Abstract
This Hewlett Packard Enterprise (HPE) concepts guide is for all levels of system and storage administrators who plan storage policies, configure storage resources, or monitor the storage usage of HPE 3PAR StoreServ Storage systems.
Notices

The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.


Links to third-party websites take you outside the Hewlett Packard Enterprise website. Hewlett Packard Enterprise has no control over and is not responsible for information outside the Hewlett Packard Enterprise website.

Acknowledgments

Google™ is a trademark of Google Inc.

Linux® is a trademark of Linus Torvalds in the U.S. and other countries.

Microsoft®, Windows®, and Hyper-V® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Mozilla® and Firefox® are trademarks of Mozilla Incorporated.

Red Hat® is a trademark of Red Hat, Inc. in the United States and other countries.

UNIX® is a registered trademark of The Open Group.

VMware®, VMware® ESX®, VMware®ESXi™, VMware®vCenter™, and VMware vSphere® are U.S. registered trademarks of VMware, Inc.
## Contents

### HPE 3PAR Storage concepts and terminology overview

- Physical Disks (PD) ......................................................... 8
- Chunklets ........................................................................ 9
- Logical Disks (LD) .......................................................... 9
- Common Provisioning Groups (CPG) ................................. 9
- Virtual Volumes (VV) ....................................................... 9
  - Fully Provisioned Virtual Volumes (FPVV) ...................... 9
  - Thinly Provisioned Virtual Volumes (TPVV) .................... 10
  - Thinly Deduplicated Virtual Volumes (TDVV) ............... 10
  - Physical Copies .......................................................... 10
  - Virtual Copy Snapshots .............................................. 10
- Exporting Virtual Volumes .............................................. 10

### HPE 3PAR software products and features

- HPE 3PAR software licensing ......................................... 11
  - Types of HPE 3PAR All-inclusive Software License .......... 15
    - All-inclusive Single-System HPE 3PAR Software License 15
    - HPE 3PAR All-inclusive Multi-System Software License 16
  - Data-at-rest encryption software license .......................... 17
  - HPE 3PAR All-inclusive Software Matrix ....................... 17
  - HPE 3PAR Transition License (Old to New) .................... 18

### HPE 3PAR StoreServ storage system users

- User account roles ......................................................... 20
- Local user authentication and authorization ..................... 21
- LDAP user authentication and authorization ..................... 21
- Domain user access ....................................................... 21
- Strong passwords .......................................................... 21
  - Time-based passwords .............................................. 22
  - Encrypted ciphertext passwords .................................. 22
    - Exporting ciphertext ............................................. 22
    - Changing the ciphertext password ......................... 22
    - Setting or changing the password mode ................... 22
- Lightweight Directory Access Protocol ............................ 24
  - Active Directory ....................................................... 24
  - OpenLDAP .................................................................. 24
  - LDAP users .............................................................. 24
  - LDAP server data organization .................................. 25
  - LDAP and domains .................................................... 25
  - LDAP authentication and authorization ....................... 25
    - LDAP authentication ............................................. 26
    - Simple binding .................................................... 26
    - SASL binding ....................................................... 26
    - LDAP authorization .............................................. 26
      - Authorization on systems using virtual domains .... 27
Reclaiming unused space ............................................................... 55
Reclaiming unmapped LD space from CPGs .................................. 55
Reclaiming unmapped LD space from volumes ................................ 56
Automatically reclaiming unused snapshot space from volumes ... 56
Manually reclaiming unused snapshot space from volumes .......... 56
Deleted volume snapshot space .................................................... 56
Logical disks and chunklet initialization ....................................... 56

Enhanced storage applications .................................................... 57
HPE 3PAR File Persona software ................................................. 57
HPE 3PAR Thin Express ASIC ..................................................... 58
HPE 3PAR Remote Copy software ............................................... 58
HPE 3PAR Dynamic Optimization software ............................... 58
HPE 3PAR Adaptive Flash Cache software ................................. 59
HPE 3PAR System Tuner software ............................................. 60
HPE 3PAR Thin Conversion software ......................................... 60
  Assessment ..................................................................... 60
  Data preparation ................................................................ 61
  Zeroing unused space ....................................................... 61
  Creating a physical copy .................................................... 61
HPE 3PAR Thin Persistence software ........................................... 61
HPE 3PAR Thin Copy Reclamation software ............................... 61
HPE 3PAR Virtual Lock software ............................................ 61
HPE 3PAR Adaptive Optimization software ................................ 62
HPE 3PAR Peer Motion software .............................................. 63
Data encryption ......................................................................... 63
Priority Optimization software .................................................. 64
  Virtual Volume Sets ......................................................... 65
  Quality of service rules ..................................................... 65
    Mode of operation ......................................................... 65
    QoS rule minimum and maximum .................................. 66
    QoS rule actions .......................................................... 66
    Overlapping QoS rules .................................................. 67
    Minimum QoS settings .................................................. 67
    QoS on copied volumes ................................................ 67
HPE 3PAR mySnapshot .............................................................. 67

HPE 3PAR StoreServ Storage hardware ...................................... 68
Identifying HPE 3PAR StoreServ Storage system components .... 68
HPE 3PAR StoreServ Storage hardware components ................. 68
Physical drive ......................................................................... 68
Disk enclosure ......................................................................... 69
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controller node</td>
<td>66</td>
</tr>
<tr>
<td>Service Processor 5.0</td>
<td>69</td>
</tr>
<tr>
<td>Physical Service Processor (PSP)</td>
<td>69</td>
</tr>
<tr>
<td>Virtual Service Processor (VSP)</td>
<td>69</td>
</tr>
<tr>
<td>Power Distribution Unit</td>
<td>70</td>
</tr>
<tr>
<td>Input/Output module</td>
<td>70</td>
</tr>
<tr>
<td>HPE 3PAR StoreServ Storage models</td>
<td>70</td>
</tr>
<tr>
<td>HPE 3PAR StoreServ 7000 Storage</td>
<td>71</td>
</tr>
<tr>
<td>HPE 3PAR StoreServ 8000 Storage</td>
<td>71</td>
</tr>
<tr>
<td>HPE 3PAR StoreServ 9000 Storage</td>
<td>71</td>
</tr>
<tr>
<td>HPE 3PAR StoreServ 10000 Storage</td>
<td>71</td>
</tr>
<tr>
<td>HPE 3PAR StoreServ 20000 Storage</td>
<td>71</td>
</tr>
<tr>
<td>HPE 3PAR SNMP infrastructure</td>
<td>73</td>
</tr>
<tr>
<td>About SNMP</td>
<td>73</td>
</tr>
<tr>
<td>SNMP managers</td>
<td>73</td>
</tr>
<tr>
<td>The HPE 3PAR SNMP agent</td>
<td>73</td>
</tr>
<tr>
<td>Standard compliance</td>
<td>73</td>
</tr>
<tr>
<td>Supported MIBs</td>
<td>74</td>
</tr>
<tr>
<td>MIB-II</td>
<td>74</td>
</tr>
<tr>
<td>Exposed objects</td>
<td>75</td>
</tr>
<tr>
<td>HPE 3PAR MIB</td>
<td>76</td>
</tr>
<tr>
<td>HPE 3PAR Common Information Model API</td>
<td>86</td>
</tr>
<tr>
<td>SMI-S</td>
<td>86</td>
</tr>
<tr>
<td>WBEM initiative</td>
<td>86</td>
</tr>
<tr>
<td>HPE 3PAR CIM support</td>
<td>86</td>
</tr>
<tr>
<td>Standard compliance</td>
<td>87</td>
</tr>
<tr>
<td>SMI-S profiles</td>
<td>87</td>
</tr>
<tr>
<td>Supported extensions</td>
<td>87</td>
</tr>
<tr>
<td>CIM indications</td>
<td>87</td>
</tr>
<tr>
<td>Comparing HPE 3PAR to EVA terms</td>
<td>88</td>
</tr>
<tr>
<td>Support and other resources</td>
<td>89</td>
</tr>
<tr>
<td>Accessing Hewlett Packard Enterprise Support</td>
<td>89</td>
</tr>
<tr>
<td>Accessing updates</td>
<td>89</td>
</tr>
<tr>
<td>Customer self repair</td>
<td>90</td>
</tr>
<tr>
<td>Remote support</td>
<td>90</td>
</tr>
<tr>
<td>Warranty information</td>
<td>90</td>
</tr>
<tr>
<td>Regulatory information</td>
<td>91</td>
</tr>
<tr>
<td>Documentation feedback</td>
<td>91</td>
</tr>
<tr>
<td>Glossary</td>
<td>92</td>
</tr>
<tr>
<td>A</td>
<td>92</td>
</tr>
<tr>
<td>B</td>
<td>93</td>
</tr>
<tr>
<td>C</td>
<td>93</td>
</tr>
<tr>
<td>D</td>
<td>95</td>
</tr>
<tr>
<td>E</td>
<td>96</td>
</tr>
<tr>
<td>F</td>
<td>96</td>
</tr>
<tr>
<td>G</td>
<td>97</td>
</tr>
</tbody>
</table>
HPE 3PAR Storage concepts and terminology overview

HPE 3PAR StoreServ Storage systems include hardware components that physically store your data and software applications that manage your data. The HPE 3PAR StoreServ Storage system is composed of the following logical data layers:

- **Physical Disk (PD)**
- **Chunklet**
- **Logical Disk (LD)**
- **Common Provisioning Group (CPG)**
- **Virtual Volume (VV)**

The relationship between HPE 3PAR StoreServ Storage system data layers is illustrated in the following figure. Each layer is created from elements from the layer above. Chunklets are drawn from physical disks, Logical Disks (LDs) are created from groups of chunklets, Common Provisioning Groups (CPGs) are groups of LDs, and Virtual Volumes (VV) use storage space provided by the CPGs. The virtual volumes are exported to the hosts and are the only layer visible to the hosts.

![Figure 1: HPE 3PAR StoreServ data layers](image)

**Physical Disks (PD)**

A physical disk is a hard drive mounted on a drive magazine located in an HPE 3PAR StoreServ Storage system drive cage. There are three types of physical disks:
• Fast class (FC)
• Near line (NL)
• Solid state drive (SSD)

**Chunklets**

Physical disks (PD) are divided into 1 GB chunklets. Each chunklet occupies contiguous space on a physical disk. Chunklets are automatically created by the HPE 3PAR Operating System (HPE 3PAR OS), and they are used to create Logical Disks (LD). A chunklet is assigned to only one LD. For more information about chunklets, see [Chunklets](#) on page 36.

**Logical Disks (LD)**

A Logical Disk (LD) is a collection of physical disk chunklets arranged as rows of RAID sets. Each RAID set is made up of chunklets from different physical disks. LDs are pooled together in Common Provisioning Groups (CPG), which allocate space to virtual volumes.

The underlying LDs are automatically created by the HPE 3PAR OS when you create CPGs. The RAID type, space allocation, growth increments, and other LD parameters can be set when you create a CPG, or can be modified later. HPE 3PAR StoreServ Storage systems support the following RAID types:

- RAID 0
- RAID 10 (RAID 1)
- RAID 50 (RAID 5)
- RAID MP (Multi-Parity) or RAID 6

For a detailed discussion of LDs and RAID types, see [Logical disks](#) on page 38.

**Common Provisioning Groups (CPG)**

The CPG defines the Logical Disk (LD) creation characteristics, such as RAID type, set size, disk type for chunklet selection, plus total space warning, and limit points. A CPG is a virtual pool of LDs that allocates space to virtual volumes (VV) on demand. A CPG allows VVs to share the CPG resources. You can create Fully Provisioned virtual volumes (FPVVs) and Thinly Provisioned virtual volumes (TPVVs) that draw space from a CPG LD pool. For more information about CPGs, see [Common Provisioning Groups](#) on page 43.

**Virtual Volumes (VV)**

Virtual volumes draw their resources from Common Provisioning Groups (CPG), and volumes are exported as logical unit numbers (LUN) to hosts. Virtual volumes are the only data layers visible to the hosts.

You can create physical copies of virtual volumes that remain available if the original base volume becomes unavailable. Before creating virtual volumes, you must first create CPGs to allocate space to the virtual volumes. For more information about virtual volumes, see [Virtual Volumes](#) on page 46.

**Fully Provisioned Virtual Volumes (FPVV)**

An FPVV is a volume that uses Logical Disks (LD) that belong to a Compact Provisioning Group (CPG). Unlike Thinly Provisioned Virtual Volumes (TPVV), FPVVs have a set amount of user space that is allocated for user data. The FPVV size is fixed, and the size limit is 16 TB. For more information about FPVVs, see [Fully-Provisioned Virtual Volumes (FPVV)](#) on page 47.
Thinly Provisioned Virtual Volumes (TPVV)

A TPVV is a volume that uses Logical Disks (LD) that belong to a Common Provisioning Group (CPG). TPVVs associated with the same CPG draw space from the LD pool as needed, allocating space on demand in 16 KB increments. When the volumes that draw space from the CPG require additional storage, the HPE 3PAR OS automatically creates additional LDs and adds them to the pool. The CPG can grow until it reaches the user-defined growth limit, which restricts the CPG maximum size. The TPVV volume size limit is 16 TB. For more information about TPVVs, see Thinly-Provisioned Virtual Volumes (TPVV) on page 47.

Thinly Deduplicated Virtual Volumes (TDVV)

With the HPE 3PAR Thin Deduplication feature, you can create thinly deduplicated virtual volumes. A TDVV is a Thinly Provisioned Virtual Volume (TPVV) with in-line data deduplication.

A TDVV has the same characteristics as a TPVV, with the additional capability of removing duplicated data before it is written to the volume. TDVVs are managed like any other TPVV. A TDVV must be associated with Common Provisioning Groups (CPG) that are created on Solid State Drives (SSD). For more information about TDVVs, see Thinly-Deduplicated Virtual Volumes (TDVV) on page 48.

Physical Copies

A physical copy is a full copy of a volume. The data in a physical copy is static; it is not updated with subsequent changes to the parent volume. The parent volume is the original volume that is copied to the destination volume. The parent volume can be a base volume, volume set, virtual copy, or physical copy.

A physical copy can be created only from a parent volume with enough free space to accommodate writes to that volume during the physical copy operation. Physical copies can be online physical copies or offline physical copies.

For online physical copies, the destination volume is automatically created and can be exported immediately. Offline physical copies require a destination volume with a user space size at least as large as the user space of the base volume being copied. Offline physical copies cannot be exported.

For additional information about physical copies, see Physical copies on page 49.

Virtual Copy Snapshots

A snapshot is a point-in-time virtual copy of a base volume. The base volume is the original volume that is copied.

Unlike a physical copy, which is a duplicate of an entire volume, a virtual copy only records changes to the base volume. This allows an earlier state of the original virtual volume to be restored, by starting with the current state of the virtual copy and rolling back all changes that have been made since the virtual copy was created.

You can create thousands of snapshots of each virtual volume, assuming that there is sufficient storage space available. You can make snapshots of:

- FPVVs
- TPVVs
- Physical copies
- Another virtual copy snapshot

For additional information on virtual copies, see Virtual copy snapshots on page 50.

Exporting Virtual Volumes

For a host to see a virtual volume, the volume must be exported as a logical unit number (LUN). Volumes are exported by creating virtual volume–LUN (VLUN) pairings on the system.
When you create VLUNs, the system produces both VLUN templates that establish export rules and active VLUNs that the host sees as a LUN or attached disk device. For more information about active VLUNs, VLUN templates, and VLUN template types, see Exporting virtual volumes on page 53.

HPE 3PAR software products and features

The following HPE 3PAR software products and features are available for HPE 3PAR StoreServ Storage systems. For more detailed information about all HPE 3PAR software suites and standalone software applications, see the QuickSpecs for your product at http://www.hpe.com/info/3par/.

- **HPE 3PAR Operating System Software**—independent instances of the HPE 3PAR OS running on each controller node.
- **HPE 3PAR File Persona Software**—provides file services and object access on the StoreServ creating a converged block, file, and object access storage solution.
- **HPE 3PAR Access Guard Software**—provides volume security at logical and physical levels by enabling you to secure hosts and ports to specific virtual volumes.
- **HPE 3PAR Data Encryption**—provides data encryption for HPE 3PAR StoreServ arrays using self-encrypting drives. See Data encryption on page 63.
- **HPE 3PAR Full Copy Software**—thin-aware, point-in-time clones with independent service-level parameters that can be rapidly resynchronized with base volumes as needed.
- **HPE 3PAR Rapid Provisioning Software**—instant application-tailored volume provisioning.
- **HPE 3PAR Autonomic Rebalance Software**—provides analysis for how volumes on the system use physical disk space and make intelligent, autonomic adjustments to ensure optimal volume distribution when new hardware is added to the system.
- **HPE 3PAR Thin Copy Reclamation Software**—reclaims space when snapshots are deleted from an HPE 3PAR StoreServ Storage system. As snapshots are deleted, the snapshot space is reclaimed from a TPVV or FPVV and returned to the CPG for reuse by other volumes. To learn more about HPE 3PAR thin copy reclamation, see Enhanced storage applications on page 57.
- **HPE 3PAR Persistent Ports Software**—eliminates the dependency on multipath software during the process of online software upgrades. Persistent ports enable the host paths to remain online during the online upgrade process and maintaining host I/O with no disruptions. Persistent ports are also called virtual ports.
- **HPE 3PAR Persistent Cache Software**—maintain a high level of performance and availability during node failure conditions, and during hardware and software upgrades. This feature allows the host to continue to write data and receive acknowledgments from the system if the backup node is unavailable. Persistent cache automatically creates multiple backup nodes for LDs that have the same owner. Persistent cache also maintains service levels by preserving write-caching through rapidly remirroring the cache to other nodes in the cluster, in case of a cache or controller node failure.
- **HPE 3PAR System Tuner Software**—improves performance by identifying overused physical disks and performing load balancing on those disks without interrupting access. To learn more about the HPE 3PAR System Tuner, see Enhanced storage applications on page 57.
- **HPE 3PAR Thin Provisioning Software**—allocate virtual volumes to application servers while provisioning only a fraction of the physical storage behind these volumes. By enabling a true capacity-on-demand model, a storage administrator can create TPVVs that maximize asset use. To learn more about TPVVs, see Virtual Volumes on page 46.
- **HPE 3PAR Thin Conversion Software**—converts an FPVV to a TPVV. Virtual volumes with large amounts of allocated but unused space are converted to TPVVs that are much smaller than the original volume. To use the thin conversion feature, you must have an HPE 3PAR StoreServ storage system. To learn more about HPE 3PAR thin conversion, see Enhanced storage applications on page 57.
- **HPE 3PAR Thin Persistence Software**—minimizes the size of TPVVs and read/write snapshots of TPVVs by detecting pages of zeros during data transfers and not allocating space for the zeros. This feature works in real time, and analyzes the data before it is written to the destination TPVV or read/write snapshot of the TPVV. To use the thin persistence feature, you must have an HPE 3PAR
StoreServ storage system. To learn more about HPE 3PAR thin persistence, see Enhanced storage applications on page 57.

- **HPE 3PAR EVA to HPE 3PAR Online Import Software**—manages the migration of data from a source EVA storage system to a destination HPE 3PAR StoreServ Storage system. You can migrate EVA virtual disks and host configuration information to an HPE 3PAR StoreServ destination system without changing host configurations or interrupting data access.

- **HPE 3PAR Service Processor Software**—the service processor can be deployed as a virtual machine or as a physical server. It functions as the communication interface between your IP network and HPE 3PAR Central by managing all service-related communications.

- **StoreServ Management Console (SSMC)**—The GUI for monitoring, managing, and configuring HPE 3PAR StoreServ Storage systems.

- **HPE 3PAR Command Line Interface Software**—the CLI for monitoring, managing, and configuring HPE 3PAR StoreServ Storage systems.

- **HPE 3PAR Web Services API Software**—application programming interface for incorporating the storage infrastructure into your platform, for end-to-end automation of your service delivery and management.

- **HPE 3PAR SmartStart Software**—simplifies system startup and guides the administrator through configuration of HPE 3PAR StoreServ Storage, HPE 3PAR Service Processor, and production application hosts.

- **HPE 3PAR Host Explorer Software**—automates host discovery and collection of detailed host configuration information critical to speeding storage provisioning and simplifying maintenance.

- **HPE 3PAR Autonomic Groups Software**—allows domains, hosts, and volumes to be grouped into a set that is managed as a single object. Autonomic groups allow for easy updates when new hosts are added or new volumes are provisioned. If you add a new host to the set, volumes from the volume set are autonomically provisioned to the new host with no administrative intervention. If you add a new volume or a new domain to a set, the volume or domain inherits all the rights of the set.

- **HPE 3PAR mySnapshot Software**—designed for non-storage professionals (such as database administrators, software developers, and test engineers) to copy and provision their own test data. With mySnapshot, users have instant access to test data, thus eliminating the time required to request, justify, and receive these copies from the storage administrator. To learn more about the mySnapshot, see HPE 3PAR mySnapshot on page 67.

- **HPE 3PAR Policy Server Software**—provides flexibility and control to allow or deny outbound communications or remote service connections to and from HPE 3PAR StoreServ Storage systems at the customer site and HPE 3PAR Central.

- **HPE 3PAR ODM 3.1 Software for IBM MPIO and Veritas VxDMP**—standalone software that delivers a highly available, robust, and trouble-free multipathing solution for IBM AIX deployments.

- **HPE 3PAR Multipath IO Software for Microsoft Windows 2003**—enables the host to use more than one physical I/O path to the system. Multipathing improves system reliability and availability by providing fault-tolerance and load balancing for I/O traffic.

- **HPE 3PAR ODM Software for Veritas VxVM**—an application for customers using Veritas VxVM/DMP with HPE 3PAR storage devices. It provides HPE 3PAR device definitions and a message catalog.

- **HPE 3PAR NULL INF for SCSI Enclosure Device**—HPE 3PAR NULL driver for Windows Server 2003 is used to add WHQL signature for Windows Server 2003 environments so that the storage system can be recognized without triggering an “unknown device” message.

- **HPE 3PAR Dynamic Optimization Software**—improves the performance of virtual volumes without interrupting access. Use this feature to avoid over-provisioning for peak system usage by optimizing the layout of your virtual volumes. You can change virtual volume parameters, RAID levels, set sizes, and disk filters by associating the virtual volume with a new CPG. You can also use this feature to analyze your entire system and automatically correct space usage imbalances in the system for optimal performance. To learn more about HPE 3PAR Dynamic Optimization, see Enhanced storage applications on page 57.

- **HPE 3PAR Adaptive Flash Cache**—accelerates random read workloads by improving read response time by as much as double and reducing latency. This feature effectively extends the system cache without adding more physical memory. Creating more cache space from your SSDs allows the StoreServ to dynamically and flexibly accelerate read intensive workloads. Adaptive Flash Cache
includes a simulation feature that helps determine the amount of flash that a system requires for random read acceleration. To learn more about HPE 3PAR Adaptive Flash Cache, see HPE 3PAR Adaptive Flash Cache software on page 59.

- **HPE 3PAR Thin Deduplication**—eliminates duplicated data on your SSDs. Before data is written to a TDVV, the data is compared to all other TDVVs associated with the same CPG. Any duplicated data is detected by the byte level comparison, and not written to the volume. To learn more about HPE 3PAR Thin Deduplication, see Thinly-Deduplicated Virtual Volumes (TDVV) on page 48.

- **HPE 3PAR Adaptive Optimization Software**—provides a much higher degree of control over disk usage by reserving faster and more expensive storage resources for data that is frequently accessed, and relegating occasionally accessed data to slower and less expensive drives. To learn more about HPE 3PAR Adaptive Optimization, see Enhanced storage applications on page 57.

- **HPE 3PAR Peer Motion Software**—load balance I/O workloads across HPE 3PAR StoreServ Storage systems, perform seamless technology refresh, cost-optimize asset life cycle management, and lower technology refresh capital expenditure.

- **HPE 3PAR Priority Optimization Software**—set service level targets/guarantees to application workload so that applications are guaranteed I/O quality of service, and control any interference between applications.

- **HPE 3PAR Virtual Copy Software**—take instant virtual copy snapshots of existing volumes. This feature uses copy-on-write technology so that virtual copies consume minimal capacity. Virtual copies are available to any host with read and write capabilities. In addition, virtual copies can be made from other virtual copies, providing flexibility for test, backup, and business-intelligence applications. To learn more about virtual copies, see Virtual copy snapshots on page 50.

- **HPE 3PAR Remote Copy Software**—a host-independent, array-based, data-mirroring solution that enables affordable data distribution and disaster recovery for applications. With this optional software, you can copy virtual volumes from one system to a second system. HPE 3PAR Remote Copy is configured and controlled with the HPE 3PAR CLI. For more information about the HPE 3PAR Remote Copy application, see the HPE 3PAR Remote Copy Software User Guide.

- **HPE 3PAR Peer Persistence Software**—enables federation of HPE 3PAR StoreServ Storage systems at geographically separated data centers, and allows applications to move and failover from one site to another without any application downtime.

- **HPE 3PAR GeoCluster Software**—simplifies and automates disaster recovery, reducing administration time and improving recovery time objectives (RTOs) in Windows-based environments.

- **HPE 3PAR Virtual Domains Software**—is used for access control. Virtual domains allow you to limit the access of users to subsets of volumes and hosts in a Hewlett Packard Enterprise storage system, and ensure that virtual volumes associated with a specific domain are not exported to hosts outside of that domain. To learn more about domains, see HPE 3PAR Virtual Domains on page 28.

- **HPE 3PAR Virtual Lock Software**—enforces the retention period of any volume or copy of a volume. To learn more about virtual lock, see Enhanced storage applications on page 57.

- **HPE 3PAR System Reporter Software**—monitor performance, create charge back reports, and plan storage resources for systems using either a standard web browser or the HPE 3PAR System Reporter Excel client.

- **HPE 3PAR Info Software**—a command line that provides useful information on the volume mapping between the host and the array.

- **HPE 3PAR Management Plug-in for VMware**—a web application that is deployed as a vSphere Client plug-in. A vSphere Client plug-in is an external web application that is configured with the vCenter Server so that vSphere Clients can display their pages. HPE 3PAR Management Plug-In for VMware vCenter displays virtual volume mapping for easy identification of HPE 3PAR volumes used by virtual machines and datastores.

- **HPE 3PAR Recovery Manager for VMware vSphere Software**—provides virtual copy management of HPE 3PAR virtual copies and recovery of virtual machines and datastores.

- **HPE 3PAR VASA Provider Software**—enables VMware vCenter to see the capabilities of HPE 3PAR storage LUNs and their properties, such as RAID level, TPVVs, FPVVs, VMware Virtual Volumes (VVol), and replication state automatically. The HPE 3PAR VASA Provider also allows for management of VMware VVols from the vSphere environment, creating and removing virtual volumes automatically when VMs are added or removed from the array’s VVol storage container.
• **HPE 3PAR VAAI Plug-in Software for VMware vSphere Software**—enables SCSI primitives that allow HPE 3PAR StoreServ Storage systems to take advantage of several VMware virtual machine operations at the metadata level to improve performance.

• **HPE 3PAR VMware Site Replication Manager (SRM) Adapter Software**—site replication adapter integrated with VMware SRM and HPE 3PAR Remote Copy software. This feature enables organizations to build resilient virtual and cloud computing infrastructures, protect applications at a lower cost, and recover data more quickly and efficiently than with traditional disaster recovery solutions.

• **HPE 3PAR Recovery Manager for Windows Hyper-V Software**—offers key management capabilities and facilitates the integration of HPE 3PAR Virtual Copy and Microsoft Hyper-V Virtual Machine environment.

• **HPE 3PAR Recovery Manager for Oracle Software**—a highly efficient solution for automatically creating and managing hundreds of application-consistent, reservationless, point-in-time snapshots of Oracle and Oracle RAC databases for rapid online recovery.

• **HPE 3PAR Recovery Manager for SQL Server Software**—integrates with Microsoft VSS to provide a simple, efficient, and highly scalable solution for backup and recovery of SQL Server environments. HPE 3PAR Recovery Manager Software intelligently creates, manages, and presents time-consistent snapshot images of SQL Server databases for nondisruptive backup, rapid application recovery, and data sharing.

• **HPE 3PAR VSS Provider for Microsoft Windows Software**—a server application bundled with HPE 3PAR Recovery Manager for Microsoft SQL Server. VSS coordinates the actions of database readers like the HPE 3PAR Recovery Manager backup application, database writers like Microsoft Exchange and SQL Server, and providers that create shadow copies.
HPE 3PAR software licensing

HPE 3PAR introduces a new All-inclusive licensing model for software. The **HPE 3PAR All-inclusive Software License** is offered as an alternative to the traditional spindle-based licensing model.

All existing HPE 3PAR customers of hardware and software products with spindle-based license model will be supported by HPE 3PAR OS. Any hardware and software upgrade will require the customers to switch to the new All-inclusive software license paradigm. The new licensing scheme is array/frame based in comparison to the traditional license which was drive/spindle based.

### Types of HPE 3PAR All-inclusive Software License

The HPE 3PAR All-inclusive software license can be broadly divided into three categories:

- **All-inclusive Single-System software license** — All HPE 3PAR software licenses pertaining to the functions of a single HPE 3PAR array are referred to as All-inclusive Single-System software. The various software included come pre-licensed on the storage controller and no individual software license needs to be purchased separately.

- **All-inclusive Multi-System software license** — All HPE 3PAR software licenses pertaining to the functioning of multiple HPE 3PAR arrays is available as part of the All-inclusive Multi-System software. The multi-array functionality includes but is not restricted to functionalities such as replication, federation, and disaster recovery. This license is an array/frame license and if needed, must be purchased once for every array that participates in the configuration.

- **Data-at-Rest Encryption software license** — If security is desired in the storage array, an additional array/frame license called the Data-at-Rest Encryption license is required.

### All-inclusive Single-System HPE 3PAR Software License

HPE 3PAR software bundled with the controller under the All-inclusive Single-System software pertains to a single array. The HPE 3PAR All-inclusive Single-System software can be broadly classified into four sub-categories. The sub-categories are as follows:

- HPE 3PAR Operating System software
- HPE 3PAR Optimization software
- HPE 3PAR Speciality software
- HPE Recovery Manager Central App suite

The complete list of software included in the All-inclusive Single-System software license is shown in the following tables:

#### Table 1: HPE 3PAR OS software list

<table>
<thead>
<tr>
<th>HPE 3PAR OS software</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>System Reporter</td>
<td>Rapid Provisioning</td>
<td>Adaptive Flash Cache</td>
<td>Full Copy</td>
</tr>
<tr>
<td>HPE 3PARInfo</td>
<td>Autonomic Groups</td>
<td>Persistent Cache</td>
<td>Thin Provisioning</td>
</tr>
<tr>
<td>Online Import license (1 year)</td>
<td>Autonomic Replication Groups</td>
<td>Persistent Ports</td>
<td>Thin Copy Reclamation</td>
</tr>
<tr>
<td>System Tuner</td>
<td>Autonomic Rebalance</td>
<td>Management Console</td>
<td>Thin Persistence</td>
</tr>
</tbody>
</table>

*Table Continued*
## HPE 3PAR OS software

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Explorer</td>
<td>LDAP Support</td>
</tr>
<tr>
<td>Multi Path IO SW</td>
<td>Access Guard</td>
</tr>
<tr>
<td>VSS Provider</td>
<td>Host Personas</td>
</tr>
<tr>
<td>Scheduler</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Web Services API</td>
</tr>
<tr>
<td></td>
<td>Thin Conversion</td>
</tr>
<tr>
<td></td>
<td>Thin Deduplication for SSD</td>
</tr>
<tr>
<td></td>
<td>HPE 3PAR OS Administration Tools</td>
</tr>
<tr>
<td></td>
<td>• CLI client</td>
</tr>
<tr>
<td></td>
<td>• SNMP</td>
</tr>
</tbody>
</table>

## Table 2: HPE 3PAR Optimization software list

<table>
<thead>
<tr>
<th>Optimization type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamic Optimization</td>
<td></td>
</tr>
<tr>
<td>Adaptive Optimization</td>
<td></td>
</tr>
<tr>
<td>Priority Optimization</td>
<td></td>
</tr>
</tbody>
</table>

## Table 3: HPE 3PAR Speciality software list

<table>
<thead>
<tr>
<th>Speciality software</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Persona</td>
<td></td>
</tr>
<tr>
<td>Smart SAN</td>
<td></td>
</tr>
<tr>
<td>Virtual Copy</td>
<td></td>
</tr>
<tr>
<td>Virtual Domain</td>
<td></td>
</tr>
<tr>
<td>Virtual Lock</td>
<td></td>
</tr>
<tr>
<td>Online Import</td>
<td></td>
</tr>
</tbody>
</table>

## HPE 3PAR All-inclusive Multi-System Software License

All HPE 3PAR software licenses pertaining to the functioning of multiple HPE storage arrays is available as part of the HPE 3PAR All-inclusive Multi-System software. This license is an array/frame license and if needed is required to be purchased once for every array that participates in the configuration.

The list of software included in the All-inclusive Multi-System software license is as follows:

## Table 4: HPE Recovery Manager Central App Suite

<table>
<thead>
<tr>
<th>App Suite</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vSphere</td>
<td></td>
</tr>
<tr>
<td>MS Hyper-V</td>
<td></td>
</tr>
<tr>
<td>MS Exchange</td>
<td></td>
</tr>
<tr>
<td>MS SQL</td>
<td></td>
</tr>
<tr>
<td>Oracle</td>
<td></td>
</tr>
<tr>
<td>SAP HANA</td>
<td></td>
</tr>
</tbody>
</table>

## Table 5: All-inclusive Multi-System HPE 3PAR Software

<table>
<thead>
<tr>
<th>Peer Motion (PM)</th>
<th>Peer Resistance (PR)</th>
<th>Remote Copy (RC)</th>
<th>Cluster Extension Windows (CLX)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

16  HPE 3PAR All-inclusive Multi-System Software License
Data-at-rest encryption software license

Data-at-rest encryption is designed to protect your archived data. An array/frame license called the Data-at-Rest Encryption license is required.

The following StoreServ Storage arrays and disk drives and HPE 3PAR OS are supported for use as an encrypted array.

NOTE:
All supported HPE 3PAR OS versions must have a valid Encryption license to enable encryption.

Storage Arrays

All HPE 3PAR StoreServ Storage arrays support encryption.

• HPE 3PAR StoreServ 7000 Series
• HPE 3PAR StoreServ 8000 Series
• HPE 3PAR StoreServ 9000 Series
• HPE 3PAR StoreServ 10000 Series
• HPE 3PAR StoreServ 20000 Series

For each of the listed HPE 3PAR StoreServ arrays to support encryption, the array must be populated with encryption supported disk drives and cannot have a mix of encrypted and non-encrypted.

Supported HPE 3PAR OS

The following HPE 3PAR OS versions are supported along with supported hardware components:

• HPE 3PAR OS 3.1.2 MU2 and later—Supported SED disk drives and Local Key Manager
• HPE 3PAR OS 3.1.3 MU1 and later—Supported FIPS SED disk drives
• HPE 3PAR OS 3.2.1 and later—Supports Enterprise Secure Key Manager

To learn more, see the HPE 3PAR StoreServ Data-At-Rest Encryption white paper.

HPE 3PAR All-inclusive Software Matrix

The following is a matrix that showcases the HPE 3PAR StoreServ models, the All-inclusive Single-System and All-inclusive multi-system licensed software and the Data-at-Rest encryption software:
### Table 6: HPE 3PAR All-inclusive Software Matrix

<table>
<thead>
<tr>
<th>Software</th>
<th>Licensing for 7000, 8000, 9000, 10000, 20000 and future HPE 3PAR models</th>
<th>Delivered As</th>
</tr>
</thead>
<tbody>
<tr>
<td>All-inclusive single system software</td>
<td>HPE 3PAR OS Suite</td>
<td>Software bundled into Base Controller</td>
</tr>
<tr>
<td></td>
<td>Dynamic Optimization, Adaptive Optimization, Priority Optimization</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Virtual Domains, Virtual Lock, Online Import</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Recovery Manager Central App Suite</td>
<td></td>
</tr>
<tr>
<td></td>
<td>File Persona</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Smart SAN</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Virtual Copy</td>
<td></td>
</tr>
<tr>
<td>All-inclusive Multi-System software</td>
<td>Peer Motion, Remote Copy, Peer Persistence &amp; Cluster Extension Windows</td>
<td>One Frame license per array participating in federation or replication group</td>
</tr>
<tr>
<td>Software license for titles requiring more than a single array</td>
<td>Frame License LTU</td>
<td></td>
</tr>
<tr>
<td>Data at Rest Encryption</td>
<td>Frame License LTU</td>
<td>One Frame license per array</td>
</tr>
</tbody>
</table>

**HPE 3PAR Transition License (Old to New)**

Existing HPE 3PAR customers under the spindle-based licensing scheme can transition to the new All-inclusive software licensing scheme at their own pace. They can continue to maintain their current environment as long as they want, and transition to a new license scheme when they are ready. The process is simple and can be achieved through the purchase and application of a transition license.

The Transition license will be needed under the following conditions:

- When an existing customer purchases new drives or controller nodes.
- When an existing customer purchases the All-inclusive Multi-System software.
- When an existing customer purchases any HPE 3PAR software that is not already licensed.

When applying the transition license, the following things are expected:

- Unlimited license for all software included in the All-inclusive Single-System software is made available.
- Unlimited license for all software titles not included in the All-inclusive Single-System software but already licensed in the array is made available.

For example, a customer has a Remote Copy license but not a Peer Persistence license. When the transition license is applied, it would enable unlimited license for Remote Copy but not for Peer Persistence, Peer Motion, or CLX.

The following diagram illustrates the install-based transition license:
Figure 2: Install-Based Transition License
HPE 3PAR StoreServ storage system users

To access an HPE 3PAR StoreServ storage system, you must have a user account.

User account roles

Each HPE 3PAR OS user account is assigned a role, and each role is assigned a set of rights. The roles and rights assigned to the user determine which tasks the user can perform with a system. Assign roles to users based on the tasks you intend the users to perform.

Nine roles are defined in the HPE 3PAR OS. See the following table for a description of each role.

There are four standard roles:

- Browse
- Edit
- Super
- Service

There are also five extended roles:

- Create
- Basic Edit
- 3PAR AO
- 3PAR RM
- Audit

There is no functional difference between standard and extended roles. The extended roles define a set of rights optimized for users with specialized or restricted tasks. For example, assigning the Create role allows the user to create virtual volumes and other objects, but does not allow the user to remove virtual volumes.

To maintain greater control over your system, assign users roles with the minimum set of rights they need to perform their tasks. To view a list of roles and the rights assigned to each role, see the HPE 3PAR OS Command Line Interface Reference.

User management tasks can be performed with either the HPE 3PAR CLI or the StoreServ Management Console (SSMC). See the HPE 3PAR Command Line Interface Administrator Guide or the SSMC Online Help for instructions on how to perform user management tasks.

<table>
<thead>
<tr>
<th>User Roles</th>
<th>Rights assigned to roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Browse</td>
<td>Rights are limited to read-only access.</td>
</tr>
<tr>
<td>Edit</td>
<td>Rights are granted to most operations; for example, creating, editing, and removing virtual volumes and other objects.</td>
</tr>
<tr>
<td>Super</td>
<td>Rights are granted to all operations.</td>
</tr>
<tr>
<td>Service</td>
<td>Rights are limited to operations required to service the system. Allows limited access to user information and user group resources.</td>
</tr>
<tr>
<td>Create</td>
<td>Rights are limited to creating objects; for example, virtual volumes, CPGs, hosts, and schedules.</td>
</tr>
<tr>
<td>Basic Edit</td>
<td>Rights are similar to the Edit role. For example, creating and editing virtual volumes and other objects. The rights to remove objects are more restricted for the Basic Edit role than for the Edit role.</td>
</tr>
</tbody>
</table>

Table Continued
### User Roles

<table>
<thead>
<tr>
<th>Role</th>
<th>Rights assigned to roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>3PAR AO</td>
<td>Rights are limited to internal use for Adaptive Optimization operations.</td>
</tr>
<tr>
<td>3PAR RM</td>
<td>Rights are limited to internal use for Recovery Manager operations.</td>
</tr>
<tr>
<td>Audit</td>
<td>Rights are limited to scanning the 3PAR OS for security issues. An audit user has no access to the CLI.</td>
</tr>
</tbody>
</table>

### Local user authentication and authorization

Users accessing the HPE 3PAR StoreServ Storage system with the HPE 3PAR CLI client or Secure Shell (SSH) connections are authenticated and authorized directly on the system. These users are referred to as local users. The information used to authenticate and authorize a local user is stored on the system.

For instructions on creating a local user, see the *HPE 3PAR Command Line Interface Administrator Guide* and the SSMC Online Help.

### LDAP user authentication and authorization

An LDAP user is authenticated and authorized using information from a Lightweight Directory Access Protocol (LDAP) server. If multiple systems are configured to use the same LDAP server, a user who can access one system can access all systems with the role and rights assigned to the LDAP group.

Local user roles and rights are associated with an individual user. LDAP user roles and rights are the same for all members of the group. If you want to authenticate and authorize LDAP users with different roles, you must create an LDAP group for each role.

For detailed information about LDAP users and LDAP connections, see *Lightweight Directory Access Protocol* on page 24. For instructions on setting up an LDAP connection, see the *HPE 3PAR Command Line Interface Administrator Guide*.

### Domain user access

A domain user is a user with access to a specific domain. Local users who belong to a system that uses HPE 3PAR Virtual Domains software are domain users.

In addition to the user’s roles and rights, a domain user’s activities are also limited to the domains to which they have access. A domain user’s assigned user role is applicable only within the domain to which the user has access.

For information about virtual domains and domain users, see *HPE 3PAR Virtual Domains* on page 28. For instructions on creating a domain user, see the *HPE 3PAR Command Line Interface Administrator Guide* and the SSMC Online Help.

### Strong passwords

The industry-wide use of static vendor-only service user passwords is not advised in today’s security- and compliance-aware sites. This functionality replaces those types of passwords in StoreServ systems.

The following topics explain the strong password functionality in HPE 3PAR operating systems beginning with the HPE 3PAR OS 3.3.1 release. There are two modes of support:

- Time-based passwords
- Encrypted ciphertext passwords
Time-based passwords

Time-based passwords are unique to each service user account and StoreServ. They change at the top of each hour and can only be generated in the Hewlett Packard Enterprise support center to authorized Hewlett Packard Enterprise employees and contractors. If you are operating in time-based mode, you cannot manually change passwords since they change automatically each hour.

NOTE:

If a user is logged in, the session continues even though the password is changed at the top of the hour.

If you choose time-based passwords, you do not need to change your Hewlett Packard Enterprise support processes. Service personnel from Hewlett Packard Enterprise can acquire the password when needed, without your interaction.

Encrypted ciphertext passwords

Encrypted ciphertext passwords are created at random on the StoreServ for each service user account. You can change these passwords any time; however, the passwords are not known to you or to Hewlett Packard Enterprise. Recovery is only possible by exporting the ciphertext for transmission to Hewlett Packard Enterprise, where an authorized support center user can decrypt the ciphertext to provide the password to on-site Hewlett Packard Enterprise service personnel or contractors.

If you choose encrypted ciphertext passwords, you need to export the ciphertext and provide it to the Hewlett Packard Enterprise personnel working with you. The ciphertext is pasted into a tool at Hewlett Packard Enterprise that can unwrap and decrypt the ciphertext to recover the password. After the support activity is complete, you can change the password so that the recovered password is no longer valid.

Exporting ciphertext

In the encrypted ciphertext mode, use the controlrecoveryauth ciphertext <user> command to export the ciphertext for a service account. The user will be the service account requested by the service personnel. This command displays the ciphertext associated with the specified service user account. You can copy and paste that ciphertext into an email to the Hewlett Packard Enterprise support center or to the Hewlett Packard Enterprise support engineer who is working with you.

The ciphertext is protected from exposure if you email it. The random credential contained in the ciphertext is first encrypted and is then wrapped using a public key. This makes the ciphertext secure for transmission, because only the corresponding private key at Hewlett Packard Enterprise can unwrap the encrypted credential.

Changing the ciphertext password

To change passwords in encrypted ciphertext mode, use the controlrecoveryauth rollcred <user> command. This command causes a new random ciphertext string to be generated for the specified service user account. This ciphertext string will need to be exported using the process under Exporting ciphertext, to obtain the new password for that user account.

The two accounts that are affected are root and console. On the StoreServ, these user accounts are not used for most maintenance actions.

Setting or changing the password mode

To query or change the current setting of the strong service account password system, use the HPE 3PAR CLI command controlrecoveryauth (to change the mode from time-based to encrypted ciphertext, for example).
• To query the current mode, use the command `controlrecoveryauth status`.
• To change the mode, use the command `controlrecoveryauth setmethod [totp|ciphertext]`, choosing either totp (time-based passwords) or ciphertext.
Lightweight Directory Access Protocol

Lightweight Directory Access Protocol (LDAP) is a standard protocol for communication between LDAP clients and LDAP directory servers. Data is stored as a directory hierarchy by the server, and clients add, modify, search, or remove the data. The data can be organized by using standard schemas understood by clients and servers from different vendors, or by using an application-specific schema that is used only by a particular vendor or application.

The HPE 3PAR OS contains an LDAP client that can be configured to use an LDAP server for authentication and authorization of system users. In an environment where there are multiple systems configured to use the same LDAP server in the same way, a single user with access to one system server can access all systems in the environment.

Accessing objects on systems configured to use HPE 3PAR Virtual Domains Software requires access to the domain in which those objects reside. The configuration of domains may differ from one system installation to the next. This results in differing levels of access to objects based on mapping between the LDAP configuration and domain configuration of the individual system.

The HPE 3PAR LDAP client is designed to work with various LDAP servers and schemas for data organization. The Active Directory LDAP directory implementation is supported for use by the HPE 3PAR LDAP and Red Hat Enterprise Server 5.5 client.

Active Directory

Active Directory (AD) is an implementation of Lightweight Directory Access Protocol (LDAP) directory services by Microsoft for use in Windows environments. An Active Directory server is both an LDAP and Kerberos server. The Active Directory server and Kerberos server are used for both authorization and authentication of users when Active Directory is set up for SASL binding (see SASL binding on page 26).

OpenLDAP

OpenLDAP is an open source implementation of Lightweight Directory Access Protocol (LDAP) directory services developed by the OpenLDAP Project. OpenLDAP includes a server, client library, and tools that are available for a wide variety of operating systems. Different schemas can be used for user and group information with OpenLDAP. For example, the Posix schema is typically used for user and group information in Linux/Unix systems.

LDAP users

Users created with the HPE 3PAR CLI who access the system using HPE 3PAR CLI clients, or with SSH, are authenticated and authorized directly on the system. These users are referred to as local users. A Lightweight Directory Access Protocol (LDAP) user is similar to a local user; however, an LDAP user is authenticated and authorized using information from an LDAP server.

⚠️ CAUTION:

Do not create local and LDAP users with the same user name. If local and LDAP users have the same user name, it can cause confusion about where access is controlled.

During authentication, if a username is not recognized as a local user, that user’s name and password are checked on the LDAP server. The local user’s authentication data takes precedence over the user’s LDAP authentication data. User names not associated with local user names are authenticated using LDAP data.
Additionally, for local users, the password supplied by the user during authentication must match the password assigned when that user was initially created or modified. The rights assigned to the user during authorization are the same rights associated with the user role that was assigned when that user was initially created or modified. For additional information about user roles and rights, see HPE 3PAR StoreServ storage system users on page 20.

LDAP users can access the system using the same methods as local users, although some user account creation and modification operations are unavailable. For instructions on using LDAP with the storage system, see the HPE 3PAR Command Line Interface Administrator Guide.

Another key difference between local users and LDAP users is that a local user’s rights to the system are assigned on a case-by-case basis. An LDAP user’s rights depend on that user’s group association. In other words, groups are assigned specific rights to the system, and an individual LDAP user’s rights depend on group membership.

LDAP server data organization

Lightweight Directory Access Protocol (LDAP) server data consists of user information, which includes the user’s group associations. Data can be existing data used for user account information or data created for specific use with systems. Data on the LDAP server can be organized in two different ways:

- As a list of groups associated with each user.
- As a list of users associated with each group.

The form in which data is organized depends on the type of LDAP server used and the tools used to maintain the data. Programs such as ldp.exe, which is a downloadable Windows Support Tool available from Microsoft, and ldapsearch, which is available for many UNIX and Linux systems, can be used to view data entries in the LDAP server. This can be useful when configuring the HPE 3PAR LDAP client with your LDAP server, as discussed in the “Managing User Accounts and Connections” chapter in the HPE 3PAR Command Line Interface Administrator Guide.

LDAP and domains

Lightweight Directory Access Protocol (LDAP) is also available for systems that use virtual domains for access control. As discussed in HPE 3PAR Virtual Domains on page 28, by using domains, rights to system objects, such as volumes and hosts, can be specifically defined. Accessing objects on systems configured to use virtual domains requires rights in the domain in which those objects reside. Because domains can be configured differently within a Hewlett Packard Enterprise storage system, or from one server to another (in configurations with multiple servers), a user can have different rights to domains in a single system, or across multiple systems.

As discussed in LDAP users on page 24, LDAP users must follow a process of authentication and authorization to gain access to the system. With domains in use, LDAP users must also be authorized to access domains set up within the system. For additional information, see LDAP authentication and authorization on page 25.

For instructions on setting up LDAP users on systems using domains, see “Managing User Accounts and Connections” in the HPE 3PAR Command Line Interface Administrator Guide.

LDAP authentication and authorization

The user’s user name is first checked against the authentication data stored on the local system. If the user’s name is not found, the LDAP authentication and authorization process proceeds as follows:

- The user’s user name and password are used to authenticate with the LDAP server.
- The user’s group memberships are determined from the data on the LDAP server.
- A list of groups is compared against mapping rules that specify each group’s associated roles.
If virtual domains are in use, the user’s group is mapped to a domain.
The user is assigned a system user role and a domain, if domains are in use.

**LDAP authentication**

Users are authenticated with the LDAP server by using a bind operation. The bind operation authenticates the HPE 3PAR OS LDAP client to the LDAP server. This authentication process is required for all systems that use LDAP, including systems using domains. Several binding mechanisms are supported by the HPE 3PAR OS LDAP client.

---

**NOTE:**

The binding mechanism you can use depends on your LDAP server configuration.

---

**Simple binding**

With simple binding, the user’s user name and password are sent to the LDAP server in plain text, and the LDAP server determines whether the submitted password is correct.

Simple binding is not recommended unless a secure connection to the LDAP server is established with secure sockets layer (SSL) or transport layer security (TLS).

**SASL binding**

The HPE 3PAR OS LDAP client also supports the following Simple Authentication and Security Layer (SASL) binding mechanisms: PLAIN, DIGEST-MD5, and GSSAPI. Generally, DIGEST-MD5 and GSSAPI are more secure methods of authentication, because user passwords are not sent to the LDAP server.

- The PLAIN mechanism is similar to simple binding where the user’s username and password are sent directly to the LDAP server for authentication. As with simple binding, the PLAIN mechanism should be used only if there is a secure connection (SSL or TLS) to the LDAP server.
- The GSSAPI mechanism obtains a ticket from the Kerberos server which validates the user’s identity. That ticket is then sent to the LDAP server for authentication.
- With the DIGEST-MD5 mechanism, the LDAP server sends the HPE 3PAR OS LDAP client one-time data that is encrypted by the client and returned to the server in such a way that the client proves it knows the user’s password without having to send the user’s password.

**LDAP authorization**

After a Lightweight Directory Access Protocol (LDAP) user has been authenticated, the next stage is authorization. The authorization process determines what a user is allowed to do within the system.

As discussed in LDAP users on page 24, an LDAP user’s role is tied to that user’s group membership, and a user can belong to multiple groups. Each group has an assigned role. For information about user roles, see HPE 3PAR StoreServ storage system users on page 20. The HPE 3PAR OS LDAP client performs group-to-role mapping using the following mapping parameters:

- super-map
- service-map
- edit-map
- browse-map
- create-map
- basic_edit-map
- HPE 3PAR_AO-map
- HPE 3PAR_RM-map

Each group of which a user is a member is compared against the mapping parameters. Mapping occurs sequentially. A group is first compared to the super-map parameter; if no match is made, the group is
then compared with the service-map parameter, and so on. For example, if a match is made for group A with the super-map parameter, a user who belongs to group A is authorized with Super rights to the system.

With this process, a user can be authenticated, but that user is not authorized if no group membership exists. In this case, the user is subsequently denied access to the system.

**Authorization on systems using virtual domains**

As discussed in **LDAP authorization** on page 26, a user’s group association determines that user’s role within the system. On systems using virtual domains, the user’s groups are mapped to system domains. Therefore, the user’s role within a specific group extends to the domains mapped to that group. For instructions on authorizing LDAP users on systems using domains, see “Managing User Accounts and Connections” in the *HPE 3PAR Command Line Interface Administrator Guide*.

The group-to-domain mapping relationship is shown in **Figure 3: Group-to-Domain Mapping Relationship** on page 27:

- LDAP User 1 has membership in Group B.
- Group-to-role mapping determines that Group B uses the Edit role.
- Group-to-domain mapping establishes a match between Group B and Domain A.
- LDAP User 1 has Edit role access to all objects in Domain A.

![Figure 3: Group-to-Domain Mapping Relationship](image)
HPE 3PAR Virtual Domains

To set up the HPE 3PAR StoreServ Storage system, the system administrator creates and assigns user roles and rights in the system. You can create, modify, or remove a user’s access to HPE 3PAR Virtual Domains Software in the system with either the HPE 3PAR CLI or the StoreServ Management Console (SSMC). See the HPE 3PAR Command Line Interface Administrator Guide or the SSMC Help for instructions on performing these tasks.

In addition to the security provided by this hierarchical user structure, more defined control of access to the system can be achieved by implementing virtual domains.

Domains allow an administrator to create up to 1,024 domains, or spaces, within a system, where each domain is dedicated to a specific application. A subset of the system users have assigned rights over the domains. Domains can be useful in scenarios where a single system is used to manage data from several different independent applications.

![Figure 4: Single System Managing Multiple Independent Applications](image)

Each domain allows users varying levels of accessibility to domain objects. A domain contains CPGs, hosts, Remote Copy groups, and derived domain objects, such as virtual volumes, LDs, and volume exports (VLUNs). Because objects are domain-specific, domain users cannot export virtual volumes to hosts outside of their assigned domain.

Virtual domains can be grouped into autonomic groups that can be managed as one domain. If you have a group of domains that require the same administrative procedures, it is easier to group those domains into an autonomic group and manage them together.

**Domain types**

When using domains for access control, accessibility to basic objects and derived objects is limited by a user’s role and domain assignment. For more information about roles and rights, see HPE 3PAR StoreServ storage system users on page 20.

The first tier of access control is the domain to which a subset of a system’s objects belong. The objects can be assigned to a specific domain, or have no domain association.

- The no domain contains objects that do not belong to any specified domains. For example, objects in an existing system that did not previously use domains do not belong to any domain.
- The specified domains are created by the domain administrator and contain objects specific to that domain. Only users with rights for that domain can work with those objects. For example, user A in domain A can access objects in domain A, but not in domain B. Multiple specified domains can be created.
Users and domain rights

By default, users with the Super role, and users belonging to the Edit user role in the all domain, can create and edit CPGs, hosts, and Remote Copy groups, and can assign CPGs and hosts to specified domains. Additionally, these users have access to all domains and their objects.

When setting up domains and users in the system, some users may require access to multiple domains with different user rights. Virtual domains allow users access to more than one domain, and a single user can be assigned different user roles in each domain.

NOTE:
A user having rights in multiple domains cannot perform operations between objects in different domains. Users can have access to a maximum of 32 domains.

Object and domain association rules

Domains contain basic objects such as CPGs, hosts, and Remote Copy groups, and derived objects such as virtual volumes, LDs, and VLUNs. Objects and their associations with domains must adhere to the following rules:

- Objects derived from a CPG inherit the domain of that CPG.
- Virtual volumes can be exported only to hosts that belong to the virtual volumes’ domain.
- A VLUN inherits the domain of the virtual volume and host from which the VLUN was exported.

Default and current domains

When a user is created, the user is able to access objects in all assigned domains. The user can browse or edit objects, depending on the user’s assigned user role. For example, an Edit user assigned to Domains A and B can view and work on objects in both Domains A and B (see Figure 5: Edit user access to domains on page 29). However, if it is apparent that a specific domain will receive the majority of attention from a user, virtual domains allow administrators to set a default domain for that user.

Figure 5: Edit user access to domains

An HPE 3PAR CLI user’s default domain is the domain that the user accesses at the start of each CLI session. For example, if you have Edit rights to domains A and B, and your default domain has been set to domain A, each time you start a new CLI session, you view and work with only objects in domain A. The user’s default domain can be set or reset at any time by the administrator.

If you are using the SSMC, the user selects which domain to access. There is no default domain and no domain session. To change domains, SSMC users simply select a new domain from a menu of available domains.
The HPE 3PAR StoreServ Storage system sees a host as a set of initiator port World Wide Names (WWN) or iSCSI names.

Hosts that are physically connected to ports on the system are automatically detected. The FC port WWNs and iSCSI port iSCSI names are displayed by the user interfaces. You can also add new WWNs or iSCSI names for unestablished host paths and assign them to a host before they are physically connected. These WWNs or iSCSI names do not need to be associated with target ports on the system controller nodes. This allows for plug-and-play functionality that avoids the need for manual reconfiguration after connecting new hosts. For instructions on modifying system ports and host configurations, see the HPE 3PAR Command Line Interface Administrator Guide and StoreServ Management Console (SSMC) Online Help.

FC over Ethernet (FCoE) connectivity is supported on the HPE 3PAR StoreServ Storage systems with the use of converged network adapters (CNA). CNA ports can be configured for use as FCoE or iSCSI ports.

A virtual volume can be exported, or made accessible, to one or more hosts. The host sees the exported virtual volume as a LUN connected to one or more ports. After the virtual volume is exported to a host, the host can send requests to the LUN. See Virtual Volumes on page 46 for more information about virtual volumes and exporting virtual volumes. For instructions on exporting virtual volumes, see the HPE 3PAR Command Line Interface Administrator Guide and SSMC Online Help.

Persistent ports (also called virtual ports) allow the HPE 3PAR StoreServ Storage system host-facing ports to assume the identity of partner ports that are automatically designated by the system. For iSCSI, FC, and FCoE ports, this is achieved by using N_Port ID Virtualization (NPIV). For more information about persistent ports and NPIV, see the HPE 3PAR Command Line Interface Administrator Guide.

NOTE:
Refer to the relevant HPE 3PAR implementation Guide for recommended practices and detailed configuration information about using your specific host devices with the system.

About ports

System controller nodes can use FC, Gigabit Ethernet, and iSCSI, and FCoE ports to connect the storage system to your network, host computers, storage system components, and to other systems. Serial Attached SCSI (SAS) ports are only used to connect system components. You can use the HPE 3PAR CLI or the SSMC to view port information and modify port settings. For instructions on viewing and modifying port configurations, see the HPE 3PAR Command Line Interface Administrator Guide and SSMC Online Help.

- **FC ports**—Systems use FC ports to connect controller nodes to hosts and drive cages and drive enclosures. On HPE 3PAR StoreServ 7000 and 10000 Storage systems, FC ports are designated for host connection and Remote Copy use only.
- **iSCSI ports**—Systems use iSCSI ports to connect controller nodes to hosts. The iSCSI ports in a system controller node can only be used to connect the system to a host computer.
- **Gigabit Ethernet ports**—Systems use Gigabit Ethernet ports to enable the Remote Copy over Internet Protocol (RCIP) solution and to connect the primary and secondary systems in the Remote Copy pair. For information about Remote Copy, see the HPE 3PAR Remote Copy Software User Guide.
- **SAS ports**—Systems use SAS ports to connect controller nodes to drive enclosures. SAS ports are supported only on HPE 3PAR StoreServ 7000, 8000, 9000, and 20000 Storage systems.
- **FCoE Ports**—Systems use FCoE ports to run FC as a connectivity protocol directly over Ethernet, in parallel with regular IP traffic (as opposed to using Ethernet exclusively for TCP/IP networks and FC.
Port target, initiator, and peer modes

The system controller node ports operate in different modes. Depending on the type of port, the port may operate in target, initiator, or peer mode.

FC ports use the following firmware mode settings:
- Target mode for ports that connect to hosts and receive commands from those hosts.
- Initiator mode for ports that connect to the system physical disks and send commands to those disks.
- Initiator mode for Remote Copy over FC (RCFC).

iSCSI ports use the following firmware mode setting:
- Target mode for ports that connect to hosts and receive commands from those hosts.

Gigabit Ethernet ports use the following firmware mode setting:
- Peer mode for Ethernet ports, used for RCIP.

FCoE ports use the following firmware mode setting:
- Target mode for ports that connect to hosts and receive commands from those hosts.

File Persona ports use the following firmware mode setting:
- Target mode for ports that connect to hosts and receive commands from those hosts.

Use the HPE 3PAR CLI or the SSMC to view or change the current port mode settings. For instructions on viewing or changing mode settings, see the HPE 3PAR Command Line Interface Administrator Guide and SSMC Online Help.

Active and inactive hosts

An active host is a host that is connected to a system port and recognized by the HPE 3PAR OS. Under normal operation, an active host may have a number of volumes exported to it and therefore the host has access to those volumes.

An inactive host is a host that is known to the HPE 3PAR OS but is not recognized as being connected to any system port at the moment. This inactivity may be because the host is disconnected from the system port, because the host is offline, or because of an error condition such as link failure.

When a host on a system port becomes inactive for any reason, the following happens:
- The HPE 3PAR OS recognizes that the host is missing on the port and changes the state of the host from active to inactive.
- The VLUNs become templates until the host returns. They do not remain in an active state while the host is unavailable.
- When the host reappears on the same port, the VLUNs are converted from a template to an active state.

Adding and removing hosts

The HPE 3PAR OS administration tools allow you to create, modify, and remove FC and iSCSI host paths and their properties. When you create a new host, you can assign WWNs or iSCSI names. A virtual volume that is exported to a host is exported to all the WWNs that make up the host. If you need to export virtual volumes to particular host computer WWNs or iSCSI names, you can create separate hosts on the system and assign each WWN or iSCSI name to its own host. Use the HPE 3PAR CLI or the SSMC to create, modify, and remove hosts.
Hosts can be grouped into autonomic groups that can be managed as a single host. If you have a group of hosts that require the same administrative procedures, it is easier to group those hosts into an autonomic group and manage them together. For instructions on creating, modifying, and removing hosts, see the *HPE 3PAR Command Line Interface Administrator Guide* and the SSMC Online Help.

Managing host personas

A host persona is a set of behaviors that allows hosts that are connected to FC, iSCSI, or FCoE ports on the system to deviate from the default host behavior. By assigning a persona to a host, multiple host types that require distinct customized responses can share a single system port. For example, hosts that run Microsoft Windows, Linux, and AIX operating systems can all connect to the same system port. This simplifies connecting hosts to the system and reduces management costs related to complex host connections.

A host persona defines the custom responses for certain iSCSI commands and does not affect any of the FC port settings. Host personas are tied to the host name and identified by the host persona number. You can set the host persona number when the host is created, or modify it later. Use the HPE 3PAR CLI commands or the StoreServ Management Console (SSMC) to display host personas. For instructions about displaying, creating, modifying, and removing host personas, see the SSMC online help.

Different host personas have different functions and support different host operating systems. The specific host persona is designated by the host persona number. Depending on the selected host persona number, the following additional capabilities are supported:

- **UARepLun**—Sends a unit attention when the VLUNs are added to or removed from the LUN list.
- **ALUA**—Enables the asymmetric logical unit access (ALUA) command and asymmetric state change unit attention when path counts change due to adding or removing ports in the host definition.
- **VolSetAddr**—Enables HP-UX Volume Set Addressing (VSA).
- **SoftInq**—Enables inquiry data formats for hosts such as Egenera and NetApp.
- **NACA**—Enables the Normal Auto Contingent Allegiance (NACA) bit for AIX.
- **SESLun**—Enables iSCSI Enclosure Services (SES) LUN ID 254 for Host Explorer agent support.
- **SubLun**—Enables SCSI two-level LUN addressing.
- **LUN0SCC**—Enables a SCSI Command Controller at LUN 0 for HP-UX and OpenVMS systems.
- **WSC**—Enables inquiry responses to support Windows systems.

**NOTE:**

Each host connected to the system must use a host persona with the SESLun enabled, or the Host Explorer agent cannot communicate with the system.

**Table 7: Host personas and capabilities** on page 33 describes the specific functionality for each host persona number. For a list of supported host operating systems, go to the following website:

[SPOCK](http://www.hpe.com/storage/spock)
### Table 7: Host personas and capabilities

<table>
<thead>
<tr>
<th>No.</th>
<th>Name</th>
<th>Host OS</th>
<th>Additional Capabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Generic</td>
<td>Linux, Windows, and Solaris</td>
<td>UARepLun, SESLun</td>
</tr>
<tr>
<td>2</td>
<td>Generic-ALUA</td>
<td>Linux, Windows, and Solaris</td>
<td>UARepLun, ALUA, SESLun</td>
</tr>
<tr>
<td>6</td>
<td>Generic-Legacy</td>
<td></td>
<td>None</td>
</tr>
<tr>
<td>7</td>
<td>HPUX-Legacy</td>
<td>HP-UX</td>
<td>VolSetAddr, Lun0SCC</td>
</tr>
<tr>
<td>8</td>
<td>AIX-Legacy</td>
<td>AIX</td>
<td>NACA</td>
</tr>
<tr>
<td>9</td>
<td>Egenera</td>
<td>Egenera, NetApp</td>
<td>SoftInq</td>
</tr>
<tr>
<td>10</td>
<td>NetApp ONTAP</td>
<td>Data ONTAP</td>
<td>SubLun, ALUA</td>
</tr>
<tr>
<td>11</td>
<td>VMware</td>
<td>Linux and Windows</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>OpenVMS</td>
<td></td>
<td>UARepLun, RTPG, SESLun, Lun0SCC</td>
</tr>
</tbody>
</table>

*Table Continued*
<table>
<thead>
<tr>
<th>Persona Number, Name, and Host OS</th>
<th>Additional Capabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>No.: 13</td>
<td>UARepLun, VolSetAddr, SESLun, ALUA, Lun0SCC</td>
</tr>
<tr>
<td>Name: HPUX</td>
<td></td>
</tr>
<tr>
<td>Host OS: HP-UX</td>
<td></td>
</tr>
<tr>
<td>No.: 15</td>
<td>UARepLun, SESLun, ALUA, WSC</td>
</tr>
<tr>
<td>Name: WindowsServer</td>
<td></td>
</tr>
<tr>
<td>Host OS: Windows</td>
<td></td>
</tr>
</tbody>
</table>

**NOTE:**
- Only the Generic, Generic-ALUA, and Generic-Legacy personas are supported for iSCSI connections.
- The NetApp host operating system requires unique WWNs for hosts in an FC fabric.
- A host device must use either iSCSI, FC, or FCoE connections. Mixed ports are not supported on a single device.

**Legacy host personas**
A legacy host persona is a host persona that simulates the behavior of a port persona.

Prior to the HPE 3PAR OS 2.3.1 release, port personas were used on system ports. Port personas are no longer supported.

Use the HPE 3PAR CLI commands or the SSMC to convert your legacy host personas to new host personas. See the [HPE 3PAR Command Line Interface Administrator Guide](#) or the SSMC Online Help for instructions on converting your legacy host personas.

**Host Explorer Software agent**
The HPE 3PAR Host Explorer Software agent is a program that runs on a host that is connected to a Hewlett Packard Enterprise storage system. The Host Explorer agent runs as a service on Windows and as a daemon on Linux and Solaris operating systems.

The Host Explorer agent communicates with the system over an FC or iSCSI connection and enables the host to send detailed host configuration information to the system. The information gathered from the Host Explorer agent is visible for uncreated hosts, and assists with host creation and diagnosing host connectivity issues.

When a host is created on the system, unassigned WWNs or iSCSI names are presented to the system. Without the Host Explorer agent running on the attached hosts, the system is unable to determine to which host the WWN or iSCSI name belongs, and you must manually assign each WWN or iSCSI name to a host. With Host Explorer agents running, the system automatically groups WWNs or iSCSI names for the host, to assist with creating the host.

The Host Explorer agent collects the following information and sends it to the system:
- Host operating system and version
- FC and iSCSI HBA details
- Multipath driver and current multipath configuration
- Cluster configuration information
You can install the Host Explorer agent from the HPE 3PAR Host Explorer CD. For instructions on installing and using the Host Explorer agent, see the *HPE 3PAR Host Explorer User's Guide*. For a list of supported host operating systems, go to the SPOCK website:

http://www.hpe.com/storage/spock
Chunklets

Physical disks are divided into chunklets. When a physical disk is admitted to the system, it is divided into chunklets that become available to the system. Some chunklets are used by LDs. Other chunklets are designated as spares, to hold relocated data during a disk failure or during maintenance procedures.

Creating, moving, and removing chunklets and spares can only be performed with the HPE 3PAR CLI. See the HPE 3PAR Command Line Interface Administrator Guide for instructions on performing these tasks.

To view chunklets and spares, use either the HPE 3PAR CLI or the StoreServ Management Console (SSMC). See the HPE 3PAR Command Line Interface Administrator Guide or the SSMC Online Help for instructions on performing this task.

Physical disk chunklets

Each chunklet occupies contiguous space on a physical disk.

Space on a physical disk is allocated as follows:

- All chunklets are 1 GB.
- 256 MB of space is reserved for the table of contents (TOC), which contains the internal description of the system. The TOCs on all physical disks in the system contain the same information.
- 4 MB of space is reserved for diagnostic use—2 MB beginning after the TOC and 2 MB from the end of the disk logical block address.
- One or more chunklets are allocated as spares. Any chunklet can be reserved as a spare, but the system setup script selects those chunklets as close to the end of the physical disk’s logical block space as possible.
- The remainder of the disk can be used for LDs.

Spare chunklets

Some chunklets are identified as spares when the system is first set up at installation. Data from other chunklets is moved or reconstructed to these spare chunklets in response to a chunklet or disk failure or when a drive magazine must be serviced. This initial spare storage is equal to the amount of storage in a single drive magazine, using the largest size physical disks.

How spare chunklets work:

- When a connection is lost to a physical disk or a physical disk fails, all future writes to the disk are automatically written to a logging LD until the physical disk comes back online, or until the time limit for logging is reached. Logging disk space is allocated when the system is set up. This does not apply to RAID 0 chunklets, which have no fault-tolerance.
- If the time limit for logging is reached, or if the logging LD becomes full, the relocation of chunklets on the physical disk to free chunklets designated as spares starts automatically. Free chunklets are any chunklets that are not already allocated for use by LDs.
- For automatic relocations, the system uses up to a maximum of one disk worth of chunklets per system node.
- When selecting a target chunklet for relocation, the system attempts to identify a local spare chunklet, a local free chunklet, a remote spare chunklet, and finally, a remote free chunklet.

**NOTE:**

Local chunklets are chunklets on disks whose primary path is connected to a node that owns the LD that contains the chunklets being relocated.
• If the system uses up its free or spare chunklets for relocation, an alert is generated.
• When the spare and free chunklets are used up, automatic relocation no longer occurs. In most cases, some data redundancy is lost. The system also generates an alert.
Logical disks

A Logical Disk (LD) is a collection of physical disk chunklets arranged as rows of RAID sets. Each RAID set is made up of chunklets from different physical disks. LDs are pooled together in Common Provisioning Groups (CPG), which allocate space to virtual volumes. Creating CPGs maps out the data layout parameters for creating LDs.

LDs are created automatically by the system when virtual volumes are created from CPGs. The RAID type, space allocation, growth increments, and other LD parameters can be set when you create a CPG, or can be modified after you create a CPG. For information about CPGs, see Common Provisioning Groups on page 43.

Logical disks and common provisioning groups

A CPG establishes a virtual pool of LDs that can grow on demand. When you create virtual volumes, the system creates all underlying LDs for you automatically.

Volumes associated with a CPG draw LD space from the virtual pool, allocating space on demand. As the volumes that draw from a CPG require additional storage, the system automatically creates additional LDs and adds them to the pool. After you create a CPG, you can add and remove LDs. You can also specify advanced LD parameters when you create CPGs. This allows you to exercise a greater degree of control over how the system creates LDs in the CPG.

Logical disk types

The following LD types provide storage space to virtual volumes:

- User LDs provide user storage space to virtual volumes. The user space contains the user data and is exported as a LUN to the host.
- Snapshot data LDs provide the storage space for snapshots or virtual copies. The snapshot space contains copies of user data that changed since the previous snapshot of the volume was created.
- Snapshot administration LDs provide the storage space for snapshot administration. The administration space is used to track changes to the volume since the previous snapshot was created.

The system sets aside LDs for logging, for preserved data, and for system administration. These LDs are multilevel LDs with three-way mirrors for enhanced redundancy and performance. The following LD types are created by the system:

- Logging LDs are RAID 10 LDs that are used to temporarily hold data during disk failures and disk replacement procedures. Logging LDs are created by the system during the initial installation and setup of the system. Depending on the system model you have, each controller node in the system has a 20 GB or 60 GB logging LD.
- Preserved data LDs are RAID 10 LDs used to hold preserved data. Preserved data LDs are created by the system during the initial installation and setup of the storage system. The size of the preserved data LD is based on the amount of data cache in the system.

When multiple disk failures during write operations leave data suspended in cache memory, the system temporarily preserves this data by writing it to a preserved data LD. By doing so, the system clears the data cache, and prevents the data cache from locking up and leading to wider system failures. When the
destination LDs become available again, the system automatically writes the preserved data from the preserved data LDs to the destination LDs.

- Administration volume LDs provide storage space for the admin volume, a single volume created on each system during installation. The **admin volume** is used to store system administrative data such as the system event log.

**RAID types**

The HPE 3PAR storage system supports the following RAID types:

- RAID 0
- RAID 10 (RAID 1)
- RAID 50 (RAID 5)
- RAID MP (Multi-Parity) or RAID 6

**RAID 0**

On a RAID 0 LD, data is striped across rows of chunklets on different physical disks. The number of chunklets in a RAID 0 set is the set size, which is always 1 for a RAID 0 LD. The number of sets in a row is the row size. The system accesses data from a RAID 0 LD in step sizes, where the step size is the number of contiguous bytes that the system accesses before moving on to the next chunklet. A RAID 0 LD improves performance but provides no fault-tolerance.

**Figure 6: Data striped across chunklets on a RAID 0 LD** on page 39 shows a RAID 0 LD with a set size of 1 and a row size of 3.

**RAID 1 and RAID 10**

On a RAID 10 LD, data is striped across RAID 1 (or mirrored) sets. A RAID 1 set is made up of two or more chunklets that contain the same data. The chunklets in each set are distributed across different physical disks, which may be located in different drive magazines or even different drive cages. The number of chunklets in a RAID 1 set is the set size, or mirror depth. The number of sets in each row is the row size. The maximum row size is 40.

The system accesses data from a RAID 10 LD in step sizes. A step size is the number of contiguous bytes that the system accesses before moving on to the next chunklet. A RAID 1 set can function with the loss of all but one of the chunklets in the set.

**Figure 7: Data striped across RAID 1 sets on a RAID 10 LD** on page 40 shows a RAID 10 LD with a set size of 2 and a row size of 3 in two rows:
RAID 5 and RAID 50

On a RAID 50 LD, data is striped across rows of RAID 5 sets. A RAID 5 set, or parity set, must contain at least three chunklets. A RAID 5 set with three chunklets has a total of two chunklets of space for data and one chunklet of space for parity. RAID 5 set sizes with between 3 and 9 chunklets are supported. The data and parity steps are striped across each chunklet in the set. The chunklets in each RAID 5 set are distributed across different physical disks, which may be located in different drive magazines or even different drive cages. The number of sets in a row is the row size.

The system accesses the data from a RAID 50 LD in step sizes. The step size is the number of contiguous bytes that the system accesses before moving on to the next chunklet. A RAID 5 set can function with the loss of any one of the chunklets in the set.

**Figure 8: Data striped across RAID 5 sets on a RAID 50 LD** on page 41 shows a RAID 50 LD with a set size of 3, and 2 sets in 1 row:
RAID MP or RAID 6

On a RAID MP or RAID 6 LD, data is striped across rows of RAID MP sets. A RAID MP set, or double-parity set, must contain at least 8 chunklets. A RAID MP set with eight chunklets has a total of six chunklets of space for data and two chunklets of space for parity. RAID MP set sizes of eight and 16 chunklets are supported. The data and parity steps are striped across each chunklet in the set. The chunklets in each RAID MP set are distributed across different physical disks, which may be located in different drive magazines or even different drive cages. The number of sets in a row is the row size. The system accesses the data from a RAID MP LD in step sizes. The step size varies and is dependent on the size of the RAID MP set. A RAID MP set can function with the loss of any two of the chunklets in the set.

The following example shows 2 RAID MP sets in one row, the second set is shown below the first set. In the first RAID MP set in the following example, p0 is the parity step for data steps F, L, M, Q, T, V, and X. 

Figure 8: Data striped across RAID 5 sets on a RAID 50 LD

Figure 9: Data striped across RAID MP sets on a RAID MP LD on page 42 shows a RAID MP LD with a set size of 8, and 2 sets in 1 row:
Figure 9: Data striped across RAID MP sets on a RAID MP LD

Logical disk size and RAID types

All systems round up so that the LD size is divisible by the size of one chunklet, 1 GB. The total size of the LD is determined by the number of data chunklets in the RAID set.

- A RAID 0 or RAID 1 LD must contain at least one chunklet.
- A RAID 5 set, or parity set, must contain at least three chunklets. A RAID 5 set with three chunklets has a total of two chunklets of space for data and one chunklet of space for parity. The system default is four chunklets: three for data and one for parity (3+1).
- A RAID MP set (RAID 6), or double-parity set, must contain at least eight chunklets. RAID MP set sizes of eight and 16 chunklets are supported. The system default is eight chunklets. A RAID MP set with eight chunklets has a total of six chunklets of space for data and two chunklets of space for parity (6+2). On StoreServ 10000 and StoreServ 7000 systems, RAID 6 set sizes of (4+2), (6+2), (8+2), (10+2), and (14+2) are supported.

NOTE:
The system also rounds up the size of virtual volumes, CPGs, and CPG growth increments to be divisible by the size of one chunklet, 1 GB.
Common Provisioning Groups

A CPG creates a virtual pool of Logical Disks (LD) that allows virtual volumes (VV) to share the CPG’s resources and allocate space on demand. You can create Fully Provisioned Virtual Volumes (FPVV) and Thinly Provisioned Virtual Volumes (TPVV) that draw space from the LD pool on the CPG.

CPGs enable fine-grained, shared access to pooled logical capacity. Instead of dedicating LDs to volumes, the CPG allows multiple volumes to share the buffer pool of LDs. For example, when a TPVV is running low on user space, the system automatically assigns more capacity to the TPVV by mapping new regions from LDs in the CPG associated with that TPVV. As a result, any large pockets of unused but allocated space are eliminated. FPVVs cannot create user space automatically, and the system allocates a fixed amount of user space for the volume.

By default, a CPG is configured to grow new LDs automatically when the amount of available LD space falls below a configured threshold. The initial buffer pool of LDs starts at a fraction of the exported virtual capacity of mapped volumes and automatically grows as required by application writes.

CPGs can be created by using either the HPE 3PAR CLI or the StoreServ Management Console (SSMC). See the HPE 3PAR Command Line Interface Administrator Guide or the SSMC Online Help for instructions on performing these tasks.

For more information about TPVVs and FPVVs, see Virtual Volumes on page 46.

Precautions and planning

A CPG creates a virtual pool of LDs that allows thousands of volumes to share the CPG resources and allocate space on demand. The maximum number of CPGs depends on your system configuration.

To learn about the maximum number of CPGs and volumes supported on your system, go to the Single Point of Connectivity Knowledge (SPOCK) website http://www.hpe.com/storage/spock.

Growth increments, warnings, and limits

You can create several types of volumes that draw space from the CPG LD pool. When creating a CPG, set a growth increment and an optional growth warning and growth limit to restrict the CPG growth and maximum size. It is important to plan the CPG growth increment, growth warning, and growth limit carefully and then continue to monitor the CPG closely over time.

By default, the growth warning and growth limit are set to none, which effectively disables these safety features.

⚠️ CAUTION:

Use caution in planning CPGs. The system does not prevent you from setting growth warnings or growth limits that exceed the amount of currently available storage on a system. When volumes associated with a CPG use all space available to that CPG, any new writes to TPVVs associated with the CPG will fail and snapshot volumes associated with the CPG may become invalid or stale. Under these conditions, some host applications do not handle write failures gracefully and may produce unexpected failures.

Growth increment

As volumes that draw from a CPG require additional storage, the system automatically creates additional LDs according to the CPG growth increment. The default and minimum growth increments vary according to the number of controller nodes in the system, as shown in the following table:
A larger growth increment is sometimes desirable; however, a smaller growth increment can prevent the CPG from automatically allocating too much space. The optimal growth increment depends on several factors:

- Total available space on your system
- Nature of the data running on the system
- Number of CPGs in the system
- Number of volumes associated with those CPGs
- Anticipated growth rate of the volumes associated with the CPGs

**NOTE:**
The system may round up when LDs are created to support virtual volumes and CPGs, resulting in a discrepancy between the user-specified size or growth increment and the actual space allocated to LDs created by the system.

### Growth warning

When the size of the volumes that draw from a CPG reach the CPG growth warning, the system generates an alert. This safety mechanism provides the opportunity to take early action that may prevent snapshot volumes associated with the CPG from experiencing failures, causing host or application write failures, and exhausting all free space on the system.

When you set growth warnings for CPGs, it is critical to consider the number of CPGs on the system, the total capacity of the system, and the projected rate of growth for all volumes on the system.

The storage system does not prevent you from setting growth warnings that exceed the total capacity of the system. For example, on a 3 TB system you can create two CPGs that each have a growth warning of 2 TB. However, if both CPGs grow at a similar rate, it is possible for the volumes that draw from the CPGs to consume all free space on the system before either CPG reaches the growth warning threshold.

### Growth limit

If the volumes that draw from a CPG are allowed to reach the CPG growth limit, the system prevents them from allocating additional space. This safety mechanism stops a runaway application or volume from exhausting all free space available to the CPG and causing invalid (stale) snapshot volumes or new application write failures for volumes associated with that CPG. However, the storage system does not prevent you from setting growth limits that exceed the total capacity of the system. For example, on a 4 TB system it is possible to create a CPG with a 5 TB growth limit. Likewise, it is possible to create five CPGs, each with a 2 TB growth limit.

In addition, volumes that draw from a CPG can use only the space available to that CPG based on the CPG LD parameters. For example, if you create a CPG that only uses LDs that belong to controller node 0, when the virtual volumes that draw from a CPG have filled up all space available to that CPG based on its LD parameters, the following will happen:

- New writes to any TPVVs that are mapped to that CPG will return write failures.
- Snapshot volumes mapped to the CPG may become invalid (stale), subject to the virtual copy policy associated with the base volume. For base volumes with a no stale snapshots virtual copy policy, new writes to the base volume will result in write failures.

<table>
<thead>
<tr>
<th>Number of Nodes</th>
<th>Default</th>
<th>Minimum</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>32 GB</td>
<td>8 GB</td>
</tr>
<tr>
<td>4</td>
<td>64 GB</td>
<td>16 GB</td>
</tr>
<tr>
<td>6</td>
<td>96 GB</td>
<td>24 GB</td>
</tr>
<tr>
<td>8</td>
<td>128 GB</td>
<td>32 GB</td>
</tr>
</tbody>
</table>
For base volumes with a stale snapshots virtual copy policy, new writes will cause snapshot volumes to become invalid (stale).

If the volumes that draw from a CPG reach the CPG growth limit, the system generates additional alerts to notify you that all logical capacity for the CPG has been consumed.

System guidelines for creating CPGs

Use the following guidelines to ensure maximum performance and optimal reliability in the volumes supported by those LDs:

- To provide the highest availability, chunklets in the same RAID set should be from different drive cages, and then from different drive magazines.
- Physical disks with fewer used chunklets should be used before physical disks with more used chunklets.
- Chunklets in the same row should be from different physical disks. In other words, a physical disk should not appear twice in the same row.
- Chunklets should belong to a disk that is connected through the primary path to the LD owner node.
- The system should use as many physical disks as possible.
- The load on all physical disks should be balanced.
- The system should use the largest possible row size.

**NOTE:**

The system may round up when creating LDs to support virtual volumes and CPGs, resulting in a discrepancy between the user-specified size or growth increment and the actual space allocated to LDs created by the system. For more information, see Logical disk size and RAID types on page 42.

Volume types associated with CPGs

Once a CPG is created, you can create two types of base volumes that draw from the CPG’s LD pool: TPVVs and FPVVs.

These two volume types draw from the pool in different ways. For information about TPVVs, see Thinly Provisioned Virtual Volumes (TPVV) on page 10. For information about FPVVs, see Fully Provisioned Virtual Volumes (FPVV) on page 9.
Virtual Volumes

Volumes draw their resources from Common Provisioning Groups (CPG), and volumes are exported as
Logical unit numbers (LUN) to hosts. Virtual volumes (VV) are the only data layer visible to hosts. You can
create physical copies or virtual copy snapshots of VVs for use if the original base volume becomes
unavailable. Before creating VVs, you must first create CPGs to allocate space to the VVs. For
information about CPGs, see Common Provisioning Groups on page 43.

You can organize volumes into autonomic groups that can be managed as one volume. If you have a
group of volumes that require the same administrative procedures, it is easier to group those volumes into
an autonomic group and manage them together.

Virtual volumes can be created by using either the HPE 3PAR CLI or the StoreServ Management Console
(SSMC). See the HPE 3PAR Command Line Interface Administrator Guide or the SSMC Online Help for
instructions on performing these tasks.

For the maximum number of virtual volumes and virtual volume copies that can be created with your
specific system configuration, go to the SPOCK website:

http://www.hpe.com/storage/spock

Virtual volume types

There are several types of virtual volumes:

- Fully Provisioned Virtual Volume (FPVV)
- Thinly Provisioned Virtual Volume (TPVV)
- Thinly Deduplicated Virtual Volume (TDVV)
- Administrative Volume

Administrative volumes are created by the system and are for system usage only.

FPVVs, TPVVs, and TDVVs have three separate data components:

- User space is the area of the volume that corresponds to the LD regions in the CPG that are available
to the host. The user space contains the user data and is exported as a LUN to the host.
- Snapshot space, or copy space, is the area of the volume that corresponds to LD regions in the CPG
that contain copies of user data that changed since the previous snapshot. The snapshot space
contains the copy data.
- Administration space, or admin space, is the area of the volume that corresponds to LD regions in the
CPG that track changes to the volume since the previous snapshot was created. The administration
space contains pointers to copies of user data in the snapshot space. Administration space is
managed by the system, not with the tools you use to manage user and snapshot space.

You can increase the size of volumes, the amount of user space, and the amount of snapshot space for
volumes as the requirements increase. If the user space and snapshot space use all available space, the
copy-on-write operation of the Virtual Copy feature will fail. To avoid running out of user space, use
TPVVs to automatically draw more user space from a CPG. The HPE 3PAR OS automatically reclaimed
unused snapshot space from TPVVs and FPVVs and returns the space to the LDs.

For greater administrative flexibility, you can provision the virtual-volume user space and snapshot space
from the same or different CPGs. If the virtual-volume user space and snapshot space are on different
CPGs, the user space remains available to the host if the CPG containing the snapshot space becomes
full. To save time, you can create many identical virtual volumes at one time.

If your system is accessible from an OpenStack cloud, you may see volumes with prefixes indicating that
the volumes were created through the OpenStack cloud. Volumes created through the OpenStack cloud
use the OpenStack Volume (OSV) and OpenStack Snapshot (OSS) prefixes.
Administrative Volumes

As part of installation and setup process, the administrative volume is created on the system. This volume is used by the system to store administrative data such as the system event log. The administrative volume is always named admin. This volume cannot be exported and cannot be removed from the system.

⚠️ CAUTION:

It is strongly recommended that you do not tamper with the admin volume.

Fully-Provisioned Virtual Volumes (FPVV)

A Fully-provisioned Virtual Volume (FPVV) is a volume that uses LDs that belong to a CPG. Unlike TPVVs, FPVVs have a set amount of user space allocated in the system for user data. They require the system to reserve the entire amount of space required by the FPVV whether or not the space is actually used. The FPVV size is fixed, and the size limit is 16 TB. You can set snapshot space allocation limits and usage warnings to help manage the growth of snapshot space.

Thinly-Provisioned Virtual Volumes (TPVV)

A Thinly-provisioned Virtual Volume (TPVV) uses LDs that belong to a CPG. TPVVs associated with the same CPG draw user space from that pool, allocating space on demand in one chunklet increments, beginning with 1 GB for each controller node. As the volumes that draw space from the CPG require additional storage, the system automatically creates additional LDs and adds them to the pool until the CPG reaches the user-defined growth limit that restricts the CPG maximum size. The TPVV volume size limit is 16 TB.

TPVVs can respond to host write requests by allocating space on demand in one chunklet increments, beginning with 1 GB for each controller node. These allocations are adaptive, because subsequent allocations are based on the rate of consumption for previously allocated space. For example, if a TPVV is initially allocated 1 GB for each node, but consumes that space in less than sixty seconds, the next allocation becomes 2 GB for each node. However, if the initial 1 GB is consumed more slowly, the next allocation increment remains at 1 GB for each node.

⚠️ CAUTION:

Use of allocation limits is recommended to prevent consumption of physical raw capacity beyond a tolerable limit. However, you should exercise caution when you set the value of the allocation limit. When the allocation limit is reached, any new writes to TPVVs will fail, or snapshot volumes associated with the CPG may become invalid. Under this condition, some host applications do not handle write failures gracefully and may produce unexpected failures.

⚠️ CAUTION:

Do not allow the volumes that draw from a CPG to exceed the CPG growth limit. Doing so can invalidate snapshot volumes. See Common Provisioning Groups on page 43 for additional cautions and recommendations.

TPVV Warnings and Limits

The TPVV volume size limit is 16 TB. When you create a TPVV, you can set an allocation warning threshold and an allocation limit threshold.
• **Allocation warning threshold**—For volumes capable of allocating space on demand, the user-defined threshold at which the system generates an alert. This threshold is a percentage of the volume's virtual size, the size that the volume presents to the host.

• **Allocation limit threshold**—For volumes capable of allocating space on demand, the user-defined threshold at which writes fail, preventing the volume from consuming additional resources. This threshold is a percentage of the volume’s virtual size, the size that the volume presents to the host.

When you set TPVV allocation warnings and allocation limits, you must take into account the space to be consumed by both the volume’s user data and the snapshot data.

The total amount of snapshot space consumed by a TPVV and its snapshots includes the data written to the base volume and the data written to the snapshots. The size of the data written to the snapshots equals the total writes to the base volume since the oldest existing read-only snapshot was created.

When deciding on the allocation warning and allocation limit thresholds for a TPVV, you can use an estimate of the maximum write rate to compute the snapshot data growth rate.

- If there are no read-only snapshots, and the volume is not a physical copy or used for remote copy, use the maximum write rate as the growth rate.
- If there are read-only snapshots, or if the volume is not a physical copy or used for remote copy, use twice the maximum write rate as the growth rate.
- Set the allocation warning and limit thresholds based on the growth rate and the advance warning you require before the volume reaches its limit, and writes fail.

Use the following formula to generate the allocation warning threshold:

\[
\text{Allocation warning percentage} = \left[ 1 - \frac{n \times \text{write rate} \times \text{warning period}}{\text{volume's virtual size}} \right] \times 100
\]

where the value of \(n\) is as follows:

- For a TPVV without read-only snapshots, and that TPVV is not a physical copy or used for remote copy, \(n=1\).
- For a TPVV with read-only snapshots, or that TPVV is a physical copy or used for remote copy, \(n=2\).

For example, if a 1 TB TPVV with read-only snapshots has a maximum write rate of 1 GB per day and you want 30 days warning prior to that TPVV reaching the allocation limit, use the following calculation for the allocation warning percentage:

\[
\text{Allocation warning percentage} = \left[ 1 - \frac{2 \times 1 \text{ GB per day} \times 30 \text{ days}}{1024 \text{ GB}} \right] \times 100 = 94\%
\]

### Thinly-Deduplicated Virtual Volumes (TDVV)

A Thinly-Deduplicated Virtual Volume (TDVV) is a thinly-provisioned virtual volume with in-line data deduplication. A TDVV has the same characteristics as a TPVV with the additional capability of removing duplicated data before it is written to the volume. A TDVV must be associated with CPGs that are created from Solid State Drives (SSD). Deduplication can be used in StoreSrvs with mixed drive configurations, but TDVVs can only reside on SSDs.

Deduplication allows you to use your SSDs more efficiently. Less drive space is used by TDVVs because there is no redundant data, and the life of SSDs is extended because there are fewer writes to the drives. Before data is written to a TDVV the data is compared to all other TDVVs associated with the same CPG. If any duplicated data is detected by the byte-level comparison it is not written to the volume. The StoreServ maintains a reference of any duplicated data shared by the TDVVs associated with the CPG to maintain performance when deduplication is used.
Compressed Virtual Volumes

Consolidating data in a way that preserves the information while reducing the total amount of storage is the essence of storage compression. To increase space efficiency and consolidate stored data, a new compression feature is available on HPE 3PAR StoreServ's Thinly Provisioned Virtual Volumes (TPVV) and Thinly Deduplicated Virtual Volumes (TDVV). Virtual Volumes can be marked for compression during their creation or an existing Virtual Volume can be updated with the compression feature at run time. Compression is a new feature of HPE 3PAR OS 3.3.1.

When compression is enabled, data pages belonging to the TPVV are compressed using an LZO compression algorithm. Multiple (not necessarily contiguous) pages are compressed together into a single page and written to a backend store. Thus, for a compressed volume, the written size of the volume (the total number of pages written by the application) can be much larger than the actual number of stored pages on the backend.

Deduplicated Virtual Volumes can be compressed as well. When TDVVs are compressed, incoming data is deduplicated. If the incoming data is found to be duplicate data of existing data in the deduplicated group, the new data is not written to the backend storage. Metadata is manipulated to indicate that the new incoming data is duplicate data of existing data. If the incoming data is not duplicate data of existing data in the deduplicated group, the kernel then attempts to compress the incoming data together with other in-flight data belonging to the TDVV. If the compression succeeds, compressed data is written to the backend storage. Otherwise, uncompressed data is written to the backend storage.

Virtual volume online conversion

You can convert existing FPVVVs to TPVVVs and you can convert TPVVVs to FPVVVs on the array without disrupting normal storage system operations and without requiring changes to any host applications that access the virtual volumes. If a TPVV is using most of its allocated storage capacity, you might choose to convert the volume to a fully provisioned volume to increase its storage capacity and allow for continued growth of the volume. When a TPVV reaches approximately 80% of capacity, the incremental benefit of capacity savings versus accelerating performance is weighted towards performance. In addition, converting volumes from thinly-provisioned to fully-provisioned can free up thinly-provisioned capacity for other TPVVVs. Similarly, if an FPVV storage space is largely unused, you might choose to convert it to a TPVV to save storage space.

Converting remote copy virtual volumes and virtual volumes that contain snapshots is not supported. You can, however, convert virtual volumes with snapshots and create a new virtual volume with a new WWN that contains the original LDs and snapshots.

Virtual volumes can be converted by using the HPE 3PAR CLI or the StoreServ Management Console (SSMC). See the HPE 3PAR Command Line Interface Administrator Guide and the SSMC Online Help for instructions on performing these tasks.

For more information, see HPE 3PAR software licensing on page 15.

Physical copies

A physical copy is a full copy of a volume. A physical copy duplicates all the data from one original base volume to a destination volume. Any changes to either volume causes them to lose synchronization with each other, which is corrected by resynchronizing the two volumes as described in the HPE 3PAR Command Line Interface Administrator Guide and the SSMC Online Help.

Physical copies can be created and managed in groups to reduce the number of management tasks. You can create a consistent group of physical copies from a list of virtual volumes, and group physical copies into autonomic groups that are managed as s single physical copy.

A physical copy be created only from a volume with enough free space to accommodate writes to that volume during the physical copy operation. In addition, the destination volume must meet the following conditions:
- It must have snapshot space associated with it.
- It must have at least as much user space as the volume being copied.
- It must not be exported to a host.

For the maximum number of physical copies that can be created with your specific system configuration, go to the SPOCK website:

http://www.hpe.com/storage/spock

---

**Virtual copy snapshots**

A virtual copy is a snapshot of a virtual volume. You can make virtual copies of base volumes, physical copies, or other virtual copies. Virtual copies are created using copy-on-write techniques. Unlike a physical copy, which duplicates the entire base volume, a virtual copy records only the changes to the original volume. This allows an earlier state of the original volume to be recreated by starting with the current state and rolling back all of the changes that have been made since the virtual copy was created.

The maximum number of virtual copies that can be created on a system is determined by the system configuration. For the maximum number of virtual copies that can be created with your specific system configuration, go to the HPE SPOCK website:

http://www.hpe.com/storage/spock

Virtual copies can be created and managed in groups to reduce the number of management tasks. You can create a consistent group of virtual copies from a list of virtual volumes, and group virtual copies into autonomic groups that are managed as a single virtual copy.

---

**NOTE:**

Virtual copies are consistent at the virtual volume level, but not at the host system or application level. In other words, virtual copies only preserve the data that was written on the source virtual volume before the virtual copy is created. Virtual copies do not preserve the data that is resident within the application or system buffers and is not flushed to disk before the virtual copy is created.

Hewlett Packard Enterprise offers optional HPE 3PAR Recovery Manager DBA software to enable application-level consistent snapshots. Contact Hewlett Packard Enterprise Customer Support for more information.

---

**Virtual copy snapshot relationships**

Base volumes are always read/write, but virtual copies can be read/write or read-only. The rules that govern the relationships between a base volume and its virtual copies are based on the difference between read/write and read-only volumes. Architecturally and internally, read-only copies must alternate. You can make a read-only copy of a read/write volume, and you can only make a read/write copy of a read-only volume.
Copy-on-write function

When a virtual volume or snapshot's source volume is written to, the copy-on-write function preserves the data that is to be overwritten. The data is copied to the snapshot space associated with the original virtual volume before the write operation is completed, and a pointer in the administration space points to the copied data.

See **Figure 12: Snapshot tree** on page 52 for an example of a sequence of snapshots.
In Figure 12: Snapshot tree on page 52:

• S0 is the first virtual copy made of BaseVV.
• S2 is the most recent virtual copy.
• Each copy tracks changes made to BaseVV from its own creation date until the next snapshot is made.
• S1.0 can be created at any time after S1 is created.

The relationships between the virtual copies derived from a base volume can be represented as a tree. In the example in Figure 12: Snapshot tree on page 52, the base volume BaseVV is the starting point. In this example, each new virtual copy of the original has its name incremented by 1.

Each copy of a copy has an additional level added to its name: in this example, the first copy of S1 is S1.0, and a copy of S1.0 is S1.0.0. Unlike the automatic snapshots created for physical copies, these snapshots are not assigned names by the system.

NOTE:
The naming convention used in the example is recommended, but it is not enforced by the system. You can name each virtual volume and virtual copy at the time of creation.

The following rules are enforced by the system when you create a snapshot:

• The tree grows in alternating layers of read/write and read-only snapshots. You can only make a read-only copy of a read/write volume, and you can only make a read/write copy of a read-only volume. Since base volumes are always read/write, you can only create read-only copies of a base volume.
• The maximum number of virtual copies that can be created on a system is determined by the system configuration. For the maximum number of virtual copies that can be created with your specific system configuration, go to the SPOCK website: http://www.hpe.com/storage/spock.
• A virtual volume cannot be deleted if a child copy of it exists. For example, S1 cannot be removed unless S1.0, S1.0.0, and S1.0.1 are deleted first.
Copy-of and parent relationships

In the example in Figure 12: Snapshot tree on page 52, there are two different tree structures: the solid arrows show the copy-of relationships, and the dashed arrows show the parent relationship. For example, S0 is a read-only copy of BaseVV, and S1 is the parent of S0. The copy-of relationship shows that the snapshot was created by copying another virtual volume. The parent relationship refers to the internal organization of the administration space. The parent volume contains information to reconstruct the snapshot represented by the child volume. A parent volume can have a creation date after that of its child if the parent volume was modified.

The parent relationship is useful for two reasons:

- Understanding the performance consequences of virtual copies. The tree representing the parent relationship shows the look-up paths in the administration space that are needed to reconstruct the earlier state of the virtual volume. The farther a virtual copy is from the base volume, the longer it will take to retrieve it. If a snapshot is expected to be kept in use for a long time, consider making a physical copy instead of a virtual copy.
- Understanding which virtual copies become stale if the administration space is full and the copy-on-write data cannot be written. A stale snapshot is one that cannot be completely recreated because the most recent changes will not be included. The current snapshot and all its children become stale when a write fails. For example, if there is no space to write the copy-on-write data when a host writes to S1_0, then S1_0, S1_0_1, and S1_0_0 become stale.

Exporting virtual volumes

Virtual volumes are the only data layer component visible to hosts. You export a virtual volume to make it available to one or more hosts by creating an association between the volume and a LUN. The characteristics of this association are defined when you create a VLUN. A VLUN is a pairing between a virtual volume and a LUN, expressed as either a VLUN template or an active VLUN. For the maximum number of VLUNs supported for each host with your specific system configuration, go to the SPOCK website:

http://www.hpe.com/storage/spock

Virtual volumes can be exported with the HPE 3PAR CLI and the SSMC. See the HPE 3PAR Command Line Interface Administrator Guide and the SSMC Online Help for instructions on performing this task.

VLUN templates and active VLUNs

A VLUN template sets up an association between a virtual volume and a LUN-host, LUN-port, or LUN-host-port combination by establishing the export rule. When you create a VLUN template, if the current system state meets the conditions established by the VLUN template, that template is immediately applied to create one or more active VLUNs. These active VLUNs enable virtual volumes to be exported to hosts. If the current system state does not meet the conditions of the VLUN template, no active VLUNs are created until the conditions of the template are met.

After a VLUN template is applied to create one or more active VLUNs, hosts continue to be able to access volumes based on the export rule established by that template. Removing VLUNs associated with a volume stops host access to that volume. Removing all VLUNs for a host stops the host from accessing all volumes.

VLUN template types

A VLUN template sets up an association between a virtual volume and a LUN-host, LUN-port, or LUN-host-port combination by establishing the export rule, or the manner in which the volume is exported. A VLUN template enables the export of a virtual volume as a VLUN to hosts. Those volume exports, which are seen as LUNs by the hosts, are active VLUNs.

A VLUN template can be one of the following types:
• **Host sees**—allows only a specific host to see a volume.
• **Host set**—allows any host that is a member of the host set to see a volume.
• **Port presents**—allows any host on a specific port to see the volume.
• **Matched set**—allows only a specific host on a specific port to see the volume.

**Host sees templates**

A host sees VLUN template allows only a particular host connected to any port to see a virtual volume. The system makes the virtual volume visible as a LUN to all the host WWNs, regardless of which controller node port the WWNs appear on. If the host has more than one WWN, active VLUNs are created for each host WWN. However, for any single host, there can only be one host sees VLUN template for a given LUN.

If a WWN is added to an existing host definition, all virtual volumes that are exported to the host using the host-sees VLUN template are exported to the new WWN. However, WWNs cannot be removed from a host definition if a LUN is exported to the host.

**Host set templates**

A host set VLUN template allows any host that is a member of the host set to see a volume. The system makes the virtual volume visible as a LUN to all the members of the host set. Any hosts added to the host set automatically see the VLUN, provided there are no conflicting LUN IDs. If the added host has an exported LUN ID in the LUN ID range of the host set, the host cannot see the LUN and must be assigned a new ID. If a host is removed from a host set, the removed host loses all rights of the host set and cannot access volumes exported to the host set.

The same virtual volume can be exported as different LUNs on the same or different ports.

⚠️ **CAUTION:**

If the system is operating in Common Criteria mode, there may be security risks with port presents. For more information about Common Criteria, see the *HPE 3PAR Command Line Interface Administrator Guide*.

**Port presents templates**

A port presents VLUN template allows any host connected to a particular port to see a virtual volume. The system makes the virtual volume visible as a LUN to any of the host WWNs that appear on the controller node port. As long as the VLUN template remains on the system, additional active VLUNs are created when the port is attached to additional hosts. However, there can only be one port presents VLUN template per port LUN combination.

The same virtual volume can be exported as different LUNs on the same or different ports.

**Matched set templates**

A matched set VLUN template is a combination of the host sees and port presents template types. A matched set VLUN allows a particular host on a specified port to see a virtual volume. For any single LUN, there can only be one matched set VLUN template with the same host-port combination.
Reclaiming unused space

The HPE 3PAR OS space consolidation features allow you to change the way that virtual volumes (VV) are mapped to logical disks (LD) in a common provisioning group (CPG). Moving VV regions from one LD to another enables you to compact the LDs, and frees up disk space to be reclaimed for use by the system. For more information about virtual volumes, see Virtual Volumes on page 46.

Mapping is the relationship of LD regions to VV regions. VVs are made up of multiple LDs, and each LD contains regions that are mapped to the VV. All types of volumes are created by mapping data from one or more LDs to the VV. The figure shows how data is mapped in regions from LDs to a base volume.

![Figure 13: Mapping regions from LDs to VVs](image)

LDs can be shared by multiple VVs. As volumes are deleted, or as volume copy space grows and then shrinks, LDs use space less efficiently. When LDs do not efficiently use space, the unused space consumes regions on the LD which are not available for use by the system when creating new LDs. You can use the space management features to consolidate used space into fewer LDs, so that unused regions are forced to one or more LDs, which are then deleted. Deleting these LDs frees the unused space for general use by the system.

You can also truncate LDs to free up space. The used regions on the LD are compacted by moving them to the beginning of the LD, and then the LD is shortened so that unused space can be returned to the system’s free chunklet pool.

Reclaiming unmapped LD space from CPGs

CPGs provide a shared pool of LD capacity for use by all virtual volumes that draw space from that pool. See Virtual volume types on page 46 for a discussion of volumes that can draw space from a CPG. If volumes that draw from a CPG are deleted, or if copy space for these volumes grows and then shrinks, the underlying LDs in the CPG pool can become less efficient in space usage. The LDs in the CPG pool may have only a small portion of their regions mapped to existing virtual volumes. However, the unused regions on the LDs are not available for use by the volumes mapped to the CPG. Compacting the LD regions mapped to these volumes may recover and free LD space.

Compacting a CPG allows you to reclaim space from a CPG that has become less efficient in space usage from creating, deleting, and relocating volumes. Compacting consolidates LD space in CPGs in as few LDs as possible. Compacting CPGs can be performed with the HPE 3PAR CLI and the StoreServ Management Console (SSMC). See the HPE 3PAR Command Line Interface Administrator Guide and the SSMC Help for instructions on performing this task.
Reclaiming unmapped LD space from volumes

When multiple identical virtual volumes are created as a result of a single volume creation operation, the underlying LDs that support these volumes are shared by the volume group. If several of the members of that volume group are later deleted, the underlying LDs may become less efficient in the usage of space. One or more LDs shared by the volume group may have only a small portion of their regions mapped to existing virtual volumes. However, their unused regions are not available to the system for use in creating new LDs. Compacting the LD regions mapped to these volumes may recover and free LD space.

You can compact LDs only with the HPE 3PAR CLI. See the HPE 3PAR Command Line Interface Administrator Guide for instructions on performing this task.

You can use the optional HPE 3PAR Dynamic Optimization Software feature to configure volumes to use space more efficiently. To learn about tuning volumes for optimal performance, see Enhanced storage applications on page 57.

Automatically reclaiming unused snapshot space from volumes

The HPE 3PAR OS automatically reclaims unused snapshot and administration space from TPVVs and FPVVs and returns the space to the LDs. The system examines the snapshot and administration space for large areas of unused space. The identified areas are unmapped from the corresponding LD regions and the space is returned to the LDs.

Manually reclaiming unused snapshot space from volumes

You cannot manually remove snapshot and administration space from a TPVV because the HPE 3PAR OS automatically removes any unused space.

Reclaiming dormant snapshot and administration space from an FPVV and returning the space to the LD can only be performed when the volume is not exported to a host, and if there are no snapshots of the volume. Creating physical copies of the volume does not prevent you from reclaiming space.

You can reclaim snapshot space from a virtual volume with the HPE 3PAR CLI and the SSMC. See the HPE 3PAR Command Line Interface Administrator Guide and the SSMC Online Help for instructions on performing this task.

Deleted volume snapshot space

The unused space associated with deleted snapshots of TPVVs and FPVVs is automatically returned to the pool of LDs used by the CPG.

Logical disks and chunklet initialization

After deleting logical disks, the underlying chunklets must be initialized before their space is available to build logical disks. The initialization process for chunklets generally takes about one minute per 1 GB chunklet. To see chunklets that are currently in the process of being initialized, issue the `showpd -c` command. Chunklets that are uninitialized are listed in the Uninit column.
Enhanced storage applications

HPE 3PAR offers several enhanced storage features for managing data and improving system performance. For a list of default HPE 3PAR OS Software Suite features and optional features, see HPE 3PAR software licensing on page 15.

NOTE:
Contact your local service provider to learn about adding optional features to enhance your HPE 3PAR StoreServ Storage systems.

HPE 3PAR File Persona software

With HPE 3PAR File Persona software, you can create a converged storage solution with block and file storage services. This unique solution delivers tightly integrated, converged storage for provisioning both block volumes for server workloads, and file and object shares for client workloads such as home directory consolidation. Truly converged storage management is provided by a single instance of the HPE 3PAR StoreServ Management Console (SSMC) and scriptable HPE 3PAR Command Line. You must have network interface cards that support the File Persona software installed on the StoreServ to use the File Persona software.

There are many advantages to running the HPE 3PAR File Persona software on a StoreServ:

- Block and file services can use a single pool of thinly provisioned storage.
- Autonomic data management services are applied to block and file data.
- Leverages resilient Mesh-Active architecture.
- Leverages the advanced data services of HPE 3PAR OS.

The challenge of managing dispersed directories and folders for file service users on individual personal computers and desktops can be solved with a converged storage solution. You can consolidate user directories into a home directory share, and consolidate user-generated data into group shares for collaboration on the StoreServ.

The File Persona Software Suite is built upon the resilient mesh-active architecture of the HPE 3PAR StoreServ and uses the HPE 3PAR OS wide-striped logical disks and autonomic Common Provisioning Groups (CPG). A CPG can be shared between file and block services to create the file shares or the logical unit numbers (LUN) to provide true convergence.

The HPE 3PAR File Persona architecture is comprised of the following managed objects:

- File Provisioning Groups (FPG) are an instance of the File Persona software and is the highest level file service object in the StoreServ file service hierarchy. It controls how files are stored and retrieved. Each FPG is transparently constructed from one or multiple Virtual Volumes and is the unit for replication and disaster recovery for File Persona Software Suite. Up to 16 FPGs are supported on a node pair. The FPGs contain the Virtual File Servers (VFS).
- A VFS acts as a virtual device used to control many of the network policies for communications between the StoreServ file service objects and your network. A VFS presents virtual IP addresses to clients, participates in user authentication services, and can enforce policies for user and group quota management and antivirus policies. Up to 16 VFSs are supported on a node pair, one for each FPG. Many management tasks and policy decisions can be performed at the VFS level. VFSs contain the file stores.
- File stores are created from VFSs and FPGs. At the file store level you can take snapshots, manage capacity quotas, and customize antivirus scan service policies. Up to 256 file stores are supported on a node pair, and 16 file stores are supported for each VFS.
- The file shares provide data access to clients through SMB, NFS, FTP, and the Object Access API. Multiple file shares can be created for a file store, and at different directory levels within a file store.
Access to home directories and file shares on the StoreServ system is managed by:

- Configuring network ports on the nodes and virtual IP addresses on the VFS.
- Configuring the authentication services to use either Active Directory, LDAP, or local users and group authentication.
- Setting appropriate permissions on the file shares to grant access to users.

File Persona management tasks can be performed with either the HPE 3PAR CLI or the StoreServ Management Console (SSMC). See the *HPE 3PAR Command Line Interface Administrator Guide* or the StoreServ SSMC Online Help for instructions on performing these tasks.

You can use the HPE 3PAR Web Services API (HPE 3PAR WSAPI) to manage file server objects with customized client applications. For more information, see the *HPE 3PAR Web Services API Developer Guide*.

### HPE 3PAR Thin Express ASIC

The HPE 3PAR StoreServ 8000, 9000, and 20000 systems use the fifth and latest generation of the HPE 3PAR ASIC, the HPE 3PAR Thin Express ASIC. The HPE 3PAR Thin Express ASIC is engineered and designed for solid-state performance. The ASIC enables the 9000 and 20000 series to deliver over 5X improvement in system bandwidth and faster XOR operations. It offloads CPU and evenly spreads I/O workload across 8 Node Active-Mesh scale-out architecture, ensuring lower latency. The HPE 3PAR Thin Express ASIC comes with a new powerful data deduplication engine which powers inline deduplication for block workloads without compromising performance or scale.

The Thin Express ASIC also enables Persistence Checksum that delivers T10-PI (Protection Information) for end-to-end data protection (against media and transmission errors) with no impact to applications or host operating systems.

### HPE 3PAR Remote Copy software

HPE 3PAR Remote Copy Software facilitates the automatic transparent failover of host I/O from a failed primary StoreServ to a still operating StoreServ storage system. With automatic transparent failover, there can be no coordination of operation between the storage systems. Only those actions performed on the secondary system are executed. The operation initiation sequence also differs somewhat from a manual transparent switchover host-independent, array-based, data-mirroring solution that enables affordable data distribution and disaster recovery for applications.

For more information about the HPE 3PAR Remote Copy application, see the *HPE 3PAR Remote Copy Software User Guide*.

### HPE 3PAR Dynamic Optimization software

HPE 3PAR Dynamic Optimization Software is an optional feature that allows you to improve the performance of virtual volumes without interrupting access. Use this feature to avoid over-provisioning for peak system usage by optimizing the layout of your virtual volumes. With dynamic optimization, you can change the parameters, RAID levels, and set sizes of the virtual volume by associating the virtual volume with a new CPG.

Dynamic optimization enables you to change volume parameters and update the layout of volumes to take advantage of the current system configuration. For example, when a system is upgraded by adding nodes, cages, or physical disks, the initial volume and LD layouts may no longer be optimal for the new system configuration. Updating the system layout optimizes the use of all physical resources in the system at a given time.

Dynamic optimization may improve system performance in several ways:

- **Volume layout changes after hardware upgrades**—Existing virtual volumes only take advantage of resources that were present at the time of volume creation. When a system is upgraded by adding
nodes, cages, or disks, the original volume and LD layouts may no longer be optimal. Changing the layout of a virtual volume enables volumes to take full advantage of new system resources.

By default, TPVVs and their underlying CPGs dedicate space from all available resources as they grow, both from pre-existing and new drive capacity resources. This natural expansion capability of TPVVs reduces the need for Dynamic Optimization to change the layout of TPVVs after adding disks.

- **Volume RAID level changes**—Since different RAID levels have varying capacity requirements and offer different degrees of performance, you may want to convert volumes from one RAID type to another when system requirements change.

- **Volume fault-tolerance changes**—A volume with a cage-level availability can tolerate the failure of a drive cage because its RAID sets use chunklets from different drive cages. A volume with a magazine-level availability can tolerate the failure of a drive magazine because its RAID sets use chunklets from different magazines. As applications and business requirements change, it may be advantageous to update the fault-tolerance characteristics of existing virtual volumes.

- **CPG and volume growth configuration changes**—Changing the characteristics of CPGs and changing virtual volume growth patterns can also reduce system performance over time. Tuning optimizes the system layout by balancing the use of all available resources.

With dynamic optimization, you can manually change specific parameters on any specified virtual volumes. This feature also analyzes your entire system and automatically corrects space usage imbalances in the system. Virtual volume and physical disk capacity are analyzed and rebalanced for optimal performance. The dynamic optimization automated tuning process has three phases:

1. **Internode tuning phase**—Analyze the system and detect virtual volumes that are not correctly balanced between nodes. If virtual volumes are not balanced correctly, the volumes are tuned to correct the imbalance.

2. **Intranode tuning phase**—Analyze the system and detect any chunklet imbalance between physical discs associated with the same node. After the analysis, chunklets are moved from over-used physical discs to under-used physical discs associated with the same node.

3. **CPG analysis phase**—Analyze the system and verify that logical disks associated with a CPG have the same characteristics as the CPG. If the LD characteristics do not match the CPG, the LD is modified to match the CPG characteristics.

Dynamic Optimization tasks can be performed with either the HPE 3PAR CLI or the SSMC. See the *HPE 3PAR Command Line Interface Administrator Guide* or the SSMC Online Help for instructions on performing these tasks.

### HPE 3PAR Adaptive Flash Cache software

With the Adaptive Flash Cache feature you can create a flash cache using space from your SSDs. The flash cache augments the system cache without adding more physical memory. Creating more cache space from your SSDs allows the HPE 3PAR StoreServ to deliver frequently accessed data at greater speed. The space for the flash cache on the SSDs is automatically reserved by the system; you do not need to specify which SSDs to use. Use the flash cache for specified virtual volume sets or the entire system.

Adaptive Flash Cache uses a Least-Frequently Used (LFU) algorithm to refresh flash cache data. Data is promoted to the flash cache when it is accessed, and demoted when it is not accessed. Cached data is stored in flash cache logical disks constructed from SSD drives by the system. The flash cache sits between the DRAM and the physical drives in the array and each controller has dedicated flash cache logical disks. As data pages are moved out of the system cache they are copied into the flash cache, which improves the read performance when data is requested again by hosts.

Adaptive Flash Cache creation and management tasks can be performed with the HPE 3PAR CLI. See the *HPE 3PAR Command Line Interface Administrator Guide* for instructions on performing these tasks.
HPE 3PAR System Tuner software

HPE 3PAR System Tuner software is an optional feature that improves performance by identifying overused physical disks, and performing load balancing on those disks without interrupting access.

The HPE 3PAR OS automatically creates a balanced system layout by mapping virtual volumes to many logical disks, and creating logical disks from chunklets drawn from many physical disks. The I/O for each volume is striped across many physical disks, increasing the throughput of the volume. As the system grows and new applications are introduced, new storage usage patterns can emerge, and the system performance can degrade. System Tuner maintains peak system performance by automatically detecting and resolving bottlenecks without interrupting access.

If the performance of one or more physical disks degrades, the throughput of the logical disks is reduced, and the entire system performance may decline. There are two general reasons why a physical disk may have degraded performance:

- The physical disk has reached its maximum throughput due to an unbalanced load. A disk in this state typically has unusually high average service times when compared to other disks.
- The physical disk is a bad disk. A bad disk typically has unusually high maximum service times when compared to other disks.

System Tuner allows you to:

- Perform physical disk performance tuning on an entire system or on a specified subset of disks.
- Set performance thresholds for physical disk tuning.
- Identify and relocate under-performing chunklets.

System Tuner tasks can only be performed with the HPE 3PAR CLI. See the *HPE 3PAR Command Line Interface Administrator Guide* for instructions on performing these tasks.

HPE 3PAR Thin Conversion software

HPE 3PAR Thin Conversion software is an optional feature that converts an FPVV to a TPVV.

Virtual volumes with large amounts of allocated but unused space are converted to TPVVs that are much smaller than the original volume. During the conversion process, allocated but unused space is discarded, and the result is a TPVV that uses less space than the original volume. To convert volumes located on a system, you must have an HPE 3PAR StoreServ storage system to perform the copy operation.

The conversion process has four steps.

- Assessment
- Data preparation
- Zeroing unused space
- Creating a physical copy

Assessment

Before converting your volumes, you must determine the benefits of the conversion process. The potential benefits of zeroing free space prior to copying or migrating the data to a TPVV depends on the amount of allocated but unused space. If there is relatively little unused space in the allocated physical space, then there is little benefit to zeroing the free space to recapture this relatively small amount of space. Many volumes that have been in use for a long time have significant amounts of allocated but unused space. If there is a large amount of unused space in the allocated physical space, then zeroing the data prior to copying the data results in a substantial reduction in the amount of used space.
Data preparation

Prepare your data for copying by removing unnecessary data. Perform clean-up tasks on the source volume by:

- Emptying trash cans or permanently deleting files.
- Archiving unused files.
- Shrinking databases.
- Deleting temporary files.

Zeroing unused space

Use a host application to write zeros to the allocated but unused volume space. All HPE 3PAR StoreServ Storage systems detect and discard the zeros during the volume copy operation.

Creating a physical copy

After writing zeros to the allocated but unused space, the source volume is ready for the final phase of conversion. You create a TPVV physical copy of the source volume to convert the source volume to a TPVV. When you create a physical copy, the system automatically detects the zeros and does not allocate space for them in the physical copy. The result is a TPVV that is much smaller than the original volume.

Thin conversion tasks can be performed with the HPE 3PAR CLI and the SSMC. See the HPE 3PAR Command Line Interface Administrator Guide and the SSMC Online Help for instructions on how to perform these tasks.

HPE 3PAR Thin Persistence software

HPE 3PAR Thin Persistence software is an optional feature that keeps TPVVs and read/write snapshots of TPVVs small by detecting pages of zeros during data transfers and not allocating space for the zeros. This feature works in real-time and analyzes the data before it is written to the source TPVV or read/write snapshot of the TPVV. Freed blocks of 16 KB of contiguous space are returned to the source volume; freed blocks of 128 MB of contiguous space are returned to the CPG for use by other volumes.

Thin persistence tasks can be performed with the HPE 3PAR CLI and the SSMC. See the HPE 3PAR Command Line Interface Administrator Guide and the SSMC Online Help for instructions on performing these tasks.

HPE 3PAR Thin Copy Reclamation software

HPE 3PAR Thin Copy Reclamation software is an optional feature that reclaims space when snapshots are deleted from a system. As snapshots are deleted, the snapshot space is reclaimed from a TPVV or FPVV and returned to the CPG for reuse by other volumes. Deleted snapshot space can be reclaimed from virtual copies, physical copies, or remote copies. The HPE 3PAR Thin Copy Reclamation feature works on any class of system. For more information about snapshots, see Virtual Copy Snapshots on page 10.

HPE 3PAR Virtual Lock software

HPE 3PAR Virtual Lock software is an optional feature that enforces the retention period of any volume or copy of a volume. Locking a volume prevents the volume from being deleted, intentionally or unintentionally, before the retention period elapses. You can use HPE 3PAR Virtual Lock to specify the retention period for each volume or copy of a volume.
HPE 3PAR Adaptive Optimization software

HPE 3PAR Adaptive Optimization software analyzes sub-volume, region-level disk access rates for a given array over a scheduled period of time, and then performs a data migration of regions between tiers according to a cost versus performance preference. Disk usage is optimized by moving frequently accessed data to the higher-performance tier—for example, RAID 1 using solid state disks, or SSDs—while infrequently accessed data is moved to the lower-cost tier—for example, RAID 6 on near line (NL) disks.

AO uses HPE System Reporter statistics gathered from logical disks and physical disks to relocate customer data on physical volumes in an optimal way. AO relocation accomplishes two primary goals:

- Increases performance of frequently accessed regions of data by moving those regions to higher-tier storage (for example, moving to solid state drives from normal spinning media).
- Improves cost-efficiency by moving lightly accessed regions of data to a lower performance and less expensive tier of storage (for example, moving from regular drives to nearline drives).

Because storage tiers can be of different RAID types, capacity efficiency is maximized by using RAID1 for only the most frequently accessed storage and by using RAID5 or RAID6 for less frequently accessed storage. Other benefits include:

- AO can migrate data from a fully occupied tier of storage to another tier that has more available capacity.
- AO can also be regularly scheduled to adjust the data layout as your data usage changes over time.

AO is built on top of the new version of System Reporter (SR), which also now runs as part of the HPE 3PAR OS. SR must have been actively gathering data on virtual volume regions for a period of time. Analysis of the data collected by SR is performed to identify regions within virtual volumes that are either heavily used or lightly used, and then generates a series of secondary tasks to move these regions to faster or slower storage tiers.

Running AO on the HPE 3PAR OS itself offers these advantages:

- AO configurations can now be created, modified, and removed using the CLI or the SSMC.
- Beginning with HPE 3PAR 3.1.2, the external System Reporter is no longer necessary to use Adaptive Optimization.
- The database scheme has been restructured on node to be more efficient and reliable.
- The actual movement of data can use data from a given time period in the past rather than only from the immediate past. This means data movement can occur at low-utilization time periods, while using an analysis of statistics gathered during peak periods.
- A time limit can be set for data movement so that scheduled data is moved only during low-utilization periods rather than during peak periods.

If data service times become too high and meet a latency threshold then AO will move the data from a lower-cost tier drive to a high performance drive tier.

Latency thresholds by drive type:

<table>
<thead>
<tr>
<th>Drive Type</th>
<th>Milliseconds</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solid State Drive</td>
<td>15 ms</td>
</tr>
<tr>
<td>Fast Class Drive</td>
<td>40 ms</td>
</tr>
<tr>
<td>Nearline Drive</td>
<td>60 ms</td>
</tr>
</tbody>
</table>
HPE 3PAR Peer Motion software

HPE 3PAR Peer Motion software controls the migration of a host and its data from a source system to a destination system with as little disruption to the host as possible. With peer motion, you can copy the virtual volumes and system configuration information to a new system with no changes to host configurations, no loss of access by a host to its data in an online migration, and only a minimal outage during migration.

Data encryption

HPE 3PAR encrypted storage systems provide data encryption by using self-encrypting drives (SEDs) with a local key manager (LKM), or with certificates and an external key manager (EKM).

Data encryption prevents data exposure that might result from the loss of physical control of disk drives when disk drives are:

- Decommissioned at their end of life.
- Returned for warranty or repair.
- Lost or stolen.

The HPE 3PAR StoreServ Data Encryption solution uses SED technology to encrypt all data on the physical drives and prevent unauthorized access to data-at-rest (DAR). When encryption is enabled, the SED will lock when power is removed, and it will not be unlocked until the matching key from the HPE 3PAR StoreServ Storage system is used to unlock it.

SEDs contain special firmware and an application-specific integrated circuit (ASIC) that provides encryption. Each SED has a number of bands that control access to different areas of the drive.

Each band has an internal encryption key that is not exposed outside of the drive itself. This encryption key is always used to encrypt and decrypt all data stored on that band. All data encryption is handled at the physical disk layer. System features, such as thin provisioning and dynamic optimization, work independently of encryption.

Each band has a single authentication key that controls access to data on the band. In the HPE 3PAR StoreServ data-encryption implementation, the entire disk is in one band. Access to data is controlled by setting the authentication key, which locks and unlocks the drive.

The LKM, which is part of the HPE 3PAR OS that runs on each node in a cluster, maintains the authentication key. You must back up and protect the keystore file; Hewlett Packard Enterprise does not have access to the key.

All drives in the same array will have the same authentication key. The disks become locked whenever they lose power, which guarantees that any disk removed from an HPE 3PAR StoreServ Storage system will not be accessible except in its original array. When the drive is unlocked, all I/O to the drive behaves exactly as it would on a non-SED, and encryption and decryption happen at full interface speed, without data delays.

There is a minimal delay for booting (since each drive must be unlocked before the system becomes operational) and for data encryption management functions (since each disk must be updated whenever keys are changed on the system). Each of these operations takes up to 3 seconds per disk, but happens in several threads. On a system with 160 disks, for example, enabling encryption takes about 30 seconds, and booting takes an additional 5 seconds. Rekeying under a light load takes about 15 seconds.
CAUTION:

Keep the encryption key file and password safe. If you lose the encryption key and the HPE 3PAR StoreServ Storage system is still functioning, you can always perform another backup of the encryption key file. However, should you lose the encryption key file or the password, and should the HPE 3PAR StoreServ Storage system then fail, the HPE 3PAR StoreServ Storage system will be unable to restore access to data. Ensure that backup copies of the latest encryption key file are kept and that the password is known.

The importance of keeping the encryption key file and password safe cannot be overstated. Hewlett Packard Enterprise does not have access to the encryption key or password.

Different arrays need separate backups, although the same password can be applied.

The SED DataStore provides an open interface for authentication key management. DataStore tracks the serial number of the array that owns each SED, which disallows SEDs from being used in other systems.

NOTE:

The HPE 3PAR data encryption solution will help mitigate breach notifications under the Health Information Technology for Economic and Clinical Health (HITECH) Act, but is not compliant with the Federal Information Processing Standard (FIPS) 140-2.

Priority Optimization software

During recent years, consolidation of storage systems has reduced complexity of data storage, delivering efficiency in management, occupied floor space, and energy consumption. However, the consolidation of many disjoint workloads into a single storage system also results in contention for shared system resources on the system.

Examples of such shared resources include front-end host Fiber Channel (FC), iSCSI and FCoE adapters, back-end FC or SAS disk connections, physical disks, data and control cache, ASICs, CPUs, and backplane interconnections. Data packets arriving at the front-end FC HBA adapters are handled on a first-come, first-serve basis. On the surface, this may sound fair, but it can lead to unequal and inconsistent throughput for multiple concurrent workloads.

HPE 3PAR’s Priority Optimization software manages and distributes the I/O capacity of an HPE 3PAR StoreServ Storage system across multiple workloads. The tool enables the co-location of the data of workloads of different types, such as sequential, random, online transaction processing (OLTP), with different I/O packet sizes on a single storage system while achieving adequate and stable performance in a multi-tenant environment.

The System Busy feature automatically manages IO latency goals. System Busy will be set to 0% if no latency goals are set and all items under QoS rules will be delayed or rejected I/O requests when nearing the IOPS or Max Limit of the QoS rule. If a QoS rule is defined then System Busy level will be calculated in real-time. When Priority Optimization detects a QoS rule is not meeting their latency goal then the System Busy level will increase and delay and/or reject lower priority VVset IOs. The delays and rejections can reduce VVset and Domain IOPS to their Minimum Goal IOPs, allowing higher priority QoS rules to consume more system resources to meet their latency goals. If the System Busy level continues to increase and high priority QoS rules on VVsets and Domains will be delayed to the point of exceeding their latency goal. System Busy levels are calculated every 200 ms. If the IOs miss their latency goal then the System Busy level will increase from zero to a larger value. If the IOs meet their latency goal then the System Busy level will be decreased.

HPE 3PAR Priority Optimization software introduces quality-of-service rules to manage and control the I/O capacity of an HPE 3PAR StoreServ Storage system across multiple workloads. Application of the rules enables co-location of the data from workloads of different types (such as sequential, random, and...
transactional, among others), with different I/O packet sizes on a single HPE 3PAR StoreServ Storage system. The use of QoS rules stabilizes performance in a multi-tenant environment.

Virtual Volume Sets

QoS rules operate on sets of VVs called VVsets. A VVset is an autonomic group object that is a collection of virtual volumes. VVsets help to simplify administration of volumes and reduce human error. An operation such as exporting a VVset to a host will export all member volumes of the VVset. Adding a volume to the VVset will export the new volume automatically to the host or host set.

VVsets have a number of use cases beyond reducing administration for their volume members. Most HPE 3PAR Remote Copy operations are performed on sets of virtual volumes called remote copy volume groups. VVsets also enable simultaneous point-in-time snapshots of all volumes contained in the set with a single command. Up to 8192 volumes can be part of a VVset.

The volumes in a VVset can have different RAID levels and sizes. VVsets can contain volumes with different provisioning types, RAID levels, sizes, and CPGs.

Quality of service rules

HPE 3PAR Priority Optimization software provides quality-of-service rules to manage and control the I/O capacity of an HPE 3PAR StoreServ Storage system across multiple workloads. Application of the rules enables co-location of the data from workloads of different types such as sequential, random, and transactional, among others, with different I/O packet sizes on a single HPE 3PAR StoreServ Storage system. The use of QoS rules stabilizes performance in a multi-tenant environment.

Mode of operation

HPE 3PAR Priority Optimization operates by applying upper-limit control on I/O traffic to and from hosts connected to an HPE 3PAR StoreServ Storage system. These limits, or QoS rules, are defined for front-end input/output operations per second (IOPS) and for bandwidth.

NOTE:

IOPS is a common performance measurement used to benchmark computer storage. It is indicative of how many host I/O requests the array is receiving per second. It is typically stated as a whole number, such as 50,000 IOPS.

QoS rules are applied using autonomic groups. Every QoS rule is associated with one (and only one) target object. The smallest target object to which a QoS rule can be applied is a virtual volume set (VVset) or a virtual domain. Because a VVset can consist of a single VV, a QoS rule can target a single VV.

Every QoS rule has six attributes:

<table>
<thead>
<tr>
<th>Name</th>
<th>The name of the QoS rule is the same as the name of the VVset.</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>The QoS rule can be active or disabled.</td>
</tr>
<tr>
<td>I/O</td>
<td>Sets the Min Goal and the Max Limit on IOPS for the target object.</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>Sets the Min Goal and the Max Limit in bytes-per-second transfer rate for the target objective.</td>
</tr>
<tr>
<td>Priority</td>
<td>The limit for the target object can be set to low, normal, or high.</td>
</tr>
<tr>
<td>Latency Goal</td>
<td>The goals for the target object are determined in milliseconds.</td>
</tr>
</tbody>
</table>
When an I/O packet reaches the HPE 3PAR StoreServ controllers, HPE 3PAR Priority Optimization takes one of the following actions:

- Pass the I/O packet to the domain or VV.
- Delay the I/O by stalling it in a private QoS queue that gets processed periodically.
- Return a SCSI queue-full (QFULL) message to the host.

If the current limit for IOPS or bandwidth for a particular VVset has been reached, HPE 3PAR Priority Optimization delays SCSI I/O request responses for the volumes contained in that VVset. These delayed I/O requests are pushed onto an outstanding I/O queue for the VV(s) in the VVset experiencing the limit breach.

Every QoS rule maintains its own queue for delayed I/Os. These queues are constructed inside each HPE 3PAR StoreServ controller node that receives an I/O request that needs to be delayed. Only the I/O request descriptions are queued, not the actual data. A controller node’s cache is not impacted, because the QoS rules are applied before write I/O data reaches the cache.

The size of a request queue varies by rule priority, maximum delay time, and QoS limits. When I/O requests reside longer than 100 ms, 200 ms, or 400 ms for low, normal, or high priority rules in a QoS queue, or 1 sec, 2 sec, or 3 sec of I/O based on low, normal, or high priority in the QoS queue, any more incoming I/Os to the volumes in the VVset are rejected, and a QFULL response is returned to the server using the volumes. QFULL prevents delayed I/O from holding all system resources, such as host, HBA, and VV layer buffers and queues. Hosts should respond to the QFULL message appropriately and throttle I/O. The I/O delay and the eventual QFULL response applies to all members of the VVset, even if only one of the VVs causes the QoS threshold breach.

HPE 3PAR Priority Optimization features a system-wide, built-in QoS rule called all_others that is inactive by default. This rule limits the IOPS and/or bandwidth to all volumes and VVsets that are not subject to a named rule. Enabling the all_others rule eliminates the need to define a specific, named rule for all workloads on the storage system.

QoS rule minimum and maximum

HPE 3PAR Priority Optimization sets the values for IOPS and bandwidth in QoS rules in absolute numbers, not in percentages. The IOPS number is stated as an integer between 0 and $2^{31}$-1, although a more realistic upper limit is the number of IOPS that the particular array in question is capable of providing, given its configuration. The value for bandwidth is stated as an integer between 0 and $2^{63}$-1, expressed in KB/second, although a more realistic upper limit is the throughput in KB/second that the particular array in question is capable of providing, given its configuration.

NOTE:

Throughput, also called bandwidth, is a measure of the amount of data processed by the array per unit of time. It is usually measured in MB/second.

QoS rules support specifying an IOPS upper limit and/or a lower limit. The iteration towards a new IOPS or bandwidth setting follows a damped exponential curve and is completed in a few seconds. During operation, HPE 3PAR Priority Optimization samples the IOPS and bandwidth values per VVset every 8 ms, and assembles 625 of these periods into a moving 5 second averaged window to adjust the ingress of the I/O to the QoS cap that was set.

QoS rule actions

QoS rules are subject to five distinct actions:

- **Create**—A QoS rule is created.
- **Enable**—A disabled QoS rule is made active.
- **Disable**—An active QoS rule is made inactive.
• **Change**—The limit values for a QoS rule are modified.
• **Clear**—The QoS rule is removed from the system.

A QoS rule that is created becomes active immediately. This default behavior can be overridden when using the HPE 3PAR CLI to create the rule; the HPE 3PAR SSMC does not offer that option. Changing one or both limit values in a QoS rule activates those values instantly on the VVset; there is no need to disable the QoS rule first. An active QoS rule can be removed without first disabling it.

**Overlapping QoS rules**

A VV can be a member of multiple VVsets, each of which can have a QoS rule defined. In such a case, the I/O to and from volumes in the VVset is governed by multiple, possibly overlapping rules. All active rules for a particular VVset are combined using wired-OR logic: the QoS limit that is reached first takes precedence. A QoS rule can be created on a VVset that has none, or not all, of its VVs exported to a host.

**Minimum QoS settings**

HPE 3PAR Priority Optimization provides no enforcement for minimum QoS levels. The minimum will be ensured, provided the system has been correctly sized for the expected total IOPS and throughput, and provided QoS rules against all VVsets were installed such that their combined sum does not exceed what the system is capable of delivering.

**QoS on copied volumes**

Virtual and physical copies of VVs in a VVset are not automatically a member of the parent VVset; they have to be added manually to the parent VVset in order to be governed by the same QoS rules. Virtual and physical copies can be subject to a different QoS rule than their parent VV, if desired. QoS rules are persistent across a reboot of an HPE 3PAR StoreServ Storage system. A VVset cannot be removed unless all QoS rules defined for it are removed first.

**HPE 3PAR mySnapshot**

The HPE mySnapshot feature enables safe and easy copy and provisioning access to non-storage professionals, such as database administrators, software developers, and test engineers working with systems. Users can restore their own copies of test data in seconds without relying on the storage administrator.

The mySnapshot feature uses an access control list to associate a user with certain administrative permissions and specified storage resources. After these administrative permissions are granted for the specified resources, the user can replace and restore copies of their own test database. This enables users who have only browse capabilities on the system to be able to update specific snapshots with more recent snapshots. This results in faster turnaround times for developers who must have their snapshots refreshed and alleviates workload for storage administrators. For more information about roles and rights, see **HPE 3PAR StoreServ storage system users** on page 20.

Configuring the mySnapshot feature can only be performed with the HPE 3PAR CLI. See the **HPE 3PAR Command Line Interface Administrator Guide** for instructions on performing this task.
HPE 3PAR StoreServ Storage hardware

HPE 3PAR StoreServ Storage systems are available in a variety of hardware configurations. Different hardware models address different levels of storage capacity and anticipated growth requirements. All models use the HPE 3PAR Operating System.

Hardware monitoring and configuration tasks can be performed with either the HPE 3PAR CLI or the StoreServ Management Console (SSMC). See the HPE 3PAR Command Line Interface Administrator Guide or the SSMC Online Help for instructions on performing hardware management tasks. For detailed information about ports, network adapters, cabling, and cable configurations, see the physical planning manual for your storage system model.

Identifying HPE 3PAR StoreServ Storage system components

Major HPE 3PAR StoreServ Storage system hardware components:

- Physical Drive
- Drive Enclosure
- Controller node
- Service Processor
- Power Distribution Unit
- Input/Output (I/O) Module

The HPE 3PAR StoreServ Storage systems include physical drives, controller nodes, and expansion drive enclosures (optional). The controller nodes include network ports to provide administrative datapaths to the storage system. The system utilizes a cluster-based design that incorporates sophisticated data management and fault tolerance technologies that can meet the storage needs of smaller sites and can easily be scaled for global organizations. Host servers connect to the storage system with either onboard connections or optional host adapters. Host adapter ports provide the system with additional Fibre Channel (FC), Fibre Channel over Ethernet (FCoE)/iSCSI, or Ethernet connections. The additional FC ports can be used for multiple purposes including connection to hosts and connection to other HPE 3PAR StoreServ Storage systems in a Remote Copy or Peer Motion relationship. The iSCSI/FCoE ports permit host connection in iSCSI and FCoE environments. The Ethernet ports can be used to natively host various File protocols and core file data services.

HPE 3PAR StoreServ Storage hardware components

This section describes the HPE 3PAR StoreServ Storage system hardware components.

Physical drive

A physical drive is a hard drive or a Solid-State Drive (SSD) mounted on a drive magazine or module located in drive cages. There are three types of physical disks:

- Fibre Fast Class (FC)
- Near Line (NL)
- Solid-State Drive (SSD)

Drives are installed in the drive bays at the front of either the controller node enclosures or drive enclosures. Physical drives come in two physical sizes installed in carriers (magazines):

- SFF 2.5-inch drives
- LFF 3.5-inch drives
The drive types are Fast Class (FC) drive, Near Line (NL) drive or Solid State Drive (SSD), and can be intermixed in a single array for some HPE 3PAR StoreServ Storage systems.

Disk enclosure

A disk enclosure is a specialized casing designed to hold and power disk drives while providing a mechanism to allow them to communicate. The drive enclosures hold an array of drives and can be added after initial installation to expand the configuration. The drive enclosures are intelligent, compact and extremely dense storage units, where each is capable of holding a large number of drives in a small rack space (EIA-standard rack units).

Controller node

The controller node is a system component that caches and manages data in a system and provides hosts with a coherent and virtualized view of the system. The controller nodes are located in the rear of the controller node enclosure.

Inside each controller node there are slots for network adapters, control cache DIMMs and data cache DIMMs. The number of controller nodes in each system, the type of network adapters, and number of network adapters are configurable.

The HPE 3PAR StoreServ Storage systems can contain two, four, six or eight controller nodes depending on the StoreServ system. The nodes are numbered 0, 1, 2 .. from bottom to top.

Service Processor 5.0

Each storage system requires a Service Processor (SP). An SP can either be a physical SP (PSP) or a virtual SP (VSP). An SP provides remote monitoring, error detection, and reporting. It also supports diagnostic and maintenance activities involving the storage systems. The SP contains proprietary HPE software and exists as a single undivided entity. A Service Processor sends support data to Hewlett Packard Enterprise Remote Support.

Physical Service Processor (PSP)

A physical service processor (PSP) is a hardware device mounted in the system rack. If the customer chooses a PSP, each storage system installed at the operating site includes a PSP installed in the same cabinet as the system controller nodes.

A PSP uses two physical network connections. One (eth0) requires a connection from the customer network to communicate with the storage system. The other (eth1) is for maintenance purposes only and is not connected to the customer network.

Virtual Service Processor (VSP)

The Virtual Service Processor (VSP) is provided in an Open Virtual Format (OVF) format. The VSP is tested and supported on the VMware vSphere hypervisor (supported on VMware ESXi 5.5 and later clients). The VSP has no physical connections. It runs on a customer-owned and customer-defined server and communicates with 3PAR Storage system over its own Ethernet connections.

The HPE 3PAR Service Console (SC) is an appliance which collects data from an attached HPE 3PAR StoreServ Storage system in predefined intervals, as well as an on-demand basis. If configured, the SC sends the data to the call home infrastructure. The SC comes preinstalled on an HPE 3PAR Management Module, the physical Service Processor (PSP), and on a Virtual Machine (VM) or that runs on Linux.

The SP is the platform on which the SC runs. It sends support data back to Hewlett Packard Enterprise, and provides a way for HPE Technical Support Engineers to log in remotely to remediate problems. The SC is the GUI for the SP. It provides a streamlined, more usable interface with a layout that closely resembles the HPE 3PAR StoreServ Management Console (SSMC).
Power Distribution Unit

A Power Distribution Unit (PDU) is a device with multiple outputs that fits inside the rack. Its purpose is to distribute electrical power to the entire rack. In HPE 3PAR StoreServ models, the PDUs are mounted at the bottom of the rack.

A PDU is installed inside a rack and can be set up in several different ways.

Input/Output module

Input/Output (I/O) modules connect the controller nodes to the drive enclosures using SAS cables (the 10000 series uses only FC). These modules enable data transfer between the controller nodes, the drives, PCMs, and enclosures.

The I/O modules are located at the rear of the expansion drive enclosures.

HPE 3PAR StoreServ Storage models

HPE 3PAR StoreServ is built to meet the requirements of massively consolidated cloud service providers. Its speed and system architecture has been extended to transform mainstream midrange and enterprise deployments, with solutions that scale from a few TBs up to more than 20 PB. Explosive data growth, new technology choices, and the proliferation of siloed architectures are pushing legacy storage beyond its brink. HPE 3PAR Storage offers Tier-1 architecture that is both massively scalable and flash-optimized.

The following figure describes the basic configuration of an HPE 3PAR StoreServ Storage system:

![Figure 14: Configuration of an HPE 3PAR StoreServ Storage system](image)

HPE 3PAR StoreServ Storage models

Available HPE 3PAR StoreServ Storage models:

- HPE 3PAR StoreServ 7000 Storage
- HPE 3PAR StoreServ 8000 Storage
- HPE 3PAR StoreServ 9000 Storage
HPE 3PAR StoreServ 10000 Storage

HPE 3PAR StoreServ 10000 Storage is the legacy 3PAR enterprise Tier-1 storage that meets the need of hybrid and private cloud and ITaaS environments. It has been replaced in HPE Storage portfolio by the newer HPE 3PAR StoreServ 20000 Storage.

HPE 3PAR StoreServ 20000 Storage

The HPE 3PAR StoreServ 20000 Storage family offers enterprise flash arrays ready for massive consolidation of today’s most demanding workloads with greater than 3 million IOPS, sub-millisecond response times, and high availability. Each HPE 3PAR StoreServ model differs in specifications and usage. The factors are:

- Number of storage controllers
- Number of hosts ports
- Number of initiators per system
- Drive types
- Maximum number of drives
- Maximum number of Solid State Drives
- Maximum raw capacity

HPE 3PAR StoreServ 7000 Storage

HPE 3PAR StoreServ 7000 Storage is the legacy 3PAR midrange platform. It offers enterprise Tier-1 storage at a midrange price and it has been replaced in HPE Storage portfolio by the newer HPE 3PAR StoreServ 8000 Storage.

HPE 3PAR StoreServ 8000 Storage

The HPE 3PAR StoreServ 8000 Storage offers enterprise Tier 1 storage at a midrange price. HPE 3PAR StoreServ 8000 Storage delivers the performance advantages of a purpose-built, flash-optimized architecture without compromising resiliency, efficiency, or data mobility. The new HPE 3PAR Gen5 Thin Express ASIC provides silicon-based hardware acceleration of thin technologies, including inline deduplication, to reduce acquisition and operational costs by up to 75% without compromising performance.

With unmatched versatility, performance, and density, HPE 3PAR StoreServ 8000 Storage gives you a range of options that support true convergence of block and file protocols, all-flash array performance, and the use of spinning media to further optimize costs. HPE 3PAR StoreServ 8000 Storage offers rich, Tier-1 data services, quad-node resiliency, seamless data mobility between systems, high availability through a complete set of persistent technologies, and simple and efficient data protection with a flat backup to HPE StoreOnce Backup appliances. You can choose one of four HPE 3PAR StoreServ 8000 models (8200, 8400, 8440, and 8450) for your specific needs.

HPE 3PAR StoreServ 9000 Storage

The HPE 3PAR StoreServ 9000 Storage is an enterprise-class flash array that helps you consolidate primary storage workloads - for file, block, and object - without compromising performance, scalability, data services, or resiliency. This newest 3PAR model based on the proven 3PAR architecture is purpose built for all-flash consolidation, delivering the performance, simplicity, and agility needed to support your hybrid IT environment. HPE 3PAR StoreServ 9000 Storage is available in a single all-flash model, the 9450, that offers rich Tier-1 data services, quad-node resiliency, fine-grained Quality of Service (QoS), seamless data mobility between systems, high availability through a complete set of persistent technologies, and simple and efficient data protection with a flat backup to HPE StoreOnce Backup appliances.

HPE 3PAR StoreServ 10000 Storage

HPE 3PAR StoreServ 10000 Storage is the legacy 3PAR enterprise Tier-1 storage that meets the need of hybrid and private cloud and ITaaS environments. It has been replaced in HPE Storage portfolio by the newer HPE 3PAR StoreServ 20000 Storage.
latencies, a 4X density advantage, and scalability to 15 PB of usable capacity. The family’s flash-first architecture features the HPE 3PAR Thin Express ASIC for silicon-based hardware acceleration of thin technologies, including inline deduplication to reduce acquisition and operational costs by up to 75% without compromising performance. A choice of models provide a range of options that support true convergence of block and file protocols, all-flash array performance, and the use of solid state drives (SSDs) with spinning media for unmatched versatility. Enhanced Tier-1 storage capabilities for always-on data access and fine-grained Quality of Service (QoS) controls ensure predictable service levels for all workload types while bi-directional data mobility enables virtually limitless elastic pools of storage to support the most rigorous on-demand infrastructure.
In addition to managing the system with the StoreServ Management Console (SSMC) and the HPE 3PAR CLI, the HPE 3PAR OS includes a Simple Network Management Protocol (SNMP) agent that allows you to perform some basic management functions by running network management software on a management station.

These SNMP management functions require that you have SNMP management software that is not provided by Hewlett Packard Enterprise 3PAR.

### About SNMP

SNMP is a structured management interface used by many software frameworks to manage hardware devices. SNMP requires two components: an agent and a manager. The manager is the management process that sends requests to the agent. The host that the manager runs on is called the management station.

### SNMP managers

There are four types of requests that an SNMP manager can send to an agent:

- **SET**—The SET request writes an object value in the agent. The SET request includes the object ID and a new value for the object. The agent changes the value of the object and saves it in the persistent store. Not all objects are changeable. The management information base (MIB) contains access information.

- **GET**—The GET request reads an object value in the agent. The GET request includes the object ID to be retrieved. The agent returns the value of the object.

- **GETNEXT**—The GETNEXT request reads the object instance that is next in lexicographical order to the object ID in the request. For example, if the object ID specified in the request is `.12925.0`, the returned object ID should be `.12925.1`, if it exists.

- **GETBULK**—The GETBULK operation is an optimization of the GETNEXT operation that allows multiple instances of objects to be returned.

In addition, the manager can register with the agent to receive notifications (traps) for critical events (alerts) and alert state changes. Before an SNMP manager can receive the traps generated by the SNMP agent, you must register your manager with the agent. See “Using the HPE 3PAR SNMP Infrastructure” in the *HPE 3PAR Command Line Interface Administrator Guide* for instructions on registering an SNMP manager with the SNMP agent.

### The HPE 3PAR SNMP agent

The HPE 3PAR SNMP agent runs on the system and provides a management interface to enable other software products to manage Hewlett Packard Enterprise hardware using SNMP. The SNMP agent responds to GET, SET, GETNEXT, and GETBULK SNMP requests, and generates traps for alerts and alert state changes. The SNMP agent converts all system alerts and alert state changes into SNMPv2 traps and forwards them to all SNMP management stations that are registered with the agent. These notifications, which contain detailed information that describe critical events, are generated for every alert and alert state change issued by the system.

The exact message formats are described in [HPE 3PAR MIB](#) on page 76. You can find the MIB files on the HPE 3PAR CLI and SNMP CD.

### Standard compliance

The HPE 3PAR SNMP agent supports the following standards:
• SNMPv2c—This version refers to a widely-used administrative framework for SNMPv2, also known as "community-based SNMPv2." Although this version includes SNMPv2 enhancements, such as notification and GETBULK requests, it relies on the SNMPv1 community concept for security.

• Structure of Management Interface-v2 (SMIv2)—This standard specifies the format of the MIB. The HPE 3PAR MIB definition uses SMIv2 conventions.

• SNMPv3—This version provides stronger security with user-based authentication and Protocol Data Unit (PDU) or packet encryption.

## Supported MIBs

You can find the MIB files on the HPE 3PAR CLI and SNMP CD. The HPE 3PAR SNMP agent supports the following MIBs:

- SNMPv2-MIB
- Management Information Block-II (MIB-II), **system group**—For discovery and basic information, the HPE 3PAR SNMP agent supports the MIB-II system group.
- **snmpTrap group, snmpTrapOID only**—This is the authoritative identification of the notification currently being sent. This variable occurs as the second varbind in every SNMPv2 trap.
- **HPE 3PAR MIB**—This is the HPE 3PAR proprietary MIB.

## MIB-II

MIB-II defines several groups of standard information to be provided by the agent. The SNMP agent supports only the system group objects. The following table summarizes the MIB-II information provided by the SNMP agent.

### Table 8: MIB-II Objects Supported by the SNMP Agent

<table>
<thead>
<tr>
<th>Object Descriptor</th>
<th>Description</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>sysDescr</td>
<td>Describes the system using the model number, system ID, serial number, and HPE 3PAR OS version of the master node.</td>
<td>Read-only</td>
</tr>
<tr>
<td>sysObjectID</td>
<td>The Hewlett Packard Enterprise registration object ID for the system is 12925.1. This is composed of a company-unique ID (12925) and a product ID (1).</td>
<td>Read-only</td>
</tr>
<tr>
<td>sysUpTime</td>
<td>Gives the time interval (within 1/100 of a second) since the system was initialized.</td>
<td>Read-only</td>
</tr>
<tr>
<td>sysContact</td>
<td>User-defined name of the person or group responsible for maintaining the system.</td>
<td>Read/write</td>
</tr>
<tr>
<td>sysName</td>
<td>Name of the system. This helps to identify the storage system. This name cannot be set by using SNMP.</td>
<td>Read-only</td>
</tr>
<tr>
<td>sysLocation</td>
<td>User-defined system location. For example: Building 1, room 4, rack 3.</td>
<td>Read/write</td>
</tr>
</tbody>
</table>
Exposed objects

The HPE 3PAR SNMP agent supports MIB-II system group objects. This section describes each of those objects in detail.

System Description

Access: Read-only

MIB definition: sysDescr

Data type: Display string (max. 255 characters)

Default value: HPE 3PAR InServ

Description: Identifies system model, system ID, serial number and HPE 3PAR OS version of the master node. For example, if the system has four nodes, the sysDescr might look like the following:

HPE 3PAR StoreServ7000, serial number 876541, HP HPE 3PAR OS version x.x.x

This is only a brief system description. Use the HPE 3PAR CLI to obtain further details about the system and each node. This is a read-only attribute.

System Object ID

Access: Read-only

MIB definition: sysObjectID

Data type: integer

Default value: 12925.1

Description: Identifies the unique product ID for the HPE 3PAR StoreServ Storage system. The first part of this ID is the unique enterprise ID assigned to Hewlett Packard Enterprise, Inc. by ICANN (12925). The second part of this ID is the product ID assigned to the system (1). Additional product IDs assigned incremental integers (2, 3, and so on). The manager uses this ID to identify products manufactured by Hewlett Packard Enterprise. This is a read-only attribute.

System Up Time

Access: Read-only

MIB definition: sysUpTime

Data type: time-tick (1/100 second)

Default value: 0

Description: Indicates how long the system has been operational, beginning with system initialization. This is a read-only attribute.

System Contact Information

Access: Read/write

MIB definition: sysContact

Data type: Display string (max. 255 characters)

Default value: Please provide contact information such as name, phone number, and e-mail address

Description: Specifies the name of a person or group responsible for maintaining the storage. This value can be changed by the manager at any time.

System Name

Access: Read-only
MIB definition: `sysName`

**Data type:** Display string (max. 255 characters)

**Default value:** None

**Description:** Indicates the system name, which is set during initialization and setup of the system. This helps to identify this system from other systems. The value cannot be changed by the manager.

**System Location**

**Access:** Read/write

MIB definition: `sysLocation`

**Data type:** Display string (max. 255 characters)

**Default value:** Please provide location description where the device resides such as building, room, and rack number

**Description:** Contains the user-defined location of the system. This helps to indicate where the storage system is located. For example, the location may be indicated as follows: Building 1, room 4, rack 3. This value can be changed by the manager at any time.

**HPE 3PAR MIB**

HPE 3PAR MIB contains proprietary information that defines the configuration and behavior of the system and is useful for network management. Currently, HPE 3PAR MIB contains the `cpuStatsMIB`, `alertNotify`, and `storeServAlerts` trap definitions. The `cpuStatsMIB` is comprised of the `nodeCpuStatsTable` and the `cpuStatsTable` which may be accessed with an `snmpget` or `snmpwalk`. The `nodeCpuStatsTable` is indexed by the node number plus 1 of a node in the HPE 3PAR StoreServ array, while the `cpuStatsTable` is indexed by both the node number plus 1 and the cpu number plus 1 within the node. Both tables are updated every 10 seconds.

The following table displays the contents of the `alertNotify` and `storeServAlerts` traps:

### Table 9: Contents of the alertNotify trap

<table>
<thead>
<tr>
<th>Object Descriptor</th>
<th>Description</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>component</td>
<td>Indicates which system hardware, software, or logical component caused the alert or alert state change.</td>
<td>Read-only</td>
</tr>
<tr>
<td>details</td>
<td>Detailed description of the alert or alert state change, displayed as an alert string (for example: PR table &lt;table_name&gt; is corrupt). For information about system alerts, see the <em>HPE 3PAR Alerts Reference: Customer Edition</em>.</td>
<td>Read-only</td>
</tr>
<tr>
<td>nodeID</td>
<td>Node identification number, an integer from 0 through 7 that indicates which system controller node reported the alert or alert state change.</td>
<td>Read-only</td>
</tr>
<tr>
<td>severity</td>
<td>Severity level of the alert or alert state change, an integer from 0 to 6. See <em>Severity levels of the alert state</em> on page 82 for definitions for each integer.</td>
<td>Read-only</td>
</tr>
<tr>
<td>Object Descriptor</td>
<td>Description</td>
<td>Access</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------</td>
<td>--------</td>
</tr>
<tr>
<td>timeOccurred</td>
<td>Time the alert or alert state change occurred, in <code>yyyy-mm-dd hh:mm:ss ZZZZ</code> format (for example: <code>2005-01-01 12:30:34-0800</code>).</td>
<td>Read-only</td>
</tr>
<tr>
<td>id</td>
<td>Alert ID. The alert ID uniquely identifies an outstanding alert on some object within the system. Alert IDs are automatically generated by the HPE 3PAR OS and increment when a new alert on a new object is detected. If an alert is generated on an object, and alerts already exist in the system, the alert ID is removed. For alert state traps, the alert ID is the same as the ID of the trap that indicated the original problem.</td>
<td>Read-only</td>
</tr>
<tr>
<td>messageCode</td>
<td>Code that identifies the specific type of alert or alert state change. For example, the message code for the alert state change is 1245186. For information about system alerts, see the <em>HPE 3PAR Alerts Reference: Customer Edition</em>.</td>
<td>Read-only</td>
</tr>
<tr>
<td>state</td>
<td>Current alert state, which is an integer between 0 and 6. See Alert State Values for definitions for each integer. Alert states enable users to maintain detailed tracking of alerts throughout their life cycle.</td>
<td>Read-only</td>
</tr>
<tr>
<td>serialNumber</td>
<td>The serial-number of the HPE 3PAR StoreServ system.</td>
<td>Read-Only</td>
</tr>
<tr>
<td>catalogKey</td>
<td>An extension of the message code.</td>
<td>Read-Only</td>
</tr>
<tr>
<td>detailedMessage</td>
<td>An extension of the details component. It provides more specific details of the alerting condition.</td>
<td>Read-Only</td>
</tr>
<tr>
<td>tier</td>
<td>Indicates the event-type tier, for instance &quot;general&quot; or &quot;hardware check&quot;.</td>
<td>Read-Only</td>
</tr>
<tr>
<td>sparePartNumber</td>
<td>Indicates the spare part number, if available, for events in the hardware tiers.</td>
<td>Read-Only</td>
</tr>
</tbody>
</table>

The following table displays the contents of the `nodeCpuStatsTable`:

**Table 10: Contents of the nodeCpuStatsTable**

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>nodeCpuStatsIndex</td>
<td>3PAR node ID plus 1.</td>
<td>Not-accessible. This is the index to the table</td>
</tr>
<tr>
<td>nodeCpuStatsNs</td>
<td>Node nanoseconds when stats were read.</td>
<td>Read-only</td>
</tr>
<tr>
<td>Component</td>
<td>Description</td>
<td>Access</td>
</tr>
<tr>
<td>--------------------------------------------------------</td>
<td>--------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>nodeCpuStatsNumCpus iso. 3.6.1.4.1.12925.1.9.3.1.1.3</td>
<td>The number of CPUs in the node.</td>
<td>Read-only</td>
</tr>
<tr>
<td>nodeCpuStatsInterupts iso. 3.6.1.4.1.12925.1.9.3.1.1.4</td>
<td>Total number of interrupts serviced on the node since boot time.</td>
<td>Read-only</td>
</tr>
<tr>
<td>nodeCpuStatsContextSwitches iso. 3.6.1.4.1.12925.1.9.3.1.1.5</td>
<td>Total number of context switches across all CPUs on the node since boot time.</td>
<td>Read-only</td>
</tr>
<tr>
<td>nodeCpuStatsBootTime iso. 3.6.1.4.1.12925.1.9.3.1.1.6</td>
<td>Time in the epoch when the node was booted. The epoch started at midnight on January 1 1970 UTC.</td>
<td>Read-only</td>
</tr>
<tr>
<td>nodeCpuStatsProcs iso. 3.6.1.4.1.12925.1.9.3.1.1.7</td>
<td>Total number of processes created since the node was booted.</td>
<td>Read-only</td>
</tr>
</tbody>
</table>

The following table displays the contents of the cpuStatsTable:

### Table 11: Contents of the cpuStatsTable

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>nodeCpuStatsIndex iso. 3.6.1.4.1.12925.1.9.3.1.1.1</td>
<td>3PAR node ID plus 1.</td>
<td>Not-accessible</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This is the first of the two indices to the table.</td>
</tr>
<tr>
<td>cpuStatsIndex iso. 3.6.1.4.1.12925.1.9.3.2.1.1</td>
<td>CPU number starting from 1.</td>
<td>Not-accessible</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This is the second of the two indices to the table.</td>
</tr>
<tr>
<td>cpuStatsUser iso. 3.6.1.4.1.12925.1.9.3.2.1.2</td>
<td>Total time spent executing user processes on the cpu since the node booted.</td>
<td>Read-only</td>
</tr>
<tr>
<td>cpuStatsSys iso. 3.6.1.4.1.12925.1.9.3.2.1.3</td>
<td>Total time spent executing user processes on the cpu since the node booted.</td>
<td>Read-only</td>
</tr>
<tr>
<td>Component</td>
<td>Description</td>
<td>Access</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>cpuStatsIdle iso.</td>
<td>Total idle time on the cpu since the node</td>
<td>Read-only</td>
</tr>
<tr>
<td>3.6.1.4.1.12925.1.9.3.2.1.4</td>
<td>booted.</td>
<td></td>
</tr>
<tr>
<td>cpuStatsNodeNs iso.</td>
<td>Node nanoseconds when stats were read.</td>
<td>Read-only</td>
</tr>
<tr>
<td>3.6.1.4.1.12925.1.9.3.2.1.5</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The following is sample output from an `snmpwalk` of the `cpuStatsMIB`:

```
HPE 3PAR SNMP infrastructure
```
Sent GET request to myhost.mycompany.com : 161

.iso.org.dod.internet.private.enterprises.threepar.inserv.cpuStatsMIB

nodeCpuStatsNs.1
22651696611641
nodeCpuStatsNs.2
22651697040261
nodeCpuStatsNumCpus.1
8
nodeCpuStatsNumCpus.2
8
nodeCpuStatsInterupts.1
137572801
nodeCpuStatsInterupts.2
177495998
nodeCpuStatsContextSwitches.1
234557755
nodeCpuStatsContextSwitches.2
292864989
nodeCpuStatsBootTime.1
1481834696
nodeCpuStatsBootTime.2
1481834694
nodeCpuStatsProcs.1
25035
nodeCpuStatsProcs.2
175762
cpuStatsUser.1.1
32303
cpuStatsUser.1.2
28179
cpuStatsUser.1.3
33917
cpuStatsUser.1.4
29734
cpuStatsUser.1.5
30724
cpuStatsUser.1.6
27333
cpuStatsUser.1.7
26015
cpuStatsUser.1.8
25326
cpuStatsUser.2.1
30956
cpuStatsUser.2.2
33363
cpuStatsUser.2.3
37210
cpuStatsUser.2.4
35096
cpuStatsUser.2.5
33614
cpuStatsUser.2.6
28802
cpuStatsUser.2.7
35328
cpuStatsUser.2.8

HPE 3PAR SNMP infrastructure
<table>
<thead>
<tr>
<th>cpuStatsSys.1.1</th>
<th>30641</th>
</tr>
</thead>
<tbody>
<tr>
<td>cpuStatsSys.1.2</td>
<td>35197</td>
</tr>
<tr>
<td>cpuStatsSys.1.3</td>
<td>41444</td>
</tr>
<tr>
<td>cpuStatsSys.1.4</td>
<td>40661</td>
</tr>
<tr>
<td>cpuStatsSys.1.5</td>
<td>36259</td>
</tr>
<tr>
<td>cpuStatsSys.1.6</td>
<td>35740</td>
</tr>
<tr>
<td>cpuStatsSys.1.7</td>
<td>32086</td>
</tr>
<tr>
<td>cpuStatsSys.1.8</td>
<td>34202</td>
</tr>
<tr>
<td>cpuStatsSys.2.1</td>
<td>31372</td>
</tr>
<tr>
<td>cpuStatsSys.2.2</td>
<td>31372</td>
</tr>
<tr>
<td>cpuStatsSys.2.3</td>
<td>31372</td>
</tr>
<tr>
<td>cpuStatsSys.2.4</td>
<td>31372</td>
</tr>
<tr>
<td>cpuStatsSys.2.5</td>
<td>31372</td>
</tr>
<tr>
<td>cpuStatsSys.2.6</td>
<td>31372</td>
</tr>
<tr>
<td>cpuStatsSys.2.7</td>
<td>31372</td>
</tr>
<tr>
<td>cpuStatsSys.2.8</td>
<td>31372</td>
</tr>
<tr>
<td>cpuStatsIdle.1.1</td>
<td>2167168</td>
</tr>
<tr>
<td>cpuStatsIdle.1.2</td>
<td>2175041</td>
</tr>
<tr>
<td>cpuStatsIdle.1.3</td>
<td>2166878</td>
</tr>
<tr>
<td>cpuStatsIdle.1.4</td>
<td>2173461</td>
</tr>
<tr>
<td>cpuStatsIdle.1.5</td>
<td>2169318</td>
</tr>
<tr>
<td>cpuStatsIdle.1.6</td>
<td>2177140</td>
</tr>
<tr>
<td>cpuStatsIdle.1.7</td>
<td>2168567</td>
</tr>
<tr>
<td>cpuStatsIdle.1.8</td>
<td>2178879</td>
</tr>
<tr>
<td>cpuStatsIdle.2.1</td>
<td>2146065</td>
</tr>
<tr>
<td>cpuStatsIdle.2.2</td>
<td>2137008</td>
</tr>
<tr>
<td>cpuStatsIdle.2.3</td>
<td>2138447</td>
</tr>
<tr>
<td>cpuStatsIdle.2.4</td>
<td>2136965</td>
</tr>
<tr>
<td>cpuStatsIdle.2.5</td>
<td>2144259</td>
</tr>
<tr>
<td>cpuStatsIdle.2.6</td>
<td>2138447</td>
</tr>
</tbody>
</table>
Severity levels of the alert state

The severity level of the alert (or alert state change) indicates how critical the alert should be considered. Severity is denoted by an integer, from the most severe (0) to least (6).

Table 12: Alert severity levels

<table>
<thead>
<tr>
<th>Severity Level</th>
<th>State</th>
<th>Description of the Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Fatal</td>
<td>Indicates that an error has occurred but it is too late to take any action.</td>
</tr>
<tr>
<td>1</td>
<td>Critical</td>
<td>An action is needed immediately and scope of the error is broad.</td>
</tr>
<tr>
<td>2</td>
<td>Major</td>
<td>An action is needed, the situation is serious.</td>
</tr>
<tr>
<td>3</td>
<td>Minor</td>
<td>An action is needed, but the situation is not serious.</td>
</tr>
<tr>
<td>4</td>
<td>Degraded/warning</td>
<td>The user decides whether to take an action.</td>
</tr>
<tr>
<td>Severity Level</td>
<td>State</td>
<td>Description of the Severity</td>
</tr>
<tr>
<td>----------------</td>
<td>--------</td>
<td>-----------------------------------------------------------------</td>
</tr>
<tr>
<td>5</td>
<td>Informational</td>
<td>Indicates a status change that is not an error.</td>
</tr>
<tr>
<td>6</td>
<td>Debug</td>
<td>Information is logged for later analysis.</td>
</tr>
</tbody>
</table>

For more information on alerts, see the *HPE 3PAR Alerts Reference: Customer Edition*.

**Alert state values**

The values for each alert state is as follows:

**Table 13: Alert state values**

<table>
<thead>
<tr>
<th>Value</th>
<th>Alert State</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Undefined</td>
</tr>
<tr>
<td>1</td>
<td>New</td>
</tr>
<tr>
<td>2</td>
<td>Acknowledged</td>
</tr>
<tr>
<td>3</td>
<td>Fixed</td>
</tr>
<tr>
<td>4</td>
<td>Removed</td>
</tr>
<tr>
<td>5</td>
<td>Autofixed</td>
</tr>
</tbody>
</table>

**alertNotify traps**

The snmpagent reports system alerts, as described in the *HPE 3PAR Alerts Reference: Customer Edition*, using alertNotify traps. An alertNotify trap contains details about an event that might affect system operations and performance. All alerts generated by the system and all alert status change events are translated into alertNotify traps.

The following example shows an alertNotify trap translated from an alert:
For information about system alerts, see the HPE 3PAR Alerts Reference: Customer Edition.

Alert state has changed

If you receive a trap with `messageCode == 1245186`, an alert has changed state. To find out which alert has changed state, you must extract the alert ID from the `id` trap field.

The following information describes these alert status change events:

<table>
<thead>
<tr>
<th>Message Code</th>
<th>Severity</th>
<th>Type</th>
<th>Alert String</th>
<th>Operator Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1245186 (0x0130002)</td>
<td>Info</td>
<td>Change in alert state</td>
<td>Alert &lt;alert_id&gt; changed from state &lt;old_state&gt; to &lt;new_state&gt;</td>
<td>The alert has changed state. This can be used to track the state of the existing alerts in a system.</td>
</tr>
</tbody>
</table>
An alert status change event is not an alert. It notifies you that an alert has changed status (for example, from New to Resolved by System). The following example shows an alertNotify trap translated from an alert status change event:

```
sysUpTime.0:0:0 hours, 5 minutes, 26 seconds.
snmpTrapOID.0: iso.org.dod.internet.private.enterprises.threepar.inserv.alertNotify
component.1:comp_sw_alert
details.1:Alert 647 changed from state New to Resolved by System
nodeID.1:1
severity.1:info(5)
timeOccurred.1:Thu Dec 16 14:06:36 PST 2004
id.1:647
messageCode.1:1245186
state.1:autofixed(5)
```

storeServAlert Traps

A storeServAlert trap contains details about an event that might affect system operations and performance. Selected alerts generated by the system and are translated into storeServAlert traps. StoreServAlerts are enabled for an snmp manager with the `-notify` option for the addsnmpmgr or setsnmpmgr commands.

The following example shows an storeServAlert trap translated from an alert:

```
.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0: TimeTicks: 1 day, 7 hours, 3 minutes, 25 seconds.
.iso.org.dod.internet.snmpV2.snmpModules.snmpMIB.snmpMIBObjects.snmpTrap.snm
pTrapOID.0: Object ID: .1.3.6.1.4.1.12925.1.2.0.198:
.iso.org.dod.internet.private.enterprises.threepar.inserv.alertTable.alertEn
try.component.1: sw_rmm_link: 1047: s99282_0_3_1:
.iso.org.dod.internet.private.enterprises.threepar.inserv.alertTable.alertEn
ty detalles.1: Remote Copy Link 1047(s99282_0_3_1) Failed (Down Due To Send Error Or Missing Heartbeat {0x1})
.iso.org.dod.internet.private.enterprises.threepar.inserv.alertTable.alertEn
ty.nodeID.1: Gauge: 0:
.iso.org.dod.internet.private.enterprises.threepar.inserv.alertTable.alertEn
ty.severity.1: INTEGER: 2:
.iso.org.dod.internet.private.enterprises.threepar.inserv.alertTable.alertEn
ty.timeOccurred.1: 2017-06-06 16:57:08 PDT:
.iso.org.dod.internet.private.enterprises.threepar.inserv.alertTable.alertEn
ty.id.1: Gauge: 1414:
.iso.org.dod.internet.private.enterprises.threepar.inserv.alertTable.alertEn
ty.messageCode.1: Gauge: 3801338:
.iso.org.dod.internet.private.enterprises.threepar.inserv.alertTable.alertEn
ty.state.1: INTEGER: 1:
.iso.org.dod.internet.private.enterprises.threepar.inserv.alertTable.alertEn
ty.serialNumber.1: 1999281:
.iso.org.dod.internet.private.enterprises.threepar.inserv.alertTable.alertEn
ty.tier.1: General:
.iso.org.dod.internet.private.enterprises.threepar.inserv.alertTable.alertEn
ty.sparePartNumber.1: HPE 3PAR SNMP infrastructure
```

HPE 3PAR SNMP infrastructure  85
The HPE 3PAR Common Information Model Application Programming Interface (CIM API) is the Hewlett Packard Enterprise industry-standard API based on the SNIA Storage Management Initiative Specification (SMI-S).

For detailed information about the HPE 3PAR CIM API, see the *HPE 3PAR CIM API Programming Reference*.

**SMI-S**

SMI-S enables management of SANs in a heterogeneous multi-vendor environment. SMI-S uses an object-oriented model based on the CIM to define objects and services which comprise a SAN. By leveraging vendor- and technology-independent standards, SMI-S allows management application vendors to create applications that work across products from multiple vendors.

The SMI-S model is divided into several profiles, each of which describes a particular class of SAN entities, such as disk arrays. These profiles allow for differences in implementations but provide a consistent approach for clients to discover and manage SAN resources and facilitate interoperability across vendor products within the SAN.

SMI-S also defines an automated resource discovery process using Service Location Protocol version 2 (SLPv2). This allows management applications to automatically find SAN resources, and then probe them to determine which of the SMI-S profiles and features they support.

**WBEM initiative**

SMI-S is based on the Web-Based Enterprise Management (WBEM) initiative, which is defined by the Distributed Management Task Force (DMTF). WBEM is a set of management and Internet standard technologies developed to unify the management of distributed computing environments.

The DMTF has developed a core set of standards that make up WBEM:

- **The CIM standard**—The data model for WBEM. CIM provides a conceptual framework for describing management data for systems, networks, applications and services, and allows for vendor extensions. SMI-S uses CIM to model those objects and relationships that comprise a SAN.

- **CIM-XML**—A method of exchanging CIM management data. CIM-XML uses an xmlCIM payload and HTTP (or HTTPS) as the transport mechanism.

This protocol is defined by the following specifications:

- **Specification for the Representation of CIM in XML**—Defines a standard for the representation of CIM elements and messages in XML, written in Document Type Definition (DTD).

- **CIM Operations over HTTP**—Defines a mapping of CIM Messages onto HTTP that allows implementations of CIM to interoperate in an open, standardized manner. It uses the CIM XML DTD that defines the XML Schema for CIM objects and messages.

- **WBEM Discovery using SLP**—WBEM discovery using SLP is a method for applications to identify WBEM-based management systems.

For more information regarding WBEM and CIM, see the DMTF web site: [http://www.dmtf.org](http://www.dmtf.org)

**HPE 3PAR CIM support**

The following sections provide information about the HPE 3PAR CIM API provided with HPE 3PAR OS Version 3.3.1.
Standard compliance

- The HPE 3PAR CIM Server supports SMI-S version 1.5.
- The HPE 3PAR CIM API passes SNIA-CTP conformance. For additional information, see http://www.snia.org.

SMI-S profiles

SMI-S defines profiles that are used to manage the elements of a SAN. These SMI-S Profiles are described in detail in the HPE 3PAR CIM API Programming Reference.

Supported extensions

The HPE 3PAR CIM server supports additional classes that provide management for system specific features not covered by SMI-S.

For more information, see the HPE 3PAR CIM API Programming Reference.

CIM indications

SMI-S provides for asynchronous notification of events that indicate changes in the CIM server or the managed elements that are controlled by the CIM server. CIM Indications are the mechanism for delivery of such events. A CIM client must subscribe to indications that it wants to receive the event notifications from the CIM server. For detailed information regarding indications, see SMI-S at the following website: http://www.snia.org

The HPE 3PAR CIM Server currently supports indication subscriptions for changes in the operational status of FC ports. For more information, see the HPE 3PAR CIM API Programming Reference.
Comparing HPE 3PAR to EVA terms

This comparison of EVA and HPE 3PAR terms is intended to be a General Guide to similar concepts. These terms do not necessarily represent exactly the same entities with all the same properties in both product lines. For detailed descriptions of each term, see the EVA or HPE 3PAR glossary.

<table>
<thead>
<tr>
<th>EVA term</th>
<th>HPE 3PAR term</th>
</tr>
</thead>
<tbody>
<tr>
<td>controller</td>
<td>node, controller node</td>
</tr>
<tr>
<td>EVA firmware (controller software)</td>
<td>HPE 3PAR OS</td>
</tr>
<tr>
<td>disk groups</td>
<td>CPGs</td>
</tr>
<tr>
<td>host</td>
<td>host</td>
</tr>
<tr>
<td>LUN</td>
<td>LUN</td>
</tr>
<tr>
<td>P6000 Command View</td>
<td>StoreServ Management Console (SSMC)</td>
</tr>
<tr>
<td>ports (iSCSi or FC)</td>
<td>ports (iSCSi or FC)</td>
</tr>
<tr>
<td>presentation (to host)</td>
<td>export (to host)</td>
</tr>
<tr>
<td>provisioning, thin provisioning</td>
<td>provisioning, full provisioning, thin provisioning</td>
</tr>
<tr>
<td>redundancy level (Vraid)</td>
<td>RAID</td>
</tr>
<tr>
<td>remote replication</td>
<td>Remote Copy</td>
</tr>
<tr>
<td>snapshot</td>
<td>physical copy</td>
</tr>
<tr>
<td>thinly-provisioned virtual volume (TPVV)</td>
<td>thinly-provisioned virtual volume (TPVV)</td>
</tr>
</tbody>
</table>
Support and other resources

Accessing Hewlett Packard Enterprise Support

• For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:
  
  http://www.hpe.com/assistance

• To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:
  
  http://www.hpe.com/support/hpesc

Information to collect

• Technical support registration number (if applicable)
• Product name, model or version, and serial number
• Operating system name and version
• Firmware version
• Error messages
• Product-specific reports and logs
• Add-on products or components
• Third-party products or components

Accessing updates

• Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.

• To download product updates:
  
  Hewlett Packard Enterprise Support Center
  www.hpe.com/support/hpesc

  Hewlett Packard Enterprise Support Center: Software downloads
  www.hpe.com/support/downloads

  Software Depot
  www.hpe.com/support/softwaredepot

• To subscribe to eNewsletters and alerts:
  
  www.hpe.com/support/e-updates

• To view and update your entitlements, and to link your contracts and warranties with your profile, go to the Hewlett Packard Enterprise Support Center More Information on Access to Support Materials page:
  
  www.hpe.com/support/AccessToSupportMaterials

IMPORTANT:

Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HPE Passport set up with relevant entitlements.
Customer self repair

Hewlett Packard Enterprise customer self repair (CSR) programs allow you to repair your product. If a CSR part needs to be replaced, it will be shipped directly to you so that you can install it at your convenience. Some parts do not qualify for CSR. Your Hewlett Packard Enterprise authorized service provider will determine whether a repair can be accomplished by CSR.

For more information about CSR, contact your local service provider or go to the CSR website:

http://www.hpe.com/support/selfrepair

Remote support

Remote support is available with supported devices as part of your warranty or contractual support agreement. It provides intelligent event diagnosis, and automatic, secure submission of hardware event notifications to Hewlett Packard Enterprise, which will initiate a fast and accurate resolution based on your product's service level. Hewlett Packard Enterprise strongly recommends that you register your device for remote support.

If your product includes additional remote support details, use search to locate that information.

Remote support and Proactive Care information

HPE Get Connected
www.hpe.com/services/getconnected

HPE Proactive Care services
www.hpe.com/services/proactivecare

HPE Proactive Care service: Supported products list
www.hpe.com/services/proactivecaresupportedproducts

HPE Proactive Care advanced service: Supported products list
www.hpe.com/services/proactivecareadvancedsupportedproducts

Proactive Care customer information

Proactive Care central
www.hpe.com/services/proactivecarecentral

Proactive Care service activation
www.hpe.com/services/proactivecarecentralgetstarted

Warranty information

To view the warranty for your product or to view the Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products reference document, go to the Enterprise Safety and Compliance website:

www.hpe.com/support/Safety-Compliance-EnterpriseProducts

Additional warranty information

HPE ProLiant and x86 Servers and Options
www.hpe.com/support/ProLiantServers-Warranties

HPE Enterprise Servers
www.hpe.com/support/EnterpriseServers-Warranties

HPE Storage Products
www.hpe.com/support/Storage-Warranties
Regulatory information

To view the regulatory information for your product, view the Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products, available at the Hewlett Packard Enterprise Support Center:

www.hpe.com/support/Safety-Compliance-EnterpriseProducts

Additional regulatory information

Hewlett Packard Enterprise is committed to providing our customers with information about the chemical substances in our products as needed to comply with legal requirements such as REACH (Regulation EC No 1907/2006 of the European Parliament and the Council). A chemical information report for this product can be found at:

www.hpe.com/info/reach

For Hewlett Packard Enterprise product environmental and safety information and compliance data, including RoHS and REACH, see:

www.hpe.com/info/ecodata

For Hewlett Packard Enterprise environmental information, including company programs, product recycling, and energy efficiency, see:

www.hpe.com/info/environment

Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (docsfeedback@hpe.com). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.
A

ACL
Access control list.

active host
A host that is connected to a system port and recognized by the HPE 3PAR Operating System.
A host is a path or set of paths, defined as either WWN or iSCSI names, to one or more ports on a system.

AD
Active Directory.

active VLUN
The pairing of a virtual volume and a LUN so the host can access its virtual volume and I/O writes can be saved to the virtual volume. The VLUN parameters determine whether a virtual volume is expressed as an active VLUN. VLUNs that are not active will not communicate with the HPE 3PAR StoreServ Storage system.

admin volume
The base volume that is used by the system to store administration data such as the system event log. The admin volume is created as part of the system installation and setup process.

administrative space
Also known as admin space. The area of the volume that corresponds to logical disk regions that track changes to the volume since the previous snapshot was created.

AFC
Adaptive flash cache.

alert
A system event that requires the immediate attention of the user and might also require user intervention.

allocation limit
A user-defined threshold that can be set for thinly provisioned virtual volumes and fully provisioned virtual volumes to cap their potential size.

ALPA
Arbitrated loop physical address.

ALUA
Asymmetric logical unit access.

AO
HPE 3PAR Adaptive Optimization.

aocfg
HPE 3PAR Adaptive Optimization configuration.
API
Application program interface.

ASIC
Application-specific integrated circuit.

ASM
Automatic storage management.

asynchronous periodic mode
Data replication in which the primary and secondary volumes are resynchronized at set times—for example, when scheduled or when resynchronization is manually initiated.

asynchronous streaming mode
Continuous (write-ordered) asynchronous replication between two sites over FCIP, RCIP, and RCFC on HPE 3PAR StoreServ Storage systems.

authentication key
A cryptographic key that protects data integrity on self-encrypting drives. The authentication key, maintained by a local key manager and backed up and guarded by system administrators, locks and unlocks the drive.

availability
Level of fault-tolerance for a logical disk. For example, magazine-level availability means that the logical disk can tolerate a drive magazine failure. Cage-level availability means that the logical disk can tolerate a drive cage failure.

base volume
A thinly provisioned virtual volume, thinly-provisioned deduplicated virtual volume, or fully provisioned virtual volume that has been copied.

A base volume can be considered to be the “original” VV and is either a fully-provisioned virtual volume, a thinly-provisioned virtual volume, or a thinly-provisioned deduplicated virtual volume.

Boolean
A setting which, when used for uninitialized attributes by a Jackson JSON processor, results in a value of null.

boolean
A setting which, when used for uninitialized attributes by a Jackson JSON processor, results in a value of 0 (zero).

CA
Certificate authority.

CHAP
Challenge Handshake Authentication Protocol.
chunklet
A block of contiguous storage space on a physical disk. On HPE 3PAR StoreServ Storage systems, all chunklets are 1 GB.

CIM
Common Information Model. An open standard interface for distributed storage management.

classes of service
The characteristics and guarantees of the transport layer of a Fibre Channel circuit. These classes include connection services (Class 1), guaranteed frame delivery with end-to-end flow control (Class 2), and packetized frame datagrams (Class 3).

cluster
A group of controller nodes connected via the same system backplane. The nodes in a cluster operate as a unified system, separate from any other clusters that may share the same service processor.

CMP
Cache memory page. A 16 KB block of control cache memory where I/O requests are stored.

CN
Common name.

CNA
Converged network adapter.

control cache
Memory modules that support the microprocessors located in a controller node.

controller
See controller node.

controller node
An individual device that works with other controller nodes to cache and manage data in a system and to provide hosts with a coherent, virtualized view of the storage system.

controller node chassis
An enclosure that houses all the controller nodes of a system.

copy data
Data that occupies the snapshot data space (virtual copy space) on a virtual volume.

copy space
Also known as snapshot space. The area of the volume that corresponds to logical disk regions that contain copies of user data that has changed since the previous snapshot.

copy-on-write snapshot
A snapshot of a virtual volume made with the copy-on-write technique. This type of snapshot consists of a pointer to the source volume and a record of every change made to the source volume since the snapshot was created.

CPG
Common provisioning group (also known as a storage pool or logical disk pool). A set of logical disks from which you can create virtual volumes and virtual copies that are capable of allocating storage on demand.
CRLF
Carriage-return and linefeed.

CSR
Certificate signing request.
Customer self-repair.

CSV
Cluster Shared Volumes.

cURL
A command line tool for retrieving or transmitting files using URL syntax.

D
Data at rest; archived data. Data at rest may also include data that is seldom accessed and that is stored on hard drives, backup disks, or on a storage area network.

data cache
The dual in-line memory modules that support the HPE 3PAR ASIC located in a controller node.

destination volume
The virtual volume to which data is copied during a virtual or physical copy operation.

DHCP
Dynamic Host Configuration Protocol.

DIT
Directory information tree

DM
Device-mapper.

DN
Distinguished name

DNS
Domain Name System.

DO
HPE 3PAR Dynamic Optimization.

DRAM
Dynamic random access memory.

drive cage
A component in a rack or chassis that contains a drive. Drive cages connect to nodes for communication with hosts.

drive magazine
An electronic circuit board mounted on a mechanical structure that is inserted into a drive bay in a drive cage. A drive magazine holds up to four physical disks.
DSA
  Digital Signature Algorithm.

DSF
  Device special file.

EKM
  External key management.

encryption key
  A cryptographic key that is not exposed outside of the drive itself. The encryption key is used to encrypt and decrypt all data stored on a drive.

event
  A detectable system occurrence.

export
  To present a virtual volume to a host. Exporting makes a volume available to a host by creating an association between the volume name and a logical unit number for the specified host and port.

FC
  Fast class (drive type)
  Fibre Channel (port).

FC adapter
  Fibre Channel adapter. A Fibre Channel PCI host bus adapter located in a controller node. The Fibre Channel adapter connects a controller node to a host or to a drive chassis.

FCoE
  Fibre Channel over Ethernet.

file persona
  The HPE 3PAR File Persona Software solution provides file services on an HPE 3PAR StoreServ Storage system.

file share
  A storage object containing the files to which the users and groups are allowed or disallowed access.

file store
  A storage container for file shares.

FIPS
  Federal Information Processing Standards.

file share
  A storage object containing the files to which the users and groups are allowed or disallowed access.

file store
  A storage container for file shares.
flash cache
The HPE 3PAR OS Adaptive Flash Cache feature extends your cache space using space on your SSDs.

FMP
Flash cache memory page.

FPG
File provisioning group. An FPG is the highest-level object in the HPE 3PAR StoreServ Storage file service object hierarchy. FPGs contain the virtual file servers.

FPVV
Fully provisioned virtual volume. A virtual volume with a fixed amount of user space.

FQDN
Fully qualified domain name.

FRA
Flash recovery area.

fstore
File store.

GB
Gigabyte.

Gb/s
Gigabits per second.

GB/s
Gigabytes per second.

Gbps
Gigabytes per second.

GigE
Gigabit Ethernet.

GiB
1 gibibyte = $2^{30}$ bytes = 1,073,741,824 bytes = 1024 mebibytes.

grow
To increase the size of a virtual volume or common provisioning group.

growth increment
The unit of storage space by which the system creates and allocates additional logical disks to a CPG when the volumes in that CPG require additional resources. The minimum growth increment varies according to the number of controller nodes in the system (from 8 GB for a two-node system to 32 GB for an eight-node system).
growth limit
   An optional setting that enables you to specify the maximum size to which a common provisioning group can grow.

growth warning
   An optional setting that enables you to specify the size at which the system alerts you to the amount of growth in a common provisioning group.

GSSAPI
   Generic Security Service Application Program Interface.

HA
   High availability.

HBA
   Host bus adapter.

HCS
   Hitachi Command Suite.

HDLM
   Hitachi Dynamic Link Manager.

host
   A path or set of paths, defined as either WWN or iSCSI names, to one or more ports on a system.

host cluster
   A VMware ESX cluster or a Windows Server failover cluster.

host definition
   The name of the host and the list of the paths (WWN or iSCSI) assigned to the host, if any. If you remove all the paths assigned to the host, the host name becomes the host definition.

host group
   An HDS Storage object that contains World Wide Names of hosts and logical unit numbers presented to them.

host persona
   A set of behaviors that allows hosts connected to FC or iSCSI ports on the system to deviate from the default host behavior.

host sees VLUN template
   A VLUN template that allows a specified host connected to any port to see a virtual volume as a specified logical unit number (LUN).

host set VLUN template
   A VLUN template that allows any host that is a member of the host set to see a volume.

HPE 3PAR Recovery Manager software
   A data-protection solution that provides restore operations for a variety of platforms, such as Oracle, SQL Server, Exchange, and more.
HPE 3PAR Remote Copy software
Software that enables you to create and continually update backup remote copies of virtual volumes and use those copies for disaster recovery, if necessary.

HPE 3PAR System Tuner software
A utility that enables the system to reallocate space usage in order to take advantage of additional resources, such as added hardware or updated CPGs. The system tuner identifies underused chunklets and overused volumes, and balances the usage.

HPE 3PAR Thin Provisioning software
Software that enables you to create a virtual volume that allocates resources from the CPG on demand and in small increments.

HPE 3PAR Virtual Copy software
Software that enables you to create virtual copies (also known as snapshots) of virtual volumes. To create a virtual copy, the system uses the copy-on-write technique, which creates an up-to-date snapshot at the same time as data is written to the host.

HPE 3PAR Virtual Domains software
Software that enables you to create distinct domains with domain-specific users and objects.

HTTPS
Hypertext Transfer Protocol Secure.

ID
Identifier.

IETF
Internet Engineering Task Force.

inactive host
A host that is known to the HPE 3PAR OS, but is not recognized as connected to any system port at the moment.

initiator port
A port that is connected to and relays commands to physical disks within a drive cage. Also known as a disk port.

IOPS
Input/output per second.

iSCSI
Internet Small Computer System Interface.

iSCSI name
The name of an iSCSI path. You use an iSCSI name to identify that iSCSI path to a host.

iSNS
Internet Storage Name Service.

ISO
International Standards Organization.
JFS
Journaling file system.

JSON
Javascript Object Notation.

KB/s
Kilobytes per second.

Latency
A measure of time delay experienced in a network. Round-trip latency measures the time for a signal to go from source to destination and back to the source.

LD
Logical disk. A collection of chunklets that reside on different physical disks and that are arranged as rows of RAID sets. When you create a CPG, the system creates and groups logical disks and assigns those logical disks to the CPG.

LDAP

LDEV
Logical device. HDS Storage term for volume.

LDRG
Logical drive (disk) region.

LFF
Large form factor.

LIP
Loop Initialization Primitive. The protocol by which a Fibre Channel Arbitrated Loop network initializes upon power-up or recovers after a failure or other unexpected condition. During loop initialization, the nodes present on the arbitrated loop identify themselves and acquire addresses on the loop. No data can be transferred on an arbitrated loop until initialization completes.

Logging
Temporarily saving data to logging logical disks when physical disks are out of service (due to failure or during replacement procedures).

Logging LD
Logging logical disk. A logical disk used for logging. During system setup, the system creates a logging LD for each controller node in the system.

LSI
Large-scale integration.
**LUN**

Logical unit number. A number used to access a virtual volume that has been assigned to a particular host on a particular port.

**LUSE**

Logical unit size expansion.

**LVM**

HP-UX Logical Volume Manager.

**MAC address**

Media Access Control address.

**management console**

The HPE 3PAR StoreServ Management Console is a graphical user interface for monitoring, managing, and configuring HPE 3PAR StoreServ Storage systems.

**mapping**

The correspondence of LD regions to virtual volume regions.

**matched-set VLUN template**

A rule that allows a particular host connected to a particular port to see a virtual volume as a specified LUN.

**MB**

Megabyte (1,000,000 or \(10^6\) bytes).

**Mb**

Megabit (1,048,576 or \(2^{20}\) bits).

**MB/s**

Megabytes per second.

**MC**

HPE 3PAR Management Console (formerly IMC).

**message code**

A keycode that identifies a system alert.

**MDM**

Minimally disruptive migration.

**MIB**

Management information base.

**MiB**

Mebibyte (1,048,576 or \(2^{20}\) bytes).

**mirror**

One member of a group of mirrored chunklets, which is also known as a RAID 1 set.
mirroring
A data redundancy technique used by some RAID levels (in particular, RAID 1) to provide data protection on a storage array.

MPIO
Multipath input/output.

MSCS
Microsoft Cluster Service.

MSFC
Microsoft Failover Cluster.

MTU
Maximum transmission unit.

MU
Maintenance update.

N

ACA
Normal Auto Contingent Allegiance.

NFS
Network File System.

NIC
Network interface card.

NL
Near line.

node cabinet
A cabinet that houses the system backplane and controller nodes.

NPIV
N_Port ID Virtualization.

NTP
Network Time Protocol.

OCR
Optical character recognition.

ODM
IBM AIX Object Data Manager.

OLTP
Online transaction processing.
parent volume
A virtual volume from which a virtual or physical copy is made.

PCI
Peripheral component interconnect.

Pct
Percent.

PD
Physical disk. A dual-ported Fibre Channel or SAS disk mounted onto a drive enclosure.

PE
Protocol endpoint.

PEM
Privacy Enhanced Mail.

PFC
Primary flow control.

physical copy
A point-in-time copy of an entire virtual volume.

physical size
The total actual raw storage allocated to a logical disk, as determined by its size and RAID type.

PLOGI ACC
Port Login Accept Payload.

port-presents VLUN template
A VLUN template that allows any host connected to a particular port to see a virtual volume as a specified LUN.

presentation (to host)
EMC Storage and HDS Storage term for export (to host).

preserved data
Data that is suspended in the system cache memory due to backend failure.
primary path
Connection between a controller node initiator port and a physical disk that is used by default. When the primary path cannot be used (a failure condition), the secondary path is used. The primary and secondary paths are not user configurable and are determined by drive magazine placement.

primary storage system
One of two storage systems in a remote copy pair. The primary storage system holds the original virtual volumes which are replicated to the secondary storage system.

primary volume group
The volume group that resides on the primary storage system and that receives data from the host. The primary volume group is linked to a secondary volume group on the secondary storage system.

PRLI
Process login.

promote
For physical copies: to break the association between a physical copy and a base volume by changing the physical copy into an independent base volume.
For virtual copies: to copy the changes from a virtual copy back onto the base volume, therefore overwriting the base volume with the virtual copy.

PVID
Physical-volume identifier.

Q
QA
Quorum announcer.

QoS
Quality of service. HPE 3PAR Priority Optimization software provides quality-of-service rules to manage and control the I/O capacity of an HPE 3PAR StoreServ Storage system across multiple workloads.

QW
Quorum witness.

R
RAID
Redundant array of independent disks.

RAID 0 set
Striped rows of chunklets on two or more physical disks. A RAID 0 set offers no data redundancy.

RAID set
A grouping of mirrored or parity-protected chunklets.

RAID type
RAID 0, RAID 10 (1), RAID 50 (5), and RAID MP (6) are all supported RAID types; however, not all RAID types may be available on your system.
RC
HPE 3PAR Remote Copy.

RCFC
Remote copy over Fibre Channel. The use of remote copy with two systems that are connected through Fibre Channel ports.

RCIP
Remote copy over IP. The use of remote copy with two systems that are connected via Ethernet ports.

RDM
Raw device mapping.

region
A subdivision of a logical disk or virtual volume. The size of a region is always a multiple of 32 MB.

remote copy volume group
A pair of virtual volume sets that are logically related and that are used when data needs to be consistent between specified sets of virtual volumes.

remote replication
EMC Storage term for remote copy

resynchronize
To copy changes from one volume in a physical copy pair to the other volume because the original volume was modified at some point after the physical copy operation took place.

RFC
Request for comments.

RHEL
Red Hat Enterprise Linux.

RO
Read-only.

roles and rights
The roles and rights assigned to a user determine which tasks the user can perform with a system.

RPO
Recovery point objective—the maximum amount of acceptable data loss in the event of a disaster. RPO is generally specified as an amount of time (minutes, hours, days, …). The RPO may be zero.

RSA
Rivest-Shamir-Adleman cryptosystem.

RTPG
Report target port group.

RTT
Round-trip time—the time, in milliseconds, that a signal takes to be sent plus the time it takes for receipt of the signal to be acknowledged.

RW
Read-write.
SAS
Serial attached SCSI.

SASL
Simple Authentication and Security Layer.

SATA
Serial Advanced Technology Attachment.

SATP
Storage array type plugin.

SC
HPE 3PAR Service Console.

secondary path
Connection between a controller node initiator port and a physical disk that is used when the primary path is inaccessible (a failure condition). The primary and secondary paths are not user-configurable; they are determined by drive magazine placement.

secondary storage system
The second storage system in a remote copy pair.

SDK
Software developer kit.

secondary volume group
The volume group that resides on the secondary storage system and that receives data from the primary volume group in a remote copy pair.

SED
Self-encrypting drive. An SED uses Advanced Encryption Standard keys to protect data from unauthorized access. SEDs contain special firmware and an ASIC that provides encryption. When encryption is enabled, the SED will lock when power is removed, and it will not be unlocked until the matching key from the HP 3PAR StoreServ system is used to unlock it.

SELinux

service console
The HPE 3PAR Service Console provides access to the HPE 3PAR Service processor through a browser. Using the service console, you can initialize the service processor, manage service processor services, add HPE 3PAR StoreServ Storage systems, and collect support data.

service processor
The HPE 3PAR Service Processor is a hardware device inserted into a rack, or virtual software, that enables you to monitor and service HPE 3PAR StoreServ Storage systems. The service processor functions as the communication interface between the IP network and the HPE PAR support center by managing all service-related communications.

set size
The number of chunklets in a set. Also known as mirror depth for RAID 1 sets and parity set for RAID 5 sets.
SFF
Small form factor.

SFP
Small form factor pluggable.

SIOC
Semantically-Interlinked Online Communities.

SLD
Synchronous long distance. In an SLD configuration, remote copy volume groups from the primary system are replicated to two separate target arrays simultaneously. Data is replicated to one target in synchronous mode and to the other target in asynchronous periodic mode.

SLES
SUSE Linux Enterprise Server.

SLVM
Shared Logical Volume Manager.

SMB
Server Message Block protocol.

SMI-S
Storage Management Initiative Specification.

SMI-S CIM
Storage Management Initiative Specification Common Information Model.

snapshot
A virtual or physical copy of a virtual volume.

snapshot administration space
The space on a virtual volume that is used to track changes to the data from the time that a snapshot of a virtual volume was created.

source volume
The virtual volume from which a copy is made.

SP
HPE 3PAR Service Processor.

spare chunklet
A chunklet that is reserved for use in case of a failure in the system. A certain number of chunklets are reserved for use as spares during the system setup and installation process; however, the system may temporarily set aside additional spares even though these chunklets are not permanently designated for use as spares.

spare status
Indicates whether a chunklet is reserved as a spare or has been selected by the system for use in sparing on a temporary basis.

sparing
The automatic relocation of chunklets on a physical disk when a logging logical disk becomes full.
SPLOR data
Health data collected by the HPE 3PAR Service Console from the service processor and sent to Hewlett Packard Enterprise.

SPOCC
Service Process Online Customer Care.

SPOCK
Single Point of Connectivity Knowledge for HPE Storage Products website. SPOCK is the primary portal used to obtain detailed information about supported HPE 3PAR StoreServ Storage product configurations.

SPOCK (http://www.hpe.com/storage/spock)

SR
HPE 3PAR System Reporter.

SRDF
Symmetrix Remote Data Facility.

SRU
System resource usage.

SSD
Solid-state drive.

SSL
Secure Sockets Layer.

SSMC
HPE 3PAR StoreServ Management Console.

storage group
An EMC Storage object that contains WWNs of hosts and LUNs presented to them.

Storage DRS
VMware vSphere Storage Distributed Resource Scheduler.

STGT
SendTargets Group Tag.

storage system
A storage system includes the hardware components that physically store data as well as the software applications that manage the data.

STP
Spanning Tree Protocol.

SVP
See service processor.
support data
Support data can be retrieved for the service processor and the storage system and sent to Hewlett Packard Enterprise Support. The data collected by the service processor is used to maintain, troubleshoot, and upgrade the HPE 3PAR Service Processor and the HPE 3PAR StoreServ Storage system.

synchronization mode
The method by which data on a remote copy pair are made consistent. Synchronization modes are:
• Synchronous
• Asynchronous periodic
• For HPE 3PAR OS 3.3.1 and later: Asynchronous streaming

system mode
Data replication that writes data to the primary and secondary sites simultaneously over a network, such that data remains current between sites.

tsysmgr
System manager. Software component that negotiates between the system and the user interfaces such as the HPE 3PAR StoreServ Management Console and the HPE 3PAR CLI.

system
Refer to the HPE 3PAR StoreServ Storage and all its hardware and software components.

system backplane
An electronic circuit board that contains sockets into which power supplies and controller nodes are plugged.

target mode
The firmware setting for a port that is connected to a host.

target port
The port that is connected to and receives commands from a host computer. Also known as a host port.

TB
Terabytes.

Tcl
Tool command language.

TDVV
Thinly provisioned deduplicated virtual volume. TDVVs are thinly provisioned virtual volumes with in-line data deduplication. A TDVV has the same characteristics as a TPVV, with the additional capability of removing duplicated data before it is written to the volume.

TiB
Tebibyte [1 tebibyte = \(2^{40}\) bytes= 1099511627776 bytes = 1024 gigabytes].

TLS
Transport Layer Security.
TPVV
Thinly provisioned virtual volume. A virtual volume that maps to logical disk space associated with a common provisioning group and capable of growing on demand.

TUI
Text-based user interface. The HPE 3PAR Service Processor comes preinstalled with a service console TUI that is run automatically when you log into the Linux console as admin. The TUI enables limited configuration and management of the service processor and access to the 3PAR command line interface of an attached HPE StoreServ Storage.

UDID
Unique device identifier.

UID (light)
Unit identification (light).

URI
Uniform Resource Identifier.

UTF
Uniform Transformation Format.

utility
A software program that manages storage systems or servers.

UUID
Universally unique identifier.

user data
For standard base volumes, the data that is written to the user space.

user size
The amount of user space in a virtual volume, or the size of the volume as presented to the host.

user space
The space on a virtual volume that represents the size of the virtual volume as presented to the host. For standard base volumes, the user space holds all user data. For TPVVs or TDVVs, no storage is actually allocated to user space, so the user space represents the virtual size of the volume.

VAAI
VMware vStorage APIs for Array Integration.

VASA
VMware vSphere API for Storage Awareness.

VCN
VLUN change notification.
VFS
Virtual file server. VFSs act as a virtual device that controls many of the network policies for communications between the HPE 3PAR StoreServ Storage file service objects and your network. Many management tasks and policy decisions can be performed at the VFS level. VFSs contain the file stores.

virtual copy
A snapshot created using the copy-on-write technique.

virtual size
The size that the volume presents to the host. For standard base volumes, the virtual size is equal to the user space. For thinly provisioned virtual volumes, no storage is actually allocated to user space, so the virtual size is determined by whatever value is assigned to the user space.

virtual volume
A virtual storage unit created by mapping data from one or more logical disks.

virtual volume region
A subdivision of a virtual volume. The size of a region is always a multiple of 32 MB.

VLAN
Virtual local area network.

VLUN
Virtual logical unit number. A VLUN is a virtual volume-LUN pairing expressed as either an active VLUN or as a VLUN template.

VLUN template
A rule that sets up the association between the name of the virtual volume and a LUN-host, LUN-port, or LUN-host-port combination. The three types of VLUN templates are host sees, port presents, and matched set.

VM
Virtual machine.

VMCA
VMware Certificate Authority.

VMDK
Virtual Machine Disk file format.

VMFS
Virtual Machine File System on VMware.

vMSC
VMware vSphere Metro Storage Cluster.

VRAID
EMC Storage term for RAID.

VSA
Volume set addressing.

VSP
Virtual service processor.
VV
Virtual volume.

VVol
VMware vSphere virtual volume.

WBEM
Web-Based Enterprise Management.

WORM
Write once, read many.

WSAPI
HPE 3PAR Web Services Application Program Interface.

WWN
World Wide Name. A unique 64-bit or 128-bit value used to identify Fibre Channel devices on an arbitrated loop. The WWN consists of a prefix issued by the IEEE to uniquely identify the company, and a suffix that is issued by the company.

WWPN
World Wide Port Name.

zone
A unit of physical disk space reserved by a controller node for snapshot or snapshot administration data. A single zone may occupy space on more than one disk.