisco MDS 9000 Switches for HP-UX Environments</td>
<td></td>
</tr>
<tr>
<td>Setting up MDS 9000 switches for an HP-UX environment</td>
<td>220</td>
</tr>
<tr>
<td>Appendix C End-of- Support CLARiiON Arrays</td>
<td></td>
</tr>
<tr>
<td>Change in hardware paths</td>
<td>226</td>
</tr>
<tr>
<td>Fabric address change</td>
<td>226</td>
</tr>
<tr>
<td>Sequential LUNs</td>
<td>226</td>
</tr>
<tr>
<td>MC/ServiceGuard</td>
<td>226</td>
</tr>
<tr>
<td>Appendix D Excessive Path Failovers in LVM PVLink VNX Series and CLARiiON Configurations</td>
<td></td>
</tr>
<tr>
<td>Introduction</td>
<td>230</td>
</tr>
<tr>
<td>Changing the timeout</td>
<td>230</td>
</tr>
<tr>
<td>Changing max_fcp_req</td>
<td>230</td>
</tr>
<tr>
<td>FC4500, FC5300, FC5700</td>
<td>230</td>
</tr>
<tr>
<td>FC4700, CX series</td>
<td>231</td>
</tr>
</tbody>
</table>
# FIGURES

<table>
<thead>
<tr>
<th>FIGURE</th>
<th>DESCRIPTION</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Virtual Provisioning</td>
<td>32</td>
</tr>
<tr>
<td>2</td>
<td>Thin device and thin storage pool containing data devices</td>
<td>35</td>
</tr>
<tr>
<td>3</td>
<td>VPLEX provisioning and exporting storage process</td>
<td>47</td>
</tr>
<tr>
<td>4</td>
<td>Create storage view</td>
<td>54</td>
</tr>
<tr>
<td>5</td>
<td>Register initiators</td>
<td>55</td>
</tr>
<tr>
<td>6</td>
<td>Add ports to storage view</td>
<td>55</td>
</tr>
<tr>
<td>7</td>
<td>Add virtual volumes to storage view</td>
<td>56</td>
</tr>
<tr>
<td>8</td>
<td>FC-AL hardware device mapping example</td>
<td>66</td>
</tr>
<tr>
<td>9</td>
<td>FC-SW hardware device mapping example</td>
<td>67</td>
</tr>
<tr>
<td>10</td>
<td>Fibre Channel hardware path</td>
<td>80</td>
</tr>
<tr>
<td>11</td>
<td>SCSI hardware path</td>
<td>80</td>
</tr>
<tr>
<td>12</td>
<td>Bootable disk, sample configuration</td>
<td>84</td>
</tr>
<tr>
<td>13</td>
<td>Checking the boot configuration</td>
<td>85</td>
</tr>
<tr>
<td>14</td>
<td>Volume map: System _Impf</td>
<td>93</td>
</tr>
<tr>
<td>15</td>
<td>PVLInks/alternate path, physical configuration for device multipathing</td>
<td>94</td>
</tr>
<tr>
<td>16</td>
<td>Volume group information</td>
<td>95</td>
</tr>
<tr>
<td>17</td>
<td>Fabric connections example</td>
<td>115</td>
</tr>
<tr>
<td>18</td>
<td>Unisphere/Navisphere Manager display</td>
<td>133</td>
</tr>
<tr>
<td>19</td>
<td>Connectivity status menu</td>
<td>133</td>
</tr>
<tr>
<td>20</td>
<td>Group Edit Initiators menu</td>
<td>134</td>
</tr>
<tr>
<td>21</td>
<td>Failover Setup Wizard dialog box</td>
<td>134</td>
</tr>
<tr>
<td>22</td>
<td>Select Host dialog box</td>
<td>135</td>
</tr>
<tr>
<td>23</td>
<td>Select Storage Systems dialog box</td>
<td>135</td>
</tr>
<tr>
<td>24</td>
<td>Specify Settings dialog box</td>
<td>136</td>
</tr>
<tr>
<td>25</td>
<td>Create initiator record</td>
<td>139</td>
</tr>
<tr>
<td>26</td>
<td>HP-UX installation ioscan output</td>
<td>140</td>
</tr>
<tr>
<td>27</td>
<td>SAM disk output</td>
<td>141</td>
</tr>
<tr>
<td>28</td>
<td>Corrected SAM disk output</td>
<td>142</td>
</tr>
<tr>
<td>29</td>
<td>Create Storage pool dialog box</td>
<td>155</td>
</tr>
<tr>
<td>30</td>
<td>Pool % Full threshold</td>
<td>157</td>
</tr>
<tr>
<td>31</td>
<td>Thin Pool Properties dialog box</td>
<td>158</td>
</tr>
<tr>
<td>32</td>
<td>Create LUN dialog box</td>
<td>160</td>
</tr>
<tr>
<td>33</td>
<td>Inquiry output example</td>
<td>211</td>
</tr>
<tr>
<td>34</td>
<td>Cisco MDS 9000 family, Domain Manager</td>
<td>222</td>
</tr>
<tr>
<td>35</td>
<td>Cisco MDS 9000 family, Device Manager</td>
<td>223</td>
</tr>
</tbody>
</table>
TABLES

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Dell EMC models and minimum operating system requirements</td>
</tr>
<tr>
<td>2</td>
<td>Minimum Engine requirements</td>
</tr>
<tr>
<td>3</td>
<td>PowerMax and VMAX models</td>
</tr>
<tr>
<td>4</td>
<td>Required Symmetrix FA bit settings for connection to VPLEX</td>
</tr>
<tr>
<td>5</td>
<td>Supported hosts and initiator types</td>
</tr>
<tr>
<td>6</td>
<td>OS versions currently supported</td>
</tr>
<tr>
<td>7</td>
<td>Minimum system firmware, HP 9000 entry-level servers</td>
</tr>
<tr>
<td>8</td>
<td>Minimum system firmware, HP 9000 mid-range and high-end servers</td>
</tr>
<tr>
<td>9</td>
<td>Minimum system firmware, HP Integrity entry-level servers</td>
</tr>
<tr>
<td>10</td>
<td>Minimum system firmware, HP Integrity mid-range and high-end servers</td>
</tr>
<tr>
<td>11</td>
<td>Operating environment applications</td>
</tr>
<tr>
<td>12</td>
<td>Maximum supported size limits</td>
</tr>
<tr>
<td>13</td>
<td>Maximum supported HFS file and file system sizes</td>
</tr>
<tr>
<td>14</td>
<td>Maximum supported (VxFS) JFS file and file system sizes</td>
</tr>
<tr>
<td>15</td>
<td>HP Virtual Machine host OS support</td>
</tr>
<tr>
<td>16</td>
<td>HP-UX Guest OS support</td>
</tr>
<tr>
<td>17</td>
<td>HP High Availability features summary</td>
</tr>
<tr>
<td>18</td>
<td>Initiator setting table</td>
</tr>
<tr>
<td>19</td>
<td>Minimum FLARE requirements</td>
</tr>
<tr>
<td>20</td>
<td>Threshold alerts</td>
</tr>
<tr>
<td>21</td>
<td>Available view blocks for Unisphere dashboards</td>
</tr>
<tr>
<td>22</td>
<td>Relationship between BCVs and standard devices</td>
</tr>
<tr>
<td>23</td>
<td>Systems with changes in hardware paths</td>
</tr>
</tbody>
</table>
Tables
PREFACE

As part of an effort to improve and enhance the performance and capabilities of its product line, Dell EMC from time to time releases revisions of its hardware and software. Therefore, some functions described in this document may not be supported by all revisions of the software or hardware currently in use. For the most up-to-date information on product features, refer to your product release notes.

If a product does not function properly or does not function as described in this document, please contact your Dell EMC representative.

This guide describes the features and setup procedures for HP host interfaces to EMC VNX and Dell EMC VMAX, Symmetrix, and CLARiiON systems over Fibre Channel and (Symmetrix only) SCSI.

Audience

This guide is intended for use by storage administrators, system programmers, or operators who are involved in acquiring, managing, or operating VMAX, Symmetrix, VNX, and CLARiiON and host devices.

Readers of this guide are expected to be familiar with the following topics:

- VMAX, Symmetrix, VNX, or CLARiiON system operation
- HP-UX operating environment

VMAX and Symmetrix references

Unless otherwise noted:

- Any general references to Symmetrix or Symmetrix array include the VMAX3 Family, VMAX Family, and DMX-4 and DMX-3.
  - The VMAX3 Family includes VMAX 400K, VMAX 200K, and VMAX 100K.
  - The VMAX Family includes VMAX 40K, VMAX 20K/VMAX, VMAX 10K (Systems with SN xxx987xxxx), VMAX 10K (Systems with SN xxx959xxxx), and VMAXe.

Table 1 lists the minimum Dell EMC Enginuity™ and Dell EMC HYPERMAX™ OS requirements for various Dell EMC VMAX and Symmetrix models.

Table 1

<table>
<thead>
<tr>
<th>Dell EMC model</th>
<th>Minimum operating system</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMAX 400K</td>
<td>HYPERMAX 5977.250.189</td>
</tr>
<tr>
<td>VMAX 200K</td>
<td>HYPERMAX 5977.250.189</td>
</tr>
<tr>
<td>VMAX 100K</td>
<td>HYPERMAX 5977.250.189</td>
</tr>
<tr>
<td>VMAX 40K</td>
<td>Enginuity 5876.82.57</td>
</tr>
<tr>
<td>VMAX 20K</td>
<td>Enginuity 5876.82.57</td>
</tr>
<tr>
<td>VMAX 10K (Systems with SN xxx987xxxx)</td>
<td>Enginuity 5876.159.102</td>
</tr>
<tr>
<td>VMAX</td>
<td>Enginuity 5876.82.57</td>
</tr>
<tr>
<td>VMAX 10K (Systems with SN xxx959xxxx)</td>
<td>Enginuity 5876.82.57</td>
</tr>
<tr>
<td>VMAXe</td>
<td>Enginuity 5876.82.57</td>
</tr>
</tbody>
</table>
Table 1

<table>
<thead>
<tr>
<th>Dell EMC model</th>
<th>Minimum operating system</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symmetrix DMX-4</td>
<td>Enginuity 5773.79.58</td>
</tr>
<tr>
<td>Symmetrix DMX-3</td>
<td>Enginuity 5773.79.58</td>
</tr>
</tbody>
</table>

Related documentation

For documentation, refer to Dell EMC Online Support.

For the most up-to-date information, always consult the Dell EMC Simple Support Matrices (ESM), available through Dell EMC E-Lab Navigator (ELN).

Conventions used in this guide

Dell EMC uses the following conventions for notes and cautions.

**Note:** A note presents information that is important, but not hazard-related.

**IMPORTANT**

An important notice contains information essential to software or hardware operation.

Typographical conventions

Dell EMC uses the following type style conventions in this document:

- **Normal**
  - Used in running (nonprocedural) text for:
    - Names of interface elements, such as names of windows, dialog boxes, buttons, fields, and menus
    - Names of resources, attributes, pools, Boolean expressions, buttons, DQL statements, keywords, clauses, environment variables, functions, and utilities
    - URLs, pathnames, filenames, directory names, computer names, links, groups, service keys, file systems, and notifications

- **Bold**
  - Used in running (nonprocedural) text for names of commands, daemons, options, programs, processes, services, applications, utilities, kernels, notifications, system calls, and man pages
  - Used in procedures for:
    - Names of interface elements, such as names of windows, dialog boxes, buttons, fields, and menus
    - What the user specifically selects, clicks, presses, or types

- **Italic**
  - Used in all text (including procedures) for:
    - Full titles of publications referenced in text
    - Emphasis, for example, a new term
    - Variables

- **Courier**
  - Used for:
    - System output, such as an error message or script
    - URLs, complete paths, filenames, prompts, and syntax when shown outside of running text

- **Courier bold**
  - Used for specific user input, such as commands

- **Courier italic**
  - Used in procedures for:
    - Variables on the command line
    - User input variables

- `< >`
  - Angle brackets enclose parameter or variable values supplied by the user

- `[ ]`
  - Square brackets enclose optional values
Where to get help

Dell EMC support, product, and licensing information can be obtained as follows.

Dell EMC support, product, and licensing information can be obtained on the Dell EMC Online Support site as described next.

Note: To open a service request through the Dell EMC Online Support site, you must have a valid support agreement. Contact your Dell EMC sales representative for details about obtaining a valid support agreement or to answer any questions about your account.

Product information

For documentation, release notes, software updates, or for information about Dell EMC products, licensing, and service, go to Dell EMC Online Support.

Technical support

Dell EMC offers a variety of support options.

Support by Product — Dell EMC offers consolidated, product-specific information on Dell EMC Online Support.

The Support by Product web pages offer quick links to Documentation, White Papers, Advisories (such as frequently used Knowledgebase articles), and Downloads, as well as more dynamic content, such as presentations, discussion, relevant Customer Support Forum entries, and a link to Dell EMC Live Chat.

Dell EMC Live Chat — Open a Chat or instant message session with a Dell EMC Support Engineer.

eLicensing support

To activate your entitlements and obtain your Symmetrix license files, visit the Service Center on Dell EMC Online Support, as directed on your License Authorization Code (LAC) letter e-mailed to you.

For help with missing or incorrect entitlements after activation (that is, expected functionality remains unavailable because it is not licensed), contact your Dell EMC Account Representative or Authorized Reseller.

For help with any errors applying license files through Solutions Enabler, contact the Dell EMC Customer Support Center.

If you are missing a LAC letter, or require further instructions on activating your licenses through the Dell EMC Online Support site, contact the Dell EMC worldwide Licensing team at licensing@emc.com or call:

• North America, Latin America, APJK, Australia, New Zealand: SVC4EMC (800-782-4362) and follow the voice prompts.
• EMEA: +353 (0) 21 4879862 and follow the voice prompts.
We'd like to hear from you!

Your suggestions will help us continue to improve the accuracy, organization, and overall quality of the user publications. Send your opinions of this document to:

techpubcomments@emc.com
This section of the HP Host Connectivity Guide provides configuration guidelines in the HP-UX environment. The topics covered in this section include VMAX and Symmetrix setup, host OS versions, server models, HBA information, volume managers, clusters, and Fibre Channel environments.

Part 1 includes:

- Chapter 1, "PowerMax and VMAX Environments"
- Chapter 2, "Virtual Provisioning on VMAX and Symmetrix Systems"
- Chapter 3, "Dell EMC VPLEX"
- Chapter 4, "Fibre Channel Environment"
- Chapter 5, "Host Environment"
CHAPTER 1

PowerMax and VMAX
Environments

This chapter covers the VMAX and PowerMax configuration for HP 9000 and Integrity Itanium hosts in the HP-UX environment.

- Hardware connectivity 20
- Minimum Dell EMC PowerMAX OS, HYPERMAX OS and Enginuity requirements 21
- Boot device support 22
- Common serial number 23
- Logical devices 24
- Allocating/deallocating devices and LUNs 25
- VMAX and Symmetrix models 26
- VMAX and PowerMax configuration for HP-UX 11i v3.0 27
Hardware connectivity

Refer to Dell EMC E-Lab Navigator or contact your Dell EMC representative for the latest information on qualified hosts, host bus adapters (HBAs), and connectivity equipment.

Initiators from servers running any currently supported HP-UX 11x versions may share the same FA port.

HP-UX initiators currently support only Volume Set Addressing method. Dell EMC Solutions Enabler LUN masking is required to set Volume Set Addressing for HP-UX initiators if port sharing is configured with non-HP-UX initiators.
Minimum Dell EMC PowerMAX OS, HYPERMAX OS and Enginuity requirements

Table 2 lists the minimum PowerMax OS HYPERMAX™ OS or Enginuity™ or requirements needed for PowerMAX and VMAX models.

Table 2 Minimum Enginuity requirements

<table>
<thead>
<tr>
<th>Dell EMC model</th>
<th>HP-UX version</th>
<th>Minimum operating system</th>
</tr>
</thead>
<tbody>
<tr>
<td>PowerMax 2000</td>
<td>HP-UX 11iv3</td>
<td>PowerMAX OS 5978.144.144</td>
</tr>
<tr>
<td>PowerMax 8000</td>
<td>HP-UX 11iv2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HP-UX 11iv1</td>
<td></td>
</tr>
<tr>
<td>VMAX All Flash</td>
<td>HP-UX 11iv3</td>
<td>HYPERMAX 5977.1125.1125</td>
</tr>
<tr>
<td>950F/950FX</td>
<td>HP-UX 11iv2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HP-UX 11iv1</td>
<td></td>
</tr>
<tr>
<td>VMAX All Flash</td>
<td>HP-UX 11iv3</td>
<td>HYPERMAX 5977.691.684</td>
</tr>
<tr>
<td>450F/450FX/850F/850FX</td>
<td>HP-UX 11iv2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HP-UX 11iv1</td>
<td></td>
</tr>
<tr>
<td>VMAX All Flash</td>
<td>HP-UX 11iv3</td>
<td>HYPERMAX 5977.945.890</td>
</tr>
<tr>
<td>250F/250FX</td>
<td>HP-UX 11iv2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HP-UX 11iv1</td>
<td></td>
</tr>
<tr>
<td>VMAX 100K</td>
<td>HP-UX 11iv3</td>
<td>HYPERMAX 5977.250.189</td>
</tr>
<tr>
<td>VMAX 200K</td>
<td>HP-UX 11iv2</td>
<td></td>
</tr>
<tr>
<td>VMAX 400K</td>
<td>HP-UX 11iv1</td>
<td></td>
</tr>
<tr>
<td>VMAX 40K</td>
<td>HP-UX 11iv3</td>
<td>Enginuity 5876.82.57</td>
</tr>
<tr>
<td></td>
<td>HP-UX 11iv2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HP-UX 11iv1</td>
<td></td>
</tr>
<tr>
<td>VMAX 20K</td>
<td>HP-UX 11iv3</td>
<td>Enginuity 5876.82.57</td>
</tr>
<tr>
<td></td>
<td>HP-UX 11iv2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HP-UX 11iv1</td>
<td></td>
</tr>
<tr>
<td>VMAX 10K (Systems with</td>
<td>HP-UX 11iv3</td>
<td>Enginuity 5876.159.102</td>
</tr>
<tr>
<td>SN xxx987xxxx)</td>
<td>HP-UX 11iv2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HP-UX 11iv1</td>
<td></td>
</tr>
<tr>
<td>VMAX</td>
<td>HP-UX 11iv3</td>
<td>Enginuity 5876.82.57</td>
</tr>
<tr>
<td></td>
<td>HP-UX 11iv2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HP-UX 11iv1</td>
<td></td>
</tr>
</tbody>
</table>
Boot device support

HP 9000 and Integrity Itanium hosts running HP-UX 11x have been qualified for booting from VMAX and PowerMax devices. Refer to Dell EMC E-Lab Navigator for supported configurations. For further information regarding external boot setup refer to “External boot from a VMAX or Symmetrix device” on page 82.

Note that in a Fibre Channel fabric environment with cascaded switches, the boot device cannot be located more than two hops from the initiator.

Solutions Enabler LUN masking is recommended for boot LUNs, especially in an HA environment where multiple servers access the same set of physical devices.

For direct attached FC-AL boot or dump from a VMAX or PowerMax FA port, the Symmetrix auto-negotiation director flag must also be enabled on the FA port.
Common serial number

The VMAX and PowerMax system typically generates its serial number information using the last two digits of the cabinet serial number, the three-digit Symmetrix device number, the director number to which that device is attached, and the port number to which that device is connected. The Common Serial Number option should be used for Dell EMC PowerPath™ and VxVM environments.

The Dell EMC Customer Engineer can set the Common Serial Number option on a port-by-port basis during Symmetrix system configuration. This option causes the last three digits of the serial number information generated by the Symmetrix system (director number and port) to be set to zero on all Symmetrix ports with the option enabled for the same Symmetrix device.
Logical devices

Supported logical unit numbers (LUNs) can be obtained from Product Details in Dell EMC E-Lab Navigator. Select the array model and operating environment.

**Note:** Refer to “HP-UX 11i v3.0” on page 74 for more information on HP-UX 11i v3.0.

HP-UX supports target IDs 0–F, and LUNs 0–7 for each target ID.

VxFS file systems are recommended with high device and LUN counts due to recovery times associated with HFS file systems.

High LUN counts per node will serve to increase boot and `ioscan` completion times. The following HP-UX patches are recommended to improve boot and ioscan completion times, especially when high LUN counts are configured:

- HP-UX 11i v1.0: PHCO_24198, PHKL_24163, and PHKL_28513, or patches that replace or supersede these
- HP-UX 11i v2.0: PHKL_30309 and PHKL_30351
Allocating/deallocating devices and LUNs

A host can be allocated or deallocated device or LUN access through:

- Allocation/Deallocation with Dell EMC ControlCenter™
- Allocation/Deallocation with Symmetrix Management Console (SMC)
- LUN masking with Solutions Enabler SYMCLI vcmdb device (devices/LUNs) prior to Enginuity 5874 code
- LUN masking with Solutions Enabler SYMCLI ACLX device (devices/LUNs) as of Enginuity 5874 code
VMAX and Symmetrix models

This document contains references to VMAX and PowerMax models by series name. Table 3 lists the specific models in each series.

Table 3  PowerMax and VMAX models

<table>
<thead>
<tr>
<th>Series</th>
<th>Models</th>
</tr>
</thead>
<tbody>
<tr>
<td>PowerMax 8000</td>
<td>PowerMax 8000 models</td>
</tr>
<tr>
<td>PowerMax 2000</td>
<td>PowerMax 2000 models</td>
</tr>
<tr>
<td>VMAX All Flash 950F/950FX</td>
<td>VMAX All Flash 950F/950FX models</td>
</tr>
<tr>
<td>VMAX All Flash 250F/250FX/450F/450FX/850F/850FX</td>
<td>VMAX All Flash 250F/250FX/450F/450FX/850F/850FX models</td>
</tr>
<tr>
<td>VMAX 400K</td>
<td>VMAX 400K models</td>
</tr>
<tr>
<td>VMAX 200K</td>
<td>VMAX 200K models</td>
</tr>
<tr>
<td>VMAX 100K</td>
<td>VMAX 100K models</td>
</tr>
<tr>
<td>VMAX 40K</td>
<td>VMAX 40K models</td>
</tr>
<tr>
<td>VMAX 20K</td>
<td>VMAX 20K models</td>
</tr>
<tr>
<td>VMAX 10K (Systems with SN xxx987xxxx)</td>
<td>VMAX 10K (Systems with SN xxx987xxxx) models</td>
</tr>
<tr>
<td>VMAX</td>
<td>VMAX models</td>
</tr>
</tbody>
</table>
VMAX and PowerMax configuration for HP-UX 11i v3.0

This section provides information to configure VMAX and PowerMax for HP-UX 11i v3.0. Refer to the following VMAX and PowerMax Simple Support Matrices, located in E-Lab Interoperability Navigator, for the most up-to-date information:

- PowerMax 8000
- PowerMax 2000
- VMAX 950F
- VMAX 850F
- VMAX 450F
- VMAX 250F
- VMAX 400K
- VMAX 200K
- VMAX 100K
- VMAX 40K
- VMAX 20K
- VMAX 10K (Systems with S/N xxx987xxxx)
- VMAX

Required director bit settings for HP-UX 11iv3 (HP-UX 11.31) initiators

Refer to the following VMAX and Symmetrix DMX Director Bits Simple Support Matrices, located in Dell EMC E-Lab Navigator, for the most up-to-date director port flags configuration requirements:

- VMAX 400K, VMAX 200K, and VMAX 100K Director Bit Settings and Features (T10 and SRDF Metro)
- VMAX 40K, VMAX 20K, and VMAX 10K SN xxx987xxxx Director Bit Settings
- Symmetrix VMAX, VMAX 10K SN xxx959xxxx, and VMAXe Director Bit Settings
- Symmetrix DMX-3 and DMX-4 Director Bit Settings

SPC-2 DMX, VMAX 20K/VMAX, VMAX 10K (Systems with SN xxx959xxxx), and VMAXe director flag

HP-UX 11i v3.0 is unsupportable without the Symmetrix DMX, VMAX 20K/VMAX, VMAX 10K (Systems with SN xxx959xxxx), and VMAXe SPC-2 port flag enabled for the HP-UX 11i v3.0 initiators, SPC-2 must be enabled on the Symmetrix, in addition to the C (common serial number) and V (Volume Set addressing) bits, for all HP-UX 11.31 device paths. The PP (Point-to-Point) director bit is also required for all FC-SW topology connections. These flags may be set on a per FA port basis in the DMX, VMAX 20K/VMAX, VMAX 10K (Systems with SN xxx959xxxx), and VMAXe configuration or they may be set on an initiator basis in heterogeneous attachment environments utilizing Solution Enabler.

The SPC-2 flag is supported with Solutions Enabler beginning with rev 6.2 for heterogeneous initiator types and can be configured on an initiator WWN basis beginning with SE 6.4 for DMX and SE 7.0 for VMAX 20K/VMAX, VMAX 10K (Systems with SN xxx959xxxx), and VMAXe.
VMAX 400K, VMAX 200K, VMAX 100K, VMAX 40K, VMAX 20K/VMAX, VMAX 10K (Systems with SN xxx959xxxx), VMAXe, and Symmetrix DMX minimum microcode requirements for HP-UX 11iv3 (11.31)

See Table 2 on page 21 for the minimum microcode for the VMAX3 Family, VMAX Family, and Symmetrix DMX.

Note: The VMAX3 Family includes VMAX 400K, VMAX 200K, and VMAX 100K.

The VMAX Family includes VMAX 40K, VMAX 20K/VMAX, VMAX 10K (Systems with SN xxx987xxxx), VMAX 10K (Systems with SN xxx959xxxx), and VMAXe.

VMAX and DMX os07 director flags

Note: The VMAX3 Family includes VMAX 400K, VMAX 200K, and VMAX 100K.

The VMAX Family includes VMAX 40K, VMAX 20K/VMAX, VMAX 10K (Systems with SN xxx987xxxx), VMAX 10K (Systems with SN xxx959xxxx), and VMAXe.

HP-UX 11i v3.0 introduces the following new host-based functionalities:

- Automated device discovery of newly configured devices and/or device paths.
- Automated creation of DSFs (device special files) for newly configured devices.
- Automated detection and adaptation of certain device attribute changes inclusive of LUN capacity change event.
- User configurable device aliases (support for SET DEVICE IDENTIFIER and REPORT DEVICE IDENTIFIER commands).

The related required VMAX 400K, VMAX 200K, and VMAX 100K, VMAX 40K, VMAX 20K/VMAX, VMAX 10K (Systems with SN xxx987xxxx), VMAX 10K (Systems with SN xxx959xxxx), and VMAXe, and Symmetrix DMX microcode enhancements for support of this functionality will be enabled with the VMAX 400K, VMAX 200K, and VMAX 100K, VMAX 40K, VMAX 20K/VMAX, VMAX 10K (Systems with SN xxx987xxxx), VMAX 10K (Systems with SN xxx959xxxx), and VMAXe, and Symmetrix DMX os07 director flag. This flag should be set in addition to the SPC-2 director flag. The VMAX 400K, VMAX 200K, and VMAX 100K, VMAX 40K, VMAX 20K/VMAX, VMAX 10K (Systems with SN xxx987xxxx), VMAX 10K (Systems with SN xxx959xxxx), and VMAXe, and Symmetrix DMX os07 port flag setting must be consistent across all device paths to any given Symmetrix volume from any HP-UX 11iv3 (HP-UX 11.31) host.

- The related required VMAX 400K, VMAX 200K, and VMAX 100K, VMAX 40K, VMAX 20K/VMAX, VMAX 10K (Systems with SN xxx987xxxx), VMAX 10K (Systems with SN xxx959xxxx), and VMAXe, and Symmetrix DMX microcode enhancements for support of this functionality will be enabled with the VMAX 400K, VMAX 200K, and VMAX 100K, VMAX 40K, VMAX 20K/VMAX, VMAX 10K (Systems with SN xxx987xxxx), VMAX 10K (Systems with SN xxx959xxxx), and VMAXe, and Symmetrix DMX os07 director flag.

This flag should be set in addition to the SPC-2 director flag. The VMAX 400K, VMAX 200K, and VMAX 100K, VMAX 40K, VMAX 20K/VMAX, VMAX 10K (Systems with SN xxx987xxxx), VMAX 10K (Systems with SN xxx959xxxx), and VMAXe, and Symmetrix DMX os07 port flag setting must be consistent across all device paths to any given
Symmetrix volume from any HP-UX 11iv3 (HP-UX 11.31) host.

**Note:** Refer to Table 2 on page 21 for limitations and restrictions.

### VMAX and DMX minimum microcode requirements for os07 director configuration flag support

**Note:** The VMAX3 Family includes VMAX 400K, VMAX 200K, and VMAX 100K.

The VMAX Family includes VMAX 40K, VMAX 20K/VMAX, VMAX 10K (Systems with SN xxx987xxxx), VMAX 10K (Systems with SN xxx959xxxx), and VMAXe.

See Table 2 on page 21 for the minimum microcode requirements.

HP-UX 11i v3.0 is supportable without the os07 VMAX 400K, VMAX 200K, and VMAX 100K, VMAX 40K, VMAX 20K/VMAX, VMAX 10K (Systems with SN xxx987xxxx), VMAX 10K (Systems with SN xxx959xxxx), and VMAXe, and Symmetrix DMX configuration port flag set; however, the new HP-UX 11i v3.0 functionalities will not be supported, and the following events will have to be managed manually.

- Device discovery of newly configured devices and/or device paths.
- Creation of DSFs (device special files) for newly configured devices.
- Detection and adaptation of certain online device attribute changes inclusive of LUN Capacity change event.

Support for the HP-UX 11i v3.0 user configurable device aliases cannot be supported until the VMAX 400K, VMAX 200K, and VMAX 100K, VMAX 40K, VMAX 20K/VMAX, VMAX 10K (Systems with SN xxx987xxxx), VMAX 10K (Systems with SN xxx959xxxx), and VMAXe, and Symmetrix DMX microcode enhancements are made available and enabled with the os07 director flag.
CHAPTER 2

Virtual Provisioning on VMAX and Symmetrix Systems

This chapter provides information about Dell EMC Virtual Provisioning and HP-UX on VMAX and Symmetrix systems.

**Note:** For further information regarding the correct implementation of Virtual Provisioning, refer to the *Symmetrix Virtual Provisioning Implementation and Best Practices Technical Note*, available at Dell EMC E-Lab Navigator.

- Symmetrix Virtual Provisioning 32
- Implementation considerations 36
- Symmetrix Virtual Provisioning in the HP-UX environment 39

**Note:** For information on Virtual Provisioning on a Symmetrix system, refer to Chapter 7, "Virtual Provisioning on VNX Series and CLARiiON Systems."
Symmetrix Virtual Provisioning

Dell EMC Symmetrix Virtual Provisioning™ enables organizations to improve speed and ease of use, enhance performance, and increase capacity utilization for certain applications and workloads. Virtual Provisioning integrates with existing device management, replication, and management tools, enabling customers to easily build Virtual Provisioning into their existing storage management processes.

Virtual Provisioning is the ability to present an application with more capacity than is physically allocated. The physical storage is then allocated to the application “on demand” from a shared pool of capacity as it is needed. Virtual Provisioning increases capacity utilization, improves performance, and simplifies storage management when increasing capacity.

Virtual Provisioning, which marks a significant advancement over technologies commonly known in the industry as “thin provisioning,” adds a new dimension to tiered storage in the array, without disrupting organizational processes.

Figure 1 Virtual Provisioning
**Terminology**

This section provides common terminology and definitions for Symmetrix and thin provisioning.

**VMAX/Symmetrix**

Basic VMAX and Symmetrix terms include:

- **Device**: A logical unit of storage defined within an array.
- **Device capacity**: The storage capacity of a device.
- **Device extent**: Specifies a quantum of logically contiguous blocks of storage.
- **Host accessible device**: A device that can be made available for host use.
- **Internal device**: A device used for a Symmetrix internal function that cannot be made accessible to a host.
- **Storage pool**: A collection of internal devices for some specific purpose.

**Thin provisioning**

Basic thin provisioning terms include:

- **Thin device**: A host accessible device that has no storage directly associated with it.
- **Data device**: An internal device that provides storage capacity to be used by thin devices.
- **Thin pool**: A collection of data devices that provide storage capacity for thin devices.
- **Thin pool capacity**: The sum of the capacities of the member data devices.
- **Thin pool allocated capacity**: A subset of thin pool enabled capacity that is allocated for the exclusive use of all thin devices bound to that thin pool.
- **Thin device user pre_allocated capacity**: The initial amount of capacity that is allocated when a thin device is bound to a thin pool. This property is under user control.
- **Bind**: Refers to the act of associating one or more thin devices with a thin pool.
- **Pre-provisioning**: An approach sometimes used to reduce the operational impact of provisioning storage. The approach consists of satisfying provisioning operations with larger devices that needed initially, so that the future cycles of the storage provisioning process can be deferred or avoided.
Thin device

Symmetrix Virtual Provisioning introduces a new type of host-accessible device called a thin device that can be used in many of the same ways that regular host-accessible Symmetrix devices have traditionally been used. Unlike regular Symmetrix devices, thin devices do not need to have physical storage completely allocated at the time the devices are created and presented to a host. The physical storage that is used to supply disk space for a thin device comes from a shared thin storage pool that has been associated with the thin device.

A thin storage pool is comprised of a new type of internal Symmetrix device called a data device that is dedicated to the purpose of providing the actual physical storage used by thin devices. When they are first created, thin devices are not associated with any particular thin pool. An operation referred to as binding must be performed to associate a thin device with a thin pool.

When a write is performed to a portion of the thin device, the Symmetrix allocates a minimum allotment of physical storage from the pool and maps that storage to a region of the thin device, including the area targeted by the write. The storage allocation operations are performed in small units of storage called data device extents. A round-robin mechanism is used to balance the allocation of data device extents across all of the data devices in the pool that have remaining un-used capacity.

When a read is performed on a thin device, the data being read is retrieved from the appropriate data device in the storage pool to which the thin device is bound. Reads directed to an area of a thin device that has not been mapped does not trigger allocation operations. The result of reading an unmapped block is that a block in which each byte is equal to zero will be returned. When more storage is required to service existing or future thin devices, data devices can be added to existing thin storage pools. New thin devices can also be created and associated with existing thin pools.

| Over-subscribed thin pool | A thin pool whose thin pool capacity is less than the sum of the reported sizes of the thin devices using the pool. |
| Thin device extent       | The minimum quantum of storage that must be mapped at a time to a thin device. |
| Data device extent       | The minimum quantum of storage that is allocated at a time when dedicating storage from a thin pool for use with a specific thin device. |
It is possible for a thin device to be presented for host use before all of the reported capacity of the device has been mapped. It is also possible for the sum of the reported capacities of the thin devices using a given pool to exceed the available storage capacity of the pool. Such a thin device configuration is said to be *over-subscribed*.

![Thin Device and Thin Storage Pool](image)

**Figure 2** Thin device and thin storage pool containing data devices

In **Figure 2**, as host writes to a thin device are serviced by the Symmetrix array, storage is allocated to the thin device from the data devices in the associated storage pool. The storage is allocated from the pool using a round-robin approach that tends to stripe the data devices in the pool.
Implementation considerations

When implementing Virtual Provisioning, it is important that realistic utilization objectives are set. Generally, organizations should target no higher than 60 percent to 80 percent capacity utilization per pool. A buffer should be provided for unexpected growth or a “runaway” application that consumes more physical capacity than was originally planned for. There should be sufficient free space in the storage pool equal to the capacity of the largest unallocated thin device.

Organizations also should balance growth against storage acquisition and installation timeframes. It is recommended that the storage pool be expanded before the last 20 percent of the storage pool is utilized to allow for adequate striping across the existing data devices and the newly added data devices in the storage pool.

Thin devices can be deleted once they are unbound from the thin storage pool. When thin devices are unbound, the space consumed by those thin devices on the associated data devices is reclaimed.

**Note:** Users should first replicate the data elsewhere to ensure it remains available for use.

Data devices can also be disabled and/or removed from a storage pool. Prior to disabling a data device, all allocated tracks must be removed (by unbinding the associated thin devices). This means that all thin devices in a pool must be unbound before any data devices can be disabled.

This section provides important considerations:

- “Over-subscribed thin pools” on page 36
- “Thin-hostile environments” on page 37
- “Pre-provisioning with thin devices in a thin hostile environment” on page 37
- “Host boot/root/swap/dump devices positioned on Symmetrix VP (tdev) devices” on page 38
- “Cluster configuration” on page 38

Over-subscribed thin pools

It is permissible for the amount of storage mapped to a thin device to be less than the reported size of the device. It is also permissible for the sum of the reported sizes of the thin devices using a given thin pool to exceed the total capacity of the data devices comprising the thin pool. In this case the thin pool is said to be over-subscribed. Over-subscribing allows the organization to present larger-than-needed devices to hosts and applications without having to purchase enough physical disks to fully allocate all of the space represented by the thin devices.

The capacity utilization of over-subscribed pools must be monitored to determine when space must be added to the thin pool to avoid out-of-space conditions.

Not all operating systems, filesystems, logical volume managers, multipathing software, and application environments will be appropriate for use with over-subscribed thin pools. If the application, or any part of the software stack underlying the application, has a tendency to produce dense patterns of writes to all available storage, thin devices will tend to become fully allocated quickly. If thin devices belonging to an over-subscribed pool are used in this type of environment, out-of-space and undesired conditions may be encountered before an administrator can take steps to add storage capacity to the thin data pool. Such environments are called thin-hostile.
Thin-hostile environments

There are a variety of factors that can contribute to making a given application environment thin-hostile, including:

- One step, or a combination of steps, involved in simply preparing storage for use by the application may force all of the storage that is being presented to become fully allocated.
- If the storage space management policies of the application and underlying software components do not tend to reuse storage that was previously used and released, the speed in which underlying thin devices become fully allocated will increase.
- Whether any data copy operations (including disk balancing operations and de-fragmentation operations) are carried out as part of the administration of the environment.
- If there are administrative operations, such as bad block detection operations or file system check commands, that perform dense patterns of writes on all reported storage.
- If an over-subscribed thin device configuration is used with a thin-hostile application environment, the likely result is that the capacity of the thin pool will become exhausted before the storage administrator can add capacity unless measures are taken at the host level to restrict the amount of capacity that is actually placed in control of the application.

Pre-provisioning with thin devices in a thin hostile environment

In some cases, many of the benefits of pre-provisioning with thin devices can be exploited in a thin-hostile environment. This requires that the host administrator cooperate with the storage administrator by enforcing restrictions on how much storage is placed under the control of the thin-hostile application.

For example:

- The storage administrator pre-provisions larger than initially needed thin devices to the hosts, but only configures the thin pools with the storage needed initially. The various steps required to create, map, and mask the devices and make the target host operating systems recognize the devices are performed.
- The host administrator uses a host logical volume manager to carve out portions of the devices into logical volumes to be used by the thin-hostile applications.
- The host administrator may want to fully preallocate the thin devices underlying these logical volumes before handing them off to the thin-hostile application so that any storage capacity shortfall will be discovered as quickly as possible, and discovery is not made by way of a failed host write.
- When more storage needs to be made available to the application, the host administrator extends the logical volumes out of the thin devices that have already been presented. Many databases can absorb an additional disk partition non-disruptively, as can most file systems and logical volume managers.
- Again, the host administrator may want to fully allocate the thin devices underlying these volumes before assigning them to the thin-hostile application.

In this example it is still necessary for the storage administrator to closely monitor the over-subscribed pools. This procedure will not work if the host administrators do not observe restrictions on how much of the storage presented is actually assigned to the application.
Host boot/root/swap/dump devices positioned on Symmetrix VP (tdev) devices

A boot /root /swap /dump device positioned on Symmetrix Virtual Provisioning (thin) device(s) is supported with Enginuity 5773 and later. However, some specific processes involving boot /root/swap/dump devices positioned on thin devices should not have exposure to encountering the out-of-space condition. Host-based processes such as kernel rebuilds, swap, dump, save crash, and Volume Manager configuration operations can all be affected by the thin provisioning out-of-space condition. This exposure is not specific to Dell EMC’s implementation of Thin Provisioning. Dell EMC strongly recommends that the customer avoid encountering the out-of-space condition involving boot / root /swap/dump devices positioned on Symmetrix VP (thin) devices using the following recommendations;

- It is strongly recommended that Virtual Provisioning devices utilized for boot /root/dump/swap volumes must be fully allocated or the VP devices must not be oversubscribed.
  Should the customer use an over-subscribed thin pool, they should understand that they need to take the necessary precautions to ensure that they do not encounter the out-of-space condition.

- It is not recommended to implement space reclamation, available with Enginuity 5874 and later, with pre-allocated or over-subscribed Symmetrix VP (thin) devices that are utilized for host boot/root/swap/dump volumes. Although not recommended, Space reclamation is supported on the listed types of volumes
  Should the customer use space reclamation on this thin device, they need to be aware that this freed space may ultimately be claimed by other thin devices in the same pool and may not be available to that particular thin device in the future.

Cluster configuration

When using high availability in a cluster configuration, it is expected that no single point of failure exists within the cluster configuration and that one single point of failure will not result in data unavailability, data loss, or any significant application becoming unavailable within the cluster. Virtual provisioning devices (thin devices) are supported with cluster configurations; however, over-subscription of virtual devices may constitute a single point of failure if an out-of-space condition should be encountered. To avoid potential single points of failure, appropriate steps should be taken to avoid under-provisioned virtual devices implemented within high availability cluster configurations.
Symmetrix Virtual Provisioning in the HP-UX environment

Symmetrix Virtual Provisioning introduces advantages to the HP-UX environment otherwise not possible:

• Reduction of System Administration tasks
  The frequency of tasks such as extending volume groups, extending logical volumes, and expansion of file systems can be reduced significantly. System administrators can configure their environments initially for future capacity requirements without the necessity of having the physical storage needed for future growth requirements available.

• Reduction and simplification of storage management tasks
  The frequency and complexity of making new storage capacity available to hosts is significantly reduced. Storage management operations such as device assignments, LUN masking, LUN capacity changes, device discovery operations, and storage capacity availability monitoring can be reduced or simplified. Monitoring of remaining available storage capacity is simplified and more accurate. Dell EMC tools for the monitoring of thin pool capacity utilization can accurately indicate the current amount of available capacity remaining in the thin pools.

• Efficient storage capacity management
  Efficient utilization of storage capacity is easily achieved since actual physical storage is not allocated to a Symmetrix thin device until the thin device is written to. Only the required amount storage capacity to save the update is utilized unless the user optionally pre-allocates capacity to the thin device.

• Performance considerations
  Data written to thin devices is striped across data devices of the related thin pool (or thin pools) the thin devices are bound to. This can alleviate back-end contentions or complement other methods of alleviating contentions, such as host-based striping.

HP-UX Virtual Provisioning support

Symmetrix Virtual Provisioning is supported with HP-UX 11iv3 (HP-UX 11.31), HP-UX 11iv2 (HP-UX 11.23), and HP-UX 11iv1 (HP-UX 11.11).

A Virtual Provisioning thin device configured as a boot, swap, or dump device is not currently supported.

Precaution considerations

Virtual Provisioning and the industry’s thin provisioning are new technologies. Relevant industry specifications have not yet been drafted. Virtual Provisioning, like thin provisioning, has the potential to introduce events into the environment which would not otherwise occur. The unavailability of relevant industry standards results in deviations with the host-based handling of these events and the possibility of undesirable implications when these events occur. However, with the proper precautions these exposures can be minimized or eliminated.
Thin pool out-of-space event

Insufficient monitoring of the thin pool can result in all of the thin pool enabled capacity to be allocated to thin devices bound to the pool. If over-subscription is implemented, the thin pool out-of-space event can result in a non-recoverable error being returned to a write request when it is sent to a thin device area that does not have capacity allocated from the thin pool. Simple precautions can avoid this from occurring, including the following.

- Monitoring of the consumption of the thin pool enabled capacity using Solutions Enabler or the Symmetrix Management console will keep the user informed when additional data devices should be added to the thin pool to avoid the thin pool out-of-space event. Threshold-based alerts can also be configured to automatically notify of the event or to add to capacity to the thin pool.
- Thin device allocation limits can be set to limit the amount of capacity a thin device can withdraw from the thin pool.
- Predictable growth of capacity utilization results in avoiding unexpected capacity demands. Implementing Virtual Provisioning with applications which have predictable growth of capacity utilization will avoid unexpected thin pool enabled capacity depletion.
- Avoid unnecessary block-for-block copy of a device to a thin device. Block-for-block copy of a device to a thin device results in the entire capacity of the source volume to be written to the thin device, regardless of how much user data the source volume contains. This can result in unnecessary allocation of space to the thin device.
- Plan for thin pool enabled capacity utilization not to exceed 60% – 80%

File system compatibility

Choose to implement file system types which are Virtual Provisioning compatible.

- Vxfs only 1% or less of thin device space is allocated at file system creation. (Best choice.)
- Hfs up to 36% of thin device space is allocated at file system creation. (Not Virtual Provisioning friendly.)
- Avoid defragmenting file systems positioned on thin devices since this can result in unnecessary capacity allocation from the thin pool.
- Avoid implementing Virtual Provisioning in Virtual Provisioning hostile environments.

Possible implications of the thin pool out-of-space event

The following are possible implications of thin pool out-of-space event.

**HP-UX 11.31** — Thin pool out-of-space and write request to an area of a thin device which has not had capacity allocated from the thin pool.
- Write request to a raw device (no fs) results in unrecoverable error which is not retried.
- VxFS write request results in unrecoverable write error, which is not retried.
- HFS write request continuously retried by fs, killable process hang, or fs must be unmounted to recover.

**HP-UX 11.23** — Thin pool out-of-space and write request to an area of a thin device which has not had capacity allocated from the thin pool.
- Write request to raw device (no fs) continuously retried (non-killable process hang).
- VxFS write request continuously retried by fs (non-killable process hang).
- HFS write request continuously retried by fs, killable process hang, or fs, must be unmounted to recover.

**HP-UX 11.11** — Thin pool out-of-space and write request to an area of a thin device which has not had capacity allocated from the thin pool.
- Write request to raw device (no fs) continuously retried (non-killable process hang).
- VxFS write request continuously retried by fs (non-killable process hang).
• HFS (supported on PA-Risc only) write request continuously retried by fs, killable process hang, or fs, must be unmounted to recover.

Unbound thin devices

Host-visible thin devices which are not bound to a thin pool have the same behavior as any other Symmetrix device inclusive of standard and bound thin devices, except for the handling of write requests. A process attempting to write to an unbound thin device will receive an error. An unbound thin device will appear to system administration utilities and a Volume Manager as an eligible device to be utilized or configured since all device discovery operations, device OPENs, and READ requests will successfully complete. However, when the system administration process attempts to write to the unbound thin device, an error will be returned.

Avoid attempting to utilize a thin device before it is bound to a thin pool.

Possible implications of write request received by an unbound thin device

**HP-UX 11.31** — With visible unbound TDEVs, write request to unbound thin device results in unrecoverable write error which is not retried.

**HP-UX 11.23** — With visible unbound TDEVs, write request to unbound thin device results in write error which is continuously retried (non-killable process hang).

**HP-UX 11.11** — With visible unbound TDEVs write request to unbound thin device results in write error which is continuously retried (non-killable process hang).
This chapter describes VPLEX-specific configuration in the HP-UX environment and contains support information.

- VPLEX overview 44
- Prerequisites 45
- Provisioning and exporting storage 46
- Storage volumes 48
- System volumes 50
- Required storage system setup 51
- Host connectivity 53
- Exporting virtual volumes to hosts 54
- Front-end paths 57
- Configuring HP-UX to recognize VPLEX volumes 59
- Volume Manager recommended settings 60
VPLEX overview

For detailed information about VPLEX, refer to the documentation available at Dell EMC E-Lab Navigator.

VPLEX documentation

Refer to the following documents for configuration and administration operations:

• EMC VPLEX with GeoSynchrony 5.0 Product Guide
• EMC VPLEX with GeoSynchrony 5.0 CLI Guide
• EMC VPLEX with GeoSynchrony 5.0 Configuration Guide
• EMC VPLEX Hardware Installation Guide
• EMC VPLEX Release Notes
• Implementation and Planning Best Practices for EMC VPLEX Technical Notes
• VPLEX online help, available on the Management Console GUI
• VPLEX Procedure Generator, available at Dell EMC E-Lab Navigator
• EMC Simple Support Matrix, EMC VPLEX and GeoSynchrony, available at Dell EMC E-Lab Navigator.

For the most up-to-date support information, you should always refer to the Dell EMC Simple Support Matrices.
Prerequisites

Before configuring VPLEX in the HP-UX environment, complete the following on each host:

• Confirm that all necessary remediation has been completed. This ensures that OS-specific patches and software on all hosts in the VPLEX environment are at supported levels according to the Dell EMC Simple Support Matrices.

• Confirm that each host is running VPLEX-supported failover software and has at least one available path to each VPLEX fabric.

  Note: Always refer to the Dell EMC Simple Support Matrices for the most up-to-date support information and prerequisites.

• If a host is running PowerPath, confirm that the load-balancing and failover policy is set to Adaptive.

• The following are supported with VPLEX:
  • HPUX 11iv3 with VxVM 5.1 SP1
  • HP-UX 11iv3 with VxMP 5.0 - 6.0
  • HP-UX 11iv2 with VxMP 4.1 - 5.0

IMPORTANT

For optimal performance in an application or database environment, ensure alignment of your host's operating system partitions to a 32 KB block boundary.

Veritas DMP settings with VPLEX

• Veritas DMP 5.1 SP1 requires the asl package 5.1.100.100 to correctly detect the VPLEX array.

• If a host attached to VPLEX is running Veritas DMP multipathing, change the following values of the DMP tunable parameters on the host to improve the way DMP handles transient errors at the VPLEX array in certain failure scenarios:
  • dmp_lun_retry_timeout for the VPLEX array to 60 seconds using the following command:
    "vxdmpadm setattr enclosure emc-vplex0 dmp_lun_retry_timeout=60"
  • recoveryoption to throttle and iotimeout to 30 using the following command:
    "vxdmpadm setattr enclosure emc-vplex0 recoveryoption=throttle iotimeout=30"
Provisioning and exporting storage

This section provides information for the following:

- “VPLEX with GeoSynchrony v4.x” on page 46
- “VPLEX with GeoSynchrony v5.x” on page 47

VPLEX with GeoSynchrony v4.x

To begin using VPLEX, you must provision and export storage so that hosts and applications can use the storage. Storage provisioning and exporting refers to the following tasks required to take a storage volume from a storage array and make it visible to a host:

1. Discover available storage.
2. Claim and name storage volumes.
3. Create extents from the storage volumes.
4. Create devices from the extents.
5. Create virtual volumes on the devices.
6. Create storage views to allow hosts to view specific virtual volumes.
7. Register initiators with VPLEX.
8. Add initiators (hosts), virtual volumes, and VPLEX ports to the storage view.

You can provision storage using the GUI or the CLI. Refer to the VPLEX Management Console Help or the *EMC VPLEX CLI Guide*, located at Dell EMC E-Lab Navigator, for more information.

*Figure 3 on page 47* illustrates the provisioning and exporting process.
VPLEX with GeoSynchrony v5.x

VPLEX allows easy storage provisioning among heterogeneous storage arrays. After a storage array LUN volume is encapsulated within VPLEX, all of its block-level storage is available in a global directory and coherent cache. Any front-end device that is zoned properly can access the storage blocks.

Two methods available for provisioning: EZ provisioning and Advanced provisioning. For more information, refer to the *EMC VPLEX with GeoSynchrony 5.0 Product Guide*, located at Dell EMC Online Support.
Storage volumes

A storage volume is a LUN exported from an array. When an array is discovered, the storage volumes view shows all exported LUNs on that array. You must claim, and optionally name, these storage volumes before you can use them in a VPLEX cluster. Once claimed, you can divide a storage volume into multiple extents (up to 128), or you can create a single full size extent using the entire capacity of the storage volume.

**Note:** To claim storage volumes, the GUI supports only the Claim Storage wizard, which assigns a meaningful name to the storage volume. Meaningful names help you associate a storage volume with a specific storage array and LUN on that array, and helps during troubleshooting and performance analysis.

This section contains the following information:

- “Claiming and naming storage volumes” on page 48
- “Extents” on page 48
- “Devices” on page 48
- “Distributed devices” on page 48
- “Rule sets” on page 49
- “Virtual volumes” on page 49

Claiming and naming storage volumes

You must claim storage volumes before you can use them in the cluster (with the exception of the metadata volume, which is created from an unclaimed storage volume). Only after claiming a storage volume can you use it to create extents, devices, and then virtual volumes.

Extents

An extent is a slice (range of blocks) of a storage volume. You can create a full size extent using the entire capacity of the storage volume, or you can carve the storage volume up into several contiguous slices. Extents are used to create devices, and then virtual volumes.

Devices

Devices combine extents or other devices into one large device with specific RAID techniques, such as mirroring or striping. Devices can only be created from extents or other devices. A device's storage capacity is not available until you create a virtual volume on the device and export that virtual volume to a host.

You can create only one virtual volume per device. There are two types of devices:

- Simple device — A simple device is configured using one component, which is an extent.
- Complex device — A complex device has more than one component, combined using a specific RAID type. The components can be extents or other devices (both simple and complex).

Distributed devices

Distributed devices are configured using storage from both clusters and therefore are only used in multi-cluster plexes. A distributed device's components must be other devices and those devices must be created from storage in different clusters in the plex.
Rule sets

Rule sets are predefined rules that determine how a cluster behaves when it loses communication with the other cluster, for example, during an inter-cluster link failure or cluster failure. In these situations, until communication is restored, most I/O workloads require specific sets of virtual volumes to resume on one cluster and remain suspended on the other cluster.

VPLEX provides a Management Console on the management server in each cluster. You can create distributed devices using the GUI or CLI on either management server. The default rule set used by the GUI makes the cluster used to create the distributed device detach during communication problems, allowing I/O to resume at the cluster. For more information, on creating and applying rule sets, refer to the *EMC VPLEX CLI Guide*, available at Dell EMC Online Support.

There are cases in which all I/O must be suspended resulting in a data unavailability. VPLEX with GeoSynchrony 5.0 is introduces the new functionality of VPLEX Witness. When a VPLEX Metro or a VPLEX Geo configuration is augmented by VPLEX Witness, the resulting configuration provides the following features:

- High availability for applications in a VPLEX Metro configuration (no single points of storage failure)
- Fully automatic failure handling in a VPLEX Metro configuration
- Significantly improved failure handling in a VPLEX Geo configuration
- Better resource utilization

For information on VPLEX Witness, refer to the *EMC VPLEX with GeoSynchrony 5.0 Product Guide*, located at Dell EMC Online Support.

Virtual volumes

Virtual volumes are created on devices or distributed devices and presented to a host via a storage view. Virtual volumes can be created only on top-level devices and always use the full capacity of the device.
System volumes

VPLEX stores configuration and metadata on system volumes created from storage devices. There are two types of system volumes. Each is briefly discussed in this section:

- “Metadata volumes” on page 50
- “Logging volumes” on page 50

Metadata volumes

VPLEX maintains its configuration state, referred to as metadata, on storage volumes provided by storage arrays. Each VPLEX cluster maintains its own metadata, which describes the local configuration information for this cluster as well as any distributed configuration information shared between clusters.

For more information about metadata volumes for VPLEX with GeoSynchrony v4.x, refer to the *EMC VPLEX CLI Guide*, available at Dell EMC Online Support.

For more information about metadata volumes for VPLEX with GeoSynchrony v5.x, refer to the *EMC VPLEX with GeoSynchrony 5.0 Product Guide*, located at Dell EMC Online Support.

Logging volumes

Logging volumes are created during initial system setup and are required in each cluster to keep track of any blocks written during a loss of connectivity between clusters. After an inter-cluster link is restored, the logging volume is used to synchronize distributed devices by sending only changed blocks over the inter-cluster link.

For more information about logging volumes for VPLEX with GeoSynchrony v4.x, refer to the *EMC VPLEX CLI Guide*, available at Dell EMC Online Support.

For more information about logging volumes for VPLEX with GeoSynchrony v5.x, refer to the *EMC VPLEX with GeoSynchrony 5.0 Product Guide*, located at Dell EMC Online Support.
Required storage system setup

VMAX, Symmetrix, VNX series, and CLARiiON product documentation and installation procedures for connecting a VMAX, Symmetrix, VNX series, or CLARiiON storage system to a VPLEX Instance are available at Dell EMC Online Support.

Required Symmetrix FA bit settings

For VMAX or Symmetrix-to-VPLEX connections, configure the Symmetrix Fibre Channel directors (FAs) as shown in Table 4.

Note: Dell EMC recommends that you download the latest information before installing any server.

Table 4 Required Symmetrix FA bit settings for connection to VPLEX

<table>
<thead>
<tr>
<th>Set</th>
<th>Do not set</th>
<th>Optional</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPC-2 Compliance (SPC2)</td>
<td>Disable Queue Reset on Unit Attention (D)</td>
<td>Linkspeed</td>
</tr>
<tr>
<td>SCSI-3 Compliance (SC3)</td>
<td>AS/400 Ports Only (AS4)</td>
<td>Enable Auto-Negotiation (EAN)</td>
</tr>
<tr>
<td>Enable Point-to-Point (PP)</td>
<td>Avoid Reset Broadcast (ARB)</td>
<td>VCM/ACLX1</td>
</tr>
<tr>
<td>Unique Worldwide Name (UWN)</td>
<td>Environment Reports to Host (E)</td>
<td></td>
</tr>
<tr>
<td>Common Serial Number (C)</td>
<td>Soft Reset (S)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Open VMS (OVMS)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Return Busy (B)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enable Sunapee (SCL)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sequent Bit (SEQ)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Non Participant (N)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>OS-2007 (OS compliance)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Linkspeed</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enable Auto-Negotiation (EAN)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>VCM/ACLX1</td>
<td></td>
</tr>
</tbody>
</table>

1. Must be set if VPLEX is sharing Symmetrix directors with hosts that require conflicting bit settings. For any other configuration, the VCM/ACLX bit can be either set or not set.

Note: When setting up a VPLEX-attach version 4.x or earlier with a VNX series or CLARiiON system, the initiator type must be set to CLARiiON Open and the Failover Mode set to 1. ALUA is not supported.

When setting up a VPLEX-attach version 5.0 or later with a VNX series or CLARiiON system, the initiator type can be set to CLARiiON Open and the Failover Mode set to 1 or Failover Mode 4 since ALUA is supported.

Refer to Table 18 on page 126 for more information.

If you are using the LUN masking, you will need to set the VCM/ACLX flag. If sharing array directors with hosts which require conflicting flag settings, VCM/ACLX must be used.

Note: The FA bit settings listed in Table 4 are for connectivity of VPLEX to Symmetrix arrays only. For host to Symmetrix FA bit settings, please refer to the Dell EMC Simple Support Matrices.
Supported storage arrays

The Dell EMC VPLEX Simple Support Matrix lists the storage arrays that have been qualified for use with VPLEX.

Refer to the VPLEX Procedure Generator, available at Dell EMC Online Support, to verify supported storage arrays.

VPLEX automatically discovers storage arrays that are connected to the back-end ports. All arrays connected to each director in the cluster are listed in the storage array view.

Initiator settings on back-end arrays

Refer to the VPLEX Procedure Generator, available at Dell EMC Online Support, to verify the initiator settings for storage arrays when configuring the arrays for use with VPLEX.

Notes
Be aware of the following issue and workaround.

Problem
The HP-UX initiator is not logging into VPLEX. The current discovery method used by the tachyon driver does not report the WWNs of the N_Ports that have not already logged into the VPLEX ports.

Workaround
If the HP-UX initiator is not displayed, manually register the initiator. The port WWN can be found either on the HP-UX system or from the zoning on the switch. For example:

```
export initiator-port register -p <wwn_you_found_for_the_port_name> -i <name> -t hpux
```
Host connectivity

For the most up-to-date information on qualified switches, hosts, host bus adapters, and software, always consult the Dell EMC Simple Support Matrices, or contact your Dell EMC Customer Representative.

The latest Dell EMC-approved HBA drivers and software are available for download at the following websites:

- http://www.emulex.com
- http://www.qlogic.com
- http://www.brocade.com

The Dell EMC HBA installation and configurations guides are available at the Dell EMC-specific download pages of these websites.

**Note:** Direct connect from a host bus adapter to a VPLEX engine is not supported.
Exporting virtual volumes to hosts

A virtual volume can be added to more than one storage view. All hosts included in the storage view will be able to access the virtual volume.

The virtual volumes created on a device or distributed device are not visible to hosts (or initiators) until you add them to a storage view. For failover purposes, two or more front-end VPLEX ports can be grouped together to export the same volumes.

A volume is exported to an initiator as a LUN on one or more front-end port WWNs. Typically, initiators are grouped into initiator groups; all initiators in such a group share the same view on the exported storage (they can see the same volumes by the same LUN numbers on the same WWNs).

An initiator must be registered with VPLEX to see any exported storage. The initiator must also be able to communicate with the front-end ports over a Fibre Channel switch fabric. Direct connect is not supported. Registering an initiator attaches a meaningful name to the WWN, typically the server’s DNS name. This allows you to audit the storage view settings to determine which virtual volumes a specific server can access.

Exporting virtual volumes consists of the following tasks:

1. Creating a storage view, as shown in Figure 4.

![Figure 4 Create storage view](image-url)
2. Registering initiators, as shown in Figure 5.

![Figure 5 Register initiators](image)

**Note:** When initiators are registered, you can set their type as indicated in Table 5 on page 58.

3. Adding ports to the storage view, as shown in Figure 6.

![Figure 6 Add ports to storage view](image)
4. Adding virtual volumes to the storage view, as shown in Figure 7.

![Figure 7 Add virtual volumes to storage view](image_url)
Front-end paths

This section contains the following information:

- "Viewing the World Wide Name for an HBA port" on page 57
- "VPLEX ports" on page 58
- "Initiators" on page 58

Viewing the World Wide Name for an HBA port

Each HBA port has a World Wide Name (WWN) associated with it. WWNs are unique identifiers that the VPLEX engine uses to identify its ports and host’s initiators. You can use one of the following ways to view WWNs:

- Switch’s name server output
- `syminq` command (Symmetrix users)
- `fcmsutil`
  
  This is an FC HBA command. This command provides HBA WWN, hardware path, fabric login, and status (online/offline) information.

  To use `fcmsutil`, you must know the device file name. Enter the following command to determine the device file:

  `ioscan -fknd fcd`

  The output varies depending on the device, and the version of HP-UX which you are using (HP-UX 11i v2 and 11i v3 outputs vary considerably). A sample for HP-UX 11i v2 follows:

  ```
  fc      1   1/0/2/1/1    fcd    CLAIMED    INTERFACE    HP AB379-60001 4Gb Dual Port PCI/PCI-X
  Fibre Channel Adapter (FC Port 2)
  /dev/fcd1
  ```

  If the device file does not display in the ioscan output, run

  `/sbin/rc2.d/S900hpfcms start` to recreate the device file.

  To use the basic `fcmsutil` command, enter the following command:

  `/opt/fcms/bin/fcmsutil /dev/<device_filename>`

  If you use `fcmsutil` with dual port universal adapter A6826A, enter the following command:

  `fcmsutil /dev/fcdx`

  where: \( x \) is the number assigned to the adapter port being accessed.

  The output is similar to the following example:

  ```
  Vendor ID is = 0x001077
  Device ID is = 0x002312
  PCI Sub-system Vendor ID is = 0x00103c
  PCI Sub-system ID is = 0x0012ba
  PCI Mode = PCI-X 66 MHZ
  ISP Code version = 3.2.26
  ISP Chip Version = 3
  Topology = PTTOPT_FABRIC
  Link Speed = 1Gb
  Local N_Port_id is = 0x211413
  Previous N-Port_id is = None
  N_Port Node World Wide Name = 0x50060b00001d21fd
  ```
VPLEX ports

The virtual volumes created on a device are not visible to hosts (initiators) until you export them. Virtual volumes are exported to a host through front-end ports on the VPLEX directors and HBA ports on the host/server. For failover purposes, two or more front-end VPLEX ports can be used to export the same volumes. Typically, to provide maximum redundancy, a storage view will have two VPLEX ports assigned to it, preferably from two different VPLEX directors. When volumes are added to a view, they are exported on all VPLEX ports in the view, using the same LUN numbers.

Initiators

For an initiator to see the virtual volumes in a storage view, it must be registered and included in the storage view's registered initiator list. The initiator must also be able to communicate with the front-end ports over Fibre Channel connections through a fabric.

A volume is exported to an initiator as a LUN on one or more front-end port WWNs. Typically, initiators are grouped so that all initiators in a group share the same view of the exported storage (they can see the same volumes by the same LUN numbers on the same same WWN host types).

Ensure that you specify the correct host type in the Host Type column as this attribute cannot be changed in the Initiator Properties dialog box once the registration is complete. To change the host type after registration, you must unregister the initiator and then register it again using the correct host type.

VPLEX supports the host types listed in Table 5. When initiators are registered, you can set their type, also indicated in Table 5.

<table>
<thead>
<tr>
<th>Host</th>
<th>Initiator type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows, MSCS, Linux</td>
<td>default</td>
</tr>
<tr>
<td>AIX</td>
<td>Aix</td>
</tr>
<tr>
<td>HP-UX</td>
<td>Hp-ux</td>
</tr>
<tr>
<td>Solaris, VCS</td>
<td>Sun-vcs</td>
</tr>
</tbody>
</table>
Configuring HP-UX to recognize VPLEX volumes

You must configure a HP-UX host to recognize VPLEX virtual volumes. To do this, complete the following steps:

1. On a HP-UX host, type `ioscan` to scan for new disks.
2. Type `ioscan -fnC disk` to see the new volumes.

   ```
   disk 6 0/4/0/0/0.23.41.0.0.0.0 sdisk CLAIMED DEVICE EMC Invista
   /dev/dsk/c5t0d0 /dev/rdsk/c5t0d0
   disk 4 0/4/0/0/0.1.23.40.0.0.0.0 sdisk CLAIMED DEVICE EMC Invista
   /dev/dsk/c3t0d0 /dev/rdsk/c3t0d0
   ```

3. On an HP-UX host, type `insf -e` to create device’s special files.

   If you are running volume management software, follow the necessary procedures in your volume management software documentation.

4. On an HP-UX host with VxVM/DMP, type `vxdisk scandisks` to detect new disks by Veritas.

   If the Veritas asl is installed properly, `vxdmpadm listenclosure` will list the enclosure name correctly.

   ```
   # vxdmpadm listenclosure
   
   ENCLR_NAME    ENCLR_TYPE    ENCLR_SNO      STATUS       ARRAY_TYPE     LUN_COUNT
   ==============================================================
   emc-vplex0    EMC-VPLEX    FNM00103700051  CONNECTED    VPLEX-A/A     31
   ```
Volume Manager recommended settings

Dell EMC recommends the following settings.

**pvtimeout**  Controls how long an I/O will wait before timing out on a physical path to a device before it fails the I/O and attempts an alternate path. This path switching will continue for the length of time lvtimeout is set.

The default behavior allows an I/O to wait for 30 seconds on a path before attempting another path. This continues until the I/O completes *without ever returning a failure* to the overlying application. This causes the application to stall for as long as necessary to allow at least one path to a device to be restored.

Dell EMC supports the default HP lvm pvtimeout and default VxVM pftimeout, timeout parameters with HP-UX and VPLEX. This includes in-family and out-of-family NDU upgrades.

**lvtimeout**  By default, lvtimeout = 0. An error is never returned to the application from the Volume Manager.

When this value is non-zero, an error returns to the application upon its expiration. Typically the default lvtimeout (lvtimeout = 0) is configured, with the exception of a few DB applications utilizing async I/O. If, for this reason, it is set to non-zero, the value configured also has a dependency on the configured pvtimeout parameter setting. The lvtimeout parameter is application dependent.

The only known situation where lvtimeout should be changed from default is for applications that *must* perform their own retries. Currently, the only application in wide use that requires this behavior is Sybase.
This chapter covers the Fibre Channel environment for HP 9000 and Integrity Itanium hosts with HP-UX 11x and VMAX or Symmetrix. It includes device addressing, HBA, and switch information.

- Addressing 62
- Fabric configuration 62
- HBA 63
- Switch 63
- Incorporating VMAX or Symmetrix/Fibre Channel 64
- HP hardware device mapping 65
- Addressing VMAX or Symmetrix devices 68
Addressing

HP-UX currently uses only the Volume Set addressing method for accessing Fibre Channel devices. Volume Set addressing supports up to 16,384 addresses and up to 512 logical devices (depending on the type of host bus adapter used).

Refer to “Addressing VMAX or Symmetrix devices” on page 68 for more information.

Fabric configuration

- The supported fan-in ratio is 1:24 for all supported DMX and VMAX systems. The supported fan-out ratio, however, the type of IO module, topology, Symmetrix/VMAX model, and microcode release in use can be factors in determining the supported fan-out ratio, refer to Dell EMC E-Lab Navigator for more specifics on the supported fan-out ratio for your configuration.

  **Note:** Refer to the storage array properties table in the Dell EMC Simple Support Matrices for the latest supportable numbers.

  **Note:** Refer to Table 3 on page 26 for specific Symmetrix models.

- VMAX and Symmetrix systems support zoning by both WWN and port.
- A boot device located on the VMAX or Symmetrix system cannot be more than two hops from the initiator it boots.
HBA

Follow the HP recommendations for installation and setup of the appropriate host bus adapter (HBA) for your system. Refer to Dell EMC E-Lab Navigator for supported HBAs in the HP-UX environment.

Switch

Refer to Dell EMC E-Lab Navigator for supported switches in the HP-UX environment. Additional information is provided in the following notes.

- An HP-UX external boot/dump (FC-SW) port on a Brocade switch must be locked as a G port by executing, ‘portcfggport port_number,1’ through a telnet session on the switch.
- For FC-SW 2 Gb boot and/or dump using A6795A the auto-negotiation flag must be enabled on the switch port to which the HBA is attached.
- Boot support in an HP-UX environment with Brocade 12000 or Dell EMC ED-12000B requires minimum firmware revision 4.0.2a.
- Domain value 8 cannot be utilized when attaching HP-UX initiators (HBAs).
- Following a zone config change on a switch, execute ioscan -fn on the host in order for the changes to be recognized by the server.
- On a system with PowerPath installed and WWN zoning on the switch, if a path is deleted from the zone, that path may still be accessible on the host. The path must be manually removed from the PowerPath configuration on the host. If the path is part of an LVM volume group, it must first be removed from the volume group (vgreduce /dev/dsk/cxtxdx) otherwise PowerPath will not allow the path to be deleted from its configuration.
- For fabric switches, Dell EMC recommends single initiator WWN zoning, but will support both WWN and port, single, or multi-initiator zoning.
- Heterogeneous storage attachments are supported in a Fibre Channel fabric configuration provided the different storage types are isolated in different fabric zones. Shared fabric and shared server are allowed with heterogeneous storage.
Incorporating VMAX or Symmetrix/Fibre Channel

The host can see all the VMAX or Symmetrix devices assigned to that host interface after all of the following are accomplished:

- The VMAX or Symmetrix system has devices assigned with device addresses.
- The VMAX or Symmetrix Fibre Channel directors are switched on line.
- `ioscan` with `Probe` is done.
- Device files were built with `insf`.

Devices are presented to the host in the same manner as devices accessed through a standard SCSI interface.

Note: If upgrading an existing Symmetrix SCSI interface to Fibre Channel, refer to Appendix A, “Migrating from SCSI Connections to Fibre Channel”.
HP hardware device mapping

The hardware path format for HP-UX 11i v1.0 and HP-UX 11i v2.0, as well as HP-UX 11i v3.0 legacy dsf is:


where:

- **Bus_Converter** — One of the possible bus converters providing the interconnect to the bus to which the Fibre Channel adapter is connected.
- **Adapter** — Module address of the Fibre Channel adapter.
- **Protocol_Type** — Depends on the Fibre Channel topology:
  - FC-AL — FCP, represented by the value 8.
  - FC-SW — 1st byte (domain portion) of the N_Port identifier of the Symmetrix system.
- **Area** — 2nd byte (area portion) of the N_Port identifier of the Symmetrix system:
  - FC-AL — 0.
  - FC-SW — The value is determined by the switch port to which the device is attached.
- **Port**:
  - For hardware paths of SCSI FCP targets connected directly to Fibre Channel, the port element of the hardware path is set to value 255, and the 3rd byte (port portion) of the target (Symmetrix) N_Port identifier (loop ID for FC-AL, port number for FC-SW) is used to form the values of the bus and target elements of the hardware path.
  - For hardware paths of devices or volumes associated with an array-type device, the port element of the hardware path is set to the 3rd byte (port portion) of the N_Port identifier of the Symmetrix system.

**Note:** For an arbitrated loop device attached to an FL_Port, this is the hard physical address of the Fibre Channel target.

- **Bus**:
  - For hardware paths of SCSI FCP targets connected directly to Fibre Channel, the bus element of the hardware path gets its value from the upper 4 bits of the port portion of the N_Port identifier, which is the upper 4 bits of the loop ID (FC-AL) or port number (FC-SW).
  - For the hardware path of a device connected to an array-type device, the bus element of the hardware path is set to the bus number (0 through 7) in the array associated with the device.
  - For the hardware path of a volume associated with an array-type device the bus element of the hardware path is set to the value of the upper 7 bits of the 14-bit volume number.
- **Target**:
• For hardware paths of SCSI FCP targets connected directly to Fibre Channel, the target element of the hardware path gets its value from the lower 4 bits of the port portion of the N_Port identifier, which is the lower 4 bits of the loop ID (FC-AL) or port number (FC-SW).

• For a hardware path of a device connected to an array-type device the target element of the hardware path is set to the target number (0 through 15) of the device on the specified bus in the array.

• For a hardware path of volume associated with an array-type device the target element of the hardware path is set to the value of bits 6 through 3 (0 is least significant bit) of the 14-bit volume number.

• **LUN:**
  • For hardware paths of SCSI FCP targets connected directly to Fibre Channel, the LUN element of the hardware path is the actual LUN ID (0 through 7) of the device.
  • For a hardware path of a device connected to an array-type device the LUN element of the hardware path is set to the LUN ID (0 through 7) of the device on the specified bus in the array.
  • For a hardware path of volume associated with an array-type device the LUN element of the hardware path is set to the value of bits 2 through 0 of the 14-bit volume number.

— **N_Port ID** — (FC-SW only) The ID of the Symmetrix Fibre Channel director port the HBA is zoned to see.

Figure 8 and Figure 9 show device mapping.

![Diagram of FC-AL hardware device mapping example](image_url)

**Figure 8** FC-AL hardware device mapping example
### Class I H/W Path

<table>
<thead>
<tr>
<th>H/W Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local PCI Bus Adapter (782)</td>
<td></td>
</tr>
<tr>
<td>HP Tachyon TL/TS FC Adapter</td>
<td></td>
</tr>
<tr>
<td>FCP Domain</td>
<td></td>
</tr>
<tr>
<td>FCP Array Interface</td>
<td></td>
</tr>
<tr>
<td>EMC SYMMEIRX</td>
<td></td>
</tr>
</tbody>
</table>

#### Domain.port.area = ID of 221313 = domain of 2

<table>
<thead>
<tr>
<th>Driver</th>
<th>S/W State</th>
<th>H/W Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>lba</td>
<td>CLAIMED</td>
<td>BUS_NEXUS</td>
<td>Local PCI Bus Adapter (782)</td>
</tr>
<tr>
<td>td</td>
<td>CLAIMED</td>
<td>INTERFACE</td>
<td>HP Tachyon TL/TS FC Adapter</td>
</tr>
<tr>
<td>fc</td>
<td>CLAIMED</td>
<td>INTERFACE</td>
<td>FCP Domain</td>
</tr>
<tr>
<td>fcp</td>
<td>CLAIMED</td>
<td>INTERFACE</td>
<td>FCP Array Interface</td>
</tr>
<tr>
<td>tgt</td>
<td>CLAIMED</td>
<td>DEVICE</td>
<td>EMC SYMMEIRX</td>
</tr>
<tr>
<td>sdisk</td>
<td>CLAIMED</td>
<td>DEVICE</td>
<td>EMC SYMMEIRX</td>
</tr>
<tr>
<td>sctl</td>
<td>CLAIMED</td>
<td>DEVICE</td>
<td>EMC SYMMEIRX</td>
</tr>
</tbody>
</table>

#### Domain.port.area = ID of 221313 = domain of 2

- **N_Port ID**: Port Area Domain
- **Port**: Area Domain
- **Area**: Domain
- **Domain**: Domain

---

**Figure 9** FC-SW hardware device mapping example
Addressing VMAX or Symmetrix devices

This section describes the methods of addressing VMAX or Symmetrix devices over Fibre Channel.

Arbitrated loop addressing

The Fibre Channel arbitrated loop (FC-AL) topology defines a method of addressing ports, arbitrating for use of the loop, and establishing a connection between Fibre Channel NL_Ports (level FC-2) on HBAs in the host and Fibre Channel directors (via their adapter cards) in the Symmetrix system. Once loop communications are established between the two NL_Ports, device addressing proceeds in accordance with the SCSI-3 Fibre Channel Protocol (SCSI-3 FCP, level FC-4).

The Loop Initialization Process (LIP) assigns a physical address (AL_PA) to each NL_Port in the loop. Ports that have a previously acquired AL_PA are allowed to keep it. If the address is not available, another address may be assigned, or the port may be set to non-participating mode.

**Note:** The AL-PA is the low-order 8 bits of the 24-bit address. (The upper 16 bits are used for Fibre Channel fabric addressing only; in FC-AL addresses, these bits are x'0000'.)

MVAX or Symmetrix Fibre Channel director bit settings (listed in Dell EMC E-Lab Navigator) control how the VMAX or Symmetrix system responds to the Loop Initialization Process.

After the loop initialization is complete, the VMAX/Symmetrix port can participate in a logical connection using the hard-assigned or soft-assigned address as its unique AL_PA. If the Symmetrix port is in non-participating mode, it is effectively off line and cannot make a logical connection with any other port.

A host initiating I/O with the VMAX/Symmetrix system uses the AL_PA to request an open loop between itself and the Symmetrix port. Once the arbitration process has established a logical connection between the Symmetrix system and the host, addressing specific logical devices is done through the SCSI-3 FCP.

Fabric addressing

Each port on a device attached to a fabric is assigned a unique 64-bit identifier called a World Wide Port Name (WWPN). These names are factory-set on the HBAs in the hosts, and are generated on the Fibre Channel directors in the VMAX/Symmetrix system.

When an N_Port (host server or storage device) connects to the fabric, a login process occurs between the N_Port and the F_Port on the fabric switch. During this process, the devices agree on such operating parameters as class of service, flow control rules, and fabric addressing. The N_Port’s fabric address is assigned by the switch and sent to the N_Port. This value becomes the Source ID (SID) on the N_Port outbound frames and the Destination ID (DID) on the N_Port inbound frames.

The physical address is a pair of numbers that identify the switch and port, in the format s,p, where s is a domain ID and p is a value associated to a physical port in the domain. The physical address of the N_Port can change when a link is moved from one switch port to
another switch port. The WWPN of the N_Port, however, does not change. A Name Server in the switch maintains a table of all logged-in devices, so N_Ports can automatically adjust to changes in the fabric address by keying off the WWPN.

The highest level of login that occurs is the process login. This is used to establish connectivity between the upper-level protocols on the nodes. An example is the login process that occurs at the SCSI FCP level between the HBA and the VMAX/Symmetrix system.

**SCSI-3 FCP addressing**

The VMAX/Symmetrix Fibre Channel director extracts the SCSI Command Descriptor Blocks (CDB) from the frames received through the Fibre Channel link. Standard SCSI-3 protocol is used to determine the addressing mode and to address specific devices.

HP-UX and the VMAX/Symmetrix system support Volume Set addressing as defined by the SCSI-3 Controller Commands (SCC). Volume Set Addressing uses the first two bytes (0 and 1) of the 8-byte LUN addressing structure. (Bits 7 and 6 of byte 0 are 01, identifying the addressing mode as Volume Set.) The remaining six bytes are set to zeros.

The VMAX/Symmetrix port identifies itself as an array controller in response to a host Inquiry command sent to LUN 00. This identification is done by returning the byte 0x0C in the Peripheral Device Type field of the returned data for Inquiry. If the Symmetrix system returns the byte 0x00 in the first byte of the returned data for Inquiry, the VMAX/Symmetrix system is identified as a direct access device.

Upon identifying the VMAX/Symmetrix system as an array controller device, the host should issue a SCSI-3 Report LUNS command (0xA0), in order to discover the LUNs.
CHAPTER 5

Host Environment

This chapter covers currently supported OS versions, servers, volume managers, boot configuration, and MC/ServiceGuard clusters when working with HP 9000 and Integrity Itanium hosts.

- HP-UX OS support 72
- HP-UX patches and support 77
- Useful HP-UX 11x utilities and functions 78
- Maximum LUN and file system sizes 79
- Recognizing new devices and LUNs 80
- Adding devices on line 81
- External boot from a VMAX or Symmetrix device 82
- System partitions 87
- Volume managers 90
- I/O time-out parameters 99
- Cluster 105
- VMAX and Symmetrix boot device in an HA environment 117
HP-UX OS support

Table 6 lists the OS versions currently supported.

Table 6 OS versions currently supported

<table>
<thead>
<tr>
<th>Release Name</th>
<th>OS Release Identifier</th>
<th>Platform</th>
<th>Introduced</th>
<th>Discontinued</th>
<th>Obsoleted</th>
</tr>
</thead>
<tbody>
<tr>
<td>HP-UX 11i v1.0</td>
<td>11.11</td>
<td>PA-RISC</td>
<td>12/00</td>
<td>12/31/09</td>
<td>12/31/13</td>
</tr>
<tr>
<td>HP-UX 11i v2.0</td>
<td>11.23</td>
<td>Integrity</td>
<td>9/26/03</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HP-UX 11i v2.0 September 2004 (and later)</td>
<td>11.23</td>
<td>Integrity &amp; PA-RISC</td>
<td>10/04</td>
<td>12/31/09</td>
<td>12/31/13</td>
</tr>
<tr>
<td>HP-UX 11i v3.0</td>
<td>11.31</td>
<td>Integrity &amp; PA-RISC</td>
<td>03/07</td>
<td>TBD</td>
<td>TBD</td>
</tr>
</tbody>
</table>

HP-UX 10.20 on PA-Risc

Dell EMC no longer supports HP-UX 10.20.

HP support for HP-UX 10.20 ended on July 1, 2003.

HP-UX 11.00

HP-UX 11.00 runs on HP PA-RISC servers only.

Note: Dell EMC no longer supports HP-UX 11.00.

HP support for HP-UX 11.00 ended December 31, 2006.

HP-UX 11i v1

HP-UX 11i v1 (11.11) runs on HP PA-RISC servers only.

HP-UX 11i v2

HP-UX 11i v2 (11.23) prior to the September 2004 release runs on HP Integrity Itanium-based servers only. Although this pre-September 2004 release is still supported, HP and Dell EMC strongly recommends that customers upgrade to the September 2004 release or later. HP no longer provides new updates or patches for the HP-UX 11i v2 pre-September 2004 Integrity-only release.

HP-UX 11i v2 September 2004 (and later)

HP-UX 11i v2 (11.23) September 2004 is also referred to as HP-UX 11i v2.0 Update 2.

The PA-RISC servers and the required processor-dependent code (pdc) level that support the HP-UX 11i v2 update 2 OS are listed in the following tables. Additional servers that support the HP-UX 11i v2 update 2 are the 64-bit A-Class, L-Class, and N-Class. This OS release is not supported on all 32-bit servers and the D, R, E, K, T, V Class servers.

**Table 7** Minimum system firmware, HP 9000 entry-level servers

<table>
<thead>
<tr>
<th>Server Model</th>
<th>PDC</th>
<th>BMC</th>
<th>MP</th>
</tr>
</thead>
<tbody>
<tr>
<td>rp2400</td>
<td>43.50</td>
<td></td>
<td></td>
</tr>
<tr>
<td>rp2430</td>
<td>43.50</td>
<td></td>
<td></td>
</tr>
<tr>
<td>rp2450</td>
<td>43.50</td>
<td></td>
<td></td>
</tr>
<tr>
<td>rp2470</td>
<td>43.50</td>
<td></td>
<td></td>
</tr>
<tr>
<td>rp5400</td>
<td>44.28</td>
<td></td>
<td></td>
</tr>
<tr>
<td>rp5430</td>
<td>44.12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>rp5450</td>
<td>44.28</td>
<td></td>
<td></td>
</tr>
<tr>
<td>rp5470</td>
<td>44.12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>rp7400</td>
<td>43.43</td>
<td></td>
<td></td>
</tr>
<tr>
<td>rp3410</td>
<td>44.24</td>
<td>02.34</td>
<td>E.02.29</td>
</tr>
<tr>
<td>rp3440</td>
<td>44.24</td>
<td>02.34</td>
<td>E.02.29</td>
</tr>
<tr>
<td>rp4410</td>
<td>44.21</td>
<td>02.37</td>
<td>E.02.29</td>
</tr>
<tr>
<td>rp4440</td>
<td>44.21</td>
<td>02.37</td>
<td>E.02.29</td>
</tr>
</tbody>
</table>


**Table 8** Minimum system firmware, HP 9000 mid-range and high-end servers

<table>
<thead>
<tr>
<th>System</th>
<th>Firmware</th>
<th>Release/Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>rp7405</td>
<td>17.008 (pdc)</td>
<td>v6.3</td>
</tr>
<tr>
<td>rp7410</td>
<td>17.008 (pdc)</td>
<td>v6.3</td>
</tr>
<tr>
<td>rp7420</td>
<td>21.003 (PA SFW)</td>
<td>v2.0</td>
</tr>
<tr>
<td>rp8400</td>
<td>17.008 (pdc)</td>
<td>v6.3</td>
</tr>
<tr>
<td>rp8420</td>
<td>21.003 (PA SFW)</td>
<td>v2.0</td>
</tr>
<tr>
<td>Superdome (PA8600 &amp; PA8700)</td>
<td>36.7 (pdc)</td>
<td>rel_5.4</td>
</tr>
<tr>
<td>Superdome (PA8600 &amp; PA8700)</td>
<td>21.2 (PA SFW)</td>
<td>rel_4.0</td>
</tr>
</tbody>
</table>

This section provides a summary overview of some of the new features in HP-UX 11i v3.0. For detailed information refer to HP's documentation website at http:/www.docs.hp.com/en/oshpux11iv3.html.

**HP-UX 11i v3.0**

HP-UX 11.31 with VMAX and Symmetrix overview

**Native load balancing**

Native IO load balancing and path failover with the following load balancing policies are available for configuration:

- round_robin
- least_cmd_load
- cl_round_robin
- preferred_path

**New style DSFs (device special files)**

The new style DSFs are:

- SCSI-3 agile addressing path independent io_nodes.
- Single new style dsf bound to LUN identifier.
- 256 bus instance limitation eliminated for new style DSFs (Device Special files).

**Legacy DSF (device special files)**

Dell EMC supports legacy HP-UX (11.11, 11.23) DSFs up to legacy HP-UX architectural limitations of 256 bus instances and 32K legacy DSFs.

**Automatic device discovery**

New devices and device paths are automatically discovered and new DSFs are created when needed. The insf daemon automatically creates DSFs for newly discovered devices.

**Automatic online discovery of LUN capacity changes**

LUN capacity changes are automatically discovered.

**Enhancements to ioscans**

Increased parallelism significantly increases completion times.

---

**Table 9** Minimum system firmware, HP Integrity entry-level servers

<table>
<thead>
<tr>
<th>System</th>
<th>BMC</th>
<th>MP</th>
<th>SFW</th>
</tr>
</thead>
<tbody>
<tr>
<td>rx1600</td>
<td>02.33</td>
<td>E.02.29</td>
<td>01.10</td>
</tr>
<tr>
<td>rx2600</td>
<td>01.52</td>
<td>E.02.29</td>
<td>02.31</td>
</tr>
<tr>
<td>rx4640</td>
<td>02.35</td>
<td>E.02.29</td>
<td>02.13</td>
</tr>
<tr>
<td>rx5670</td>
<td>01.30</td>
<td>E.02.29</td>
<td>02.23</td>
</tr>
</tbody>
</table>


---

**Table 10** Minimum system firmware, HP Integrity mid-range and high-end servers

<table>
<thead>
<tr>
<th>System</th>
<th>Firmware</th>
<th>Release/version</th>
</tr>
</thead>
<tbody>
<tr>
<td>rx7620</td>
<td>1.015 (IA SFW)</td>
<td>v2.0</td>
</tr>
<tr>
<td>rx8620</td>
<td>1.015 (IA SFW)</td>
<td>v2.0</td>
</tr>
<tr>
<td>Integrity Superdome</td>
<td>2.22 (IA SFW)</td>
<td>rel_4.0</td>
</tr>
</tbody>
</table>

**Host Environment**

- **ioscan -N** (upper case N)
  Displays ioscan output in scsi-3 agile addressing view.

- **ioscan -n** (lower case n)
  Displays ioscan output in legacy hardware path and DSF output view. (Default)

- **ioscan -m lun**
  Maps devices to lun paths.

- **ioscan -m dsf**
  Maps legacy DSFs to new style agile DSFs.

- **ioscan -m hwpath**
  Maps legacy to agile h/w paths.

- **ioscan -s**
  Displays stale io_nodes in ioconfig. (not in io tree).

---

**Support of 16 byte cdb and device > 2 TB**

HP-UX 11i v3.0 supports 16 byte cdb and devices greater than 2 TB.

**Device alias** *

Persistent device alias maximum of 128 bytes can be configured by user (ex: “My device number 1”).

**LVM**

Support dynamic LUN expansion of HP LVM physical volumes (vgmodify cmd) inclusive of:

- Modify max PE
- Modify max PV
- Modify max LV

**Volume group quiesce and resume**

- pvmove enhancement to support relocation of first extent of the PV allowing for modification of LVM metadata via vgmodify cmd.
- maxvg kernel parameter obsoleted, maximum number of configurable HP LVM volume groups always 256.

**Note:** Functionality not supported until 5772 microcode version or future release of 5771 or 5671 microcode is released.
The following are imposed configuration limitations for HP-UX 11.31:

- Maximum devices per host: 16K
- Maximum device paths per device: 32K
- Maximum device paths per host: 64K
- Maximum LUNs per hba: 1.5K

**HP-UX bundled applications**

HP-UX 11i v1.0, HP-UX 11i v2.0, and HP-UX 11i v3.0 offer multiple operating environments which are bundled applications geared towards specific computing environments. Table 11 lists some of the applications included in each of the operating environments.

<table>
<thead>
<tr>
<th>Applications</th>
<th>Foundation</th>
<th>Enterprise</th>
<th>Mission Critical</th>
<th>Technical computing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base VxFS</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Full VxFS (Online JFS)</td>
<td>--</td>
<td>X</td>
<td>X</td>
<td>--</td>
</tr>
<tr>
<td>Base VxVM</td>
<td>X</td>
<td>X</td>
<td>x</td>
<td>X</td>
</tr>
<tr>
<td>Full VxVM</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>MirrorDisk/UX</td>
<td>--</td>
<td>X</td>
<td>X</td>
<td>--</td>
</tr>
<tr>
<td>MC/ServiceGuard</td>
<td>--</td>
<td>--</td>
<td>X</td>
<td>--</td>
</tr>
</tbody>
</table>
HP provides updates and patch fixes for the HP-UX operating system by releasing both standard patch bundles and individual patches. For more detailed information on HP-UX patching, including where to find and how to install patch bundles and individual patches, please refer to the Patch Management User Guide available on the HP website: http://docs.hp.com/en/5991-4825/index.html.

HP-UX patch bundles are cumulative, prepackaged sets of patches that can be installed as a group at the same time. Proactive patching and installation of standard HP-UX patch bundles is strongly recommended to establish a stable patch level baseline for HP-UX systems.

Dell EMC qualifies and supports all standard HP-UX Quality Pack (QPK), Hardware Enablement (HWE), and required patch bundles as they become available upon release. However, support for standard HP-UX patch bundles will not be stated or noted in the Dell EMC E-Lab Navigator unless a particular patch bundle is required in order to support specific hardware or feature functionality in Dell EMC storage configurations. Standard HP-UX Quality Pack patch bundles and Hardware Enablement patch bundles that are not stated in the Dell EMC E-Lab Navigator are still supported and do not require an RPQ, unless otherwise noted.

HP-UX individual patches are single patches with a unique patch ID and are targeted for specific defects or functionality. Individual patches may be more recent patches that may have not yet been included in standard patch bundles. In most cases, individual patches are installed during reactive patching to fix a problem that has occurred.

Dell EMC does not test and qualify every HP-UX individual patch released. Dell EMC only tests and qualifies individual patches that enhance functionality or address interoperability issues specifically related to, or impacting, Dell EMC storage products and configurations. Consequently, the Dell EMC E-Lab Navigator will only note or list patches that are known to affect or impact Dell EMC storage configurations. Any individual patches that are required or recommended for interoperability with Dell EMC storage products will be noted and listed in the Dell EMC E-Lab Navigator. If an individual patch is not noted or listed, the patch is not known to be required for Dell EMC storage configurations.
Useful HP-UX 11x utilities and functions

This section lists HP-UX 11x functions and utilities you can use to define and manage Symmetrix devices. The use of these functions and utilities is optional. They are listed for reference only:

- **ioscan** — Provides a listing of devices connected to the host. This online hardware mapping program scans the system hardware for usable I/O systems devices or kernel I/O system data structures as appropriate and lists the results.
  
  Useful options for this function are:
  
  - `-C disk`  
    
    Restrict the output to all devices belonging to the disk class.
    
  - `-f`  
    
    Generate a full listing.
    
  - `-F`  
    
    Generate a compact listing.
    
  - `-n`  
    
    List device file names in the output.
    
  - `-M -H <hardware path>`  
    
    Force the software driver-specified hardware path into the kernel.

- **insf** — Installs special files and assigns logical unit numbers to devices in the system. Used for introducing newly attached devices to the system without rebooting.

- **fcmsutil** — FC HBA command. Provides HBA WWN, hardware path, fabric login, and status (online/offline) information.

- The **System Administration Manager** (SAM) is a menu-driven HP utility for managing system resources. Users familiar with SAM might find it more useful to use SAM for configuring new Symmetrix disks.

- HP-UX 11i v2.0 and HP-UX 11i v3.0 uses the web-based **pdweb** tool from the command line or through SAM to manage peripheral devices and cards.

- The **kcweb** tool is available for kernel tuning on HP-UX 11i v2.0 and HP-UX 11i v3.0.
Maximum LUN and file system sizes

The maximum LUN size supported in HP-UX environments is dependent on the usage of the LUN device. The maximum supported size limits of HP-UX volume managers and file systems are listed in Table 12, Table 13, and Table 14 on page 79. Refer to HP technical documentation for versions, licenses, and patches required for support.

Table 12 Maximum supported size limits

<table>
<thead>
<tr>
<th>Type</th>
<th>Device/volume</th>
<th>Size</th>
<th>OS version</th>
</tr>
</thead>
</table>
| LVM   | Physical device | • Maximum support size for LVM 1.0: 2 TB  
              • Maximum support size for LVM 2.x (2.0 and 2.1): 16 TB | HP-UX 11i v1.0, 11i v2.0 and 11i v3.0 |
|       | Logical volume | 2 TB | HP-UX 11i v1.0, 11i v2.0   |
|       | Logical volume | 16 TB | HP-UX11i v3.0              |
| VxVM  | Physical device | 2 TB |                             |
|       | Logical volume | 256 TB |                            |

1. The value is actually 1 byte less than 2 TB due to both 32-bit applications limitations and OS limitations.

Table 13 Maximum supported HFS file and file system sizes

<table>
<thead>
<tr>
<th>Type</th>
<th>File size¹</th>
<th>File system size¹</th>
<th>OS version</th>
</tr>
</thead>
<tbody>
<tr>
<td>HFS</td>
<td>128 GB</td>
<td>128 GB</td>
<td>HP-UX 11i v1.0, 11i v2.0 and 11i v3.0</td>
</tr>
</tbody>
</table>


Table 14 Maximum supported (VxFS) JFS file and file system sizes

<table>
<thead>
<tr>
<th>Version</th>
<th>Disk layout version</th>
<th>File size¹</th>
<th>File system size¹</th>
<th>OS version</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.5</td>
<td>4</td>
<td>2 TB</td>
<td>2 TB</td>
<td>11i v1.0</td>
</tr>
<tr>
<td>3.5</td>
<td>4</td>
<td>2 TB</td>
<td>2 TB</td>
<td>11i v2.0</td>
</tr>
<tr>
<td>3.5</td>
<td>5</td>
<td>2 TB</td>
<td>32 TB</td>
<td>11i v2.0</td>
</tr>
<tr>
<td>4.1</td>
<td>6</td>
<td>2 TB</td>
<td>32 TB</td>
<td>11i v2.0</td>
</tr>
<tr>
<td>4.1</td>
<td>6</td>
<td>2 TB</td>
<td>32 TB</td>
<td>11i v3.0</td>
</tr>
<tr>
<td>5.0</td>
<td>7</td>
<td>2 TB</td>
<td>32 TB</td>
<td>11i v2.0</td>
</tr>
</tbody>
</table>

Recognizing new devices and LUNs

**Note:** The information in this section pertains to HP-UX 11i v1.0 and HP-UX 11i v2.0, as well as HP-UX 11i v3.0 legacy dsf.

The host can identify the connected devices and create the block device (/dev/rdsk) and character device files (/dev/dsk).

To verify that the host has identified the connected devices:

1. Type `ioscan -fn [> filename]` and press Enter, where `filename` is the name of the file that will store this information. A listing of all devices found will be stored in the given filename.

2. Type `insf -e` and press Enter, or reboot the host.

In HP-UX 11x, your screen display will appear similar to Figure 10 or Figure 11. Note the card instance number next to the hardware path for the disk devices. Also note that the hardware path will differ from one machine model to another.

![Figure 10 Fibre Channel hardware path](image1)

![Figure 11 SCSI hardware path](image2)
Adding devices on line

Whenever devices are added to the Symmetrix system on line or device channel addresses are changed, you must perform the actions described below to introduce the new devices to the system.

You can define newly connected physical volumes to the system without rebooting the host. This requires use of the **insf** command in a statement similar to the following:

```
insf -H 2/4.0.0
```

where (in this example) `2/4.0.0` is a hardware path to which the new device has been connected.

Alternatively, you can use the following command sequence to look for all new hardware devices:

```
ioscan -fn
  -- (HP-UX 11i v1.0 and HP-UX 11i v2.0, as well as HP-UX 11i v3.0 legacy dsf)

insf -e

ioscan -fN
  -- (HP-UX 11i v3.0 new style dsf)
```
External boot from a VMAX or Symmetrix device

Both Dell EMC and HP support the use of VMAX or Symmetrix devices as external boot disks with LVM or VxVM volume managers. The high availability and data protection features of the VMAX/Symmetrix system make its disks attractive candidates for selection as the system root disk. Refer to the Dell EMC Simple Support Matrices for supported HBAs, servers, and pdc requirements. Following points should be considered when selecting a root device:

- Root, stand, and primary swap must reside on the same physical device.
- The following formula should be considered when selecting a root disk with sufficient space for a fresh install:

\[
\text{disk size} = n \times ('\text{system memory}' \text{ for swap/dump} + 'root' \text{ file system} + 'boot' \text{ (stand) file system})
\]

For example, if 'system memory' for swap/dump is 16 G, 'root' file system is 500 MB, and 'boot' (stand) file system is 500 MB, then the root device needs 17 G.

An external boot device can be set up in one of the following ways:

- “Fresh install,” next
- “Mirroring an internal OS to an external device” on page 83
- “Migrating an internal OS to an external device” on page 84

Fresh install

HP-UX may be installed on a VMAX/Symmetrix device using either HP Ignite Server or the OS cd or dvd. External boot with VxVM is an option with HP-UX 11i v1.0, HP-UX 11i v2.0, and HP-UX 11i v3.0. Refer to Dell EMC E-Lab Navigator for supported configurations.

---

Mirroring an internal OS to an external device

**Note:** The information in this section pertains to HP-UX 11i v1.0 and HP-UX 11i v2.0.

If the internal device is an LVM volume group, MirrorDisk-UX can be used to move boot to an external LVM VMAX/Symmetrix device. Factors to consider:

- MirrorDisk-UX is an add-on product on the Foundation Operating Environment on HP-UX 11i v1 and HP-UX 11i v2
- Device addition to the volume group may be restricted by LVM Max PV' limit
- LVM Max PE per PV could be a limitation

An LVM root volume group may also be converted to VxVM on an external Symmetrix device using `/etc/vx/bin/vxcp_lvmroot` command.

A VxVM internal root disk group may be mirrored to an external Symmetrix VxVM disk using the `/etc/vx/bin/vxrootmir` command.

Factors to consider in moving boot from LVM-to-VxVM and VxVM-to-VxVM:

- All root volumes must be in the rootdg disk group
- Root, boot, swap, and dump vols must be named rootvol, standvol, swapvol and dumpvol respectively
- Root, boot, swap and dump volumes must be contiguous
- Root, boot, swap and dump volumes must all reside on one disk (cannot span disks)
- Root, boot, swap and dump volumes can only have one subdisk
- Rootvol and swapvol volumes must be designated as special usage volume types root and swap respectively
- The target mirror device size may be identical or larger than the source
- Root disk group may be mirrored with Base VxVM
- Mirroring is LIF physical device to another physical device

---

1. Refer to “LVM guide” on page 90.
Migrating an internal OS to an external device

This section describes how to create an external boot disk using HP LVM on PA-RISC systems running HP-UX 11i.

The following example is for HP PA-RISC only. The boot configuration process for HP Integrity systems running HP-UX 11i v2.0 is entirely different.

To create an external boot disk:

1. Create a new volume group containing the disk c20t0d0 by entering statements similar to the following:

```
pvcreate -B /dev/rdsk/c20t0d0
mkboot /dev/rdsk/c20t0d0
mkboot -a "hpux /stand/vmunix" /dev/rdsk/c20t0d0
mkdir /dev/vgalt
mknod /dev/vgalt/group c 64 0x010000
vgcreate /dev/vgalt /dev/dsk/c20t0d0
```

2. Create the logical volumes required to boot the system (root, swap, and usr) in the new volume group by entering statements similar to the following:

```
lvcreate -L 200 -n altroot -r n -s y -C y /dev/vgalt
lvcreate -L 500 -n altswap -r n -s y -C y /dev/vgalt
lvcreate -l 50 -n altdump -r n -s y -C y /dev/vgalt
lvcreate -L 100 -n altusr /dev/vgalt
```

The sizes here are arbitrary; create the sizes you require.

3. Create filesystems and copy data from the original filesystems to the newly created filesystems using statements similar to the following:

```
newfs -F hfs /dev/vgalt/raltroot
newfs -F hfs /dev/vgalt/raltusr
mkdir /altroot
mkdir /altusr
mount /dev/vgalt/altroot /altroot
mount /dev/vgalt/altusr /altusr
```

4. Use the copy utility to copy all files from the original filesystems to the new filesystems.

```
cd /
cd /usr
find . -xdev | cpio -pdmux /altroot
cd /usr
find . -xdev | cpio -pdmux /altusr
```
4. Update BDRA for the new volume group to ensure that the system can boot from the alternative disk using statements similar to the following:

```
lvlnboot -R
lvlnboot -r /dev/vgalt/altroot /dev/vgalt
lvlnboot -s /dev/vgalt/altswap /dev/vgalt
lvlnboot -d /dev/vgalt/altdump /dev/vgalt
```

5. Check the boot configuration by entering the following:

```
lvlnboot -v
```

The boot configuration should appear similar to Figure 13.

```
# Boot Definitions for Volume Group /dev/vg00:
# Physical Volumes belonging in Root Volume Group:
# /dev/dsk/c0t0d0 -- Boot Disk
#    Root: lvol1  on: /dev/dsk/c0t0d0
#    Swap: lvol2  on: /dev/dsk/c0t0d0
#    Dump: lvol8  on: /dev/dsk/c0t0d0

# Boot Definitions for Volume Group /dev/vgalt:
# Physical Volumes belongs in Root Volume Group:
# /dev/dsk/c20t0d0 -- Boot Disk
#    Root: altroot on: /dev/dsk/c20t0d0
#    Swap: altswap on: /dev/dsk/c20t0d0
#    Dump: altdump on: /dev/dsk/c20t0d0
```

Figure 13 Checking the boot configuration


Then, update the `fstab` file on the alternate boot disk to reflect its `root`, `swap`, and `usr`, as well as any other filesystems, by entering the following statement:

```
vi /alroot/etc/fstab
```

Change the `vg` name and the `lvol` names to reflect their correct assignments.

7. Try rebooting from the alternate disk by booting from the hardware path of the new disk as follows:

a. Reboot the system:

```
shutdown -r now
```

b. When the `interact with boot` message appears, press any key to interrupt the boot process.

c. Change the primary boot path to the new boot disk by entering a statement similar to the following:

```
pa pri 0/4/0/0.1.19.0.3.0.0
```

d. Verify that the change took place by entering the following to display the new boot path:

```
pa pri
```

e. Boot from the new disk by entering:

```
bo pri
```

f. Answer `no` to interact with the boot process.
Migrating root volume group

An LVM root volume group may be moved by creating an alternate root volume group on an external Symmetrix device and copying the data over. By migrating the root volume group the user avoids:

- LVM Max PV limitations
- LVM Max PE per PV restrictions
System partitions

The HP-UX environment supports three types of partitions:

- Hardware partitions (npars)
- Virtual partitions (vpars)
- Integrity Virtual Machines (Integrity VMs)

Each of these partitioning methods allow the user to configure a single server into multiple, independent subsystems. This section provides an overview of npars, vpars, and Integrity VMs. For detailed information and usage guidelines, refer to HP's documentation on the "Virtual Server Environment" at http://www.docs.hp.com/en/vse.html.

nPartitions

Hardware partitioning enables a single server to run multiple instances of the HP-UX operating system. For more information on HP hardware partitioning and servers that support nPartitions, refer to the HP System Partitions Guide.

An nPartition includes one or more cells (containing processors and memory) that are assigned to the nPartition as well as all I/O chassis connected to those cells. Each nPartition runs its own instance of the Boot Console Handler (BCH) interface and independently boots and reboots instances of HP-UX 11i v1.0 or 11i v2.0.

The HP-UX 11i v1.0 June 2002 or later release supports nPartitions. nPartitions is supported on both HP-UX 11i v1.0, HP-UX 11i v2.0, and HP-UX 11i v3.0.

The following is a list of some of the main features of nPartitions:

- Certain cell-based servers may be split into smaller systems by allocating one or more cells to each partition
- Each partition is hardware and software independent
- Each partition is isolated from hardware or software faults on other partitions on the same server
- Each partition may have a different (supported) OS version
- Supported OS versions include 11.11, 11.23, 11.31
- Supported on both PA-RISC and IA Integrity systems
- Host-based management software (i.e., PowerPath) must be installed on each partition
- A two node cluster with two npars on the same server is not recommended

Partition commands include the following:

- parcreate (1M) — Creates a new partition.
- parmodify (1M) — Modifies an existing partition.
- parstatus (1) — Provides information about an entire Superdome complex, including partition information and available resources in the complex.
- parremove (1M) — Removes an existing partition.
- parunlock (1M) — Unlocks the Stable Complex Configuration Data or Partition Configuration Data.
- fruled (1) — Turns locator LEDs on/off for cells, cabinets and I/O chassis.
- frupower (1M) — Enables or disables power to a cell or I/O chassis, or displays the power status of cells or I/O chassis.
- parmgr — partition manager — Can be run from command line, SAM or WEB browser.
- Shutdown command has two additional options:

Host Environment

- R ready to config (reboot)
- -H used with –R: ready to config but do not reboot
- setboot — Autosearch and autoboot interpretation changed on npar systems — fw interprets bits in combo and not individually.

vPartitions

Virtual Partition software enables you to further subdivide an nPartition active hardware resources by using software partitioning to create one or more virtual partitions (vPars). Virtual partitions can be created on nPar and non-nPar systems.1

The following is a list of some of the main features of vpars:

- vpars are software partitions of a server or an npar
- Each vpar is allocated its own cpu, i/o, and memory
- vpar partition resources are managed by the vpar monitor
- vpar configuration information is held in the vpar partition database
- Each vpar partition must have the vpar software installed
- Each vpar is isolated from software faults or reboots/panics on other vpar (on the same system)
- Each partition may have a different (supported) HP-UX version
- Supported OS versions include 11.11, 11.23, 11.31
- vpars is supported on both PA-RISC and IA Integrity systems
- Host-based management software (i.e., PowerPath) must be installed on each partition
- Host-based management software (i.e., PowerPath) must be installed on each partition
- Each virtual partition may be configured as a node in a ServiceGuard cluster
- A two node cluster with two vpars on the same server is not recommended

Integrity Virtual Machines

The HP Integrity Virtual Machine environment consists of a host and guests. Guest Virtual Machines are configured to run on top of an existing HP-UX OS, the host. Each guest runs its own HP-UX OS and kernel. The guests may be configured to share the same cpu, lan, and hba resources.

The following is a list of some of the main features of Integrity VMs:

- Integrity VMs are software partitions of an Integrity server or Integrity npar running HP-UX 11i v2 (host)
- Virtual machine software must be installed on the host system
- Virtual machines (guests) run on top of the host system
- Virtual machines (guests) are able to share cpu, lan, i/o, and memory resources
- Virtual machines are isolated from OS faults, reboots/panics on other virtual machines
- Supported OS versions on guest systems are HP-UX 11i v2.0 and HP-UX 11i v3.0
- Host-based management software (that is, PowerPath) is installed on the host system only
- Integrity VMs are not supported on vpar partitions
- Host systems may be configured as ServiceGuard nodes
- Guest systems may be configured as ServiceGuard nodes

Table 15 lists HP Virtual Machine host OS support.

Table 15  HP Virtual Machine host OS support

<table>
<thead>
<tr>
<th>Integrity VM Host Revision</th>
<th>Integrity VM version B.3.00</th>
<th>Integrity VM version B.3.50</th>
<th>Integrity VM version B.4.00</th>
<th>Integrity VM version B.4.10</th>
</tr>
</thead>
</table>

Note: Integrity VM is supported on all Integrity servers.

Table 16 lists HP-UX Guest OS support.

Table 16  HP-UX Guest OS support

<table>
<thead>
<tr>
<th>Guest OS revision</th>
<th>Integrity VM version B.3.00</th>
<th>Integrity VM version B.3.50</th>
<th>Integrity VM version B.4.00</th>
<th>Integrity VM version B.4.10</th>
</tr>
</thead>
<tbody>
<tr>
<td>requirements</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>requirements</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note: Refer to HP’s VM 4.0.1 Release Notes for additional details or requirements.
Volume managers

A volume manager is a tool that lets you create units of disk storage known as storage groups. Storage groups contain logical volumes for use on single systems and in high-availability clusters. In ServiceGuard clusters, storage groups are activated by package control scripts.

Dell EMC currently supports the following Volume Managers on HP-UX with Symmetrix arrays:

- HP Logical Volume Manager (LVM)
- Veritas Volume Manager (VxVM)

ServiceGuard clusters can include both the HP-UX Logical Volume Manager (LVM) and the Veritas Volume Manager (VxVM).

**Note:**

LVM

- Contains no load balancing. If load balancing is needed, either the PowerPath or Veritas DMP multipathing driver should be used.
- Veritas Volume Manager is supported only for HP-UX 11i v1, HP-UX 11i v2, and HP-UX 11i v3.0.

**Note:** Refer to the [Dell EMC Simple Support Matrices](http://docs.hp.com/hpux/11i) for the most up-to-date information on supported versions.

- HP and Dell EMC support external boot with LVM and VxVM.
  (VxVM)-Base is bundled in HP-UX 11i v1 and HP-UX 11i v2, and HP-UX 11i v3.0. On HP-UX 11i v3.0, Symantec VxVM only recognizes the legacy device files.

Related documentation is available at [http://docs.hp.com/hpux/11i](http://docs.hp.com/hpux/11i) in the section titled *Veritas Volume Manager*.

For the latest supported volume managers, refer to the Dell EMC E-Lab Navigator.

LVM guide

The Logical Volume Manager (LVM) is the HP default volume manager for managing boot/root/swap devices and MC/ServiceGuard cluster lock disks. Host-based volume manager mirroring is included with the HP-UX 11i v1, HP-UX 11i v2, and HP-UX 11i v3 'Enterprise OE' and 'Mission Critical OE' only.

**LVM options and parameters**

The following table lists various LVM options and their value ranges. The options are set at the time the volume group is created and cannot be changed after the fact. These options can affect future expansion or modification of the volume group, including data migration. Volume group planning should take into account current needs and requirement as well as possible future expansion.

<table>
<thead>
<tr>
<th>Volume group options</th>
<th>Parameter</th>
<th>Default</th>
<th>Maximum</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Physical Extents</td>
<td>max_pe</td>
<td>1016</td>
<td>65535</td>
<td>1 – 65535</td>
</tr>
</tbody>
</table>

1. Veritas DMP provides multipathing only to VxVM volumes; PowerPath provides multipathing to LVM, Veritas VxVM and raw devices. Currently, there is no PowerPath or DMP support in HP-UX 11iv3.0.
The formulas listed below may be used to plan for the accommodation of larger physical device sizes, as well as large logical volume sizes to match the 2T file systems supported by HP.

To determine the pe_size to accommodate a particular physical device size in a volume group:

\[ 2 \times (30 + \text{max}_\text{pe}) / 1024 \]

To determine the largest logical volume which can be supported in a volume group:

\[ \text{pe}_\text{size} \times \text{max}_\text{pe} \]

**LVM PVLinks**

HP LVM provides primary and alternate links to a physical device with pvlinks. If the primary link fails, LVM automatically switches to the alternate device. When the primary link recovers, LVM automatically switches back to the primary device. Because there is no load balancing with pvlinks, the PowerPath multipathing driver is recommended, especially in an HA environment.

**Note:** HP-UX 11i v3.0 — The native multipathing driver handles path failure detection, path failovers, as well as io load balancing.

HP LVM features include:

- Primary + 7 alternate for non-root volume groups
- Primary + 3 alternate for root volume groups
- Basic path failover/failback capabilities
- No load balancing capability

**Example:**

To set up an alternate path to a set of Symmetrix devices (with Fibre Channel) using two HBAs on a host and two Symmetrix FA ports:

- VMAX/Symmetrix
  
  VMAX/Symmetrix configuration should be performed by an Dell EMC Customer Engineer (CE) through the Symmetrix Service Processor:
  
  - Assign the same set of devices to two FA ports (Figure 14 on page 93)\(^1\)
  - Enable the C bit (common serial number)
  - Enable the V bit (volume set addressing)

- Cable/Zoning

---

\(^1\) To avoid single points of failure for Symmetrix 8000 and earlier, assign the devices to directors alternating between odd and even bus.
• Cable two HBAs on the host as illustrated in Figure 15 on page 94
• Cable the two FA ports on the Symmetrix as illustrated in Figure 15 on page 94
• Zoning should be single initiator with each HBA linked to one FA port

**Host**

• Run `ioscan -fnC disk` (to discover the devices)
• Run `insf -C disk` (to create host device files)
• Run `inq` to get the device mapping for the primary and alternate paths
• Create a list of the primary paths using `/dev/rdsk/cxtxdx` (character device)
  - `pv.lst`
• Create a list of the primary paths using `/dev/dsk/cxtxdx` (block special)
  - `vg_p.lst`
• Create a list of the alternate paths using `/dev/dsk/cxtxdx` (block special)
  - `vg_a.lst`
• Create the volume group directory `/dev/vgxx`
  
  ```
  mkdir /dev/vg01
  ```
• Create the group special file under `/dev/vgxx`
  
  ```
  mknod /dev/vg01/group c 64 0x010000
  ```
• Run `pvcreate` using the devices in `pv.lst`
  
  ```
  pvcreate /dev/rdsk/c6t0d0
  ```
• Create the volume group using the devices in `vg_p.lst`
  
  ```
  vgcreate /dev/vg01 `cat vg_p.lst`
  ```
• Extend the volume group using the devices in `vg_a.lst`
  
  ```
  vgextend /dev/vg01 `cat vg_a.lst`
  ```
• Run `vgdisplay` against the volume group to check whether the primary and alternate paths are listed in the volume group. Refer to Figure 16 on page 95 for volume group information.
  
  ```
  vgdisplay -v /dev/vg01
  ```
Figure 14 Volume map: System_Impf
Figure 15  PVLinks/alternate path, physical configuration for device multipathing
Bad Block Relocation

Bad Block Relocation should be set to `none` for the Symmetrix, because the array detects and handles bad blocks relocation, unless MirrorDisk-UX is used. Unless the LVM 'Bad Block Relocation' is set to `none`, there could be a potential discrepancy between the array and LVM that can lead to possible data corruption. This option can be set when the logical volume is created or later using one of the following commands:

```
lvcreate -r N
lvchange -r N
```

LVM commands

The following is a list of the most common LVM commands:

- `mknod` — Creates a directory, special, or ordinary file.
- `pvcreate` — Creates a physical volume.

--- Volume groups ---

<table>
<thead>
<tr>
<th>VG Name</th>
<th>/dev/vg01</th>
</tr>
</thead>
<tbody>
<tr>
<td>VG Write Access</td>
<td>read/write</td>
</tr>
<tr>
<td>VG Status</td>
<td>available</td>
</tr>
<tr>
<td>Max LV</td>
<td>255</td>
</tr>
<tr>
<td>Cur LV</td>
<td>0</td>
</tr>
<tr>
<td>Open LV</td>
<td>0</td>
</tr>
<tr>
<td>Max PV</td>
<td>16</td>
</tr>
<tr>
<td>Cur PV</td>
<td>8</td>
</tr>
<tr>
<td>Act PV</td>
<td>8</td>
</tr>
<tr>
<td>Max PE per PV</td>
<td>2137</td>
</tr>
<tr>
<td>VGDA</td>
<td>8</td>
</tr>
<tr>
<td>PE Size (Mbytes)</td>
<td>8</td>
</tr>
<tr>
<td>Total PE</td>
<td>4274</td>
</tr>
<tr>
<td>Alloc PE</td>
<td>0</td>
</tr>
<tr>
<td>Free PE</td>
<td>4274</td>
</tr>
<tr>
<td>Total PVG</td>
<td>0</td>
</tr>
<tr>
<td>Total Spare PVs</td>
<td>0</td>
</tr>
<tr>
<td>Total Spare PVs in use</td>
<td>0</td>
</tr>
</tbody>
</table>

--- Physical volumes ---

<table>
<thead>
<tr>
<th>PV Name</th>
<th>/dev/dsk/c94t2d0</th>
</tr>
</thead>
<tbody>
<tr>
<td>PV Status</td>
<td>available</td>
</tr>
<tr>
<td>Total PE</td>
<td>2137</td>
</tr>
<tr>
<td>Free PE</td>
<td>2137</td>
</tr>
<tr>
<td>Autoswitch</td>
<td>On</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PV Name</th>
<th>/dev/dsk/c94t2d1</th>
</tr>
</thead>
<tbody>
<tr>
<td>PV Status</td>
<td>available</td>
</tr>
<tr>
<td>Total PE</td>
<td>2137</td>
</tr>
<tr>
<td>Free PE</td>
<td>2137</td>
</tr>
<tr>
<td>Autoswitch</td>
<td>On</td>
</tr>
</tbody>
</table>

Figure 16  Volume group information
Host Environment

- **pvchange** — Changes characteristics of a physical volume in a volume group. It also redirects I/O to different physical volume paths.
- **pvdisplay** — Displays information about physical drives within a volume group.
- **vgscan** — Scans physical volumes for volume groups.
- **vgcreate** — Create volume group on a set of physical volumes.
- **vgchange** — Sets volume group availability.
- **vgdisplay** — Displays information about volume groups.
- **vgexport** — Exports a volume group and its associated logical volumes.
- **vgimport** — Imports a volume group onto a system.
- **vgremove** — Removes a volume group definition from the system.
- **lvcreate** — Stripes; creates logical volume in volume group.
- **lvchange** — Changes logical volume characteristics.
- **lvdisplay** — Displays information about logical volumes.
- **lvextend** — Increases space for logical volumes, but not size of filesystems.
- **lvreduce** — Decreases number of physical extents allocated to logical volume.
- **lvremove** — Removes one or more logical volumes.
- **newfs** — Creates a new filesystem.
- **bdf** — Shows all mounted filesystems and available free space.
- **lsdev** — Lists device drivers in the system.

For more information on individual LVM commands, refer to the LVM man pages.

**VxVM**

Veritas VxVM Base version is bundled with HP-UX 11i v1.0 and HP-UX 11i v2.0 operating environments. Both versions are supported on the VMAX/Symmetrix arrays. The Base version does not include DMP, Mirror, RAID5, and DRL support. With the purchase of a full license the additional feature/functionality can be enabled. External boot support is offered with VxVM 3.5 only. Root device mirroring does not require the full VxVM license. VxVM volumes on HP-UX 11ix are supported on MC/ServiceGuard clusters.

Load balancing of IOs (DMP) is only available with the Full Veritas VxVM version. VxVM DMP load balancing is round-robin whereas PowerPath balances the io load dynamically based on the path of least resistance.

**Creating Rootdg from the command line**

In high LUN count environments, the Veritas vxinstall process to create rootdg may take a few hours to complete. The vxinstall process may be bypassed by creating rootdg from the command line. Starting with Veritas VxVM 4.1, rootdg is not required for volume manager configurations. The following instructions only pertain to VxVM 3.5 environments.

1. If using the full VxVM licensed product – B9116AA, install the license.
   
   `vxlicinst xxxxxxxxx`

2. Start the `vxconfigd` process in disabled mode.
   
   If process exists, restart.
   
   `vxconfigd -k -m disable`

   Otherwise, start the process.
   
   `vxconfigd -m disable`

3. Initialize `vxconfigd` and create `/etc/vx/volboot` file. This file is required by `vxconfigd` to determine disk ownership.
vxdctl init

4. Initialize the rootdg disk group.

   vxdg init rootdg

5. Initialize the device to be used in rootdg.

   vxdisk -f init cxydz type=simple

6. Add the device to rootdg.

   vxdg add disk cxydz

7. Add the device to the volboot file.

   vxdctl add disk cxydz type=simple

8. Enable vxconfigd.

   vxdctl enable

9. Remove the install-db file. This file disables automatic VxVM startup during a reboot.

   rm /etc/vx/reconfig.d/state.d/install-db

10. Verify rootdg configuration.

    vxdg list
    vxprint

11. Enable configuration either by rebooting the host or enabling vxconfigd.

    vxconfigd -k -m enable
VxVM commands

The following is a list of the most common VxVM commands:

- `vxdisk list [diskname]` — Lists disks under control of VxVM.
- `vxdg list [diskgroup]` — Lists information about disk groups.
- `vxdg -s list` — Lists information about shared disk groups in a cluster.
- `vxinfo [-g diskgroup] [volume ...]` — Displays information about the accessibility and usability of volumes.
- `vxdiskadm` — Administers disks in VxVM using a menu-based interface.
- `vxdiskadd [devicename]` — Adds a disk specified by device name.
- `vxedit rename olddisk newdisk` — Renames a disk under control of VxVM.
- `vxdg -s init diskgroup \[diskname=]devicename` — Creates a shared disk group in a cluster using a pre-initialized.
- `vxdg deport diskgroup` — Deports a disk.
- `vxdg import diskgroup` — Imports a disk.
- `vxdg -s import diskgroup` — Imports a disk group as shared by a cluster.
- `vxdg -g diskgroup set activation=ew|ro|sw|off` — Sets the activation mode of a shared disk group in a cluster.
- `vxrecover -g diskgroup -sb` — Starts all volumes in an imported disk group.
- `vxdg destroy diskgroup` — Destroys a disk group and releases its disks.
- `vxdisk offline devicename` — Takes a disk off line.
- `vxdg -g diskgroup rmdisk diskname` — Removes a disk from its disk group.
- `vxdisk rm diskname` — Removes a disk from control of VxVM.
- `vxmake sd subdisk diskname,offset,length` — Creates a subdisk.
- `vxsd assoc plex subdisk ...` — Associates subdisks with an existing plex.
- `vxsd assoc plex:subdisk1:0 subdiskM:N-1 ...` — Adds subdisks to the ends of the columns in a striped or RAID-5 volume.
- `vxsd dis subdisk` — Dissociates a subdisk from a plex.
- `vxedit rm subdisk` — Removes a subdisk.
- `vxsd -o rm dis subdisk` — Dissociates and removes a subdisk from a plex.

For more information on individual VxVM commands, refer to the VxVM man pages.
I/O time-out parameters

This section discusses when and why tuning of the I/O time-out parameters may be needed for online VMAX/Symmetrix operations.

The VMAX/Symmetrix online operations (online code updates, online component replacement, and online configuration changes) can have implications resulting in transient error conditions in the form of I/O time-outs. The exposure to these implications depends on many factors such as:

- VMAX/Symmetrix model and microcode revision
- VMAX/Symmetrix array configuration
- I/O load at the time of the operation
- bus type affected
- LUNs active on the host bus adapters at the time of the operation
- fan-in and fan-out ratios
- LUNs per VMAX/Symmetrix port

The successful execution of an online VMAX/Symmetrix operation, even when resulting in transient-type errors, should have minimal consequences when the HP-UX environment is properly configured and all components of the environment involved in handling of the transient errors properly do so.

The most serious of these consequences should be device path failures (VxVM, PowerPath), device power fails (HP LVM), device path switches (VxVM, PowerPath), and LUN switches (HP LVM)—all of these events being recoverable on a retry. A possible exception is when an application has asynchronous I/O implemented, making proper tuning of the I/O time-out parameters imperative.

However, even recoverable transient errors, which can be alarming to some customers, can be avoided with the use of the configurable I/O time-out parameters in volume managers.

I/O requests in the HP-UX environment to devices not configured by a volume manager are indefinitely retried in the case transient error conditions without returning an error. A tunable I/O time-out parameter is not user-configurable for devices not owned by a volume manager in the HP-UX environment. However, due to the HP-UX behavior of indefinitely retrying I/O requests due to I/O time-outs for nonvolume manager devices without returning an error to the caller, such a tunable parameter is not needed.

I/O requests in the HP-UX environment to devices configured into a volume manager would return an error following the unsuccessful completion of the I/O request and the expiration of an I/O time-out value configurable by the volume manager in use. The default I/O time-out value for returning an error for an I/O request to a device owned by a volume manager is 30 seconds. This time-out value can be modified with a configurable I/O time-out parameter within the volume manager for each device owned by the volume manager.

I/O time-out parameter settings can be configured to accommodate Symmetrix online operations on a permanent basis, or left at their default values during normal operations and just modified in preparation for the online operation.

HP LVM physical volume time-out (PVtimeout)

The physical volume I/O time-out value, PVtimeout parameter, establishes how long an I/O request has to successfully complete before an error is returned to LVM and LVM retries the I/O through an alternate link if available, else on the same path. The default PVtimeout
value is 30 seconds, and the maximum valid physical volume I/O time-out value for the LVM
PVtimeout is 300 seconds. The PVtimeout parameter is configured on a device basis for
all devices owned by HP LVM, and is persistent through reboots.

You can display the PVtimeout parameter setting using the HP LVM pvdisplay command

```
pvdisplay /dev/dsk/cxtxdx
```

```
# pvdisplay /dev/dsk/c1t2d1
--- Physical volumes ---
PV Name                     /dev/dsk/c1t2d1
VG Name                     /dev/vg01
PV Status                   available
Allocatable                 yes
VGDA                        2
Cur LV                      6
PE Size (Mbytes)            4
Total PE                    3595
Free PE                     0
Allocated PE                3595
Stale PE                    0
IO Timeout (Seconds)        default
Autoswitch                  On
```

You can configure the LVM PVtimeout parameter using the HP LVM pvchange command

```
pvchange -t <PV IO_timeout in seconds>/dev/dsk/cxtxdx
```

```
# pvchange -t 90 /dev/dsk/c1t2d1
Physical volume "/dev/dsk/c1t2d1" has been successfully changed.
Volume Group configuration for /dev/vg01 has been saved in /etc/lvmconf/vg01.conf
```

```
# pvdisplay /dev/dsk/c1t2d1
--- Physical volumes ---
PV Name                     /dev/dsk/c1t2d1
VG Name                     /dev/vg01
PV Status                   available
Allocatable                 yes
VGDA                        2
Cur LV                      6
PE Size (Mbytes)            4
Total PE                    3595
Free PE                     0
Allocated PE                3595
Stale PE                    0
IO Timeout (Seconds)        90
Autoswitch                  On
```

**HP LVM logical volume time-out (LVtimeout)**

The default behavior for HP LVM is such that an I/O request is not returned to the caller until
the I/O request successfully completes. LVM will indefinitely retry the I/O request upon I/O
failures until successful completion of the I/O request.

You can modify this default behavior on an LVM logical volume basis using the LVM logical
volume time-out parameter (LVtimeout). The default value of this parameter, zero, results in
LVM never returning an I/O error to the caller. With a nonzero LVtimeout value, LVM
assumes that an I/O request that does not successfully complete within the specified
LVtimeout interval cannot be completed, and LVM fails the I/O request.
The LVM LVtimeout parameter is persistent through reboots. The LVtimeout parameter is typically left at the default value (zero), but may require a nonzero value for specific applications as recommended by the application vendor or Dell EMC. One such example is Sybase implementing asynchronous I/O.

Improper use of the HP LVM LVtimeout parameter can have very serious consequences. You should specify a nonzero value for the LVM LVtimeout parameter only when it is desired for the application to be informed of the I/O failure to successfully complete within the specified time interval.

Do not confuse the HP LVM logical volume time-out (LVtimeout) with the HP LVM physical volume time-out parameter (PVtimeout):

- PVtimeout specifies on a physical device basis how long to wait for I/O requests to successfully complete to the device configured by LVM before LVM is informed of the failure and retries the I/O on an alternate link, if available.
- LVtimeout specifies on a logical volume basis how long to wait for the successful completion of the I/O request to the logical volume before giving up on the I/O request (default of zero specifies LVM to retry indefinitely).

There are considerations for selecting a nonzero LVtimeout value when it is desired for the caller to be informed of the unsuccessful completion of an I/O request:

- HP LVM cannot conclude an I/O request cannot be completed within a lesser time interval than that specified by PVtimeout, as an unsuccessful I/O would not be returned to LVM before expiration of PVtimeout; therefore, LVtimeout should be configured for a value larger than PVtimeout.
- It would be desirable to allow for at least one retry of the I/O request by LVM, especially if one or more alternate links are available or if an underlying multipathing driver is implemented (PowerPath), before the I/O request is declared failed by LVM. The LVtimeout would have to be configured to a larger value than PVtimeout plus the LVM alternate link switch time or retry time. If LVtimeout is configured for a nonzero value, it should be configured at a minimum larger than PVtimeout + 60 seconds, but preferably at least twice PVtimeout + 60 seconds, in order to allow for one retry of the I/O request before LVM fails the I/O if deviating from the default behavior.
You can display the HP LVM logical volume time-out parameter (LVtimeout) setting using the LVM `lvdisplay` command, `lvdisplay /dev/<vg_name>/<lvol_name>`

```
# lvdisplay /dev/vg00/lvol1
--- Logical volumes ---
LV Name                  /dev/vg01/lvol1
VG Name                  /dev/vg01
LV Permission            read/write
LV Status                available/syncd
Mirror copies            0
Consistency Recovery     MWC
Schedule                 parallel
LV Size (Mbytes)         512
Current LE               128
Allocated PE             128
Stripes                  0
Stripe Size (Kbytes)     0
Bad block                off
Allocation               strict/contiguous
IO Timeout (Seconds)     default
```

You can configure the HP LVM logical volume time-out parameter (LVtimeout) using the LVM `lvchange` command, `lvchange -t <lvol IO_timeout in seconds> /dev/<vg_name>/<lvol_name>`

```
# lvchange -t 240 /dev/vg01/lvol1
Logical volume "/dev/vg01/lvol1" has been successfully changed.
Volume Group configuration for /dev/vg01 has been saved in /etc/lvmconf/vg01.conf
```

```
# lvdisplay /dev/vg00/lvol1
--- Logical volumes ---
LV Name                  /dev/vg01/lvol1
VG Name                  /dev/vg01
LV Permission            read/write
LV Status                available/syncd
Mirror copies            0
Consistency Recovery     MWC
Schedule                 parallel
LV Size (Mbytes)         512
Current LE               128
Allocated PE             128
Stripes                  0
Stripe Size (Kbytes)     0
Bad block                off
Allocation               strict/contiguous
IO Timeout (Seconds)     240
```

Configure the LVtimeout to value zero (the default) so that HP LVM indefinitely retries I/O requests.

```
# lvchange -t 0 /dev/vg01/lvol1
Logical volume "/dev/vg01/lvol1" has been successfully changed.
Volume Group configuration for /dev/vg01 has been saved in /etc/lvmconf/vg01.conf
```

```
# lvdisplay /dev/vg00/lvol1
--- Logical volumes ---
LV Name                  /dev/vg01/lvol1
VG Name                  /dev/vg01
LV Permission            read/write
LV Status                available/syncd
Mirror copies            0
Consistency Recovery     MWC
Schedule                 parallel
LV Size (Mbytes)         512
```

--- End of Document ---
Veritas VxVM powerfail time-out (pfto)

The VxVM powerfail time-out value (pfto) specifies how long an I/O request must successfully complete before an error is returned to VxVM. You can configure the VxVM pfto time-out parameter using the vxpfto command. The default pfto value is 30 seconds. The pfto parameter is persistent through reboots.

To display the pfto parameter value, use vxprint –l <volume_name>

```bash
# vxdisk list disk1
Device:   c3t2d0
devicetag: c3t2d0
type:      simple
hostid:   hpint062
disk:     name=disk1 id=1072812571.2052.hpint062
timeout:  30
flags:    name-dg_062 id=1072812753.2181.hpint062
pubpaths: block=/dev/vx/dmp/c3t2d0 char=/dev/vx/rdmp/c3t2d0
version:  2.2
iosize:   min=1024 (bytes) max=256 (blocks)
public:   slice=0 offset=1152 len=2206368
private:  slice=0 offset=128 len=1024
update:   time=1080614533 seqno=0.306
headers:  0 248
configs:  count=1 len=727
logs:     count=1 len=110
Defined regions:
  config  priv 000017-000247[000231]: copy=01 offset=000000 enabled
  config  priv 000249-000744[000496]: copy=01 offset=000000 enabled
  log     priv 000745-000854[000110]: copy=01 offset=000000 enabled
  lockrgn priv 000855-000919[000065]: part=00 offset=000000
Multipathing information:
numpaths:  2
c3t2d0  state=enabled
c13t2d0 state=enabled
```

```bash
To display the pfto parameter value, use vxprint -l <volume_name>
```

```bash
# vxprint -l disk1
Disk group:  dg_062
Disk:       disk1
info:       diskid=1072812571.2052.hpint062
assoc:      device=c3t2d0 type=simple
flags:      autoconfig
device:     path=/dev/vx/dmp/c3t2d0
devinfo:    publen=2206368 privlen=1024
timeout:    30
```

To configure the pfto parameter for all devices belonging to a specific disk group, use the command vxpfto -t <pfto value in seconds> -g <dg_name>

```bash
# /usr/lib/vxvm/bin/vxpfto -t 90 -g dg_062
```

```bash
# vxdisk list disk1
```

I/O time-out parameters
Host Environment

Device: c3t2d0
devicetag: c3t2d0
type: simple
hostid: hpint062
disk: name=disk1 id=1072812571.2052.hpint062
timeout: 90
group: name=dg_062 id=1072812753.2181.hpint062
flags: online ready private autoconfig noautoimport imported
pubpaths: block=/dev/vx/dmp/c3t2d0 char=/dev/vx/rdmp/c3t2d0
version: 2.2
iosize: min=1024 (bytes) max=256 (blocks)
public: slice=0 offset=1152 len=2206368
private: slice=0 offset=128 len=1024
update: time=1080614533 seqno=0.306
headers: 0 248
configs: count=1 len=727
logs: count=1 len=110
Defined regions:
  config priv 000017-000247[000231]: copy=01 offset=000000 enabled
  config priv 000249-000744[000496]: copy=01 offset=000231 enabled
  log priv 000745-000854[000110]: copy=01 offset=000000 enabled
  lockrgn priv 000855-000919[000065]: part=00 offset=000000
Multipathing information:
numpaths: 2
c3t2d0 state=enabled
c13t2d0 state=enabled

To configure the pfto parameter for underlying device or devices of one or more VxVM volumes, use the command vxpfto –t <pfto value in seconds> <volume1_name> <volume2_name>...

Recommended I/O time-out values

Note the following about the recommended I/O time-out value for HP LVM PVtimeout and VxVM pfto:

- The time-out value may be configured only for the duration of the online VMAX/Symmetry operation or on a permanent basis.
- You can obtain the recommended time-out value from Dell EMC Customer Support or from the Dell EMC Simple Support Matrices.
Cluster

Configuring a cluster system requires careful planning, with consideration of the type of usage, critical data, failover planning, and more. This section is intended only to introduce available tools and general procedures for incorporating the VMAX/Symmetrix system into an MC/ServiceGuard cluster and to assist in planning.

For detailed guidelines on MC/ServiceGuard release notes and cluster administration, refer to www.docs.hp.com/hpux/ha.

Table 17 lists currently supported MC/ServiceGuard features.

Table 17  HP High Availability features summary

<table>
<thead>
<tr>
<th>High Availability feature</th>
<th>Earliest supported</th>
<th>Latest supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>MC/ServiceGuard</td>
<td>11.14</td>
<td>11.20 ab</td>
</tr>
<tr>
<td>Supports HA cluster</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Supports Parallel Database Cluster</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Maximum number of nodes in HA cluster</td>
<td>16</td>
<td>16 c</td>
</tr>
<tr>
<td>Maximum number of active nodes</td>
<td>16</td>
<td>16</td>
</tr>
<tr>
<td>HP operating system</td>
<td>HP-UX 11i v1.0</td>
<td>HP-UX 11i v3.0</td>
</tr>
<tr>
<td>Supports Oracle database</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Supports public IP interface failover</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Supports heartbeat link via disk</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Supports virtual IP or IP alias addressing</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Supports vPars</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Supports Quorum Server</td>
<td>Yes d</td>
<td>Yes d</td>
</tr>
<tr>
<td>Supports VxVM</td>
<td>Yes e</td>
<td>Yes e</td>
</tr>
<tr>
<td>External Boot</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

a. The latest supported version of MC/ServiceGuard for HP-UX 11i v3 is 11.20.
b. All nodes must have the same OS versions. HP-UX 11i v1 and HP-UX 11i v2 or HP-UX 11i v3.0 are not supported in the same cluster.
c. HP-UX 11i v2 only supports 8 nodes in a cluster.
d. On MC/ServiceGuard 11.14 and later only.
e. VxVM 3.5 is supported only on HP-UX 11i v1 with MC/SG 11.14 or later and HP-UX 11i v2 with MC/SG 11.15 or later. VxVM 4.1 is supported on HP-UX 11i v2 with MC/SG.

Refer to “Addressing” on page 62 and Dell EMC E-Lab Navigator for boot support requirements.

Cluster overview

MC/ServiceGuard and MC/ServiceGuard OPS clusters consist of HP 9000 Series 800 servers, which ensure access to critical data through redundancy of components to protect against a single point of failure. The cluster daemon monitors and manages the various components, including the LAN, SP, HBA, disk, application, and system. If a failure is detected, the service is transferred to a backup component or to another system. Current versions of ServiceGuard also offer a graphical user interface to view, monitor, and run some administrative commands.
This section provides an overview of an MC/ServiceGuard cluster in a VMAX/Symmetrix environment, including:

- Types of cluster
- Node support
- Cluster quorum
- Cluster components
- Volume managers and mirroring
- Partitions
- Symmetrix configuration

MC/ServiceGuard supports different cluster environments, including:

- MC/ServiceGuard
- ServiceGuard Extension for Real Application Cluster (RAC)
- MetroClusters
- Continental Clusters
- HP ServiceGuard Storage Foundation Suite

This section deals primarily with the MC/ServiceGuard environment, sometimes referred to as HA (high availability).

HA cluster

An HA cluster is a failover cluster of one primary node and up to 15 failover nodes. Cluster packages are a grouping of LAN, volume groups, file systems, and applications that are failed over to an alternate host (node) in case of an application or system failure. An HA cluster may consist of multiple packages (and nodes), each with its own primary and failover node.

The primary and failover nodes of a cluster package must have shared access to the same set of Symmetrix devices:

- If using HP LVM, identical volume groups must be created and imported to all nodes, and identical file systems must be created across all nodes.
- If using Veritas Volume Manager, refer to Integrating Veritas Volume Manager (VXVM) with MC/ServiceGuard on www.docs.hp.com.

Each host should have redundant paths configured to the Symmetrix devices through separate channel directors using HP LVM PVLinks, PowerPath or Veritas DMP. Refer to the Dell EMC E-Lab Navigator for Veritas VxVM support on HP-UX. In a multipath environment with PowerPath, LVM, or DMP configured, if a path to a device fails, the host switches automatically to an alternate link. Both PowerPath and DMP provide load balancing of I/O, as well as path failover capability. On HP-UX 11i v3.0, the native multipathing driver handles path failovers and io load balancing.

Cluster services

MC/ServiceGuard clusters consist of three main services: the Cluster Manager, the Package Manager, and the Network Manager. Each of these services monitors and manages the various components of the cluster, such as the heartbeat, nodes, packages, cluster volumes, and LAN. Certain daemon processes associated with these services run on all nodes in the cluster. At cluster formation, a primary daemon process is designated for each of the services.

The Cluster Manager initializes the cluster, monitors it, detects node failure, and controls cluster reformation on the exit and rejoining of a node. The Network Manager provides highly available network services to the cluster clients by monitoring the health of all LAN interfaces and managing backup services when required. The cmcmd daemon, associated with both
services, runs on all nodes but has a designated coordinator process on one node that is primarily responsible for cluster activities. The cmrsvassistd daemon resides on all the nodes and executes the Package Manager run and halt scripts for the package and its services. The coordinator cmrsvassistd daemon associated with the cluster coordinator decides when and where to run, halt, or move packages.

Each cmcld daemon in the cluster exchanges heartbeat messages with the cluster coordinator cmcld process. If a heartbeat message is not received by a node within the specified time, a cluster reformation is initiated. MC/ServiceGuard uses TCP/IP networks or RS232 serial lines for monitoring heartbeat messages. Serial heartbeat may only be used in a two-node cluster, and is highly recommended if there is only one heartbeat LAN. A serial line should not be used in two-node cluster with more than one heartbeat LAN.

ServiceGuard uses the following daemons to manage the various cluster services:

- cmclconfd — Cluster configuration daemon
- cmcld — Cluster monitor and management daemon
- cmlogd — syslog daemon
- cmvlmd — Keeps track of cluster aware LVM volume groups
- cmomd — Cluster object manager daemon
- cmsnmpd — Cluster snmp agent daemon
- cmrsvassistd — Executes package run and halt scripts as required by the cmcld daemon

### Configuring and managing MC/ServiceGuard

Three files associated with MC/ServiceGuard may be edited and customized as required by the user:

- **Cluster configuration file** — Contains cluster-specific information such as cluster name, node information including heartbeat and cluster lock disk, cluster timing parameters, maximum number of packages, cluster aware volume groups.
- **Package configuration file** — Defines the services included in the package, the list of failover nodes in order of priority, the failover policy, and the run and halt scripts for the packages.
- **Package control script** — Contains information required to run, to monitor, to respond to failures, and to halt the services pertaining to the package.

The following steps are a basic overview of the commands in building and managing a cluster:

- To query the named nodes for cluster configuration (including volume group and network information) and create a configuration file to be edited and customized as required:
  ```
  cmquerycl -v -C /etc/cmcluster/clustername.config -n node1 -n node2
  ```

- To verify the cluster configuration in the cluster configuration file:
  ```
  cmcheckconf -k -v -C /etc/cmcluster/clustername.config
  ```

- To generate and distribute the cluster binary file to all nodes in the cluster:
  ```
  cmapplyconf -k -v -C /etc/cmcluster/clustername.config
  ```

- To create a package configuration file to be edited and customized as required:
  ```
  cmmakepkg -p /etc/cmcluster/pkg1/pkg1.config
  ```

- To create a package control script file:
  ```
  cmmakepkg -s /etc/cmcluster/pkg1/pkg1.sh
  ```

- To check cluster and package configurations:
  ```
  cmcheckconf -C /etc/cmcluster/cluster.config -P 
  /etc/cmcluster/pkg1/clock.config
  ```

Cluster 107
• To generate and distribute cluster binary files to all nodes in cluster:
  cmapplyconf -v -C /etc/cmcluster/cluster.config -P
  /etc/cmcluster/pkg1/clock.config

• To manually start the cluster:
  cmrunc1 -v

• To check status of cluster, including nodes and packages:
  cmviewcl -v

• To manually move a package to a different node:
  • To halts package on current node:
    cmhaltpkg pkgname
  • To run package on alternate node:
    cmrunpkg -n altnodename pkgname.
  • To re-enable package switching:
    cmmodpkg -e pkgname

• To halt a node, halt the package, and fail it over to another node:
  cmhaltnode -f nodename

• To enable a node to rejoin the cluster:
  cmrunnode nodename

• To manually halt the cluster, as well as its nodes and packages:
  cmhaltcl -f

Note: For detailed steps required to configure an HA cluster, refer to Managing
MC/ServiceGuard Version 11.14 at www.docs.hp.com. SAM also can be used to configure and
manage the cluster.

Failover/failback policies

The three types of failover policies for ServiceGuard packages are:

• **Configured_node** (default) — The package fails over to the next node on the list.
• **Min_package_node** — The package fails over to the node currently running the minimum
  number of packages.
• **Rotating Standby** — The policy is set to **min_package_node**, and a node with no running
  packages becomes the failover node. The original node becomes the standby when it
  rejoins the cluster.

The failback policies are **manual** (default) and **automatic**. The manual policy allows the system
administrator to determine the least-disruptive time to switch the package back to the original
node.

If the failback policy is set to automatic, the package switching occurs as soon as the node
rejoins the cluster, which can be disruptive to the users.

The automatic failback policy impacts the behavior of the switching based on how the failover
policy is set:

• If the failover policy is **configured node**, the package automatically attempts to fail back as
  soon as the original node rejoins the cluster.
• If the failover policy is set to min_package_node, package switching can occur each time there is cluster reformation.

ServiceGuard Manager

The ServiceGuard Manager is a graphical user interface for HP-UX clusters, including:

• MC/ServiceGuard
• ServiceGuard Extension for RAC
• MetroClusters
• Continental Clusters

On servers running MC/ServiceGuard 11.13 or later, a user can also run basic commands to:

• Run or halt a cluster, node, or package.
• Move a package to another node.
• Change node and package switching flags.

Cluster quorum

A cluster quorum requires that more than 50% of the previously running nodes form a new cluster. In certain situations, however, 50% of the previously running nodes can form a cluster, which could lead to a split-brain syndrome (two independent clusters of 50% each of the previously running nodes writing to the same data, which can lead to data corruption). To prevent this, a cluster lock is required to act as a tie breaker. A cluster lock may be a lock disk or a quorum server. With the use of the cluster lock, whichever split subcluster gets to the lock disk first forms the cluster.

A cluster lock is required in a two-node cluster and strongly recommended in a four-node cluster. A cluster lock disk should not be used in clusters of five or more nodes; however, a quorum server can be used. A data disk can be used as a cluster lock disk, because a dedicated device is not required.

Single-lock disk

In cluster configurations requiring a cluster lock, a single-lock device is recommended. The only exceptions are in a campus cluster or when the cluster devices are mounted internally in the same cabinet.

Dual-lock disk

A dual cluster lock is recommended only in campus cluster environments or when the cluster devices are internally mounted in the same cabinet. In both cases, a single cluster lock device is a single point of failure.

IMPORTANT

The use of dual cluster locks, except when recommended, could lead to split-brain situations and possible data corruption.

A campus cluster must have a cluster lock device configured at each site accessible to all nodes in the cluster. If one site fails, the other site can re-form the cluster. To prevent split-brain situations, a campus cluster requires multiple network and heartbeat configurations.

Quorum server

A quorum server may be used in place of a lock disk to provide a tie breaker in cluster re-formations. Clusters of any node size may use a quorum server. The quorum server is not part of the cluster, but provides quorum services to up to 50 clusters. A single quorum server can service both Linux and HP-UX clusters. A single quorum server also can service various ServiceGuard versions and OS version clusters.
If the quorum server is down during a cluster failure and re-formation, the cluster might become unavailable.

The quorum server uses TCP/IP for connection requests from cluster nodes.

**Mirroring**

As protection against a single point of failure, ServiceGuard recommends that the data be mirrored through storage-based RAID or host-based software. Symmetrix volumes can be configured as mirrors (RAID 1), Parity RAID (3+1), or Parity RAID (7+1), depending on microcode version. Host-based mirroring may be configured using either HP MirrorDisk-UX or Veritas VxVM.

**Clustering in partitioned environments**

There are two types of partitions in the HP environment:

- **nPartitions** — Partitions at the hardware level
- **vPars** — Virtual partitions through software

A system, such as the SuperDome or the rp8400, may be partitioned at the hardware level, and each of the nPartitions may be further divided into virtual partitions. ServiceGuard is supported with nPartitions and vPars with certain restrictions. A cluster may contain a combination of vPars, nPartitions and non-partitioned systems. Due to latency issues with vPars, the NODE_TIMEOUT value in such clusters will need to be set higher to avoid unnecessary cluster reformations.

Partitioned systems within a cluster must be distributed among the various systems/cabinets such that a single failure does not lead to the loss of more than 50% of the nodes. For example, a cluster may not contain three partitions from one system and two other non-partitioned systems. This rule does not apply in a *cluster in a box* environment, which may consist of nPartitions in a single cabinet or VPARS on a single system. Although supported, cluster in a box is not a true high-availability environment, since it is subject to a single point of failure.

Cluster lock is required when there is potential for loss of exactly 50% of the members in two-node and four-node clusters distributed across two systems.

For example, each of these situations requires a cluster lock:

- A four-node cluster with two nPartitions on two SuperDomes
- A four-node cluster with two vPar partitions on two rp7400s

Refer to *ServiceGuard Cluster Configuration for Partitioned Systems* at [www.docs.hp.com](http://www.docs.hp.com) for further information.

**Mixed OS cluster**

File system and volume manager restrictions should be considered when configuring package failovers. ServiceGuard does not support a mix of HP-UX 11i v2 with either HP-UX 11i v1 or HP-UX 11i v3.0.

MC/ServiceGuard 11.16 and later supports a mix of PA-RISC and Intel Itanium architectures with the fusion release of HP-UX (HP-UX 11i v2 update 2 - Sept 04 Release).
ServiceGuard Storage Management Suite

HP ServiceGuard Storage Management Suite bundles ServiceGuard with Veritas VxVM and VxFS (JFS) file systems, as well as Veritas Cluster Volume Manager (CVM) and Veritas Cluster File Systems (CFS). There are seven different versions of the bundle, only some of which include the Veritas Cluster Volume Manager (CVM) and Cluster Files Systems (CFS).\(^1\)

Veritas’ CFS allows concurrent data access from multiple nodes in a cluster, whereas VxVM and VxFS are accessible on (one) designated node in a cluster.

Although multiple nodes may access the same data in a CFS cluster, metadata updates are managed by a single node in the cluster, thus avoiding the possibility of data corruption.

The first node to mount the CFS file systems becomes the primary and all other nodes in the cluster become secondary. The primary node manages all the file system metadata updates, including requests from the secondary nodes, and maintains the intent log. If the primary node fails, then one of remaining nodes is elected to be the primary node. The new primary node reads the intent log and performs the required updates. The failure of a secondary node does not impact the metadata.

ServiceGuard CFS clusters support up to 4 nodes while non-CFS clusters support up to 16 nodes.\(^2\)

\(^1\) For detailed information, refer to HP ServiceGuard Storage Management Suite Release Notes and Veritas Storage Foundation, Cluster File System, located at [http://www.docs.hp.com](http://www.docs.hp.com).

\(^2\) Refer to E-Lab Interoperability Navigator for current supported versions and configurations.
**HP ServiceGuard Storage Management Suite configuration**

This section documents the details of configuring a ServiceGuard Storage Management environment with Dell EMC arrays (DMX, DMX-2, DMX-3, DMX-4, VMAX 40K, VMAX 20K/VMAX, VMAX 10K (Systems with SN xxx987xxxx), VMAX 10K (Systems with SN xxx959xxxx), and VMAXe = 128:1, CX-3 and CX series). In addition to configuring the cluster, the user will create the appropriate logical volume infrastructure to provide access to data from different nodes. This is done with Veritas Cluster Volume Manager (CVM). CVM configuration is done after cluster configuration.

**Note:** PowerPath is a requirement for all VNX series and CLARiiON systems integrated into an HP ServiceGuard Storage Management environment.

**Preparing the cluster and the system multi-node package**

To prepare the cluster and system multi-node package:

1. Verify the following timeout settings are in the ServiceGuard configuration:

   HEARTBEAT_INTERVAL 15000000
   NODE_TIMEOUT 60000000
   AUTO_START_TIMEOUT 600000000
   NETWORK_POLLING_INTERVAL 2000000

   If the values are not set correctly, edit the cluster configuration file and use the `cmcheckconf` and `cmapplyconf` commands to check and apply the configuration changes.

2. Verify the cluster is running:

   # cmviewcl

3. If the cluster is not running, start it by using the command:

   # cmruncl -v -f

4. If you have not initialized your disk groups, or if you have an old install that needs to be re-initialized, use the `vxinstall` command to initialize VxVM/CVM disk groups.

5. Use the `cfscluster` command to create the CVM package:

   # cfscluster config -t 4000 -s
The Veritas cluster volumes are managed by a ServiceGuard-supplied system multi-node package which runs on all nodes at once. The package has the following responsibilities:

- Maintain Veritas configuration files /etc/llttab, /etc/llhosts, /etc/gabtab
- Launch required services: cmvxd, cmvxpingd, vxfsckd
- Start/halt Veritas processes in the proper order: llt, gab, vx fen, odm, cvm, and cfs

Do not edit system multi-node package configuration files, such as VxVM-CVM-pkg.conf and SG-CFS-pkg.conf.

Create and modify the configuration using the cfsadmin commands. Activate the SG-CFS-pkg and start up CVM with the cfsclecluster command. The command can also be used to create the SG-CFS-pkg.

6. Verify the system multi-node package is running and CVM is up, using the cmviewcl or cfsclecluster command. The following is an example of using the cfsclecluster command. In the last line, you can see that CVM is up, and that the mount point is not yet configured:

```
# cfsclecluster status
Node            : hpint036
Cluster Manager : up
CVM state       : up
MOUNT POINT TYPE SHARED VOLUME DISK GROUP STATUS

Node            : hpint091
Cluster Manager : up
CVM state       : up
MOUNT POINT TYPE SHARED VOLUME DISK GROUP STATUS

Node            : hpint021
Cluster Manager : up
CVM state       : up (MASTER)
MOUNT POINT TYPE SHARED VOLUME DISK GROUP STATUS
```

Because the CVM system multi-node package automatically starts up the Veritas processes, do not edit these files:

```
/etc/llthosts, /etc/llttab, /etc/gabtab
```
Creating the disk groups

To create disk groups, initialize the disk group from the master node.

1. Find the master node using vxdctl or cfscluster status:

```
# cfscluster status
Node            : hpint036
Cluster Manager : up
CVM state       : up
MOUNT POINT     TYPE  SHARED VOLUME DISK GROUP STATUS
Node            : hpint091
Cluster Manager : up
CVM state       : up
MOUNT POINT     TYPE  SHARED VOLUME DISK GROUP STATUS
Node            : hpint021
Cluster Manager : up (MASTER)
CVM state       : up
MOUNT POINT     TYPE  SHARED VOLUME DISK GROUP STATUS
```

2. Initialize a new disk group, or import an existing disk group, in shared mode, using the `vxdg` command.
   - For a new disk group use the init option:
     ```
     # vxdg -s init cvm_dg01 c19t4d0
     ```
   - For an existing disk group, use the import option:
     ```
     # vxdg -C -s import cvm_dg01
     ```

3. Verify the disk group. The state should be enabled and shared:

```
# vxdg list
NAME            STATE                       ID
  cvm_dg01     enabled,shared,cds   1171460381.535.hpint021
```

Creating the disk group cluster packages

To create the disk group cluster packages:

1. Use the `cfsdgadm` command to create a ServiceGuard CFS disk group package. The SG-CFS-DG-1 package will be generated to control the disk group cvm_dg01, in shared write mode:

   ```
   # cfsdgadm add cvm_dg01 all=sw
   ```

2. Use the `cmviewcl` or the `cfsdgadm display` command to verify the package has been created.

```
# cfsdgadm display
Node Name : hpint036
  DISK GROUP  ACTIVATION MODE
cvm_dg01    sw (sw)

Node Name : hpint091
  DISK GROUP  ACTIVATION MODE
cvm_dg01    sw (sw)

Node Name : hpint021 (MASTER)
  DISK GROUP  ACTIVATION MODE
cvm_dg01    sw (sw)
```
3. Activate the disk

**Symmetrix configuration**

MC/ServiceGuard Clusters in a VMAX/Symmetrix environment support FWD SCSI and Fibre Channel (fabric and loop). Refer to the Dell EMC E-Lab Navigator Single Host and Cluster sections for supported:

- Host models and firmware versions
- HBAs and driver versions
- Switches and firmware versions
- Symmetrix director flag settings
- HP-UX and MC/ServiceGuard versions

The VMAX/Symmetrix system should be configured so that each node in a cluster package has access to the same set of devices, and so each node has multiple paths to the devices through separate VMAX/Symmetrix channel directors. The same VMAX/Symmetrix volume should be defined on multiple channel directors to provide for multipathing capability from the host.

The shared volumes should be assigned to alternate between odd and even channel directors. If neither PowerPath nor Veritas DMP is used, the primary path of each of the packages should be configured to alternate among the different paths, to provide basic I/O load balancing.

Figure 17 on page 115 shows a switched fabric example, in which each host shares the same set of devices on the VMAX/Symmetrix system through two separate paths.

**Figure 17** Fabric connections example
**Note:** Each host uses two HBAs to the same Symmetrix device to allow the use of channel failover (PowerPath, for example) to eliminate the Symmetrix directors, HBAs, and cables as single points of failure.

If host-level mirroring is not used, the VMAX/Symmetrix volumes in the cluster should be protected with RAID 1 (Symmetrix mirroring) or Parity RAID.
VMAX and Symmetrix boot device in an HA environment

Both Dell EMC and HP support the use of VMAX/Symmetrix devices for booting HP-UX hosts in an HA environment. For detailed information regarding boot requirements, restrictions, setup, and configuration, refer to “External boot from a VMAX or Symmetrix device” on page 82 and the Dell EMC E-Lab Navigator.
Host Environment
Part 2 includes:

- Chapter 6, "HP-UX Hosts and VNX Series and CLARiiON Systems"
- Chapter 7, "Virtual Provisioning on VNX Series and CLARiiON Systems"
- Chapter 8, "HP-UX Hosts and Unity Series"
CHAPTER 6

HP-UX Hosts and VNX Series and CLARiiON Systems

This chapter provides information specific to HP Servers running HP-UX and connecting to VNX series and CLARiiON systems.

**Note:** Refer to Dell EMC E-Lab Navigator or contact your Dell EMC representative for the latest information on qualified hosts.

- HP-UX in a VNX series and CLARiiON environment 124
- VNX series and CLARiiON configuration for HP-UX hosts 126
- Configuration requirements for VNX series and CLARiiON support with 11iv3 130
- External boot from VNX series and CLARiiON 137
- HP-UX System Administration Manager (SAM) 141
- Logical Volume Manager (LVM) 144
- Veritas Volume Manager (VxVM) 148
- MC/ServiceGuard 149
HP-UX in a VNX series and CLARiiON environment

This section lists VNX series and CLARiiON support information for the HP-UX environment.

Host connectivity

Refer to the Dell EMC Simple Support Matrices, Dell EMC E-Lab Navigator, or contact your Dell EMC representative for the latest information on qualified HP-UX host servers, operating system versions, switches, and host bus adapters.

Boot support

HP 9000 and Integrity Itanium servers running HP-UX 11x have been qualified for booting from VNX series and CLARiiON systems. Refer to the Dell EMC Support Matrices, Dell EMC E-Lab Navigator, or contact your Dell EMC representative for information on supported VNX series and CLARiiON boot configurations.

Logical device support

VNX series systems can present up to 8192 devices. The maximum LUNs per storage group for a VNX system is up to 1024.

CLARiiON storage arrays can present up to 2048 LUNs depending on the array model (CX700 arrays can support 2048 LUNs, CX600/CX500 arrays can support 1024 LUNs.

The maximum number of LUNs per host initiator or storage group is 256, so the maximum number of LUNs per array that can be presented to any connected HP-UX host or cluster is 256. Multiple VNX series or CLARiiON systems would be necessary to configure more than 256 VNX series or CLARiiON LUNs on a single HP-UX host or cluster.

VNX series maximum LUNs are as follows:

<table>
<thead>
<tr>
<th>VNX series systems</th>
<th>Maximum LUNs</th>
</tr>
</thead>
<tbody>
<tr>
<td>VNX 5100</td>
<td>512</td>
</tr>
<tr>
<td>VNX 5300</td>
<td>2048</td>
</tr>
<tr>
<td>VNX 5500</td>
<td>4096</td>
</tr>
<tr>
<td>VNX 5700</td>
<td>4096</td>
</tr>
<tr>
<td>VNX 7500</td>
<td>8192</td>
</tr>
</tbody>
</table>

CLARiiON CX4 arrays with R29 Dell EMC FLARE™ offers increased LUN limits. The LUN limits are:

<table>
<thead>
<tr>
<th>CLARiiON CX4 systems</th>
<th>LUNs per array</th>
</tr>
</thead>
<tbody>
<tr>
<td>CX4-120</td>
<td>1024</td>
</tr>
</tbody>
</table>
The maximum number of LUNs that a specific server can access is 512 for CX4-120 and CX4-240 storage systems and 1024 for CX4-480 and CX4-960 storage systems, but it may be lower depending on the operating system running on the server. For details, refer to Dell EMC E-Lab Navigator.

### Storage component overview

The basic components of a VNX series or CLARiiON storage system configuration are:

- One or more storage systems.
- One or more servers (running a supported operating system such as HP-UX) connected to the storage array(s), directly or through switches.
- For Unisphere/Navisphere® 5.X or lower, a Windows NT or Windows 2000 host (called a management station) running Unisphere/Navisphere Manager and connected over a LAN to the servers and the storage processors (SPs) in VNX series, CLARiiON, and/or CX-series storage arrays. (A management station can also be a storage system server if it is connected to a storage system.)
- For Unisphere/Navisphere 6.X, a host running an operating system that supports the Unisphere/Navisphere Manager browser-based client, connected over a LAN to the servers and the SPs in VNX series, CLARiiON, and/or CX-series storage arrays. For a current list of such operating systems, refer to the Unisphere/Navisphere Manager 6.X release notes at Dell EMC Online Support.

### Required storage system setup

VNX series and CLARiiON system configuration is performed by a Dell EMC Customer Engineer (CE) through Unisphere/Navisphere Manager. The CE will configure the initial storage system settings for each SP. The procedures described in this chapter assume that all hardware equipment (such as switches and storage systems) used in the configurations have been properly installed and connected.
VNX series and CLARiiON configuration for HP-UX hosts

VNX series and CLARiiON systems must be properly configured for HP-UX hosts. This section provides guidelines and general procedures to set up a VNX series and CLARiiON system for HP-UX.

VNX series and CLARiiON SPs and LUNs

VNX series and CLARiiON systems have an active/passive LUN ownership model. Each VNX series and CLARiiON LUN device is owned and serviced by only one Storage Processor (SP) at a time, either SP A or SP B. The following terminology is used in this chapter:

- **Active/passive path**: In configurations with multiple paths to VNX series and CLARiiON SP ports, a device path to the SP that currently owns the LUN is an active path, and a device path to the SP that does not currently own the LUN is a passive path.
- **Trespass**: A LUN trespass is the movement of a LUN or transfer of ownership from one SP to the other SP. When a LUN is trespassed, the previously active paths will become passive paths, and vice versa the previously passive paths will become active paths.
- **Default SP/default path**: Each VNX series and CLARiiON LUN has a default owner, either SP A or SP B. A default path is a device path to the default SP of the LUN.

HP-UX initiator settings

Due to the active/passive LUN ownership model of VNX series and CLARiiON SPs, the initiator records on the VNX series and CLARiiON system must be set accordingly for the specific HP-UX environment to avoid access and trespass problems when paths to multiple SPs have been or will be configured. The two initiator settings of importance are **Initiator Type** and **Failover Mode**. The appropriate initiator settings to select will depend on the number of paths configured to the VNX series and CLARiiON system and the multipath or failover software configured on the HP-UX host.

<table>
<thead>
<tr>
<th>HP-UX Configuration</th>
<th>Initiator Type</th>
<th>Failover Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>No failover or multipath, single path to one SP</td>
<td>HP No Auto Trespass</td>
<td>0</td>
</tr>
<tr>
<td>Native LVM PV Links failover, paths to both SPs</td>
<td>HP Auto Trespass</td>
<td>0</td>
</tr>
<tr>
<td>PowerPath</td>
<td>HP No Auto Trespass</td>
<td>1</td>
</tr>
<tr>
<td>Veritas DMP with ASL (HP-UX 11i v1.0 only)</td>
<td>HP No Auto Trespass</td>
<td>2</td>
</tr>
<tr>
<td>Veritas VxVM without ASL – no DMP or PowerPath (HP-UX 11i v1, HP-UX 11i v2, HP-UX 11iv3)</td>
<td>HP No Auto Trespass</td>
<td>0</td>
</tr>
</tbody>
</table>

**Note:** When setting up a VPLEX-attach with VNX series or CLARiiON, the initiator type must be set to CLARiiON Open and the Failover Mode set to 1. ALUA is not supported. Refer to “Required storage system setup” on page 51 for more information on VPLEX requirements.
Enable VNX series and CLARiiON write cache

VNX series and CLARiiON LUNs that are assigned to HP-UX hosts must have write cache enabled. The write cache can be enabled via the Storage Systems Properties window in Unisphere/Navisphere or through the use of Navisphere CLI navicli commands. Note that write cache for VNX series and CLARiiON RAID 3 LUNs must be specially enabled for each individual LUN.

Registering HP-UX initiator connections

The HP-UX host must be connected and registered with the VNX series and CLARiiON system before LUNs can be assigned or presented to the host:

1. Install one or more host bus adapters (HBAs) into the HP-UX host, and upgrade drivers and firmware if required or specified in the Dell EMC Simple Support Matrices. Refer to HP documentation for instructions on installing HBAs and upgrading drivers/firmware. Check the label on each HBA or the documentation shipped with the HBA and note the unique World Wide Name (WWN) of each HBA.

2. Connect the HP-UX HBA(s) to the VNX series or CLARiiON system according to your planned path configuration. If the HP-UX HBAs will be attached via a fibre channel switch fabric, configure zones on the switch for connectivity to VNX series or CLARiiON system SP(s). If the WWN of each HBA was not found in the previous step, check the name server table or port information of the fibre channel switch to which the HBAs are connected to determine the WWNs of the HBAs.

Note: Refer to “Adding the alternate path to a volume group using UNIX commands” on page 145 for CISCO switch configuration guidelines.

3. Run the ioscan –fn and insf –e commands on the HP-UX host to scan new devices and create new device special files.

4. Install the Unisphere/Navisphere Host Agent and CLI software on the HP-UX host according to the instructions in the EMC Navisphere Host Agent and CLI for HP-UX Version 6.X Installation Guide.

5. After the Unisphere/Navisphere Host Agent is installed on the HP-UX host, edit the /etc/Navisphere/agent.config file to enable or disable Auto Trespass according to Table 18 on page 126 by adding or commenting out the line OptionsSupported AutoTrespass. Add the nomegapoll keyword as a new line at the top of the agent.config file. Save the file, and restart the Unisphere/Navisphere Host Agent by running /sbin/init.d/agent stop followed by /sbin/init.d/agent start.

Note: You must ensure that AutoTrespass is set correctly in the agent.config file, because the AutoTrespass setting in the agent.config file will override any AutoTrespass Initiator Type set manually in Unisphere/Navisphere Manager whenever the Unisphere/Navisphere Host Agent is restarted.

6. From a Unisphere/Navisphere Manager browser-based client logged in to the VNX series or CLARiiON system, right-click the array icon and select Connectivity Status from menu. You should see initiator records for each of the HP-UX HBA connections logged in to the array. If you do not see any of your HP-UX HBA connections in the initiator
records, select **Update Now** from the Unisphere/Navisphere Manager right-click menu, then recheck the initiator records. If you still do not see your HBA connections after 15 minutes, verify or repeat steps 2 through 5 above.

7. This step will depend on the results of previous steps. Check the HP-UX HBA initiator records in the **Connectivity Status** window:

   a. If you see all expected HP-UX HBA initiator records and the Registered column shows Yes for each initiator record, then click **Info** for each initiator record to verify the settings of each initiator connection. If there are any incorrect settings, use **Group Edit** or **Deregister** to modify the initiator settings.

   b. If you see all expected HP-UX HBA initiator records but the Registered column shows No for the initiator records, then select **Register** to register each unregistered initiator record.

   c. If you do not see any HP-UX HBA initiator records (for example, if you did not install the Unisphere/Navisphere Host Agent), then select **New** to manually create and register each of your HP-UX HBA initiator connections. For each HP-UX HBA connection, enter the full WWN of the HBA and the SP and Port to which it is connected.

8. The HP-UX HBA initiator settings should be as follows:

   a. **ArrayCommPath** should be enabled.

   b. **Unit Serial Number** should be set to Array.

   c. Set **Initiator Type** and **Failover Mode** according to Table 18 on page 126.

   d. Fill in the **Host Name** and **IP Address** of the HP-UX host or select the **Existing Host** to which the HBA belongs.

### Making LUNs available to HP-UX

The following procedure provides the general steps for creating and making LUNs available to an HP-UX host.

1. Create RAID Groups of the desired RAID type and bind LUNs on the VNX series or CLARiiON system for use by the HP-UX host(s).

2. Create a Storage Group on the array and select the newly bound or existing LUNs to be assigned to the HP-UX host(s). Then select the HP-UX host(s) to be connected to the new Storage Group and LUNs from the list of available hosts.

3. Verify that write cache has been enabled on the array by checking the Cache settings in the Storage System Properties of the array. If there are RAID 3 LUNs, check the Cache settings in the LUN Properties of each individual RAID 3 LUN.

4. On the HP-UX host, run the `ioscan -fn` and `insf -e` commands on the HP-UX host to scan new devices and create new device special files. Run `ioscan -fnC disk > scan.out` to save ioscan output to a file for review and verify that all expected VNX series and CLARiiON LUNs and paths have been discovered by the HP-UX host.

5. Create volume groups, logical volumes, and/or filesystems on the VNX series and CLARiiON LUNs as desired. Use any VNX series and CLARiiON LUN just as you would any newly acquired disk device. If you have configured multiple hardware paths to the
same VNX series and CLARiiON logical disk device, the HP-UX host ioscan and insf
utilities will create a new hardware path entry and new device special file for each
hardware path to the same VNX series and CLARiiON logical disk device.
Configuration requirements for VNX series and CLARiiON support with 11iv3

This section provides the requirements for support of VNX series and CLARiiON systems with HP-UX 11i v3.0 (HP-UX 11.31). Support of the T10 Asymmetric Logical Unit Access (ALUA) standard was introduced with CLARiiON FLARE-Operating-Environment Release 26.

Prerequisites

To run 11i v3 with VNX series or CLARiiON systems you must have the following prerequisites:

- VNX series systems support ALUA.
- To disable legacy DSF's run the command `rmsf -L`.
- The CLARiiON array (CX3 series, CX300, CX500, and CX700) must be running the FLARE-Operating-Environment release 26 or later and is required to support HP-UX 11iv3. This version of FLARE introduced the ALUA support for HP-UX 11i v3. Refer to Table 19 on page 131 for the minimum FLARE requirements needed for other CLARiiON models.
- ALUA support was introduced into HP-UX 11iv3 (11.31) with the September 2007 11iv3 release. The host must be running the March 2008 release of the 11iv3 operating system.
- Configure the initiators for ALUA failover mode (failover mode 4).
- CLARiiON Open and HP No Auto Trespass initiator types are supported with HP-UX 11iv3 (11.31). CLARiiON Open initiator type implements peripheral device addressing resulting in expected HP-UX behavior of creating only eight legacy device special files (DSFs) per target port.

HP No Auto Trespass initiator type implements the Volume Set Addressing method. You must configure only **HP No Auto Trespass** if there are any legacy DSFs dependencies that have the format /dev/dsk/c2t1d0 and /dev/rdsk/c2t1d0.

You may configure either CLARiiON Open or HP No Auto Trespass if there are no legacy DSFs dependencies and only persistent DSFs (also known as agile DSFs) are utilized that have the format /dev/disk/disk42 and /dev/rdisk/42.

For more information, refer to the *HP-UX 11i v3 Persistent DSF Migration Guide* at [http://docs.hp.com](http://docs.hp.com).

**Note:** If using the Unisphere/Navisphere agent.config file, ensure that the appropriate **OptionsSupported** setting is in the file, otherwise the initiator setting on the array will be changed when the Unisphere/Navisphere agent starts up. To maintain the Unisphere/Navisphere Manager initiator setting, uncomment the **OptionsSupported** line in the agent.config file and change it to state **OptionsSupported ArrayType**.

---

**VNX series minimum requirements**

VNX OE for Block Version 31 is the minimum requirement for VNX series systems.
Table 19 lists the minimum FLARE requirements needed for CLARiiON models.

<table>
<thead>
<tr>
<th>CLARiiON model</th>
<th>HP-UX version</th>
<th>Storage operating environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>AX4-5</td>
<td>11iv1, 11iv2</td>
<td>02.23.050.5.004</td>
</tr>
<tr>
<td>AX4-5SC</td>
<td>11iv1, 11iv2</td>
<td>02.23.050.5.703</td>
</tr>
<tr>
<td>AX4-5i</td>
<td>11iv1, 11iv2</td>
<td>02.23.050.5.004</td>
</tr>
<tr>
<td>AX4-5SCi</td>
<td>11iv1, 11iv2</td>
<td>02.23.050.5.703</td>
</tr>
<tr>
<td>CX400</td>
<td>11iv1, 11iv2</td>
<td>02.19.400.5.007</td>
</tr>
<tr>
<td>CX600</td>
<td>11iv1, 11iv2</td>
<td>02.19.600.5.007</td>
</tr>
<tr>
<td>CX300</td>
<td>11iv1, 11iv2, 11iv3</td>
<td>02.19.300.5.007, 02.19.300.5.007, 02.26.300.5.014</td>
</tr>
<tr>
<td>CX500</td>
<td>11iv1, 11iv2, 11iv3</td>
<td>02.19.500.5.007, 02.19.500.5.007, 02.26.500.5.014</td>
</tr>
<tr>
<td>CX700</td>
<td>11iv1, 11iv2, 11iv3</td>
<td>02.19.700.5.007, 02.19.700.5.007, 02.26.700.5.014</td>
</tr>
<tr>
<td>CX3-10c</td>
<td>11iv1, 11iv2, 11iv3</td>
<td>03.22.010.5.xxx, 03.22.010.5.xxx, 03.26.010.5.xxx</td>
</tr>
<tr>
<td>CX3-20, CX3-20c, CX3-20f</td>
<td>11iv1, 11iv2, 11iv3</td>
<td>03.22.020.5.xxx, 03.22.020.5.xxx, 03.26.020.5.xxx</td>
</tr>
<tr>
<td>CX3-40, CX3-40c, CX3-40f</td>
<td>11iv1, 11iv2, 11iv3</td>
<td>03.22.040.5.xxx, 03.22.040.5.xxx, 03.26.040.5.xxx</td>
</tr>
<tr>
<td>CX4-120/CX4-240/CX4-480/CX4-960</td>
<td>11iv1, 11iv2, 11iv3</td>
<td>04.28.000.5.003, 04.28.000.5.003, 04.28.000.5.003</td>
</tr>
<tr>
<td>CX4-120C8/CX4-240C8/CX4-480C8/CX4-960C8</td>
<td>11iv1, 11iv2, 11iv3</td>
<td>04.28.000.5.704, 04.28.000.5.704, 04.28.000.5.704</td>
</tr>
</tbody>
</table>

System configuration

After verifying that the prerequisites have been met, proceed and configure the array. There are three methods to configure the array for ALUA support, each discussed briefly in this section.
Using the Naviseccli command line

To use Naviseccli, you must have:

- **Naviseccli** installed on a host with network access to the VNX series and CLARiiON system
- **Unisphere/Navisphere Agent** running on the 11iv3 host you are connecting to the VNX series and CLARiiON system

The following example uses the command line to configure the array:

```
naviseccli -h 172.23.180.130 -h 172.23.180.131 storagegroup -sethost -host hpint064
-failovermode 4 -arraycommpath 1 -type 10
```

**WARNING:** Changing configuration options may cause the array to stop functioning correctly. Do you wish to continue (y/n)? y

The syntax for the command is as follows:

```
-h 172.23.179.130 — the array ips
-host hpint064 — the host name (provided by Unisphere/Navisphere Agent)
-failovermode 4 — the failover mode for ALUA support
-type 10 — the host initiator options
```

For ALUA, the only option (other than host) that can be modified for support is the “type” options.

There are two supported values for the initiator options:

- **10**
  
  Using **10** sets the system for **HP No Auto Trespass** initiator options.

- **3**
  
  Using **3** sets the system for **CLARiiON Open** initiator options.

For detailed information on the command line options, refer to the EMC **Navisphere Command Line Interface (CLI) Reference** manual, available on Dell EMC Online Support.

Unisphere/Navisphere Manager using Connectivity Status

This method assumes that security is enabled and active on the target array. If security is not configured, please refer to **EMC Navisphere Manager Installation Guide**, available on Dell EMC Online Support, for information on configuring security.
To use the Unisphere/Navisphere Manager, point your Web browser to the IP address of one of your storage arrays. You should see a display similar to Figure 18.

**Figure 18** Unisphere/Navisphere Manager display

To use this method, you will need:

- Unisphere/Navisphere Agent running on the 11iv3 host that you are connecting to the VNX series and CLARiiON system.
- A list of the initiators that the host has attached to the VNX series and CLARiiON system.

To configure ALUA support using this mode:

1. Right-click on the array serial number.
2. Select **Connectivity Status** from the pop-up list.

   The connectivity status menu, similar to Figure 19, displays.

3. Click **Group Edit**.

**Figure 19** Connectivity status menu
The **Group Edit Initiators** menu, similar to Figure 20, displays.

![Group Edit Initiators menu](image)

**Figure 20** Group Edit Initiators menu

4. Select the initiators associated with the host that you are configuring.

5. Change the **Initiator Type** to **HP No Auto Trespass** or **CLARiiON Open**, depending on the initiator options you require.

6. Set **Failover Mode** to 4 for ALUA support.

7. Select the host information and press **OK** to complete the configuration.

**Unisphere/Navisphere Manager using Failover Setup Wizard**

To use this method you will need Unisphere/Navisphere Agent running on the 11iv3 host you are connecting to the VNX series and CLARiiON system.

To use the **Failover Setup Wizard**:

1. Right click the **Tools** menu bar.

2. Select **Failover Setup Wizard** and a dialog box, similar to Figure 21, displays.

![Failover Setup Wizard dialog box](image)

**Figure 21** Failover Setup Wizard dialog box
3. Click **Next** to proceed.
   A **Select Host** dialog box displays, as shown in **Figure 22**.

   ![Select Host dialog box](image1)

   **Figure 22** Select Host dialog box

4. Select the new host and click **Next**.
   A **Select Storage systems** dialog box displays..

   ![Select Storage Systems dialog box](image2)

   **Figure 23** Select Storage Systems dialog box

5. Highlight the storage array and click **Next**.
The **Specify Settings** dialog box displays.

![Specify Settings dialog box](image)

**Figure 24** Specify Settings dialog box

6. Set the initiator option to either **HP No Auto Trespass** or **CLARiiON Open**, depending on the initiator options you require.

7. Set the failover mode to **4** for ALUA support.

8. Select **Next** and a screen displays prompting you to confirm your choices.

9. Verify the changes are correct and click **Next**.

10. You will receive a final confirmation about the changes that you are making. Select **Yes** to continue.

11. The screen will confirm the operation completed successfully. Click **Finish** to exit from the **Failover Setup Wizard**.
External boot from VNX series and CLARiiON

This section provides guidelines and general procedures for configuring external boot of HP-UX hosts from VNX series and CLARiiON systems in Fibre Channel switch SAN environments. Refer to the Dell EMC Simple Support Matrices or Dell EMC E-Lab Navigator for the specific VNX series and CLARiiON models, HP servers, and HBAs supported with external boot.

General guidelines

Because many variables determine the topology of a SAN and each customer may have different requirements, some general guidelines have been defined for supported configurations:

- Configure high availability with multiple hardware paths to your boot, root, dump, and swap volumes if possible.
- Both data devices and boot devices can share the same HBA or VNX series and CLARiiON Storage Processor (SP) port. However, system performance and boot times may be affected depending on the utilization and I/O load on the shared HBA or SP port.
- Although LUNs from any RAID type can be used as operating system boot devices, a high redundancy RAID type such as RAID 1 is recommended.
- Include “Hot Spare” disks in your VNX series and CLARiiON LUN configuration.

Firmware requirements

The HP-UX operating system currently runs on two different hardware platforms:

- HP 9000 Systems – PA-RISC processor family
  An HP 9000 Server uses the Boot Console Handler (BCH) interface. If your system displays the BCH, then you are booting an HP 9000 Server. Please refer to the HP IT Resource Center for the latest and minimum required PDC to support external boot.
  http://us-support.external.hp.com

- Integrity Servers – Itanium processor family
  An HP Integrity Server uses the Extensible Firmware Interface (EFI). If your system displays the EFI boot manager following the initial firmware test results, then you are booting an HP Integrity Server. Please refer to the HP IT Resource Center for the latest and minimum required "system firmware" to support external boot.
  http://us-support.external.hp.com

Minimum EFI firmware to support external boot on Integrity-based servers is as follows:

- A6795A: Minimum EFI driver version 1.10
- A6826A/A9782A/A9784A: Minimum EFI driver version 1.30 and RISC firmware 3.2.168 or later, HP-UX 11i v2.0 (HP-UX 11.23) Pre-Sept 2004 release
- A6826A/A9782A/A9784A: Minimum EFI driver version 1.37 and RISC firmware 3.2.170 or later, HP-UX 11i v2.0 (HP-UX 11.23) Sept 2004 release

The EFI Driver is available to customers from the HP Software Depot at:
http://www.software.hp.com/
Mirroring the HP-UX operating system and boot to VNX series and CLARiiON

One method of configuring a HP-UX host to boot from external disk devices on a VNX series and CLARiiON system is to mirror existing internal operating system and boot devices to VNX series and CLARiiON systems by using functionality in the LVM or VxVM volume managers. Refer to “Mirroring an internal OS to an external device” on page 65 for guidelines and example procedures. Since VNX series and CLARiiON SPs have an active/passive LUN ownership model, you must ensure that active default device paths to VNX series and CLARiiON systems are specified when configuring LVM or VxVM mirroring.

Configuring VNX series and CLARiiON for new HP-UX installation and boot

The following procedure explains the general steps for a new install of the HP-UX operating system and boot devices on a VNX series and CLARiiON system.

1. Create a RAID Group and bind LUNs for use in the HP-UX boot device configuration. New RAID Group and LUNs are not necessary if there are existing unallocated LUNs available on the VNX series and CLARiiON system.

2. Verify that the intended boot LUNs are large enough in size to be used as HP-UX operating system disks. Minimum operating system disk sizes for boot, dump, swap, etc. can vary depending on the HP-UX version to be installed and the hardware configuration of the HP server, so refer to HP-UX installation documentation for recommended disk sizes.

3. Check the default SP of the intended boot LUNs (the Default Owner SP A or SP B is displayed in LUN Properties). It is important for the boot LUNs to be owned by their default SP during the installation process, otherwise there could be potential trespass issues resulting in boot failures. If more than one device is selected for a boot volume group, ensure all LUN devices are owned by the same default SP.

4. Select the LUNs that you intend to use as operating system disks and add them into a VNX Storage Group.

5. Manually register an HP-UX HBA initiator connection using the Create Initiator Record dialog, as shown in Figure 25 on page 139. If you have multiple hardware paths from HP-UX HBAs to VNX series and CLARiiON SPs configured or planned, only register a single HBA initiator connection path to one SP port at this point. Registering only one HBA initiator connection path will help prevent undesired LUN trespassing between SPs and reduce hardware device scan times during installation. Any remaining or additional HBA initiator connection paths can be registered after the HP-UX installation is completed.

   a. Determine the unique World Wide Name (WWN) of the HBA through which the HP-UX host will be booting. Some HP HBAs will have a WWN label on the adapter card itself or on documentation or packaging shipped with the adapter card. If not, find out the WWN of the HBA by checking the name server table or port information of the fibre channel switch to which the HBA is connected.

   b. Right-click the array icon in Unisphere/Navisphere Manager, select the Connectivity Status menu item and then click New.

   c. Fill in the full HBA WWN of the adapter through which the HP-UX host will be booting and the SP and SP Port to which that adapter is connected or zoned to.

   d. Verify that ArrayCommPath is enabled and Unit Serial Number set to Array.
e. Set \textit{Initiator Type} to HP No Auto Trespass and \textit{Failover Mode} to 0. These are the recommended settings for HP-UX installation. After the installation is completed, these settings may need to be changed as required for the intended or planned HP-UX environment.

f. Enter the \textit{Host Name} and \textit{IP Address} of the HP-UX host, and then click \textbf{OK}.

\begin{figure}[h]
\centering
\includegraphics[width=0.8\textwidth]{figure25.png}
\caption{Create initiator record}
\end{figure}

6. After the HP-UX HBA connection is registered with the array, right-click the Storage Group icon in Unisphere/Navisphere Manager and select \textbf{Connect Hosts} from the menu list. Add the HP-UX host to the Storage Group to grant it access to the intended boot LUNs.

7. Insert the HP-UX OS installation media CD/DVD or launch a remote Ignite-UX session to begin installation of the OS on the VNX series and CLARiiON system. Refer to HP-UX installation documentation for details on the actual operating system installation process.

8. The HP-UX installation program will allow you to choose which disk devices to use for installation of the operating system. Select the desired VNX series and CLARiiON disk devices from the list of available disks displayed by the installation program. If you see one or more of the following problems, then the HP-UX HBA connection to the VNX series and CLARiiON system may not be configured correctly, exit the installation and verify steps 3 to 6:
• The LUNs configured in your VNX series and CLARiiON Storage Group do not appear in the list of disk devices available for installation.

• The VNX series and CLARiiON disk devices appear as “LUNZ” or end in “UNB”.

• The VNX series and CLARiiON disk devices have H/W Paths with .255 in the hardware path address.

• The VNX series and CLARiiON disk devices have a size of 0 (zero) MB.

**Note:** Refer to Appendix Appendix B, “Setting Up Cisco MDS 9000 Switches for HP-UX Environments,” for CISCO switch configuration guidelines.

---

**Figure 26** HP-UX installation ioscan output

9. After the HP-UX installation is completed, configure your remaining planned HP-UX HBA path connections and your desired multipath or failover software and volume manager groups.

10. Configure the VNX series and CLARiiON initiator settings for your existing HBA boot path connection(s) and any new HBA connections as specified in Table 18 on page 126. Refer to *Registering HP-UX Initiator Connections* for details.
HP-UX System Administration Manager (SAM)

SAM is an HP-UX utility that provides a menu-driven graphical interface for performing system administration tasks as an alternative to using conventional UNIX command line utilities.

When using the SAM utility to configure VNX series and CLARiiON LUN devices, the number of paths reported by SAM may be incorrect. Figure 27 shows how the information may appear.

Figure 27  SAM disk output

The problem is how the inquiry information is being interpreted by the SAM utility. The following changes need to be implemented to correct this issue.

For 11i v1.0, and 11i v2.0, you must edit the file /usr/sam/lib/C/pd_devinfo.txt file as follows:

1. Find the existing entry that begins:

   DISK:::sdisk:::.*DGC.*3400.*::::::::::::::HPMODEL 30 LUN

2. Add the following new entries after that entry. These lines must be put after the existing entry for this fix to work:

   DISK:::sdisk:::.*DGC.*CX*.*::::::::::::::CX Series LUN:::::DISK_ARRAY,CLARIION
DISK:::sdisk:::*DGC.*C47*.*::::::::::::FC Series LUN::::::DISK_ARRAY,CLARIION

3. Next search for the following entry:
DISK:::disc3:::*DGC.*3400.*::::::::::::HP Model 30 LUN::::::DISK_ARRAY,CLARIION

4. Add the following new entries after that entry. These lines must be put after the existing entry for this fix to work:
DISK:::disc3:::*DGC.*CX.*::::::::::::CX Series LUN::::::DISK_ARRAY,CLARIION
DISK:::disc3:::*DGC.*C47*.*::::::::::::FC Series LUN::::::DISK_ARRAY,CLARIION

5. Save these edits and restart SAM. The output in SAM should be similar to Figure 28 on page 142.

Figure 28 Corrected SAM disk output
Note that if you use SAM to configure your LVM volume groups, it is possible to configure the primary and alternate paths to a volume group incorrectly. It is strongly recommended that you use command lines to create, expand, export, import, or perform other LVM operations. This will allow you to explicitly specify your hardware paths for LVM operations.

Failure to specify the primary and alternate links correctly in an “AutoTrespass” environment may lead to undesirable behavior.
Logical Volume Manager (LVM)

This section provides information on Logical Volume Manager (LVM).

Creating volume groups on LUNs

Logical volumes, as managed by the Logical Volume Manager (LVM), is the preferred method for managing disks on an HP-UX system. LVM provides the capacity for dual cabling (using dual controllers) to the same physical device, which increases the availability of the data in case one of the paths fails. This capacity is referred to as alternate paths but is also known as physical volume links (PVLinks).

Note: In LVM PVLinks alternate path configurations, you must specify active device paths as your initial primary device paths when creating LVM volume groups. Before creating volume groups, use Unisphere/Navisphere Manager (or navicli) to determine the owner SP of your intended LVM devices. An active device path is a path to the owner SP (either SP A or SP B) of a LUN, and a passive device path is a path to the other non-owner SP of a LUN. Do not use passive paths as the initial primary device paths when creating volume groups.

Creating a volume group on a LUN using UNIX commands

To create a volume group on a LUN using UNIX commands:

1. Create a directory to contain the files associated with the volume group:

   mkdir /dev/vgname

   where vgname is the name of the new volume group.

2. Examine the output for the major and minor device numbers (man “ls” and “mknod” for details) by entering the command:

   ls -l /dev/*group

3. Use the mknod command to create a device file named group in the newly created directory to contain the volume group definition:

   mknod /dev/vgname/group c 64 0xNN0000

   In this command, the c indicates that this is a character-device file, 64 is the major device number for the group device file, and 0xNN0000 is the minor number for the group device file. By default, NN is in the range 00–0F and must be unique.

   If you want to increase the range of NN values, increase the maxvgs kernel parameters:

   a. Using SAM, select Kernel Configuration, and click Configurable Parameters.

   b. Set the maxvgs to the desired value.

   c. Reboot the system.

4. Initialize each device you will be using for the volume group by entering the command:

   pvcreate /dev/rdsk/clt2d3

   where clt2d3 is the name of the device to be included in the volume group.

   Ensure that the device file specified is an active device path to the owner SP of the LUN device.
5. Use the `vgcreate` command to define the new volume group specifying the files created in the previous commands:

   \[ \texttt{vgcreate} \ \textit{vgname} \ /dev/dsk/c1t2d3 \]

6. Create a logical volume on the volume group:

   \[ \texttt{lvcreate} \ -r \ N \ /dev/\textit{vgname} \]

   **Note:** LVM \textit{bad block relocation} (BBR) should be disabled, and the LVM mechanism for marking blocks defective when a medium error is returned should also be disabled for all LVM volumes on Dell EMC devices. The LVM bad block handling can be disabled by specifying the `-r N` option flag when creating the logical volume or with the `lvchange` command if the logical volume has already been created. The exception to this rule is logical volumes that use HP Mirror-UX for host mirroring, in which case the option flag to disable bad block handling should not be set.

   This command creates the logical volume `/dev/\textit{vgname}/lvol1`.

7. To view the status of all volume groups, type:

   \[ \texttt{vgdisplay} \ -v \]

Adding the alternate path to a volume group using UNIX commands

Follow these steps:

1. Use the `vgextend` command to define the alternate path. For example:

   \[ \texttt{vgextend} \ /dev/\textit{vgname} \ /dev/dsk/c5t4d3 \]

   where \textit{vgname} is the volume group name and `/dev/dsk/c5t4d3` indicates the alternate path to the device.

2. View and verify the alternate path connection:

   \[ \texttt{vgdisplay} \ -v \]

Creating a volume group on a LUN using SAM

To create a volume group on a LUN using SAM:

1. From the SAM main menu, follow this menu path:

   **Disks and File Systems > Volume Groups**

   **Note:** You might see an error message that starts as shown below. Disregard this error message and click \texttt{OK} when the prompt appears to continue.

   The command used to retrieve information about HP A323x Disk Arrays has failed. The stderr is shown below. The SCSI command returned with the following Sense bytes: 0x52400 (See Manual)

   SAM is unable to communicate with the device controller at hardware path, 8/0.xxx...

2. In the **Disks and File Systems** dialog box, follow this menu path:
Actions > Create or Extend

For a single-path configuration, SAM displays a list of available LUNs similar to the following, where the SP has access to all LUNs owned by that SP:

<table>
<thead>
<tr>
<th>Unused disks: Hardware Path</th>
<th>Description</th>
<th>Total MB</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/12.8.0.1.0.0.0</td>
<td>DGC CS300WDR5</td>
<td>4768</td>
</tr>
<tr>
<td>12/12.8.0.1.0.0.1</td>
<td>DGC CS300WDR5</td>
<td>4768</td>
</tr>
<tr>
<td>12/12.8.0.1.0.0.2</td>
<td>DGC CS300WDR5</td>
<td>4768</td>
</tr>
<tr>
<td>12/12.8.0.1.0.0.3</td>
<td>DGC CS300WDR5</td>
<td>4768</td>
</tr>
<tr>
<td>12/12.8.0.1.0.0.4</td>
<td>DGC CS300WDR5</td>
<td>4768</td>
</tr>
<tr>
<td>12/12.8.0.1.0.0.5</td>
<td>DGC CS300WDR5</td>
<td>4768</td>
</tr>
<tr>
<td>12/12.8.0.1.0.0.6</td>
<td>DGC CS300WDR5</td>
<td>4768</td>
</tr>
<tr>
<td>12/12.8.0.1.0.0.7</td>
<td>DGC CS300WDR5</td>
<td>4768</td>
</tr>
</tbody>
</table>

For an alternate-path configuration, SAM displays a list of available LUNs, similar to the following where both SPs have access to all LUNs:

**Note:** 12/0.8.0.0.0.0.0 is the same as 12/12.8.0.1.0.0.0, and so on.

<table>
<thead>
<tr>
<th>Unused disks: Hardware Path</th>
<th>Description</th>
<th>Total MB</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/0.8.0.0.0.0.0</td>
<td>DGC CS300WDR5</td>
<td>4768</td>
</tr>
<tr>
<td>12/0.8.0.0.0.0.1</td>
<td>DGC CS300WDR5</td>
<td>4768</td>
</tr>
<tr>
<td>12/0.8.0.0.0.0.2</td>
<td>DGC CS300WDR5</td>
<td>4768</td>
</tr>
<tr>
<td>12/0.8.0.0.0.0.3</td>
<td>DGC CS300WDR5</td>
<td>4768</td>
</tr>
<tr>
<td>12/0.8.0.0.0.0.4</td>
<td>DGC CS300WDR5</td>
<td>4768</td>
</tr>
<tr>
<td>12/0.8.0.0.0.0.5</td>
<td>DGC CS300WDR5</td>
<td>4768</td>
</tr>
<tr>
<td>12/0.8.0.0.0.0.6</td>
<td>DGC CS300WDR5</td>
<td>4768</td>
</tr>
<tr>
<td>12/0.8.0.0.0.0.7</td>
<td>DGC CS300WDR5</td>
<td>4768</td>
</tr>
<tr>
<td>12/12.8.0.1.0.0.0</td>
<td>DGC CS300WDR5</td>
<td>4768</td>
</tr>
<tr>
<td>12/12.8.0.1.0.0.1</td>
<td>DGC CS300WDR5</td>
<td>4768</td>
</tr>
<tr>
<td>12/12.8.0.1.0.0.2</td>
<td>DGC CS300WDR5</td>
<td>4768</td>
</tr>
<tr>
<td>12/12.8.0.1.0.0.3</td>
<td>DGC CS300WDR5</td>
<td>4768</td>
</tr>
<tr>
<td>12/12.8.0.1.0.0.4</td>
<td>DGC CS300WDR5</td>
<td>4768</td>
</tr>
<tr>
<td>12/12.8.0.1.0.0.5</td>
<td>DGC CS300WDR5</td>
<td>4768</td>
</tr>
<tr>
<td>12/12.8.0.1.0.0.6</td>
<td>DGC CS300WDR5</td>
<td>4768</td>
</tr>
<tr>
<td>12/12.8.0.1.0.0.7</td>
<td>DGC CS300WDR5</td>
<td>4768</td>
</tr>
</tbody>
</table>

3. In the Select a Disk dialog box, select a disk on which you want to build a volume group, and click OK.
4. In the Add a Disk using LVM dialog box, click Create or Extend a Volume Group.
5. In the Create a Volume Group dialog box, enter a name for the volume group, and click OK twice.

SAM returns you to the Add a disk using LVM dialog box.
6. If you want to create logical volumes on the new volume group, complete the following steps. If not, continue to step 7:
   a. In the Add a Disk using LVM dialog box, click Add New Logical Volume.

   SAM displays the Create New Logical Volume dialog box.
   b. Enter a logical volume name, the size for the logical volume, and the mount directory.
c. Click **Modify LV defaults** and review the settings. Then click **OK**.

d. Click **Modify FS faults** and review the settings. Then click **OK**.

e. Click **Add** to add to the list of logical volumes to be created.

   SAM displays an entry for the new logical volume in the **to be created** logical volume list.

f. To create more logical volumes for this volume group, repeat steps b through e.

g. When you have created a list of all the logical volumes you want, click **OK**.

h. Click **OK** to apply the list.

   SAM returns you to the **Add A disk using LVM** dialog box.

7. In the **Add a Disk using LVM** dialog box, click **OK**.

   If data already exists on the device, SAM displays a confirmation dialog asking if you want to overwrite existing data.

8. If you want to overwrite the data, click **Yes**. If not, click **No**.

   In alternate-path configurations, SAM displays a second confirmation dialog box asking if you want to create an alternate connection for this disk device.

9. Click **No**.

   **Note:** To set an alternate path, finish creating all volume groups and then complete the task “Adding the alternate path to a volume group using UNIX commands” on page 145.

   In the **Disks and File Systems** dialog box, SAM displays an entry for the new volume group.

10. For each additional LUN on which you want to create a volume group, repeat steps 3 through 9.

11. Exit SAM.

12. To view a status of all the volume groups, type:

    ```
    vgdisplay -v
    ```

**What next?**

Create filesystems as described in your HP documentation. After creating filesystems, the LUNs will be ready to use.

Refer to:

- HP-UX system reference manuals for information on mounting your volume groups.
- HP MirrorDisk/UX documentation.
- HP MC/ServiceGuard documentation for information on installing and using the optional MC/ServiceGuard multiple host failover software.
Veritas Volume Manager (VxVM)

Veritas Volume Manager (VxVM) is another volume manager product available on HP-UX providing functionality similar to the native LVM. Base VxVM is a basic version of Veritas Volume Manager 3.5 that is bundled with HP-UX 11i. Users of Base VxVM have the option to upgrade to full-functioned VxVM 3.5 (via license key) or to VxVM 4.1.

**Note:** External boot from VNX series-based and CLARiiON-based VxVM volumes is not supported.

In multipath configs with PowerPath installed, VxVM may have problems importing disk groups containing VNX series and CLARiiON systems due to duplicate diskids. There are two options for resolving the duplicate diskid import issue:

**Option A (preferred)**
- Requires full VxVM 3.5 license to be installed.
- Run the `vxddladm addjbod vid=DGC pagecode=0x83` command
- After running the above command, run `vxddladm listjbod` to verify new VNX series or CLARiiON entry.
- Run `vxconfigd -k -m enable` followed by `vxdisk scandisks` to reinitialize and rediscover VNX series or CLARiiON devices.

**Option B**
- Create a new file `/etc/vx/disks.exclude`
- Add cXtYdZ entries into `/etc/vx/disks.exclude` for each duplicate device path.

For example, if the HP-UX host has 4 available paths to a CLARiiON device c1t0d1, c2t0d1, c5t0d1, c6t0d; then add a new line entry into disks.exclude for each of the 3 duplicate paths c2t0d1, c5t0d1, c6t0d.

**Note:** You can run `powermt display dev=all > powermt.list` to generate a list of all VNX series or CLARiiON device paths.

- Run `vxconfigd -k -m enable -x exclude_enable` to reinitialize.
- Edit the file `/sbin/init.d/vxvm-startup` to change the line `vxconfigd -k -m enable` to `vxconfigd -k -m enable -x exclude_enable`. 
MC/ServiceGuard

PowerPath is required for all VNX series or CLARiiON HP-UX MC/Service Guard configurations.

The minimum requirements for MC/ServiceGuard configurations with VNX series or CLARiiON are:

- **CX400 base software:**
  - If no Access Logix — 02.04.0.40.5.002
  - If Access Logix — 02.04.1.40.5.002

- **CX600 base software:**
  - If no Access Logix — 02.04.0.60.5.002
  - If Access Logix — 02.04.1.60.5.002

- **HP/UX 11i Dec 2002 release**
- **MC/ServiceGuard A11.14**

The following patches are required for MC/ServiceGuard 11.16 configurations (refer to Dell EMC Knowledgebase solution emc94930 for additional details):

- **HP-UX 11i v1.0 PHSS_31075**
  Prior to installation of this patch you also need to install the following prerequisite patches
  - PHNE_28810, PHSS_31071, and PHSS_31073

- **HP-UX 11i v2.0 PHSS_31076**
  Prior to installation of this patch you also need to install the following prerequisite patches
  - PHSS_31074, and PHSS_31072

CX-series storage systems have been qualified to operate as a lock device in a two-node MC/ServiceGuard cluster.

- Create a highly available RAID group (RAID 1, RAID 1/0, RAID 5).
- Create a small LUN (approximately 4 MB).
- If you are using an array with Access Logix LIC, create a shared storage group, and attach both hosts to the storage group.
- On a system with PowerPath 3.0.2 b41 or later (with VNX series and CLARiiON license keys installed), identify the devices to the host system (ioscan and insf).
- After device is recognized, issue the command `powermt config`, followed by `powermt display`, to verify that the new device was added to your PowerPath configuration. Then issue the command `powermt save` to save the current configuration.
- Create a single volume group to use as a lock device.
- In MC/ServiceGuard, configure the LUN as your primary lock device.
CHAPTER 7

Virtual Provisioning on VNX Series and CLARiiON Systems

This chapter provides information about Dell EMC Virtual Provisioning and HP-UX on VNX series and CLARiiON systems.

Note: For further information regarding the correct implementation of Virtual Provisioning, refer to the Symmetrix Virtual Provisioning Implementation and Best Practices Technical Note, available at Dell EMC Online Support.

- Virtual Provisioning on VNX series and CLARiiON systems 152
- Thin pools 155
- Thin pool capacity 157
- Thin LUNs 159
- Architecture and features 161
- Using thin LUNs with applications 162
- HP-UX Virtual Provisioning support 163

Note: For information on Virtual Provisioning on a Symmetrix system, refer to Chapter 2, "Virtual Provisioning on VMAX and Symmetrix Systems.”
Virtual Provisioning on VNX series and CLARiiON systems

Virtual Provisioning enables organizations to reduce storage costs by increasing capacity utilization, simplifying storage management, and reducing application downtime. Virtual Provisioning also helps companies to reduce power and cooling requirements and delay capital expenditures.

The VNX and the CLARiiON CX4 series use thin LUN technology that builds on CLARiiON's virtual LUN capabilities and seamlessly integrates with existing CLARiiON management and replication software. With Virtual Provisioning, you can choose between traditional LUNs, metaLUNs, and thin LUNs. VNX series and CLARiiON's thin LUN technology also supports features such as hot sparing, proactive sparing, and the ability to migrate data between thin LUNs, traditional LUNs, and metaLUNs without incurring application downtime. The ability to nondisruptively migrate data to different LUN and disk types provides the best solution for meeting your changing application and business requirements without incurring downtime. This flexibility separates Virtual Provisioning on VNX series and CLARiiON from typical thin provisioning implementations.

One of the biggest challenges facing storage administrators is balancing how much storage space will be required by the various applications in their data centers. Administrators are typically forced to allocate space based on anticipated storage growth. They do this to reduce the management expense and application downtime required to add storage later on. This generally results in the over-provisioning of storage capacity, which then leads to higher costs; increased power, cooling, and floor space requirements; and lower capacity utilization rates. Even with careful planning, it may be necessary to provision additional storage in the future. This may require application downtime depending on the operating systems involved.

To address these concerns, the VNX series introduced thin LUN technology with VNX OE for Block Version 31. The CLARiiON CX4 series introduced thin LUN technology with FLARE release 28.5. This technology works with VNX series and CLARiiON's metaLUNs and traditional LUNs to provide powerful, cost-effective, flexible solutions. CLARiiON thin LUNs can present more storage to an application than is physically available. Storage managers are freed from the time-consuming administrative work of deciding how to allocate drive capacity. Instead, an array-based mapping service builds and maintains all of the storage structures based on a few high-level user inputs. Disk drives are grouped into storage pools that form the basis for provisioning actions. Physical storage is automatically allocated only when new data blocks are written.

Thin provisioning improves storage capacity utilization and simplifies storage management by presenting an application with sufficient capacity for an extended period of time. When additional physical storage space is required, disk drives can be nondisruptively added to the central storage pool. This reduces the time and effort required to provision additional storage, and avoids provisioning storage that may not be needed.

Virtual Provisioning for VNX series and CLARiiON is a licensed feature that requires a software enabler. It is available for VNX systems running VNX OE for Block Version 31. This is also available for CLARiiON CX4 storage systems running FLARE release 28.5 and later. You can manage thin LUNs using the same Unisphere/Navisphere Manager GUI and Secure CLI commands that you use to manage traditional LUNs and metaLUNs. VNX series and CLARiiON replication products, Unisphere/Navisphere Analyzer, and Unisphere/Navisphere Quality of Service Manager work seamlessly across thin LUNs, traditional LUNs, and metaLUNs. Dell EMC RecoverPoint also supports the replication of VNX series and CLARiiON thin LUNs.
Terminology

This section provides common terminology and definitions for this chapter.

% Full
The percentage of physical user capacity that is currently consumed. It is calculated using this formula:

\[ \% \text{ Full} = \frac{\text{Consumed capacity}}{\text{user capacity}} \]

% full threshold
A parameter that is set by the user. The system generates an alert when this threshold is exceeded.

Allocated capacity
For a thin pool this is the space currently used by all thin LUNs in the pool. For a thin LUN, this is the physical space used by the LUN. See “Consumed capacity.”

Available capacity
The amount of actual physical thin pool space that is currently not allocated for thin LUNs.

Consumed capacity
For a thin pool this is the space currently used by all thin LUNs in the pool. For a thin LUN, this is the physical space used by the LUN. See “Allocated capacity.”

LUN migration
A CLARiiON feature that dynamically migrates data to another LUN, thin LUN, or metaLUN without disrupting running applications. LUN migration has many uses, for example:

- To change the type of disk drive (for example, from economical SATA to faster FC, or vice versa)
- To select a RAID type that better matches the current performance or availability requirements
- To re-create a LUN with more disk space

After migration is complete, the destination LUN assumes the identity (World Wide Name and other IDs) of the source LUN, and the source LUN is destroyed. LUN migration can be tuned by setting it to one of four speed settings: Low, Medium, High, or ASAP.

MetaLUN
A collection of traditional LUNs that are striped and/or concatenated together and presented to a host as a single LUN. A single metaLUN can be striped across any number of disk spindles, providing a much wider range of performance and configuration options. Additional LUNs can be added dynamically, allowing metaLUNs to be expanded on the fly.

Oversubscribed capacity
The amount of user capacity configured for thin LUNs that exceeds the physical capacity in a thin pool.

RAID group
A type of storage pool that contains a set of disks on which traditional LUNs and metaLUNs can be created.

Storage pool
A general term used to describe RAID groups and thin pools. In the Navisphere Manager GUI, the storage pool node contains RAID groups and thin pool nodes.

Subscribed capacity
The total amount of capacity configured for thin LUNs in the pool. This number can be greater than the available user capacity. The user capacity can be expanded by adding drives to the pool.
| **Thin friendly** | This term is frequently used for file systems and applications that do not preallocate all of the storage space during initialization. This term is also used for file systems that reuse deleted space before consuming additional storage. Both features, reuse of deleted space and not preallocating, improve capacity utilization in thin provisioning. |
| **Thin LUN** | A logical unit of storage where physical space allocated on the storage system may be less than the user capacity seen by the host server. |
| **Thin pool** | A group of disk drives used specifically by thin LUNs. There may be zero or more thin pools on a system. Disks may be a member of no more than one thin pool. Disks that are in a thin pool cannot also be in a regular RAID group. |
| **Threshold alert** | An alert issued when the % Full Threshold has been exceeded. |
| **Traditional LUN** | A logical unit of storage that can span a number of disks on a storage system but looks like a single disk or partition to the server. The amount of physical space allocated is the same as the user capacity seen by the host server. |
| **User capacity** | The total amount of physical storage capacity in the thin pool that is available for thin LUNs. This is also referred to as "usable capacity." It is measured as raw disk capacity minus overhead (RAID overhead and mapping overhead). For a thin LUN, this is the size of the thin LUN as it appears to the host. (This term also applies to traditional LUNs, where user capacity equals consumed capacity.) For thin LUNs, this is sometimes called host visible capacity. |
Thin pools

A thin pool is a collection of disks that are dedicated for use by thin LUNs. A thin pool is somewhat analogous to a CLARiiON RAID group. Thin pools can contain a few disks or hundreds of disks, whereas RAID groups are limited to 16 disks. Thin pools are simple to create because they require only three user inputs, as shown in Figure 29:

1. Pool Name: For example, "Application Pool 2"
2. Resources: Number of disks
3. Protection level: RAID 5 or 6

Thin pools are flexible. They can consist of any supported Fibre Channel, SATA, SAS, or Enterprise Flash Drives (EFD) disk drives. Refer to the product specifications sheet for your specific storage system to determine what drive types are supported. The VNX series or CLARiiON CX4 can contain one or many thin pools. RAID 5 is the default selection for thin pools and is recommended for most situations.

Thin pools are easy to expand by adding drives to the pool. Dell EMC recommends adding disks in multiples of five drives for expanding RAID 5 thin pools and multiples of eight drives for expanding RAID 6 thin pools.

With EFDs in thin pools, you can maximize the capacity utilization for your high-performance drives. It combines the ease-of-use features of Virtual Provisioning with the high performance of EFDs, which can be attractive for certain types of applications. However, if you are looking for the highest available performance from your EFDs, then Dell EMC recommends deploying traditional LUNs with EFDs.

There are a few restrictions on what type of disks can be used in a thin pool:

1. Vault drives (the first five drives in a storage system) cannot be part of a thin pool.

Unisphere/Navisphere dialog boxes and wizards do not allow you to select these drives.
Fibre Channel and SATA drives cannot be mixed with EFDs in a thin pool. Unisphere/Navisphere dialog boxes and wizards do not allow you to mix these drives.

Although it is not a restriction, it is a best practice to deploy Fibre Channel and SATA drives in separate pools. Drives within a thin pool should be rated at the same rpm. These recommendations are similar to recommendations for traditional RAID groups.

Disks in a thin pool should be the same size to maximize space utilization. When using different capacity drives to create a thin pool, it is best to do this in stages. For example, if you have ten 450 GB drives and five 300 GB drives, first create the pool selecting only the ten 450 GB drives, and then expand the pool by adding the other five 300 GB drives.
Thin pool capacity

As illustrated in Figure 30:

- User capacity is the total physical capacity available to all thin LUNs in the pool.
- Consumed capacity is the total physical capacity currently assigned to all thin LUNs.
- Subscribed capacity is the total host reported capacity supported by the pool.

![Image of pool capacity](image)

**Figure 30** Pool % Full threshold

Thin pools are monitored using the % Full Threshold Alert setting and storage capacity reports. You can specify the value for % Full Threshold (Consumed capacity/User capacity) when a thin pool is created. It can be changed at any time. It ranges from 1% to 84%.

When % Full Threshold is exceeded, an alert is triggered at the warning severity level. When the % Full value reaches 85%, the pool issues a built-in alert at the critical severity level. Beyond 85%, the built-in alert mechanism continues to track the actual % Full value as the pool continues to fill.

Alerts can be monitored via the Alerts tab in Unisphere/Navisphere. In Unisphere/Navisphere's Event Monitor wizard, you can also select the option of receiving alerts via e-mail, a paging service, or an SNMP trap.

**Table 20** lists the thresholds for different types of alerts.

<table>
<thead>
<tr>
<th>Threshold type</th>
<th>Threshold range</th>
<th>Threshold default</th>
<th>Alert severity</th>
<th>Side-effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>User settable</td>
<td>1%-84%</td>
<td>70%</td>
<td>Warning</td>
<td>None</td>
</tr>
<tr>
<td>Built in</td>
<td>n/a</td>
<td>85%</td>
<td>Critical</td>
<td>Clears user settable alert</td>
</tr>
</tbody>
</table>

Allowing consumed capacity to exceed 90% of user capacity puts you at the risk of running out of space and impacting all applications using LUNs in the thin pool.
The **Thin Pool Properties** dialog box, shown in Figure 31, shows parameters such as subscribed capacity, over-subscribed capacity, and percent subscribed.

Oversubscribing capacity is the key to reducing disk storage costs. There is no hard and fast rule for how much or how little one should oversubscribe. Oversubscribed thin pools should be monitored closely, and pool user capacity adjusted as necessary. Adding drives to the pool nondisruptively increases thin pool user capacity for all thin LUNs in that pool. Consumed (allocated) capacity is reclaimed by the pool when thin LUNs are deleted.
Thin LUNs

A VNX series and CLARiiON thin LUN is similar to a traditional LUN in many ways. Many of the same Unisphere/Navisphere Manager GUI operations and Secure CLI commands can be used on thin LUNs and traditional LUNs. Most user-oriented functions work the same way, including underlying data integrity features, hot sparing, LUN migration, local and remote replication, and LUN properties information.

Thin LUNs are available as choices in Unisphere/Navisphere Taskbar wizards, Unisphere/Navisphere Analyzer, and Unisphere/Navisphere Quality of Service Manager. Features such as hot sparing and proactive sparing also work with thin LUNs. It is also possible to migrate a traditional LUN (or metaLUN) to a thin LUN and vice versa. This flexibility separates VNX series and CLARiiON thin provisioning from typical thin provisioning implementations.
Attributes

The primary difference between traditional and thin LUNs is that thin LUNs can consume less physical space on the storage system. Thin LUNs are simple to create, with three inputs in the Create LUN dialog box, as shown in Figure 32 on page 160:

- Thin pool name
- Host to provision
- Amount of host visible user capacity

![Figure 32 Create LUN dialog box](image)

Thin LUNs are easy to use because the system automatically manages the drives within the pool according to VNX series and CLARiiON best practices. The Mapping Service distributes data evenly throughout the pool. Thin LUNs are easy to manage because Unisphere/Navisphere Manager and Navisphere CLI commands work the same for thin LUNs as they do for traditional LUNs. New property screens and reports are available to obtain information about thin LUNs. The maximum size for a thin LUN is 14 TB.

Dell EMC recommends that you do not change the default owner of the thin LUN once it is provisioned. This can impact performance because the underlying private structures, which provide storage for the thin LUN, would still be controlled by the original SP. It is a best practice to balance the thin LUNs on both SPs when you create the thin LUNs.

It is best to only provision thin LUNs to applications that can tolerate some variation in performance. Although thin LUNs are internally striped, performance may vary. Applications whose LUNs occupy the same spindles within a thin pool will impact one another. Use traditional LUNs for applications with stringent performance requirements. Use metaLUNs for high-throughput applications that can benefit from spreading I/O over a large number of disk drives striped over multiple RAID groups.

There are only a few restrictions with thin LUNs and these are enforced through Unisphere/Navisphere:

- A thin LUN cannot be used in the reserved LUN pool (which reserves space for snapshots).
- A thin LUN cannot be used for a clone private LUN (which contains maps for clones).
- A thin LUN cannot be used for a write intent log for MirrorView operations.
- A thin LUN cannot be used as a component of a metaLUN.
Architecture and features

Specialized software known as the Mapping Service manages the placement and use of the physical storage used by thin LUNs. Data is written to 8K chunks (extents) and is optimally placed. This makes configuring thin LUNs easy, because the underlying software makes all the decisions about how to lay out actual storage blocks across the disks in a thin pool. Less experienced storage administrators will benefit from not having to be directly involved in the details of configuring storage. The Mapping Service performs these functions adhering to performance best practices.

When creating a thin LUN, the initial consumed space from the thin pool will be shown as 2 GB. Slightly more than 1 GB is used for metadata associated with the thin LUN, and the remaining space is available for incoming writes. As new writes come in, more physical space is allocated in 1 GB stripes. This storage-on-demand algorithm ensures that at least 1 GB slice is available at all times. The mapping service creates embedded metadata within these additional 1 GB slices.

It is important to consider the metadata overhead before provisioning thin LUNs for your applications. For a thin LUN, you can estimate the overhead using the following simple formula. Note that this is an approximation; the actual overhead depends on the write pattern of your application.

Metadata overhead (in GB) = LUN size (in GB units) * .02 + 3 GB.

For example, if you have a 200 GB thin LUN that gets fully allocated over a period of time, based on this formula, it will utilize approximately 207 GB from the thin pool. In this equation, the 3 GB includes 2 GB that is allocated for metadata when a thin LUN is created and 1 GB that is preallocated to ensure that storage is always available for incoming writes. (Although the 1 GB does not really contain metadata information, it is still an overhead that must be included in this calculation.) The 0.02 factor approximates the metadata for keeping track of the 1 GB slices.
Using thin LUNs with applications

Thin LUN provisioning is most appropriate for applications that have the following characteristics:

- Thin provisioning "friendly" environments
  To improve capacity utilization with file systems, use thin provisioning only when files are not frequently deleted. Many file systems do not efficiently reuse the space associated with deleted files, which reduces the capacity utilization benefits of thin provisioning.

  You should carefully consider the space consumption characteristics of databases before using thin provisioning. Some databases preallocate space and write zeros to it. This preallocated (but unused) space cannot be shared in a thin pool, thus reducing or eliminating the capacity utilization benefits.

- General purpose performance requirements
  Thin provisioning is appropriate for applications in which some performance variability can be tolerated. Some workloads will see performance improvements from wide striping with thin provisioning. However, when multiple thin devices contend for shared spindle resources in a given pool, and when utilization reaches higher levels, the performance for a given application can become more variable. Unisphere/Navisphere Quality of Service Manager can be used to manage resource contention within the pool as well as between LUNs in different thin pools and RAID groups.

- Environments that need flexible provisioning (for example, test and development)
  Thin provisioning can be an effective way to improve ease of use and capacity utilization for lower storage tiers such as test and development.

- Document repositories
  Document repositories with rapidly rising capacity requirements can benefit greatly from the improved capacity utilization offered by thin provisioning, provided their environments meet the previously outlined criteria.

- Software development/source code
  Many organizations will see an opportunity to lower TCO by improving ease of use and capacity utilization for storage associated with software development, because these development activities can usually tolerate some level of performance variability.
HP-UX Virtual Provisioning support

Virtual Provisioning is supported with all current versions of HP-UX as listed in the Dell EMC Simple Support Matrices. This section lists precaution considerations.

Precaution considerations

Virtual Provisioning and the industry’s thin provisioning are new technologies. Relevant industry specifications have not yet been drafted. Virtual Provisioning, like thin provisioning, has the potential to introduce events into the environment which would not otherwise occur. The unavailability of relevant industry standards results in deviations with the host-based handling of these events and the possibility of undesirable implications when these events occur. However, with the proper precautions these exposures can be minimized or eliminated.

Thin pool out-of-space event

Insufficient monitoring of the thin pool can result in all of the thin pool enabled capacity to be allocated to thin devices bound to the pool. If over-subscription is implemented, the thin pool out-of-space event can result in a non-recoverable error being returned to a write request when it is sent to a thin device area that does not have capacity allocated from the thin pool. Simple precautions can avoid this from occurring, including the following.

- Monitoring of the consumption of the thin pool enabled capacity using Solutions Enabler (SE) or Symmetrix Management (SMC) console will keep the user informed when additional data devices should be added to the thin pool to avoid the thin pool out-of-space event. Threshold-based alerts can also be configured to automatically notify of the event or to add to capacity to the thin pool.
- Thin device allocation limits can be set to limit the amount of capacity a thin device can withdraw from the thin pool.
- Predictable growth of capacity utilization results in avoiding unexpected capacity demands. Implementing Virtual Provisioning with applications which have predictable growth of capacity utilization will avoid unexpected thin pool enabled capacity depletion.
- Avoid unnecessary block-for-block copy of a device to a thin device. Block-for-block copy of a device to a thin device results in the entire capacity of the source volume to be written to the thin device, regardless of how much user data the source volume contains. This can result in unnecessary allocation of space to the thin device.
- Plan for thin pool enabled capacity utilization not to exceed 60% – 80%
- Avoid implementing Virtual Provisioning in Virtual Provisioning hostile environments.
Possible implications of the thin pool out-of-space event

When the thin pool is out of space, attempts to write to a device will fail with a file write error. The device will continue to be available and existing files can be accessed, but further attempts to write to the device will fail. If the failing device was the target of a "backup/image" operation, the device may be unusable and will have to be unbound from the thin pool and then rebound to the thin pool, to make it usable.

Host boot/root/swap/dump devices positioned on Virtual Provisioned devices

A boot /root /swap /dump device positioned on Symmetrix Virtual Provisioning (thin) device(s) is supported. However, some specific processes involving boot /root/swap/dump devices positioned on thin devices should not have exposure to encountering the out-of-space condition.

Host-based processes such as kernel rebuilds, swap, dump, save crash, and Volume Manager configuration operations can all be affected by the thin provisioning out-of-space condition. This exposure is not specific to Dell EMC's implementation of Thin Provisioning. Dell EMC strongly recommends that the customer avoid encountering the out-of-space condition involving boot / root /swap/dump devices positioned on Symmetrix VP (thin) devices using the following recommendations:

• It is strongly recommended that Virtual Provisioning devices utilized for boot /root/dump/swap volumes must be fully allocated or the VP devices must not be oversubscribed.
  Should the customer use an over-subscribed thin pool, they should understand that they need to take the necessary precautions to ensure that they do not encounter the out-of-space condition.
CHAPTER 8

HP-UX Hosts and Unity Series

This chapter provides information specific to HP Servers running HP-UX and connecting to Unity systems.

**Note:** Refer to Dell EMC E-Lab Navigator or contact your Dell EMC representative for the latest information on qualified hosts.

- HP-UX in a Unity environment 168
- Unity series configuration for HP-UX hosts 170
- Configuration requirements for Unity series support 172
- Configuring an external boot of HP-UX hosts 173
HP-UX in a Unity environment

This section lists Unity series support information for the HP-UX environment.

Host connectivity

Refer to Dell EMC E-Lab Navigator and the Dell EMC Simple Support Matrices, or contact your Dell EMC representative for the latest information on qualified HP-UX host servers, operating system versions, switches, and host bus adapters.

Boot support

HP 9000 and Integrity Itanium servers running HP-UX 11iv3 are qualified for booting from Unity series systems. Refer to Dell EMC E-Lab Navigator and the Dell EMC Simple Support Matrices, or contact your Dell EMC representative for information on supported Unity series boot configurations.

Storage management overview

Unisphere provides a great user experience for Unity management IP by using a web-application interface that uses HTML 5. In the initiative definition we specify that it will work for any browser that supports the HTML5 standards. For more information, refer to Unity White papers on Dell EMC Online Support.

Unisphere and the Microsoft Management Console (MMC) plug-in supports the following Microsoft Windows operating systems:

- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2003 R2 (32-bit & 64-bit)
- Windows Server 2008 R2 Core Server
- Windows 7
- Windows 8
- Vista

Table 21 lists the available view blocks for Unisphere dashboards.

Table 21  Available view blocks for Unisphere dashboards

<table>
<thead>
<tr>
<th>View blocks</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Health</td>
<td>View health status for system objects (replication sessions and hosts).</td>
</tr>
<tr>
<td>Storage Health</td>
<td>View health status for storage objects (LUNs, file systems, and datastores).</td>
</tr>
<tr>
<td>System Capacity</td>
<td>View total capacity, free, and unconfigured disk space.</td>
</tr>
<tr>
<td>Tier Capacity</td>
<td>View information about the used and free space for each storage tier.</td>
</tr>
<tr>
<td>Pools</td>
<td>View a summary of free and used pool capacity in each pool.</td>
</tr>
<tr>
<td>System Alerts</td>
<td>View all alerts for the system, categorized by severity.</td>
</tr>
<tr>
<td>System Performance</td>
<td>View a summary of system performance.</td>
</tr>
</tbody>
</table>
Use the Unisphere CLI for the same tasks that can be done in Unisphere, such as configuring and managing storage resources, protecting data, managing users, viewing performance metrics, and so on.

To use the Unisphere CLI, install the Unisphere CLI on the host and run CLI commands to the Unity system from the native command prompt.

For more information about using the Unisphere CLI, refer to the *EMC Unity Family Unisphere Command Line Interface User Guide* on Dell EMC Online Support.

**Required storage system setup**

Unity series system configuration is performed by an Dell EMC Customer Engineer (CE) through Unisphere. The CE configures the initial storage system settings for each storage processor (SP). The procedures described in this chapter assume that all hardware equipment (such as switches and storage systems) used in the configurations have been properly installed and connected.
Unity series configuration for HP-UX hosts

Unity series must be properly configured for HP-UX hosts. This section provides guidelines and general procedures to set up a Unity series system for HP-UX.

Unity series storage processors and LUNs

Unity leverages Asymmetric Logic Unit Access (ALUA) for host access. This enables multiple paths to be active for I/O, but some paths are optimized while others are non-optimized. The paths for a device that are designated as optimized are the ones connected to the storage processor that owns that particular device. If I/O is sent down the non-optimized path, the peer storage processor leverages the internal CMI (Common Messaging Interface) bus to redirect the I/O to the storage processor that owns the device. This operation is completely transparent to the host and removes the need to trespass the resource to complete the I/O. However, if a large number of I/Os is received down the non-optimized path, the Unity system trespasses the LUN to the peer storage processor to optimize the data path.

IMPORTANT

A minimum of one device path to each of the two SPs is highly recommended for redundancy reasons to avoid disruptions during some online operations, such as a non-disruptive upgrade (NDU) and to prevent the SP from being a single point of failure.

• **Multipathing**—HP-UX 11iv3 has native ALUA support. Other multi-pathing products such as PowerPath (PP) or Dynamic Multipathing (DMP) only have to be installed and configured if you use one of them instead of native ALUA. Configure multipathing software to use the optimized paths first and only use the non-optimized paths if there are no optimized paths available. If possible, use two separate Network Interface Cards (NICs) or Fibre Channel Host Bus Adapters (HBAs) on the host. This avoids a single point of failure on the card and also the slot on the server.

• **Trespass**—A LUN trespass is the movement of a LUN or transfer of ownership from one SP to the other SP. When a LUN is trespassed, the previously active paths become passive paths, and vice versa, the previously passive paths become active paths.

• **Default storage processor / default path**—Each Unity series LUN has a default owner, either SPA or SP B. A default path is a device path to the default storage processor of the LUN.

Enable Unity series write cache

Unity series LUNs that are assigned to HP-UX hosts must have write cache enabled. You can enable the write cache by using the Storage Systems Properties window in Unisphere.
Making LUNs available to HP-UX

Use the following procedure to create and make LUNs available to an HP-UX host.

1. Create pools of the desired RAID type on the Unity array for use by the HP-UX hosts.

2. Create hosts by the available initiators on the array and select the newly bound or existing LUNs to be assigned to the HP-UX hosts.

3. On the HP-UX host, run the `ioscan -fn` and `insf -e` commands to scan new devices and create new device special files.

4. Run `ioscan -m lun disk > scan.out` to save `ioscan` output to a file for review, and then verify that all expected Unity LUNs and paths are discovered by the HP-UX host.

5. Create volume groups and/or disk groups, logical volumes, and/or filesystems on the HP-UX hosts as desired.
Configuration requirements for Unity series support

This section provides the requirements for support of Unity series with HP-UX 11i v3 (HP-UX 11.31).

**IMPORTANT**

HP-UX 11iv3 is the only supported HP-UX version with Unity because ALUA cannot be supported with HP-UX 11iv2 and 11iv1. HP-UX 11iv2 and 11iv1 are also only supported with the volume set addressing method, which is currently unavailable with Unity arrays.

Prerequisites and restrictions

Unity series arrays require operating systems with ALUA support.

To temporarily remove all legacy I/O nodes and their device special files, type the `rmsf -L` command.

Only HP-UX 11iv3 persistent (agile) DSFs are supported with Unity series arrays. Legacy DSFs are not supported.
Configuring an external boot of HP-UX hosts

This section provides guidelines and procedures for configuring an external boot of HP-UX hosts from Unity series in Fibre Channel switch SAN environments. Refer to the Dell EMC E-Lab Navigator and the Dell EMC Simple Support Matrices for the specific Unity series models, HP servers, and HBAs supported with an external boot.

General guidelines

Because many variables determine the topology of a SAN and each customer may have different requirements, some general guidelines have been defined for supported configurations:

- If possible, configure high availability with multiple hardware paths to boot devices.
- Both data devices and boot devices can share the same HBA or Unity Storage Processor (SP) port. However, system performance and boot times may be affected depending on the utilization and I/O load on the shared HBA or SP port.
- Although the LUNs from Unity pools with any RAID type can be used as operating system boot devices, a high performance or redundancy RAID type such as RAID1 or RAID10 is recommended for pools that provide the boot LUN.

Configuring Unity series for new HP-UX installation and boot

Use the following procedure for a new installation of the HP-UX operating system and boot devices on a Unity system:

1. Create storage pools and LUNs for use in the HP-UX boot device configuration. New pools and LUNs are not necessary if there are existing unallocated LUNs available on the Unity system.

2. Verify that the intended boot LUNs are large enough in size to be used as HP-UX operating system disks. Use minimum operating system disk sizes for boot, dump, swap, and so on.

3. Check the default SP of the intended boot LUNs. (The Default Owner SP A or SP B is displayed in LUN Properties). It is important for the boot LUNs to be owned by the default SP during the installation process. Otherwise, there can be potential trespass issues resulting in boot failures. If more than one device is selected for a boot volume group, ensure that all LUN devices are owned by the same default SP.

4. Select the LUNs that you intend to use as operating system disks and map them to the host which will install the OS on the Unity LUN.

5. Insert the HP-UX OS installation media CD/DVD or launch a remote Ignite-UX session to begin installation of the OS on the Unity series system. Refer to HP-UX installation documentation for details on the actual operating system installation process.

6. The HP-UX installation program will enable you to choose which disk devices to use for installation of the operating system. Select the desired Unity series disk devices from the list of available disks that is displayed by the installation program.

7. After the HP-UX installation is completed, configure your remaining planned HP-UX HBA path connections and your desired multipath or failover software and volume manager groups.
Part 3 includes:

- Chapter 9, "Using Dell EMC TimeFinder in an HP-UX Environment"
- Chapter 10, "SRDF and MirrorView Remote Boot"
- Chapter 11, "OS Upgrade from HP-UX 11.23 to HP-UX 11.31"
This chapter provides guidelines for using Dell EMC TimeFinder in an HP-UX environment including MC/ServiceGuard clusters.

- TimeFinder in HP-UX environments 178
TimeFinder in HP-UX environments

Dell EMC TimeFinder™ business continuance volumes (BCVs) are specifically configured VMAX/Symmetrix devices that can function either as additional mirrors to a standard device or as independent, host-addressable devices. BCV devices are point-in-time mirror copies of data on a standard device; when split from the original, they become available for backups, application testing, and so on.

Some of the attributes and benefits of BCVs are:

- VMAX/Symmetrix volumes with special attributes
- Host-addressable independent devices
- Use as additional mirrors
- Used for backups/restores, SQL queries, or additional testing
- System resources not stressed during backup, queries, etc.
- System does not need to be taken offline for backups

This section describes how BCV devices may be imported on clustered and nonclustered hosts.

This chapter discusses HP-UX 11i 1.0, HP LVM volume groups, and HP MC/ServiceGuard clusters.

BCV operations

The following steps provide a basic outline of BCV operations:

1. Create a group.
2. Add standard devices to the group.
3. Associate BCV devices to the standard devices1.
4. Synchronize/restore data from/to the standard and from/to the BCVs.
5. Split the BCV devices from the standard devices.
6. Import the BCV volume group.
7. *fsck* and mount the BCV file systems.

During the synchronization process, the BCV device in effect becomes a third mirror, and is thereby unavailable to the host for I/O. The standard device will remain online during this process. Both the standard and BCV devices will show up as CLAIMED in the *ioscan* output and *powermt* display, but any I/O to the BCV devices will fail.

A BCV device may be reattached for resynchronization or restore to a previously paired device or to a different standard device. Synchronization may be either full or incremental. Full synchronization copies all the data over to the BCV devices, whereas incremental only copies the changed tracks from the standard to the BCV. Any modification to the BCV device data after the split is overwritten during the subsequent resynchronization.

A restore operation copies data tracks from the BCV to the standard device. The restore function offers both a full and incremental option. During the restore operation, both the standard device volume groups and the BCV volume groups should be deactivated and exported.

1. The BCV and standard device to which it is attached must be of the same size.
The split operation can only be performed after an establish or restore of the data from/to the standard from/to the BCV device has completed successfully.

Multiple BCV refers to different point-in-time copies of the standard data. This is achieved by associating a single standard with multiple BCV devices. An initial full establish is performed to each of the BCV devices associated with the standard device. Thereafter, the standard is synchronized at different times with each of the associated BCV devices. This provides the user with various point-in-time copies of the data. This relationship is maintained as long as the BCV devices are not paired with another standard device.

The concurrent BCV feature allows the user to simultaneously generate two exact copies of the data on the standard device.

**Basic procedures for HP-UX**

The following example illustrates basic BCV operations where the standard and BCV volume groups are assigned to the same nonclustered system, Host A. Volume-group-related functions are performed on Host A, and SYMCLI commands are executed from a SYMCLI management system, Host S.

Refer to the relevant documents for detailed explanations and usage of the various TimeFinder features, functions, and options.

**Example**

Host A:

Standard volume group vg01:

```
c0t1d0  c0t1d1  c0t1d2  c0t1d3 (primary path)  
c8t1d0  c8t1d1  c8t1d2  c8t1d3 (alternate path)
```

Host A:

BCV volume group bcv01:

```
c5t1d0  c5t1d1  c5t1d2  c5t1d3
```

It might be useful to create a document listing the relationship of the BCV devices to the standard devices on each host as shown in Table 22.

**Table 22 Relationship between BCVs and standard devices**

<table>
<thead>
<tr>
<th>Std Vol</th>
<th>HP Host</th>
<th>Prim Link Devs</th>
<th>Alt Link Devs</th>
<th>LVM Vol Grp</th>
<th>BCV Vol</th>
<th>HP Host</th>
<th>BCV Devs</th>
<th>LVM Vol Grp</th>
</tr>
</thead>
<tbody>
<tr>
<td>000</td>
<td>Host A</td>
<td>c0t1d0</td>
<td>c8t1d0</td>
<td>vg01</td>
<td>100</td>
<td>Host A</td>
<td>c5t1d0</td>
<td>bcv01</td>
</tr>
<tr>
<td>001</td>
<td>Host A</td>
<td>c0t1d1</td>
<td>c8t1d1</td>
<td>vg01</td>
<td>101</td>
<td>Host A</td>
<td>c5t1d1</td>
<td>bcv01</td>
</tr>
<tr>
<td>002</td>
<td>Host A</td>
<td>c0t1d2</td>
<td>c8t1d2</td>
<td>vg01</td>
<td>102</td>
<td>Host A</td>
<td>c5t1d2</td>
<td>bcv01</td>
</tr>
<tr>
<td>003</td>
<td>Host A</td>
<td>c0t1d3</td>
<td>c8t1d3</td>
<td>vg01</td>
<td>103</td>
<td>Host A</td>
<td>c5t1d3</td>
<td>bcv01</td>
</tr>
</tbody>
</table>
**Initial setup and synchronization**

1. Assign the BCV devices to Host A.

2. On Host A, execute the following commands:
   a. Run `ioscan` to discover the devices:
      ```
      ioscanned fnC disk
      ```
   b. Run `insf` to create special devices files:
      ```
      insf -C disk
      ```
   c. Configure the devices into PowerPath (if installed):
      ```
      powermt config dev=all
      ```

3. On Host S, execute the following:
   a. Create a BCV group:
      ```
      symdg create testgrp
      ```
   b. Assign standard devices to the group:
      ```
      symld -g testgrp -sid 1234 -RANGE 000:003 addall pd
      ```
   c. Pair the BCV device with the standard:
      ```
      symbcv -g testgrp -sid 1234 -RANGE 100:103 associateall dev
      ```
      The BCV and standard device to which it is attached must be of the same size.
   d. Synchronize the BCV device with the standard:
      ```
      symmir -g testgrp -full establish -noprompt
      ```
   e. Ensure the synchronization is complete:
      ```
      symmir -g testgrp -i 30 verify
      symmir -g testgrp query
      ```
   f. Split the BCV device from the standard:
      ```
      symmir -g testgrp split -noprompt
      ```
   g. Ensure the split is complete:
      ```
      symmir -g testgrp verify -split
      ```

4. On Host A, run the following:
   a. Run `vgchgid` against all BCV devices with a single command:
      ```
      vgchgid /dev/rdsk/c5t1d0 /dev/rdsk/c5t1d1 /dev/rdsk/c5t1d2 /dev/rdsk/c5t1d3
      ```
      All devices must be included in the command line; devices cannot be split up.
   b. Create a new volume group for the BCV devices:
      ```
      mkdir /dev/bcv01
      mknod /dev/bcv01/group c 64 0x020000
      ```
   c. Import the BCV devices into the new volume group:
      ```
      vgimport /dev/bcv01 /dev/dsk/c5t1d0 /dev/dsk/c5t1d1 /dev/dsk/c5t1d2 /dev/dsk/c5t1d3
      ```
Using Dell EMC TimeFinder in an HP-UX Environment

Using Dell EMC TimeFinder in an HP-UX Environment

**Resynchronization**

1. On Host A, perform the following:
   a. Stop all I/O to the BCV file systems/raw volumes.
   b. Unmount BCV file systems:
      ```shell
to /bcv01_fs1
      ```
   c. Deactivate the BCV volume group:
      ```shell
vgchange -a n /dev/bcv01
      ```
   d. Export the BCV file systems:
      ```shell
vgexport -v -f /tmp/bcv01.list /dev/bcv01
      ```

2. On Host S, run the following:
   a. Synchronize the BCV device with the standard:
      ```shell
symmir -g testgrp establish -noprompt
      ```
   b. Ensure the synchronization is complete:
      ```shell
symmir -g testgrp -i 30 verify
symmir -g testgrp query
      ```
   c. Split the BCV device from the standard:
      ```shell
symmir -g testgrp split -noprompt
      ```
   d. Ensure the split is complete:
      ```shell
symmir -g testgrp verify -split
      ```

3. On Host A, execute the following:
   a. Run `vgchgid` against all BCV devices with a single command:
      ```shell
vgchgid /dev/rdsk/c5t1d0 /dev/rdsk/c5t1d1 /dev/rdsk/c5t1d2 /dev/rdsk/c5t1d3
      ```
      All devices must be included in the command line; devices cannot be split up.
   b. Re-create the volume group for the BCV devices:
      ```shell
mkdir /dev/bcv01
mknod /dev/bcv01/group c 64 0x020000
      ```
   c. Reimport the BCV devices volume group:
      ```shell
vgimport -v -f /tmp/bcv01.list /dev/bcv01
      ```
d. Activate the BCV volume group:
   
   \texttt{vgchange -a y /dev/bcv01} \\
   \texttt{vgcfgbackup /dev/bcv01}

e. FSCK and mount the BCV file systems:
   
   \texttt{fsck -y /dev/bcv01/rlvol1} \\
   \texttt{mount /dev/bcv01/lvol1 /bcv01_fs1}

\textbf{Restore}

1. On Host A, perform the following:
   
   a. Stop all I/O to the standard and BCVs.
   b. Unmount standard file systems:
      
      \texttt{umount /std_fs1}
   c. Deactivate the standard volume group:
      
      \texttt{vgchange -a n /dev/vg01}
   d. Export the standard volume group and create the device list outfile:
      
      \texttt{vgexport -v -f /tmp/vg01.list /dev/vg01}
   e. Unmount BCV file systems:
      
      \texttt{umount /bcv_fs1}
   f. Deactivate the BCV volume group:
      
      \texttt{vgchange -a n /dev/bcv01}
   g. Export the BCV volume group:
      
      \texttt{vgexport -v -f /tmp/bcv01.list /dev/bcv01}

2. On Host S, execute the following:
   
   a. Restore from the BCV device to the standard:
      
      \texttt{symmir –g testgrp –full restore -noprompt}
   b. Ensure the restore is complete:
      
      \texttt{symmir –g testgrp –i 30 verify} \\
      \texttt{symmir –g testgrp query}
   c. Split the BCV device from the standard:
      
      \texttt{symmir –g testgrp split -noprompt}
   d. Ensure the split is complete:
      
      \texttt{symmir –g testgrp verify –split}

3. On Host A, run the following:
   
   a. Run \texttt{vgchgid} against all BCV devices:
      
      \texttt{vgchgid /dev/rdsk/c5t1d0 /dev/rdsk/c5t1d1 /dev/rdsk/c5t1d2 /dev/rdsk/c5t1d3}

      All devices must be included in the command line; devices cannot be split up.
b. Re-create the BCV volume group:

```bash
mkdir /dev/bcv01
mknod /dev/bcv01/group c 64 0x020000
```

c. Reimport the BCV the volume group:

```bash
vgimport -v -f /tmp/bcv01.list /dev/bcv01
```

d. Activate the BCV volume group:

```bash
vgchange -a y /dev/bcv01
vgcfgbackup /dev/bcv01
```

e. fsck and mount the BCV file systems:

```bash
fsck -y /dev/bcv01/rlvol1
mount /dev/bcv01/lvol1 /bcv01_fs1
```

f. Run `vgchgid` on the standard devices:

```bash
vgchgid /dev/rdsk/c0t1d0 /dev/rdsk/c0t1d1 /dev/rdsk/c0t1d2 /dev/rdsk/c0t1d3
```

All devices must be included in the command line; devices cannot be split up. This command must be run on either the primary or alternate link devices only; but not both.

g. Re-create the standard devices volume group:

```bash
mkdir /dev/vg01
mknod /dev/vg01/group c 64 0x010000
```

h. Reimport the standard devices volume group:

```bash
vgimport -v -f /tmp/vg01.list /dev/
```

i. Reactivate the standard devices volume group:

```bash
vgchange -a y /dev/vg01
vgcfgbackup /dev/vg01
```

j. fsck and remount the standard file systems:

```bash
fsck -y /dev/vg01/rlvol1
mount /dev/vg01/lvol1 /std_fs1
```

**HP-UX clusters**

The `vgchgid` command sets the activation mode to standard on a set of BCV devices that have been associated with and then split from a set of standard devices belonging to a clustered LVM volume group. This allows the BCV volume group to be imported back to the same host, a nonclustered host, or even added to a different cluster. Note that cluster commands such as `cmquerycl`, `cmcheckconf`, and `cmapplyconf` may take a long time to complete if the devices in a BCV volume group on a clustered host are in an established state while the BCV volume group is active.

For additional information on HP-UX clusters, refer to HP's *Managing MC/ServiceGuard* at [www.hp.docs.com/hpux/ha](http://www.hp.docs.com/hpux/ha).

The following examples relate to BCV devices being synchronized with clustered devices. There are four examples. In each of the examples, the BCV device is paired with a clustered LVM volume group device.
• Example A: BCV is imported on the same clustered host as the standard volume, but not added to the cluster. Refer to “Example A” on page 184.
• Example B: BCV is imported on a nonclustered host. Refer to “Example B” on page 186.
• Example C: BCV is imported on the failover host in the same cluster as the standard volume but not added to the cluster. Refer to “Example C” on page 189.
• Example D: BCV is imported on a host in a different cluster and added to the cluster. Refer to “Example D” on page 191.

**Example A**

The BCV is imported on the same clustered host as the standard volume, but not added to the cluster.

<table>
<thead>
<tr>
<th>Device</th>
<th>VG Name</th>
<th>Package Name</th>
<th>Cluster Name</th>
<th>Volume Group Active?</th>
<th>Host Name</th>
<th>Clustered Host?</th>
</tr>
</thead>
<tbody>
<tr>
<td>STD</td>
<td>vg01</td>
<td>Pkg_A</td>
<td>Clust_A</td>
<td>Y</td>
<td>A</td>
<td>Y</td>
</tr>
<tr>
<td>STD</td>
<td>vg01</td>
<td>Pkg_A</td>
<td>Clust_A</td>
<td>N</td>
<td>C</td>
<td>Y</td>
</tr>
<tr>
<td>BCV</td>
<td>bcv01</td>
<td>None</td>
<td>None</td>
<td>Y</td>
<td>A</td>
<td>Y</td>
</tr>
</tbody>
</table>

In this example:
• Cluster A includes Hosts A and C.
• The STD device is part of vg01 and is active on Host A as part of Package A/Cluster A.
• The STD device is visible on Host C, but the vg01 volume group is not active on Host C.
• When Package A fails over to Host C, vg01 will be activated on Host C (and deactivated on Host A).

The steps required to set up BCVs, synchronize, resynchronize, and restore in this configuration are described in the next section.

**Initial setup and synchronization**

To enable Host A to import a BCV copy (bcv01) of clustered LVM volume group vg01, follow the steps listed under “Initial setup and synchronization” on page 180 in the following order (replace device files, volume group, and hostnames where necessary):

1. Assign BCV device to Host A.
3. On the SYMCLI host, execute Initial Setup and Synchronization step 3.
Resynchronization

To resynchronize the BCV volume group (bcv01) with the STD volume group (vg01), follow steps under “Resynchronization” on page 181 in the following order (replace device files, volume group, and hostnames where necessary):

2. On the SYMCLI host, execute Resynchronization step 2.

Restore

To restore the STD device volume group (vg01) from the BCV device volume group (bcv01), execute the following including steps under “Restore” on page 182 in the following order (replace device files, volume group, and hostnames where necessary):

1. On Host A:
   a. Stop all I/O to vg01 and bcv01.
   b. Halt Package A:
      
   c. Export vg01:
      
2. On Host C, export vg01:
   
3. On Host A:
   a. Unmount BCV file systems:
   
   b. Deactivate BCV volume group:
   
   c. Export BCV volume group:
   
4. On the SYMCLI host, execute Restore step 2.
5. On Host A, execute the Restore steps 3a through 3h.
6. On Host C, reimport vg01:
   
7. On Host A:
   a. Restore the cluster bit on vg01:
   
   b. Start Package A:
c. Check the cluster to ensure Package A is up and running:
   `cmviewcl -v`

d. Back up the volume group configuration:
   `vgcfgbackup /dev/vg01`

**Example B**  The BCV is imported on a nonclustered host.

<table>
<thead>
<tr>
<th>Device</th>
<th>VG Name</th>
<th>Package Name</th>
<th>Cluster Name</th>
<th>Volume Group Active?</th>
<th>Host Name</th>
<th>Clustered Host?</th>
</tr>
</thead>
<tbody>
<tr>
<td>STD</td>
<td>Vg01</td>
<td>Package A</td>
<td>Cluster A</td>
<td>Y</td>
<td>A</td>
<td>Y</td>
</tr>
<tr>
<td>STD</td>
<td>Vg01</td>
<td>Package A</td>
<td>Cluster A</td>
<td>N</td>
<td>C</td>
<td>Y</td>
</tr>
<tr>
<td>BCV</td>
<td>BCV01</td>
<td>None</td>
<td>None</td>
<td>Y</td>
<td>B</td>
<td>N</td>
</tr>
</tbody>
</table>

![Diagram](https://example.com/diagram.png)
In this example:

- Cluster A includes Hosts A and C; Host B is not part of the cluster.
- The STD device is part of vg01 and is active on Host A as part of Package A/Cluster A.
- The STD device is visible on Host C but the vg01 volume group is not active on Host C.
- When Package A fails over to Host C, vg01 will be activated on Host C (and deactivated on Host A).
- The STD device is not visible to Host B.

The steps required to set up BCVs, synchronize, resynchronize, and restore in this configuration are described in the next section.

**Setup and synchronization**

To enable Host B to import a BCV copy (bcv01) of cluster LVM volume group vg01, follow the steps listed under “Initial setup and synchronization” on page 180 in the following order (replace device files, volume group, and hostnames where necessary):

1. Assign BCV device to Host B.
2. On Host B, execute Initial Setup and Synchronization step 2.
3. On the SYMCLI host, execute Initial Setup and Synchronization step 3.

**Resynchronization**

To resynchronize the BCV volume group (bcv01) with the STD volume group (vg01), follow the steps under “Resynchronization” on page 181 in the following order (replace device files, volume group, and hostnames where necessary):

2. On the SYMCLI host, execute Resynchronization step 2.

**Restore**

To restore the STD device volume group (vg01) from the BCV device volume group (bcv01), execute the following including steps under “Restore” on page 182 in the following order (replace device files, volume group, and hostnames where necessary):

1. On Host A:
   a. Stop all I/O to vg01.
   b. Halt Package A:
      ```bash
cmhaltpkg Pkg_A
   ```
   c. Export vg01:
      ```bash
vgexport -v -f /tmp/vg01.list /dev/vg01
   ```
2. On Host C, export vg01:

   \texttt{vgexport \textit{-v} \textit{-f} /tmp/vg01.list /dev/vg01}

3. On Host B:
   a. Stop all I/O to bcv01.
   b. Unmount BCV file systems:

      \texttt{umount /bcv$_{-}$fs1}

   c. Deactivate the BCV volume group:

      \texttt{vgchange \textit{-a n} /dev/bcv01}

   d. Export the BCV volume group:

      \texttt{vgexport \textit{-v} \textit{-f} /tmp/bcv01.list /dev/bcv01}

4. On the SYMCLI, host execute \textit{Restore} step 2.

5. On Host B execute \textit{Restore} steps 3a through 3e.

6. On Host A, execute \textit{Restore} steps 3f through 3h.

7. On Host C, reimport vg01:

   \texttt{mkdir /dev/vg01}

   \texttt{mknod /dev/vg01/group c 64 0x010000}

   \texttt{vgimport \textit{-v} \textit{-f} /tmp/vg01.list /dev/vg01}

8. On Host A:
   a. Restore the cluster bit on vg01:

      \texttt{vgchange \textit{-c y} /dev/vg01}

   b. Start Package A:

      \texttt{cmrunpkg Pkg\_A}

   c. Check the cluster to ensure Package A is up and running:

      \texttt{cmviewcl \textit{-v}}

   d. Back up the volume group configuration:

      \texttt{vgcfgbackup /dev/vg01}
Example C  The BCV is imported on the failover host in the same cluster as the standard volume but not added to the cluster.

<table>
<thead>
<tr>
<th>Device</th>
<th>VG Name</th>
<th>Package Name</th>
<th>Cluster Name</th>
<th>Volume Group Active?</th>
<th>Host Name</th>
<th>Clustered Host?</th>
</tr>
</thead>
<tbody>
<tr>
<td>STD</td>
<td>Vg01</td>
<td>Package A</td>
<td>Cluster A</td>
<td>Y</td>
<td>A</td>
<td>Y</td>
</tr>
<tr>
<td>STD</td>
<td>Vg01</td>
<td>Package A</td>
<td>Cluster A</td>
<td>N</td>
<td>C</td>
<td>Y</td>
</tr>
<tr>
<td>BCV</td>
<td>BCV01</td>
<td>None</td>
<td>None</td>
<td>Y</td>
<td>C</td>
<td>Y</td>
</tr>
</tbody>
</table>

In this example:

- Cluster A includes Hosts A and C.
- The STD device is part of vg01 and is active on Host A as part of Package A/Cluster A.
- The STD device is visible on Host C but the vg01 volume group is not active on Host C.
- When Package A fails over to Host C, vg01 will be activated on Host C (and deactivated on Host A).

The steps required to set up BCVs, synchronize, resynchronize, and restore in this configuration are described next.
Setup and synchronization

To enable Host C to import a BCV copy (bcv01) of clustered LVM volume group vg01, follow steps listed under “Initial setup and synchronization” on page 180 in the following order (replace device files, volume group, and hostnames where necessary):

1. Assign the BCV device to Host C.
2. On Host C, execute Initial Setup and Synchronization step 2.
3. On the SYMCLI host, execute Initial Setup and Synchronization step 3.

Resynchronization

To resynchronize the BCV volume group (bcv01) with the STD volume group (vg01), follow the steps under “Resynchronization” on page 181 in the following order (replace device files, volume group, and hostnames where necessary):

2. On the SYMCLI host, execute Resynchronization step 2.

Restore

To restore the STD device volume group (vg01) from the BCV device volume group (bcv01), execute the following including steps under “Restore” on page 182 in the following order (replace device files, volume group, and hostnames where necessary):

1. On Host A:
   a. Stop all I/O to vg01.
   b. Halt Package A:
      ```bash
cmhaltpkg Pkg_A
      ```
   c. Export vg01:
      ```bash
vgexport -v -f /tmp/vg01.list /dev/vg01
      ```
2. On Host C:
   a. Stop all I/O to bcv01.
   b. Unmount BCV file systems:
      ```bash
umount /bcv_fsl
      ```
   c. Deactivate the BCV volume group:
      ```bash
vgchange -a n /dev/bcv01
      ```
   d. Export the BCV volume group:
      ```bash
vgexport -v -f /tmp/bcv01.list /dev/bcv01
      ```
3. On the SYMCLI host, execute Restore step 2.
4. On Host C, execute Restore steps 3a through 3e.
Using Dell EMC TimeFinder in an HP-UX Environment

5. On Host A
   a. Execute Restore steps 3f through 3h.
   b. Restore the cluster bit on vg01:
      \[ \text{vgchange -c y /dev/vg01} \]
   c. Start Package A:
      \[ \text{cmrunpkg Pkg_A} \]
   d. Check the cluster to ensure Package A is up and running:
      \[ \text{cmviewcl -v} \]
   e. Back up the volume group configuration:
      \[ \text{vgcfgbackup /dev/vg01} \]

Example D
The BCV is imported on a host in a different cluster and added to the cluster.

<table>
<thead>
<tr>
<th>Device</th>
<th>VG Name</th>
<th>Package Name</th>
<th>Cluster Name</th>
<th>Volume Group Active?</th>
<th>Host Name</th>
<th>Clustered Host?</th>
</tr>
</thead>
<tbody>
<tr>
<td>STD 1</td>
<td>Vg01</td>
<td>Package A</td>
<td>Cluster A</td>
<td>Y</td>
<td>A</td>
<td>Y</td>
</tr>
<tr>
<td>STD 1</td>
<td>Vg01</td>
<td>Package A</td>
<td>Cluster A</td>
<td>N</td>
<td>C</td>
<td>Y</td>
</tr>
<tr>
<td>BCV</td>
<td>BCV01</td>
<td>Package B (or C)</td>
<td>Cluster B</td>
<td>Y</td>
<td>D</td>
<td>Y</td>
</tr>
<tr>
<td>STD 2</td>
<td>Vg02</td>
<td>Package B</td>
<td>Cluster B</td>
<td>Y</td>
<td>D</td>
<td>Y</td>
</tr>
<tr>
<td>STD 2</td>
<td>Vg02</td>
<td>Package B</td>
<td>Cluster B</td>
<td>N</td>
<td>C</td>
<td>Y</td>
</tr>
</tbody>
</table>

This example includes two clusters:
- Cluster A includes Host A and Host C.
- The STD1 device is part of vg01 and is active on Host A as part of Package A/Cluster A.
- The STD1 device is visible on Host C but the vg01 volume group is not active on Host C.
- When Package A fails over to Host C, vg01 will be activated on Host C (and deactivated on Host A).
- Cluster B includes Host D and Host E.
- Host D is the primary node in the cluster (where the cluster binary file exists).
- The STD 2 device is part of vg02 and is active on Host D as part of Package B/Cluster B.
• The STD 2 device is visible on Host E but the vg02 volume group is not active on Host E.
• When Package B fails over to Host E, vg02 will be activated on Host E (and deactivated on Host D).
• A BCV copy (bcv01) of vg01 is imported to Host D.
• The volume group bcv01 is added to one of the following:
  • An existing package (Package B) in Cluster B.
  • A new package (Package C) in Cluster B.

Setup and synchronization

To enable Host D to import a BCV copy (bcv01) of clustered LVM volume group vg01, follow the steps listed under “Initial setup and synchronization” on page 180 in the following order (replace device files, volume group, and hostnames where necessary):

1. Assign BCV devices to Host D.
2. On Host D, execute Initial Setup and Synchronization step 2.
3. On the SYMCLI host, execute Initial Setup and Synchronization step 3.
5. Perform steps 6 through 8 to add the bcv01 volume group to Package B/Cluster B.
6. On Host D:

   a. Unmount BCV file systems:
   
   umount /bcv_fs1
   vgchange –a n /dev/bcv01

   b. Create a map file of bcv01 and rcp to Host E:
   
   vgexport -p -v -s -m /tmp/bcv01.map /dev/bcv01
   rcp /tmp/bcv01.map HostE:/tmp

7. On Host E, import bcv01 to enable successful Package B failover:

   mkdir /dev/bcv01
   mknod /dev/bcv01/group c 64 0x02000
   vgimport -s -v -m /tmp/bcv01.map /dev/bcv01
   vgchange –a y /dev/bcv01
   vgcfgbackup /dev/bcv01
   mkdir /bcv_fs1
   mount /dev/bcv01/lvol1 /bcv_fs1
   bdf
   umount /bcv_fs1
   vgchange –a n /dev/bcv01

8. On Host D, modify cluster and package files:

   a. Activate the BCV volume group:
   
   vgchange –a y /dev/bcv01

   b. Add bcv01 to the Cluster B config file:
   
   vi /etc/cmcluster/cluster.conf
   add 'VOLUME_GROUP/dev/bcv01' to end of file

   c. Add bcv01 to the Package B control file:
   
   vi /etc/cmcluster/pkgB/pkgB.ctl
   add bcv01 under 'VOLUME GROUPS' as 'VG[1]=/dev/bcv01'
   add the file system information under 'FILESYSTEMS'
d. RCP the Package B control file to Host E:/etc/cmcluster/pkgB.

e. Verify and distribute new cluster configuration:

```
  cmcheckconf -C /etc/cmcluster/Clust_B
  cmapplyconf -C /etc/cmcluster/Clust_B
```

f. Deactivate the BCV volume group:

```
  vgchange -a n /dev/bcv01
```

g. Halt and restart Package B:

```
  cmhaltpkg pkgB
  cmrunpkg pkgB
```

h. Back up the volume group configuration:

```
  vgcfgbackup /dev/bcv01
```

9. Perform steps 10 through 12 to create Package C and include bcv01 volume group.

10. On Host D:

   a. Unmount BCV file systems and deactivate the BCV volume group:

```
  umount /bcv_fs1
  vgchange -a n /dev/bcv01
```

   b. Create the bcv01 map file and RCP to Host E:

```
  vgexport -p -s -v -m /tmp/bcv01.map /dev/bcv01
  rcp /tmp/bcv01.map hoste:/tmp
```

11. On Host E, import bcv01, to enable successful Package B failover:

```
  mkdir /dev/bcv01
  mknod /dev/bcv01/group c 64 0x02000
  vgimport -s -v -m /tmp/bcv01.map /dev/bcv01
  vgchange -a y /dev/bcv01
  vgcfgbackup /dev/bcv01
  mkdir /dev/bcv01/lvoll /bcv_fs1
  mount /dev/bcv01/lvoll /bcv_fs1
  bdf
  umount /bcv_fs1
  vgchange -a n /dev/bcv01
```

12. On Host D:

   a. Activate the BCV volume group:

```
  vgchange -a y /dev/bcv01
```

   b. Add bcv01 to the Cluster B config file:

```
  vi /etc/cmcluster/cluster.conf
  Add VOLUME_GROUP/dev/bcv01 to the end of the file.
```

   c. Create a new Package C with bcv01:

```
  mkdir /etc/cmcluster/pkgC
  cmmakepkg -p /etc/cmcluster/pkgC/pkgC.config (edit this file)
  cmmakepkg -s /etc/cmcluster/pkgC/pkgC.sh (edit this file, include bcv01)
```
d. RCP the Package C directory to Host E:/etc/cmcluster:

    rcp -p -r /etc/cmcluster/pkgC HostE:/etc/cmcluster

e. Verify and distribute the new cluster configuration:

    cmcheckconf -C /etc/cmcluster/Clust_B -P /etc/cmcluster/pkgC/pkcC.config
    cmapplyconf -C /etc/cmcluster/Clust_B -P /etc/cmcluster/pkgC/pkgC.config

f. Deactivate the BCV volume group, start the package, and check the cluster:

    vgchange -a n /dev/bcv01
    cmrunpkg pkgC
    cmviewcl -v
    vgcfgbackup /dev/bcv01
Resynchronization

To resynchronize the BCV volume group (bcv01) with the STD volume group (vg01), follow the steps under “Resynchronization” on page 181 in the following order (replace device files, volume group, and hostnames where necessary):

1. On Host D:
   a. Stop all I/O to the bcv01 volume group:
   b. Halt the package which owns the bcv01 volume group (pkgB or pkgC):
      ```bash
      cmhaltpkg pkgB
      ```
   c. Export the bcv01 volume group:
      ```bash
      vgexport -v -f /tmp/bcv01.list /dev/bcv01
      ```
2. On Host E, export bcv01:
   ```bash
   vgexport -v -f /tmp/bcv01.list /dev/bcv01
   ```
3. On the SYMCLI host, execute Resynchronization step 2.
4. On Host D, execute Resynchronization step 3a through 3c.
5. On Host E, reimport the bcv01 volume group:
   ```bash
   mkdir /dev/bcv01
   mknod /dev/bcv01/group c 64 0x02000
   vgimport -v -f /tmp/bcv01.list /dev/bcv01
   ```
6. On Host D:
   a. Place the cluster bit on bcv01:
      ```bash
      vgchange -c y /dev/bcv01
      ```
   b. Start the package (either pkgB or pkgC):
      ```bash
      cmrunpkg pkgB
      ```
Using Dell EMC TimeFinder in an HP-UX Environment

**Restore**

To restore the STD device volume group (vg01) from the BCV device volume group (bcv01), execute the following including steps under “Restore” on page 182 in the following order (replace device files, volume group, and hostnames where necessary):

1. On Host A:
   a. Stop all I/O to vg01.
   b. Halt Package A:
      ```
      cmhaltpkg PkgA
      ```
   c. Export vg01:
      ```
      vgexport -v -f /tmp/vg01.list /dev/vg01
      ```

2. On Host C, export vg01:
   ```
   vgexport -v -f /tmp/vg01.list /dev/vg01
   ```

3. On Host D:
   a. Stop all I/O to the bcv01 volume group.
   b. Halt the package that owns the bcv01 volume group (pkgB or pkgC):
      ```
      cmhaltpkg pkgB
      ```
   c. Export the bcv01 volume group:
      ```
      vgexport -v -f /tmp/bcv01.list /dev/bcv01
      ```

4. On Host E, export the bcv01 volume group:
   ```
   vgexport -v -f /tmp/bcv01.list /dev/bcv01
   ```

5. On the SYMCLI host, execute Restore step 2.

6. On Host D, execute Restore steps 3a through 3c.

7. On Host E, reimport bcv01:
   ```
   mkdir /dev/bcv01
   mknod /dev/bcv01/group c 64 0x02000
   vgimport -v -f /tmp/bcv01.list /dev/bcv01
   ```

8. On Host D:
   a. Restore the cluster bit on bcv01:
      ```
      vgchange -c y /dev/bcv01
      ```
   b. Start the package that owns bcv01 (pkgA or pkgB):
      ```
      cmrunpkg pkgB
      ```
   c. Check the cluster to ensure the bcv01 package is up and running:
      ```
      cmviewcl -v
      ```

9. On Host A, execute Restore steps 3f through 3h.

10. On Host C, reimport vg01:
    ```
        mkdir /dev/vg01
        mknod /dev/vg01/group c 64 0x010000
        vgimport -v -f /tmp/vg01.list /dev/vg01
    ```
11. On Host A:
   a. Restore the cluster bit on vg01:
      \texttt{vgchange -c y /dev/vg01}
   b. Start Package A:
      \texttt{cmrunpkg PkgA}
   c. Check the cluster to ensure Package A is up and running:
      \texttt{cmviewcl -v}

Refer to "Managing MC/ServiceGuard" at www.hp.docs.com/hpux/ha, “Cluster and Package Maintenance,” for guidelines on adding a volume group to an existing package in an existing cluster. “Configuring Packages and their Services” provides steps to create a new package in an existing cluster.

**File system issues**

If standard data volumes reside on an HP-UX 11i v1.0 host there may be issues with mounting the BCVs on an HP-UX 11.00 host. The default file system types are different between these two operating systems. HP-UX 11.00 default file system layout version is 3; on HP-UX 11i v1.0, it is version 4; on HP-UX 11i v2.0, it is version 5. But HP-UX 11.00 file systems may be mounted on HP-UX 11i v1.0.

On HP-UX, there are two versions of JFS (VxFS): Base JFS and Online JFS. Base JFS does not have all the features and options provided in Online JFS. For example, if the standard volume is mounted on an Online JFS host, with the large files option the BCVs may have problems being mounted on a host with only Base JFS. On HP-UX 11.00 and HP-UX 11i v1.0 OE, Base JFS is bundled with the OS and Online JFS is an add-on product. On HP-UX 11i v1.0 Enterprise OE and HP-UX 11i v1.0 Mission Critical OE, the OS is bundled with Online JFS.
CHAPTER 10

SRDF and MirrorView Remote Boot

This chapter contains information on mirroring to a disaster recovery site using Dell EMC EMC SRDF™/BCV, SnapView™, or MirrorView™.

- Remote boot 200
Remote boot

Boot may be mirrored to a disaster recovery site using SRDF/BCV, SnapView, or MirrorView. Follow the Dell EMC product guidelines in setting up the primary and secondary sites with regard to array models, microcode/system code, and so forth.

The following example procedure is for HP PA-RISC systems only. Boot configuration for HP Integrity systems is different than for PA-RISC systems. Some of the steps are not applicable for HP Integrity systems.

Environment at both sites must be setup so that:

- Server models are the same
- PDC levels are the same on both systems
- HBAs are the same on both servers
- Switch models and firmware are the same
- CLARiiON array FLARE code and array application software are the same
- VNX series with VNX OE for Block v31 and later

The following should be documented at each site to be able to recover the original configuration/setup:

- Primary hardware boot path
- /etc/lvmtab
- lvlnboot -v
- ioscan-fn output
- vgdisplay of vg00 file systems
- /etc/fstab
  ? Swap/dump configurations

The following steps detail how to successfully boot from the mirror at the secondary site after a successful sync to, and split from, the primary site device.

To boot off the mirror at the secondary site:

1. Reboot the system into LVM mode:
   ```
   shutdown -r -y now
   stop at BCH
   BCH> bo 'new hardware path'
   BCH> interact with ISL? Y
   ISL> 'hpux -lm /stand/vmunix'
   ```

   After booting into LVM mode, complete the following:

2. To probe new hardware path/LUNs.
   ```
   ioscan -fn
   ```

3. To create new device files.
   ```
   insf -e
   ```

4. Rerun ioscan to gather new boot device files (document for future use).
   ```
   ioscan -fn
   ```

5. Export root volume group.
   ```
   vgexport /dev/vg00
   ```
6. Change the vgid on the 'mirror' root devices (Include all root disks on the command line. May need to use the –f option with VNX series or CLARiiON devices).

   vgchgid /dev/rdsk/c9t0d0 /dev/rdsk/c9t0d1

7. Create root volume group directory and special file.

   mkdir /dev/vg00
   mknod /dev/vg00/group c 64 0x000000

8. Import root volume group using the mirror device files.

   vgimport /dev/dsk/c9t0d0 /dev/dsk/c9t0d01

9. Activate the root volume group.

   vgchange -a y /dev/vg00

10. Check the file systems.

   fsck -F hfs /dev/vg00/rlvol1 (/stand)
   fsck -F vxfs /dev/vg00/rlvol? (for all vxfs file systems)

11. Mount all vg00 file systems.

12. Check vg00 boot information. Ensure root, boot, swap and dump is included.

   lvlnboot -v

   For example:

   # lvlnboot -v
   Boot Definitions for Volume Group /dev/vg00:
   Physical Volumes belonging in Root Volume Group:
   /dev/dsk/c9t0d0 (0/0/1.2.0) -- Boot Disk
   /dev/dsk/c9t0d1 (0/0/1.0.0)
   Boot: lvol1 on: /dev/dsk/c9t0d0
   Root: lvol3 on: /dev/dsk/c9t0d0
   Swap: lvol2 on: /dev/dsk/c9t0d0
   Dump: lvol2 on: /dev/dsk/c9t0d0, 0

   Otherwise run:

   lvlnboot -R
   lvlnboot -r /dev/vg00/lvol3 (root vol)
   lvlnboot -b /dev/vg00/lvol1 (boot vol)
   lvlnboot -d /dev/vg00/lvol2 (dump vol)
   lvlnboot -s /dev/vg00/lvol2 (primary swap vol)

13. Next setup new boot path, etc.

   setboot -p 'new hardware path' -s off -b on


15. Edit /etc/rc.config.d/netconf to match secondary site networking information.


   hostname 'new hostname'

17. Reboot.
CHAPTER 11

OS Upgrade from HP-UX 11.23 to HP-UX 11.31

This chapter contains information on upgrading from HP-UX 11.23 to HP-UX 11.31 on VMAX and Symmetrix arrays.

- Upgrade from HP-UX 11.23 to HP-UX 11.31 204
Upgrade from HP-UX 11.23 to HP-UX 11.31

The following sections provide a guideline to upgrading from HP-UX 11.23 to HP-UX 11.31 on VMAX and Symmetrix arrays.

- “Flags,” next
- “Support” on page 204
- “Pre-OS upgrade checklist” on page 205
- “OS upgrade” on page 205

Flags

HP-UX 11.31 requires the enablement of the SPC-2 flag on the VMAX or Symmetrix target ports. Since the SPC-2 flag is supported both in HP-UX 11.23 and HP-UX 11.31, the bit may be enabled while at HP-UX 11.23 (prior to upgrading to HP-UX 11.31).

The enablement of the OSO7 flag is recommended, but not required. However, the OSO7 flag is only supported with HP-UX 11.31 and, therefore, would need to be enabled only after the OS upgrade.

For further details on HP-UX 11.31 support on Symmetrix, including minimum microcode requirements, refer to “Minimum Dell EMC PowerMAX OS, HYPERMAX OS and Enginuity requirements” on page 21.

Support

PowerPath 5.1.0 or later supports HP-UX 11.31. If the ‘upgrade host environment’ includes PowerPath, ensure that it is PowerPath 5.1.0 (or later) prior to starting the upgrade process. Currently, PowerPath only supports legacy DSF on HP-UX 11.31.

Symantec Veritas VxVM 4.1 and VxVM 5.0 are both supported with HP-UX 11.23 and HP-UX 11.31. Therefore, no VxVM upgrades would be required if the ‘upgrade host environment’ is at Symantec VxVM 4.1 or VxVM 5.0.

Note: VxVM 4.1 supports only legacy DSF, whereas VxVM 5.0 supports both the legacy and the agile DSF.
Pre-OS upgrade checklist

Before upgrading from HP-UX 11.23 to HP-UX 11.31 on VMAX/Symmetrix arrays, confirm the following:

- Ensure that the Symmetrix microcode is at the minimum support level for HP-UX 11.31 support.
- If PowerPath is installed on the host, check the version. If the version is not at PowerPath 5.1.0 (or later), upgrade the host to PowerPath 5.1.0 (or later).
- If Symantec Veritas VxVM volumes are configured on the host, check the Symantec Veritas VxVM version on the host. If the version is VxVM 3.5, then upgrade either to VxVM 4.1 or VxVM 5.0 (or later).

Note: For the most up-to-date information, always consult the Dell EMC Simple Support Matrices, available through Dell EMC E-Lab Navigator.

OS upgrade

To upgrade the OS from HP-UX 11.23 to HP-UX 11.31 on VMAX/Symmetrix arrays, perform the following steps:

1. Stop all applications on the ‘upgrade host.’
2. Set the SPC-2 flags on the target ports. This flag can be enabled in one of two ways:
   - Set globally through a Symmetrix configuration change.
   - Set using initiator wwn with Solutions Enabler 6.4 (or later):
     ```
     symmask -sid SymID -wwn HBAwwn set hba_flags on spc2 -enable -dir DirNum -port PortNum -v -noprompt
     ```
4. Following the host upgrade and subsequent reboot, set the OSO7 flag on the target ports. This flag can be enabled in one of two ways:
   - Set globally through a Symmetrix configuration change.
     - To rescan the devices run, `ioscan -fN` and `ioscan -fn`.
     - If Symantec Veritas VxVM is configured on the host, run `vxdctl enable`.
   - Set using initiator wwn with Solutions Enabler 6.4 (or later). This requires a host reboot after the flag is enabled.
     ```
     symmask -sid SymID -wwn HBAwwn set hba_flags on OS2007 -enable -dir DirNum -port PortNum -v -noprompt
     ```
Part 4 includes:

- Appendix A, “Migrating from SCSI Connections to Fibre Channel”
- Appendix C, “End-of-Support CLARiiON Arrays”
- Appendix D, “Excessive Path Failovers in LVM PVLink VNX Series and CLARiiON Configurations”
APPENDIX A

Migrating from SCSI Connections to Fibre Channel

The appendix describes the procedures used to migrate the configuration when a Symmetrix SCSI director is replaced with a Fibre Channel director.

- Introduction 210
- Running inquiry 211
- Connecting to the Dell EMC FTP server 211
- Migrating in the HP LVM environment 213
- Moving ‘rootvg’ on HP LVM 214
- Running the Dell EMC migration script 215
**Introduction**

A VMAX and Symmetrix SCSI director has four ports, and a Fibre Channel director has either two or eight. When replacing a SCSI director with a Fibre Channel director, you must follow certain procedures to assure that the hosts will know which devices are connected to which Symmetrix ports after the replacement.

Dell EMC provides a utility that automates much of the migration process. The procedure can be summarized as follows:

1. Run the Symmetrix **Inquiry** utility (inq) to identify the configuration before changing the hardware.

2. If appropriate for your host environment, perform the steps under “Migrating in the HP LVM environment” on page 213.

3. Run the Dell EMC script for HP hosts, described under *emc_s2f_hp* on “Running the Dell EMC migration script” on page 215.

   Each script must be run before and after changing the hardware, as described in the appropriate sections. Run the "before" section as described.

4. Change the hardware.

5. Run the "after" parts of the Dell EMC script, and then the host-specific steps (if applicable).
### Running inquiry

You must identify the VMAX/Symmetrix devices before making the hardware change. To do this, run `inq`; this displays information you can use to determine which the Symmetrix volume is associated with a particular device as seen by the host.

**Note:** The Inquiry utility will not work on HP devices with the NIO driver. This driver does not accept the SCSI passthrough commands that are needed by Inquiry. If you are going to run the `emc_s2f` utility under these circumstances, be sure to create pseudo devices.

An executable copy of the `inq` command for each of the supported hosts can be found on Dell EMC’s anonymous FTP server, `ftp.emc.com`, in the `/pub/sym3000/inquiry/latest` directory. Each file has a host-specific suffix. (Refer to “Connecting to the Dell EMC FTP server” on page 211.)

**Example**  
Figure 33 shows a sample output of `inq` when run from the host console:

```plaintext
Inquiry utility, Version 4.91  
Copyright (C) by EMC Corporation, all rights reserved.  -------------------------------  
-------------------------------------------------  
/dev/rdsk/c0t2d0s2 :SEAGATE :ST34371W SUN4.2G:7462 :9719D318 :4192560 :512  
/dev/rdsk/c0t3d0s2 :SEAGATE :ST34371W SUN4.2G:7462 :9719E906 :4192560 :512  
/dev/rdsk/c10t0d0s2 :EMC :SYMMETRIX :5264 :14000280 :224576 :512  
/dev/rdsk/c10t0d1s2 :EMC :SYMMETRIX :5264 :14001280 :224576 :512  
/dev/rdsk/c10t0d2s2 :EMC :SYMMETRIX :5264 :14002280 :224576 :512  
/dev/rdsk/c10t0d3s2 :EMC :SYMMETRIX :5264 :14003280 :224576 :512  
/dev/rdsk/c10t0d4s2 :EMC :SYMMETRIX :5264 :14004280 :224576 :512  
/dev/rdsk/c10t0d5s2 :EMC :SYMMETRIX :5264 :14005280 :224576 :512
```

**Figure 33** Inquiry output example

The output fields are as follows:

- **DEVICE** = UNIX device name (full pathname) for the SCSI device
- **VEND** = Vendor Information
- **PROD** = Product Name
- **REV** = Revision number — for a Symmetrix system, this will be the microcode version
  - **SER NUM** = Serial number, in the format SSVVVDDP, where:
    - **SS** = Last two digits of the Symmetrix system serial number
    - **VVV** = Logical Volume number
    - **DD** = Channel Director number
    - **P** = Port on the channel director
- **CAP** = Size of the device in kilobytes
- **BLKSZ** = Size in bytes of each block

### Connecting to the Dell EMC FTP server

Perform the following steps to connect to Dell EMC’s anonymous FTP server:

1. At the host, log in as `root`, and create the directory `/usr/ftp_emc` by typing `mkdir /usr/ftp_emc` and pressing Enter.
2. Type `cd /usr/ftp_emc`, and press Enter to change to the new directory.

3. Type `ftp ftp.emc.com`, and press Enter to connect to the FTP server:

4. At the FTP server login prompt, log in as anonymous.

5. At the password prompt, type your e-mail address.

You are now connected to the FTP server. To display a listing of FTP commands, type `help` and press Enter at the prompt.
Migrating in the HP LVM environment

**Note:** If you can remove PV/Links from the equation, it will make the migration significantly easier.

1. Type `vgcfgbackup` and press **Enter** to back up the existing LVM configuration.
2. Modify the `/etc/lvmrc` file to disable Automatic Volume Group Activation.
3. As a safety measure, you can create map files containing the `vgid` of the existing volume groups. To do so, type `vgexport -p -s -m mapfile vg_name` and press **Enter**.
4. Move the file `/etc/lvmtab` to a backup file; for example, `old.lvmtab`. 
Moving ‘rootvg’ on HP LVM

When reducing the number of channels, you should first move rootvg to the remaining channels so that it does not fail VG quorum check on reboot.

1. Identify the rootvg volumes.
2. Remap those volumes to the remaining channels on the Symmetrix.
3. Create a PV/Links association for each volume to the new channel using vgextend.
4. Remove the old mapping of the device from PV/Links using vgreduce.
Running the Dell EMC migration script

Migration script emc_s2f_hp handles volume groups, PV Links, pseudo devices, and NIO drivers in an HP host environment.

**IMPORTANT**
This script depends on another script, vgnode.ksh, that is shipped in the same distribution package as emc_s2f_hp. Verify that vgnode.ksh is present.

**Usage**
The syntax of the utility is:

```
emc_s2f_hp -<option>
```

where `<option>` is one of these:

- `b` — Specify when running `emc_s2f_hp` before converting to Fibre Channel.
- `e` — Specify to build a script to automate `vgexport`.
- `a` — Specify when running `emc_s2f_hp` after converting to Fibre Channel.
- `c` — Specify to compare the "before" and "after" configurations to plan `vgimport`.
- `i` — Specify to build a script to automate `vgimport`.

**Limitations**
Note the following limitations of `emc_s2f_hp`:

- The comparison will not be accurate if the host is connected to multiple Symmetrix devices and the last two digits in the serial number of one Symmetrix system are the same as the last two digits of the serial number of another Symmetrix system.
- If multiple paths exist to the host before and after the migration, the "before" and "after" groups of devices will be displayed, but there will be no way to tell how the devices match each other.
- The `Inquiry` utility does not work on HP devices with the NIO driver, because the driver does not accept the SCSI pass-through commands needed by `Inquiry`. Before running `emc_s2f_hp` under these circumstances, you must create pseudo devices.
- HP does not allow an export of the root volume group. If the group is on devices that will be affected by the migration, you must remove any mention of the group from the import/export scripts that `emc_s2f_hp` creates.
- `emc_s2f_hp` does not work correctly if you map some of a SCSI port’s devices to one Fibre Channel port and the rest to a different Fibre Channel port. All of the devices on a SCSI port must be mapped to a single Fibre Channel port. (If you need to map a SCSI port’s devices to multiple Fibre Channel ports, use `emc_s2f`.)

**Procedure**

1. Unmount the filesystems.
2. Type `emc_s2f_hp -b` and press Enter to take a snapshot of the configuration before you change the hardware. The information is displayed, and written to a file named `emc_s2f_hp.b`.
3. Type `emc_s2f_hp -e` and press Enter to create a shell script that will export all of the volume groups.

It is the user’s responsibility to review the script to ensure it is exporting the correct volume groups.
4. Run the export script created in step 3.

5. Replace the necessary hardware, then bring the Symmetrix back on line. Make a note of how the SCSI ports are mapped to the Fibre Channel ports.

6. Create a text file named `emc_s2f_hp.ref`, which should contain director and port assignments before and after the hardware change(s). For example, if devices originally accessed through SA 15a-a and 15a-b are now accessed through 16b-a, the text of `emc_s2f_hp.ref` should be:

```
15a-a:16b-a
15a-b:16b-a
```

**IMPORTANT**

This file assumes an n:1 mapping of SCSI ports to Fibre Channel ports. The `emc_s2f_hp` script will not work correctly if you map some of a SCSI port’s devices to one Fibre Channel port and the rest to a different Fibre Channel port.

7. Type `emc_s2f_hp -a` and press Enter to take a snapshot of the new hardware configuration. The information is displayed, and written to a file named `emc_s2f_hp.a`.

8. Type `emc_s2f_hp -c` and press Enter to compare the two files. The information is displayed, and written to a file named `emc_s2f_hp.c`.

**Note:** Check the "compare" file for missing information. If any device is missing an old or new device name, or xx is displayed instead of a device name, it means that `emc_s2f_hp` could not gather all the necessary information. Make sure all the devices are ready and available to the host, then rerun `emc_s2f_hp`.

Here is a sample output, from a Symmetrix system with a serial number ending in 65:

```
NEW=c9t1d6 OLD=c2t5d6 VG=N/A (NO-VG)
NEW=c9t1d7 OLD=c2t5d7 VG=N/A (NO-VG)
NEW=c6t3d4 OLD=c6t3d4 VG=/dev/vg04 (PRIMARY)
NEW=c6t3d5 OLD=c6t3d5 VG=/dev/vg0 (PRIMARY)
NEW=c9t2d0 OLD=c2t6d0 VG=/dev/vg04 (ALTERNATE)
NEW=c9t2d1 OLD=c2t6d1 VG=/dev/vg04 (ALTERNATE)
```

Before, two "old" devices were seen as c2t5d6 and c2t5d7. They were not part of a volume group. The devices are now named c9t1d6 and c9t1d7, respectively.

Volume group vg04 used to have two primary paths, c6t3d4 and c6t3d5, with alternate links c2t6d0 and c2t6d1. After the migration, the new primary paths are c6t3d4 and c6t3d5, with alternates c9t2d0 and c9t2d1. The `Import` script created by `s2f_hp -i` will pass this information on to the `vgimport` command, which will be able to sort everything out and bring back the volume groups.

9. Type `emc_s2f_hp -i` and press Enter to create a shell script that will import all of the volume groups, with the new names, in the correct order, preserving the primary/alternate relationships.

   It is the user’s responsibility to review the script to ensure it is importing the volume groups correctly.
The appendix describes procedures to set up CISCO MDS 9000 Switches for HP-UX environments.

- Setting up MDS 9000 switches for an HP-UX environment 220
Setting up MDS 9000 switches for an HP-UX environment

Generally, the Dell EMC Connectrix™ family of switches has similar configuration guidelines. However, this is not the case for the Cisco MDS 9000 family of switches using firmware version 1.3.x or earlier.

With the Cisco MDS 9000 switch family, default settings MUST be changed during initial setup and configuration. If any new devices are added to the switch ports, the FCID and persistence must be modified. Persistent FC IDs option must be enabled on the Vsan that contains any HP-UX initiators or target ports accessed by HP-UX initiators, and on individual switch port basis ports that have either a HP-UX initiator or a HP-UX target port attached must be configured for static and persistent FC_IDs. Cisco switch ports with HP-UX initiators attached must have unique FC_ID Area ID1s configured, firmware version 1.3.x or later should automatically configure the HP-UX initiator switch ports for unique FC_ID Area IDs, however the HP-UX initiator switch ports must have the FC_ID Area IDs manually configured to be unique with firmware version 1.2.x or earlier.

HP HBA ports require a unique area ID from any storage ports when they are both connected to the same switch. HP HBAs also reserve ID 255 (ffff hex). For example, if the storage port FC ID is 0x6f7704, the area for this port is 77. In this case, the HBA port area can be anything other than 77. The HBA-port and the target-port FC ID must be manually configured to be different from the storage array’s target port FC ID.

Switches in the Cisco MDS 9000 Family facilitate this requirement with their FC ID Persistence Feature. You can use this feature to pre-assign an FC ID with a different area or port ID to either the storage port or the HBA port or both. To configure a different area ID for the HBA port, follow these steps:

1. Obtain the Port WWN (Port Name filed) ID of the HBA using the `show flogi database` command.

```
switch# show flogi database

INTERFACE  VSAN   FCID         PORT NAME      NODE NAME
fc1/9      3  0x6f7703 50:05:08:b2:00:71:c8:c2 50:05:08:b2:00:71:c8:c0
fc1/10     3  0x6f7704 50:06:0e:80:03:29:61:0f 50:06:0e:80:03:29:61:0f
```

**Note:** Both FC IDs in this setup have the same area 77 assignment.

2. Shut down the HBA interface in the MDS switch.

```
switch# conf t
switch(config)# interface fc1/9
switch(config-if)# shutdown
switch(config-if)# end
switch#
```

3. Verify that the FC ID feature is enabled using the `show fcdomain vsan` command.

```
switch# show fcdomain vsan 1
Local switch configuration information:
State: Enabled
FCID persistence: Disabled
```
• If this feature is disabled, continue with this procedure to enable the FC ID persistence.
• If this feature is already enabled, skip to step 5.

4. Enable the FC ID persistence feature in the MDS switch.

```
switch# conf t
switch(config)# fcdomain fcid persistent vsan 1
switch(config)# end
switch#
```

5. Assign a new FC ID with a different area allocation. In this example, 77 is replaced by ee.

```
switch# conf t
switch(config)# fcdomain fcid database
switch(config-fcid-db)# vsan 3 WWN 50:05:08:b2:00:71:c8:c2 fcid 0x6 fee00
```

6. Enable the HBA interface in the MDS switch.

```
switch# conf t
switch(config)# interface fc1/9
switch(config-if)# no shutdown
switch(config-if)# end
switch#
```

7. Verify the pWWN ID of the HBA using the `show flogi database` command.

```
switch# show flogi database

<table>
<thead>
<tr>
<th>INTERFACE</th>
<th>VSAN</th>
<th>FCID</th>
<th>PORT NAME</th>
<th>NODE NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>fc1/9</td>
<td>3</td>
<td>0xfee00</td>
<td>50:05:08:b2:00:71:c8:c2</td>
<td>50:05:08:b2:00:71:c8:c0</td>
</tr>
<tr>
<td>fc1/10</td>
<td>3</td>
<td>0xfee00</td>
<td>50:05:08:b2:00:71:c8:c2</td>
<td>50:05:08:b2:00:71:c8:c0</td>
</tr>
</tbody>
</table>
```

**IMPORTANT**
Both FC IDs now have different area assignments.

This process can also be accomplished using the Device Manager from the Fabric Manager GUI.

Edits can be made by double-clicking on the FCIDs field (0x830003) and making any required changes. The Assignment Field must be changed from Dynamic to Static.

**Note:** You must click the apply button to save changes.

The following figures show typical examples of the different switches and their port configurations tables.
Figure 34, “Cisco MDS 9000 family, Domain Manager,” on page 222

Figure 35, “Cisco MDS 9000 family, Device Manager,” on page 223
<table>
<thead>
<tr>
<th>Interface</th>
<th>Description</th>
<th>VSAN(s)</th>
<th>Mode</th>
<th>Connected To</th>
<th>Speed (Gbps)</th>
<th>Rx</th>
<th>Tx</th>
<th>Errors</th>
<th>Discards</th>
<th>Log</th>
</tr>
</thead>
<tbody>
<tr>
<td>Idir 01</td>
<td></td>
<td>2F</td>
<td></td>
<td></td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Idir 02</td>
<td></td>
<td>2F</td>
<td></td>
<td></td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Figure 35** Cisco MDS 9000 family, Device Manager
Setting Up Cisco MDS 9000 Switches for HP-UX Environments
APPENDIX C

End-of-Support CLARiiON Arrays

CLARiiON array models FC5x00 and FC4500 are now end-of-support. The following guidelines and notes for CLARiiON FC arrays will be removed from future revisions of the *EMC Host Connectivity Guide for HP-UX*.

- Change in hardware paths 226
- Fabric address change 226
- Sequential LUNs 226
- MC/ServiceGuard 226
Change in hardware paths

Beginning with Core or Base Software revisions listed Table 23, the hardware paths for LUNs connected to HP-UX systems will be different.

<table>
<thead>
<tr>
<th>Model number</th>
<th>Core or base software revision</th>
</tr>
</thead>
<tbody>
<tr>
<td>FC4500</td>
<td>5.32.01 or 6.32.01, PROM 2.0.9</td>
</tr>
<tr>
<td>FC5300</td>
<td>5.24.00</td>
</tr>
<tr>
<td>FC 5600/5700</td>
<td>5.11.08</td>
</tr>
<tr>
<td>FC 5603/5703</td>
<td>5.11.59</td>
</tr>
</tbody>
</table>

This change is the result of the enhancement made within the Core or Base Software that allows a storage system attached to any HP-UX server to be configured with more than eight LUNs. This change within the Core or Base Software creates a temporary inability to access the devices until the operating system has been configured to recognize the new paths. After updating the Core or Base Software from an earlier version to the current version, device entries must be changed to reflect the new location of the devices before they can be used again. Refer to Dell EMC Technical Bulletin S000224, available from your Dell EMC Technical Support representative.

Fabric address change

The current Fibre Channel implementation over a private arbitrated loop uses the hard physical address (HPA) of the Fibre Channel target to generate a portion of the hardware path to the Fibre Channel port. Behind this port, virtual SCSI busses, targets, and LUNs will exist.

In a fabric environment, the N_Port address is used to generate this portion of the hardware path to the Fibre Channel port. Behind this port, virtual SCSI busses, targets and LUNs exist in the same manner as the existing configurations. The fabric/switch is responsible for generating the N_Port address.

Sequential LUNs

Logical units must be created in sequential order to access LUN values 8 or higher. Also, removal of a LUN from a sequence could result in a loss of access to other LUNs with higher LUN values.

MC/ServiceGuard

If you have a two-node cluster, you must configure a cluster lock. A cluster lock is a disk area located in a volume group that is shared by all nodes in a cluster. FC5400/5500, FC5600/5700, and FC5603/5703 storage systems cannot be used as lock devices. A disk contained in an FC5000 JBOD enclosure is a qualified lock device. The preferred high availability configuration utilizes hubs to provide direct connectivity to all of the devices.

FC4500, FC4700, and FC5300 storage systems have been qualified to operate as a lock device in a two-node MC/ServiceGuard cluster.
Following these guidelines when using this configuration:

- Create a highly available RAID group (RAID 1, RAID 1/0, RAID 5).
- Create two small LUNs (4 MB each) with the default owners on separate storage processors on the RAID group.
- Identify the devices to the operating system (ioscan and insf).
- Create a single volume group with one path only to each logical unit.
- Do not create logical volumes or use this volume group for data storage.
- In MC/ServiceGuard, define the logical units as primary and secondary lock devices.

The minimum requirements for this configuration are:

- FC4500 base software:
  - If no Access Logix — 5.32.07
  - If Access Logix — 6.32.07
- FC4700 base software:
  - If no Access Logix — 8.42.09
  - If Access Logix — 8.42.59
- FC5300 base software — 5.24.00
- HP/UX 11.00 with General Release Patches, June 2001
- MC/Service Guard A.11.12
End-of-Support CLARiiON Arrays
APPENDIX D

Excessive Path Failovers in LVM PVLink VNX Series and CLARiiON Configurations

Excessive path failovers in HP-UX LVM PVLink VNX series and CLARiiON configurations can occur under the conditions described in this appendix.

- Introduction 230
- Changing the timeout 230
- Changing max_fcp_req 230
Introduction

Some non-PowerPath configurations may exhibit excessive path failovers or LUN trespassing under the following conditions:

- Heavy utilization and I/O load on the array SPs.
- Alternate LVM PVLinks configured with default timeout value
- HBA initiator setting set to HP AutoTrespass

If and only if the HP-UX LVM PVLink VNX series and CLARiiON configuration is exhibiting excessive path failovers or LUN trespass notifications in the SP event logs, refer to Dell EMC technical bulletin ID emc21180 and the following possible solutions intended for non-PowerPath configurations.

Changing the timeout

Type the following command for the primary and alternate paths from the system prompt:

```
pvchange -t 180 /dev/dsk/cntndn
```

where `cntndn` is a specific device file that is used by the system to manage the array.

**Example**

To change the timeout value for the primary device (c1t1d0) and the alternate device (c2t1d0), type:

```
pvchange -t 180 /dev/dsk/c1t1d0
pvchange -t 180 /dev/dsk/c2t1d0
```

Changing `max_fcp_req`

If changing the timeout value does not correct excessive path failovers, you can change the `max_fcp_req` kernel parameter for some HBAs.

**FC4500, FC5300, FC5700**

- If this is an A3404A, A3740A, A3591A, or a Tachyon-based HBA:
  a. Using SAM, select **Kernel Configuration**, and then click **Configurable Parameters**.
  b. Set the `max_fcp_reqs` kernel parameter to 128 or less (256/number of paths to the array).

  **Note:** The default value for this parameter is 512.
  c. Reboot the system.

- If this is an A5158A, A6795A, A6684A, A6685A, or other Tach Lite-based adapter, run the following for each VNX series and CLARiiON LUN:
  
  ```
  scsictl-a /dev/rdsk/cxydz scsictl-a -mqueue_depth=4 -mqueue_depth /dev/rdsk/cxydz
  ```

  where `x` is the controller number, `y` is the target number, and `z` is the disk number of the VNX series and CLARiiON disk.
**FC4700, CX series**

- If this is an A3404A, A3740A, A3591A, or a Tachyon-based HBA:
  a. Using SAM, select **Kernel Configuration**, and then click **Configurable Values**.
  b. Set the **max_fcp_reqs** kernel parameter to 512 or less (1024/number of paths to the array).

  **Note:** The default value for this parameter is 512.

  c. Reboot the system.

- If this is an A5158A, A6795A, A6684A, A6685A, or other Tach Lite-based adapter, run the following for each VNX series and CLARiiON LUN:

  ```bash
  scsictl-a/dev/rdsk/cxtydz
  scsictl-a-mqueue_depth=4-mqueue_depth/dev/rdsk/cxtydz
  ```

  where \( x \) is the controller number, \( y \) is the target number, and \( z \) is the disk number of the VNX series and CLARiiON disk.
Excessive Path Failovers in LVM PVLInk VNX Series and CLARiiON Configurations