



Hewlett Packard
Enterprise

HPE 3PAR StoreServ Storage Concepts Guide

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.

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use, or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

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.

SUSE® and the SUSE logo are registered trademarks of SUSE LLC 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 StoreServ Storage.....	8
Overview.....	8
Physical Disks (PD).....	9
Chunklets.....	9
Logical Disks (LD).....	9
Common Provisioning Groups (CPG).....	9
Virtual Volumes (VV).....	9
Fully Provisioned Virtual Volumes (FPVV).....	10
Thinly Provisioned Virtual Volumes (TPVV).....	10
Physical Copies.....	10
Virtual Copy Snapshots.....	10
Logical Unit Number.....	11
HPE 3PAR software licensing.....	12
Types of HPE 3PAR All-inclusive Software License.....	12
All-inclusive Single-System HPE 3PAR Software License.....	12
HPE 3PAR All-inclusive Multi-System Software License.....	14
Data at Rest Encryption software license.....	14
HPE 3PAR All-inclusive Software Matrix.....	14
HPE 3PAR Transition License (Old to New).....	15
HPE 3PAR StoreServ storage system users.....	17
User account roles.....	17
Local user authentication and authorization.....	18
LDAP user authentication and authorization.....	18
Domain user access.....	18
Strong passwords.....	18
Time-based passwords.....	19
Encrypted ciphertext passwords.....	19
Ciphertext exports.....	19
Ciphertext password modification.....	19
Password mode.....	19
Two-factor authentication for StoreServ Management Console.....	20
Performing password tasks.....	21
Exporting ciphertext.....	21
Changing the ciphertext password.....	21
Setting or changing the password mode.....	21
Lightweight Directory Access Protocol.....	22
Active Directory.....	22
OpenLDAP.....	22
Red Hat Directory Server.....	22
LDAP users.....	22



LDAP server data organization.....	23
LDAP and Virtual Domains.....	23
LDAP authentication and authorization.....	23
LDAP authentication.....	24
Simple binding.....	24
SASL binding.....	24
LDAP authorization.....	24
Authorization on systems using virtual domains.....	25
HPE 3PAR Virtual Domains.....	26
Domain types.....	26
Users and domain rights.....	27
Object and domain association rules.....	27
Default and current domains.....	27
Ports and hosts.....	28
About ports.....	28
Active and inactive hosts.....	29
Host addition and removal.....	29
Legacy host personas.....	29
Host Explorer Software agent.....	29
Port and host guidelines.....	31
Port target, initiator, and peer modes.....	31
Host persona management.....	31
Chunklets.....	34
Physical disk chunklets.....	34
Spare chunklets.....	34
Logical disks.....	36
Logical disks and common provisioning groups.....	36
Logical disk types.....	36
RAID types.....	37
RAID 0.....	37
RAID 1 and RAID 10.....	37
RAID 5 and RAID 50.....	38
RAID MP or RAID 6.....	39
Logical disk size and RAID types.....	40
Common Provisioning Groups.....	41
CPG precautions, planning, and guidelines.....	42
Growth increments, warnings, and limits.....	42
Growth increments.....	42
Growth warning.....	43
Growth limit.....	43
System guidelines for creating CPGs.....	43

Volume types associated with CPGs.....	44
Virtual Volumes.....	45
Virtual volume types.....	45
Administrative Volumes.....	46
Fully Provisioned Virtual Volumes.....	46
Thinly Provisioned Virtual Volumes (TPVV).....	46
Adaptive Data Reduction (ADR).....	47
Zero Detect.....	47
Deduplication	47
Compression	48
Data Packing	48
Virtual volume online conversion.....	48
Physical copies.....	49
Virtual copy snapshots.....	49
Virtual copy snapshot relationships.....	50
Copy-on-write function.....	51
Copy-of and parent relationships.....	52
Virtual volumes exportation.....	52
VLUN templates and active VLUNs.....	52
VLUN template types.....	53
Host sees templates.....	53
Host set templates.....	53
Port presents templates.....	53
Matched set templates.....	53
TPVV warnings and limits.....	54
Reclamation of unused space.....	55
Reclamation of unmapped LD space from CPGs.....	55
Reclamation of unmapped LD space from volumes.....	56
Automatic reclamation of unused snapshot space from volumes.....	56
Manual reclamation of unused snapshot space from volumes.....	56
Deleted volume snapshot space.....	56
Logical disks and chunklet initialization.....	56
Enhanced HPE 3PAR storage software.....	57
HPE 3PAR File Persona.....	57
HPE 3PAR Thin Express ASIC.....	58
HPE 3PAR Remote Copy.....	58
HPE 3PAR Dynamic Optimization	58
HPE 3PAR Adaptive Flash Cache.....	59
HPE 3PAR Adaptive Flash Cache support for NVMe Storage Class Memory Module.....	59
HPE 3PAR System Tuner.....	60
HPE 3PAR Thin Conversion.....	60
Assessment.....	61
Data preparation.....	61
Unused space zeroing.....	61
Physical copy creation.....	61
HPE 3PAR Thin Persistence.....	61
HPE 3PAR Thin Copy Reclamation.....	62



HPE 3PAR Virtual Lock.....	62
HPE 3PAR Adaptive Optimization.....	62
HPE 3PAR Peer Motion software.....	63
Data encryption.....	63
Priority Optimization.....	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 StoreServ Storage hardware..... 68

Identifying HPE 3PAR StoreServ Storage system components.....	68
HPE 3PAR StoreServ Storage hardware components.....	68
Physical drive.....	68
Drive Enclosure.....	69
Controller Node.....	69
Service Processor 5.0.....	69
Physical Service Processor (PSP).....	69
Virtual Service Processor (VSP).....	69
VM Vision/VM Integration.....	69
Power Distribution Unit.....	70
I/O Module.....	70
HPE 3PAR StoreServ Storage models.....	70
HPE 3PAR StoreServ 7000 Storage.....	71
HPE 3PAR StoreServ 8000 Storage.....	71
HPE 3PAR StoreServ 9000 Storage.....	72
HPE 3PAR StoreServ 10000 Storage.....	72
HPE 3PAR StoreServ 20000 Storage.....	72

HPE 3PAR SNMP infrastructure..... 73

About SNMP.....	73
-----------------	----

HPE 3PAR SNMP agent guidelines..... 74

SNMP managers.....	74
Supported MIBs.....	74
MIB-II.....	74
Exposed objects.....	75
System Description.....	75
System Object ID.....	75
System Up Time.....	76
System Contact Information.....	76
System Name.....	76
System Location.....	76
HPE 3PAR MIB.....	76
Severity levels of the alert state.....	82
Alert state values.....	83
alertNotify traps.....	83
storeServAlert traps.....	84



Clearing alert traps.....	84
HPE 3PAR Common Information Model API.....	87
SMI-S.....	87
WBEM initiative.....	87
HPE 3PAR CIM support.....	88
Standard compliance.....	88
SMI-S profiles.....	88
Supported extensions.....	88
CIM indications.....	88
Comparing HPE 3PAR to EVA terms.....	89
Support and other resources.....	91
Accessing Hewlett Packard Enterprise Support.....	91
Accessing updates.....	91
Remote support.....	92
Warranty information.....	92
Regulatory information.....	92
Documentation feedback.....	93
Glossary.....	94
A.....	94
B.....	95
C.....	95
D.....	96
E.....	97
F.....	97
G.....	98
H.....	98
I.....	99
J.....	100
K.....	100
L.....	100
M.....	100
N.....	101
O.....	102
P.....	102
Q.....	103
R.....	103
S.....	104
T.....	107
U.....	107
V.....	108
W.....	109
Z.....	109



HPE 3PAR StoreServ Storage

HPE 3PAR StoreServ Storage is a family of flash-optimized storage systems that offer automated provisioning. HPE 3PAR offers an advanced storage solution that uses a multi-tenant ability that distributes the load dynamically depending on the requirements set by each tenant. In addition, this single tier-1 storage system architecture is designed for in-built data security and availability.

HPE 3PAR StoreServ Storage regulates and manages itself. The rate at which the storage resources are consumed is constantly monitored.

Compaction technologies such as thin provisioning, thin deduplication, and thin reclamation are incorporated and fully automated in HPE 3PAR StoreServ Storage systems. Thin provisioning allows a volume to be created and made available as a Logical Unit Number (LUN) to a host without the need to dedicate physical storage until it is actually needed.

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 previous layer. 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 as a Logical Unit Number (LUN). This is the only layer visible to hosts.

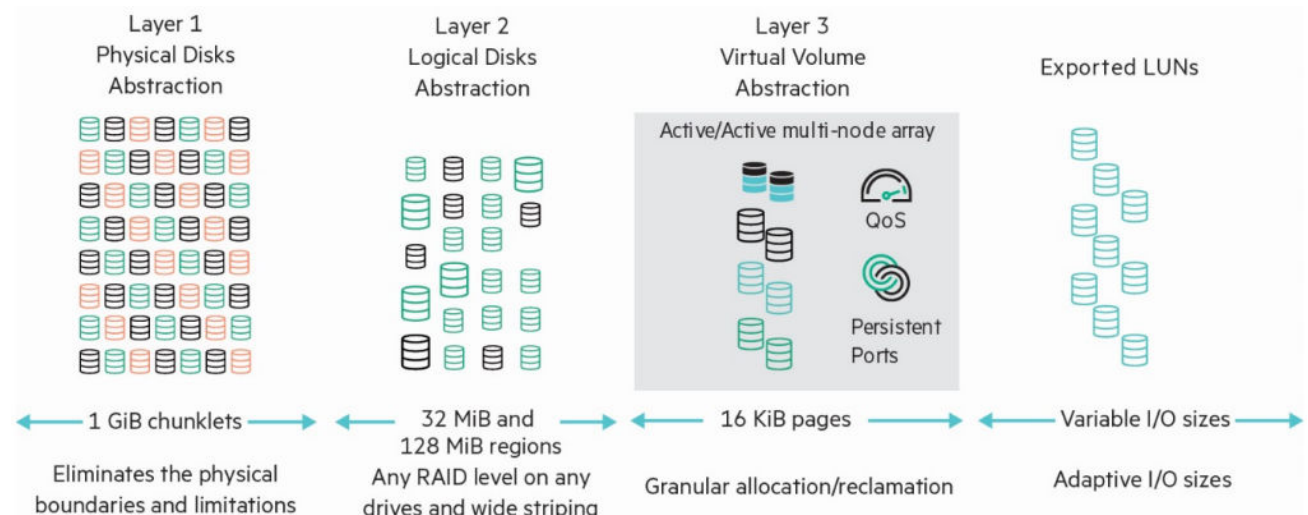


Figure 1: HPE 3PAR StoreServ system data layers

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 GiB 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.

More information

Chunklets

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

More information

Logical disks

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.

Virtual Volumes (VV)

Virtual volumes draw their resources from Common Provisioning Groups (CPG), and volumes are exported as logical unit numbers (LUN) to hosts. VVs are the only data layers visible to the hosts. If the original base volume becomes unavailable, you can create physical copies of VVs that remain available. Before creating VVs, you must first create CPGs to allocate space to the VVs.



For the maximum size limit and the number of virtual volumes and virtual volume copies that can be created with your specific system configuration, see the *HPE 3PAR Support Matrix* on the SPOCK website: <http://www.hpe.com/storage/spock>.

More information

Virtual Volumes

Fully Provisioned Virtual Volumes (FPVV)

An FPVV is a volume that uses Logical Disks (LD) that belong to a Common 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. For the maximum size limit and other limits for your specific configuration, see the *HPE 3PAR Support Matrix* on the SPOCK website: <http://www.hpe.com/storage/spock>.

More information

Fully Provisioned Virtual Volumes

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 KiB 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.

More information

Thinly Provisioned Virtual Volumes (TPVV)

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 until the `createvvcopy` operation has completed.

More information

Physical copies

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. The maximum number of snapshots that can be created is determined by the system configuration and the HPE 3PAR OS release. You can make snapshots of:

- FPVVs
- TPVVs



- Physical copies
- Another virtual copy snapshot

More information

Virtual copy snapshots

Logical Unit Number

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 Logical Unit Number (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.

More information

Virtual volumes exportation



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 subcategories. The subcategories 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

HPE 3PAR OS software			
System Reporter	Rapid Provisioning	Adaptive Flash Cache	Full Copy
HPE 3PARInfo	Autonomic Groups	Persistent Cache	Thin Provisioning

Table Continued



HPE 3PAR OS software

Online Import license (1 year)	Autonomic Replication Groups	Persistent Ports	Thin Copy Reclamation
System Tuner	Autonomic Rebalance	Management Console	Thin Persistence
Host Explorer	LDAP Support	Web Services API	Thin Conversion
Multi Path IO SW	Access Guard	SMI-S	Thin Deduplication for SSD
VSS Provider	Host Personas	Real Time Performance Monitor	HPE 3PAR OS Administration Tools <ul style="list-style-type: none"> • CLI client • SNMP
Scheduler			

Table 2: HPE 3PAR Optimization software list**HPE 3PAR Optimization software**

Dynamic Optimization	Adaptive Optimization	Priority Optimization
----------------------	-----------------------	-----------------------

Table 3: HPE 3PAR Speciality software list**HPE 3PAR Speciality software**

File Persona	Smart SAN	Virtual Copy
Virtual Domain	Virtual Lock	Online Import

Table 4: HPE Recovery Manager Central App Suite**HPE Recovery Manager Central App Suite**

vSphere	MS Hyper-V	MS Exchange	MS SQL
Oracle	SAP HANA		



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

All-inclusive Multi-System HPE 3PAR Software			
Peer Motion (PM)	Peer Persistence (PP)	Remote Copy (RC)	Cluster Extension Windows (CLX)

Data at Rest Encryption software license

HPE 3PAR StoreServ Data at Rest Encryption is designed to protect your archived data. All supported HPE 3PAR OS versions must have a valid HPE 3PAR StoreServ Data at Rest Encryption license to enable encryption.

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

Supported Storage Arrays

- HPE 3PAR StoreServ 7000 Series
- HPE 3PAR StoreServ 8000 Series
- HPE 3PAR StoreServ 9000 Series
- HPE 3PAR StoreServ 10000 Series
- HPE 3PAR StoreServ 20000 and 20000_R2 Series

To support encryption, each of the listed HPE 3PAR StoreServ arrays must be populated with encryption-supported drives. The arrays cannot have a mix of encrypted and nonencrypted drives.

Supported HPE 3PAR OS

- HPE 3PAR OS 3.1.2 MU2 and later—Supported SED drives and Local Key Manager
- HPE 3PAR OS 3.1.3 MU1 and later—Supported FIPS SED 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

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

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:

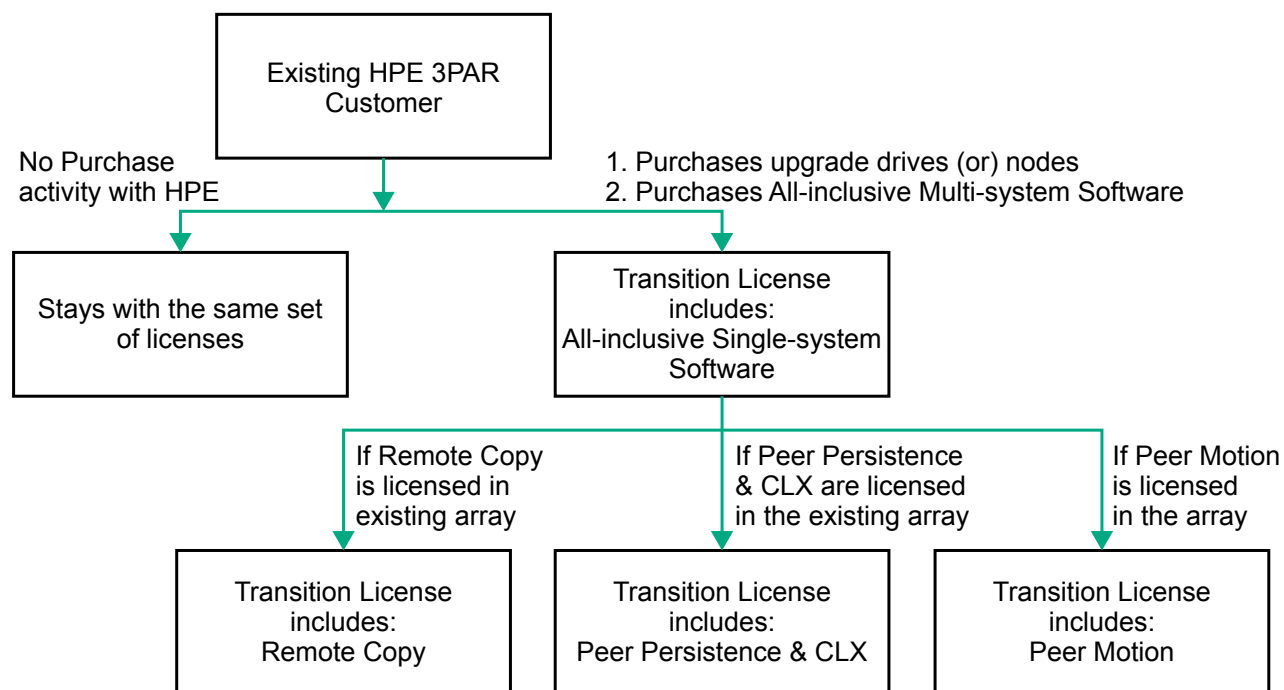


Figure 2: Install-Based Transition License

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.

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

Standard roles:

- Browse
- Edit
- Super
- Service

Extended roles:

- CO - Compliance Officer
- 3PAR AO - Adaptive Optimization
- 3PAR RM - Recovery Manager
- Audit
- Basic Edit
- Create

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 require 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.

User Role	Rights assigned to role
Browse	Rights are limited to read-only access.
Edit	Rights are granted to most operations; for example, creating, editing, and removing virtual volumes and other objects.
Super	Rights are granted to all operations.
Service	Rights are limited to operations required to service the system. Allows limited access to user information and user group resources.

Table Continued



User Role	Rights assigned to role
CO	Rights to approve any operation that can compromise the integrity of a retained file. Any user request must be approved by the CO before the operation can be executed.
Create	Rights are limited to creating objects; for example, virtual volumes, CPGs, hosts, and schedules.
Basic Edit	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.
3PAR AO	Rights are limited to internal use for Adaptive Optimization operations.
3PAR RM	Rights are limited to internal use for Recovery Manager operations.
Audit	Rights are limited to scanning the 3PAR OS for security issues. An audit user has no access to the CLI.

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**. 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**. 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.

Ciphertext exports

Ciphertext for a service account is exported using the `controlrecoveryauth` command in encrypted ciphertext mode. 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.

For instructions on using the `controlrecoveryauth` command to export ciphertext, see [Exporting ciphertext](#).

Ciphertext password modification

Ciphertext passwords are changed using the `controlrecoveryauth` command. This command causes a new random ciphertext string to be generated for the specified service user account. To obtain the new password for the user account, the ciphertext string will need to be exported using the process explained in [Exporting ciphertext](#).

For instructions on modifying the password, see [Changing the ciphertext password](#).

Password mode

The HPE 3PAR CLI command `controlrecoveryauth` is used to query or change the current setting of the strong service account password system (for example, to change the mode from time-based to encrypted ciphertext).

For instructions on using the `controlrecoveryauth` command to query and change the password mode, see [Setting or changing the password mode](#).



Two-factor authentication for StoreServ Management Console

Two-factor authentication manages access to the StoreServ Management Console (SSMC) using existing LDAP and PKI protocol. With two-factor authentication, two factors are required for SSMC authentication: something the user possesses (a smart card), and something the user knows (a personal identification number).

For SSMC, a common access card (CAC) is used to authenticate access. The smart card reader plugin in the browser reads the smart card and accesses the certificate in the card using the PIN specified by the user. The client certificate embedded in the smart card is presented to SSMC by the browser. The client certificate must be signed by a root or intermediate Certificate Authority (CA) that has been previously imported into SSMC.

SSMC extracts the user name from the certificate and sends it to the array. The 3PAR OS checks the directory server (such as LDAP) to authenticate the user and determine the user access rights.

The certificates stored on CAC cards are X.509 security certificates. They contain fields of information used to identify the certificate owner, the certificate issuer, and other certificate identification elements.



Performing password tasks

Procedure

1. Exporting ciphertext
2. Changing the ciphertext password
3. Setting or changing the password mode

Exporting ciphertext

The `controlrecoveryauth` command is used to export ciphertext for a service account.

Procedure

1. To display the ciphertext for a service account, use the `controlrecoveryauth ciphertext <user>` command, where:

`user` is the service account requested by the service personnel.
2. 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.

Changing the ciphertext password

This task affects the `root` and `console` accounts. On the HPE 3PAR StoreServ Storage system, these user accounts are not used for most maintenance actions.

Procedure

- To change a ciphertext password, use the `controlrecoveryauth rollcred <user>` command, where:

`<user>` is the service account requested by the service personnel.
- To obtain the new password for the specified user, follow the instructions in **Exporting ciphertext**.

Setting or changing the password mode

Procedure

- 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 either:

- Standard schemas understood by clients and servers from different vendors
- 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. Different domain configurations result 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 HPE 3PAR LDAP client is supported for use with the Active Directory, OpenLDAP, and Red Hat Directory Server LDAP implementations.

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](#)).

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.

Red Hat Directory Server

Red Hat Directory Server is an LDAP v3-compliant server that centralizes user identity and application information. Red Hat Directory Server provides a network-based registry for storing application settings, user profiles, and access control information.

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 username and password are checked on the LDAP server. Local user 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**.

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 local user rights to the system are assigned on a case-by-case basis. LDAP user 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 user 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`, a downloadable Windows Support Tool available from Microsoft, and `ldapsearch`, available for many UNIX and Linux systems, can be used to view data entries in the LDAP server. These programs 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 Virtual 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**, by using domains, rights to system objects, such as volumes and hosts, can be 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**, 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**.

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 username 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](#), an LDAP user role is tied to the group membership of that user. 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](#). 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`



- 3PAR_AO-map
- 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**, a user's group association determines that user's role within the system. On systems using virtual domains, user 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**:

- 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.

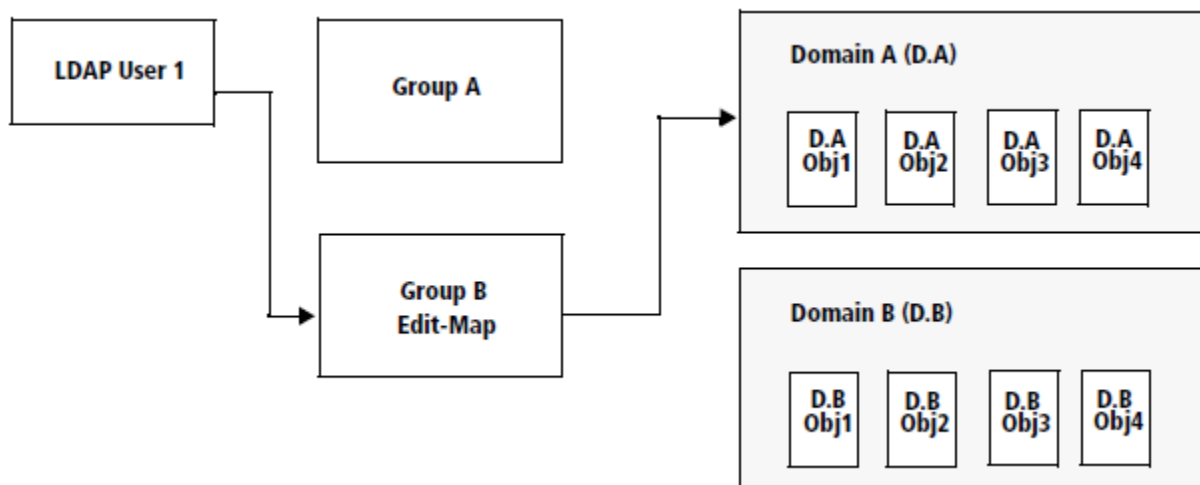


Figure 3: Group-to-Domain Mapping Relationship



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, implementing virtual domains provides more defined control of access to the system .

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 has 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.

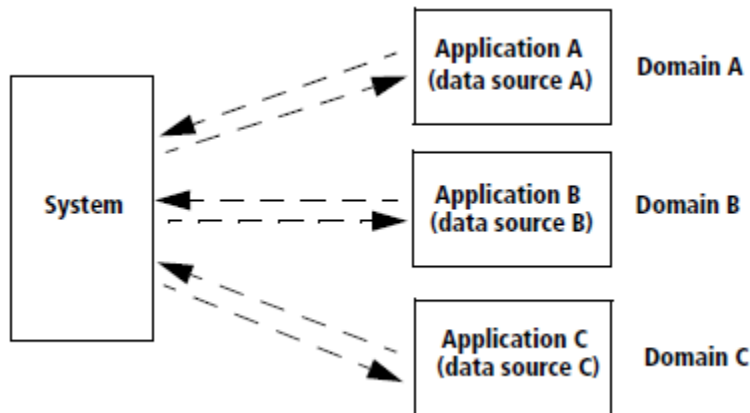


Figure 4: Single System Managing Multiple Independent Applications

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 a group of domains 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](#).

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 have rights over the entire system. Only 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 same domain as the virtual volume.
- 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 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**). However, if it is apparent that a specific domain will receive most of the attention from a user, virtual domains allow administrators to set a default domain for that user.

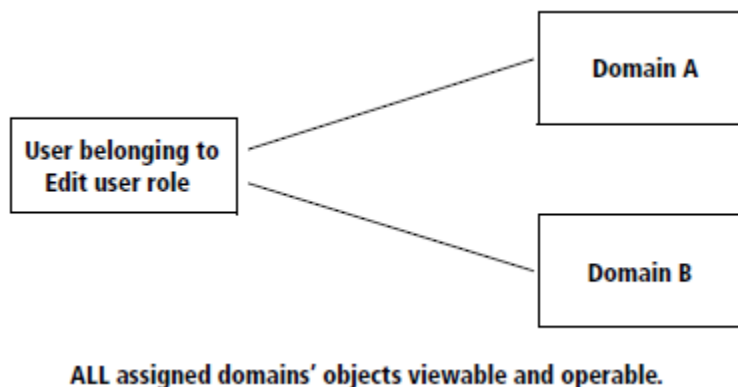


Figure 5: Edit user access to domains

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.

Ports and hosts

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** 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 exclusively for storage area networks (SANs)). CNA supports multiple storage connectivity protocols on a single host bus adapter (HBA). CNA ports can be configured to be used as an FC or iSCSI port.

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.

Host addition and removal

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 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. 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 a group of hosts requires 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.

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. 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, which assists 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
- Host application, DIF knob on the hosts and bootable from SAN
- MOUNTPOINT, CONSUMEDCAPACITY, DEVICEWWNS, and VOLUMEGROUP details

Refer to the `showhost -agent` or `showvlun -pathsum` commands in the *HPE 3PAR Command Line Interface Administrator Guide* for more information. For details on these commands, use `clihelp -col showhost` and `clihelp -col showvlun`.

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' Guide*. For a list of supported host operating systems, go to the SPOCK website:

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



Port and host guidelines

This section contains information on using port modes, hosts, and host personas.

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.

SAS ports

Initiator mode for ports that connect to the system physical disks and send commands to those disks.

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.

Host persona management

A host persona 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. Assigning a persona to a host simplifies connecting hosts to the system and reduces management costs related to complex host connection.

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 Asymmetric Logical Unit Access (ALUA) 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.

For a list of supported host operating systems, go to the following website:

SPOCK (<https://www.hpe.com/storage/spock>)

Table 7: Host personas and capabilities

Persona Number, Name, and Host OS	Additional Capabilities
No.: 1 Name: Generic Host OS: Linux, Windows, and Solaris	UAREpLun, SESLun
No.: 2 Name: Generic-ALUA Host OS: Linux, Windows, and Solaris	UAREpLun, ALUA, SESLun
No.: 6 Name: Generic-Legacy	None
No.: 7 Name: HPUX-Legacy Host OS: HP-UX	VolSetAddr, Lun0SCC
No.: 8 Name: AIX-Legacy Host OS: AIX	NACA

Table Continued



Persona Number, Name, and Host OS	Additional Capabilities
No.: 9 Name: Egenera Host OS: Egenera, NetApp	Softlnq
No.: 10 Name: NetApp ONTAP Host OS: Data ONTAP	Softlnq
No.: 11 Name: VMware Host OS: Linux and Windows	SubLun, ALUA
No.: 12 Name: OpenVMS	UAREpLun, RTPG, SESLun, Lun0SCC
No.: 13 Name: HP-UX Host OS: HP-UX	UAREpLun, VolSetAddr, SESLun, ALUA, Lun0SCC
No.: 15 Name: WindowsServer Host OS: Windows	UAREpLun, SESLun, ALUA, WSC
No.: 16 Name: AIX-ALUA Host OS: AIX	UAREpLun, NACA, ALUA

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.



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 these tasks.

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 GiB.
- 256 MiB 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 MiB of space is reserved for diagnostic use—2 MiB beginning after the TOC and 2 MiB 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**.

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 GiB or 60 GiB 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 (default)

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 shows a RAID 0 LD with a set size of 1 and a row size of 3.

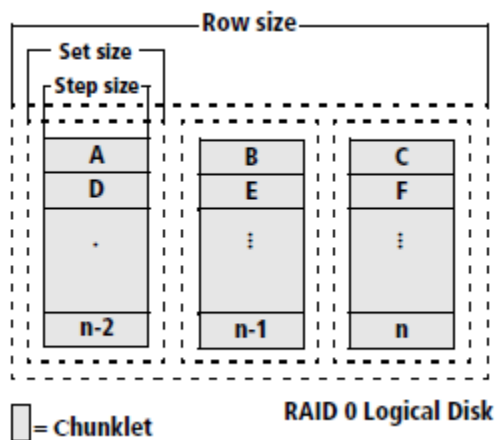


Figure 6: Data striped across chunklets on a RAID 0 LD

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 shows a RAID 10 LD with a set size of 2 and a row size of 3 in two rows:



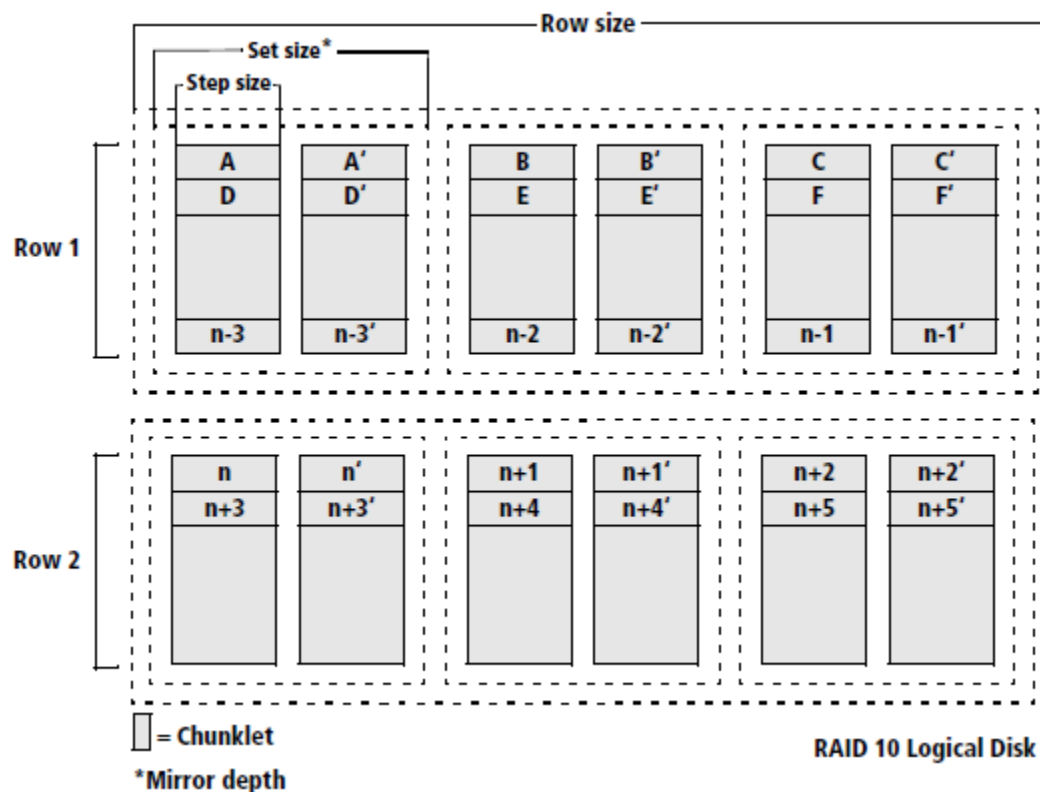


Figure 7: Data striped across RAID 1 sets on a RAID 10 LD

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 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 shows a RAID 50 LD with a set size of 3, and two sets in one row:

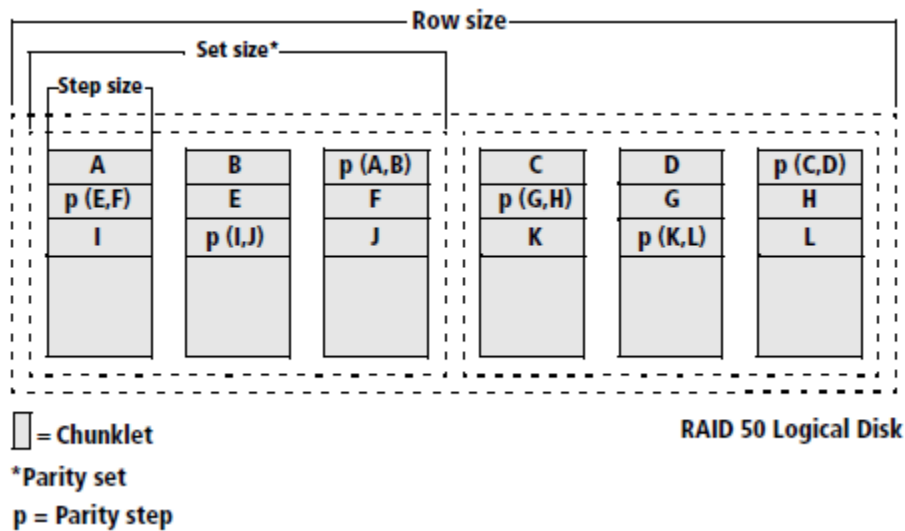


Figure 8: Data striped across RAID 5 sets on a RAID 50 LD

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 eight chunklets. A RAID MP set with eight chunklets has a total of six chunklets of space for data and two for parity. RAID MP set sizes of 8 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 two 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 9: Data striped across RAID MP sets on a RAID MP LD** shows a RAID MP LD with a set size of 8, and two sets in one row:

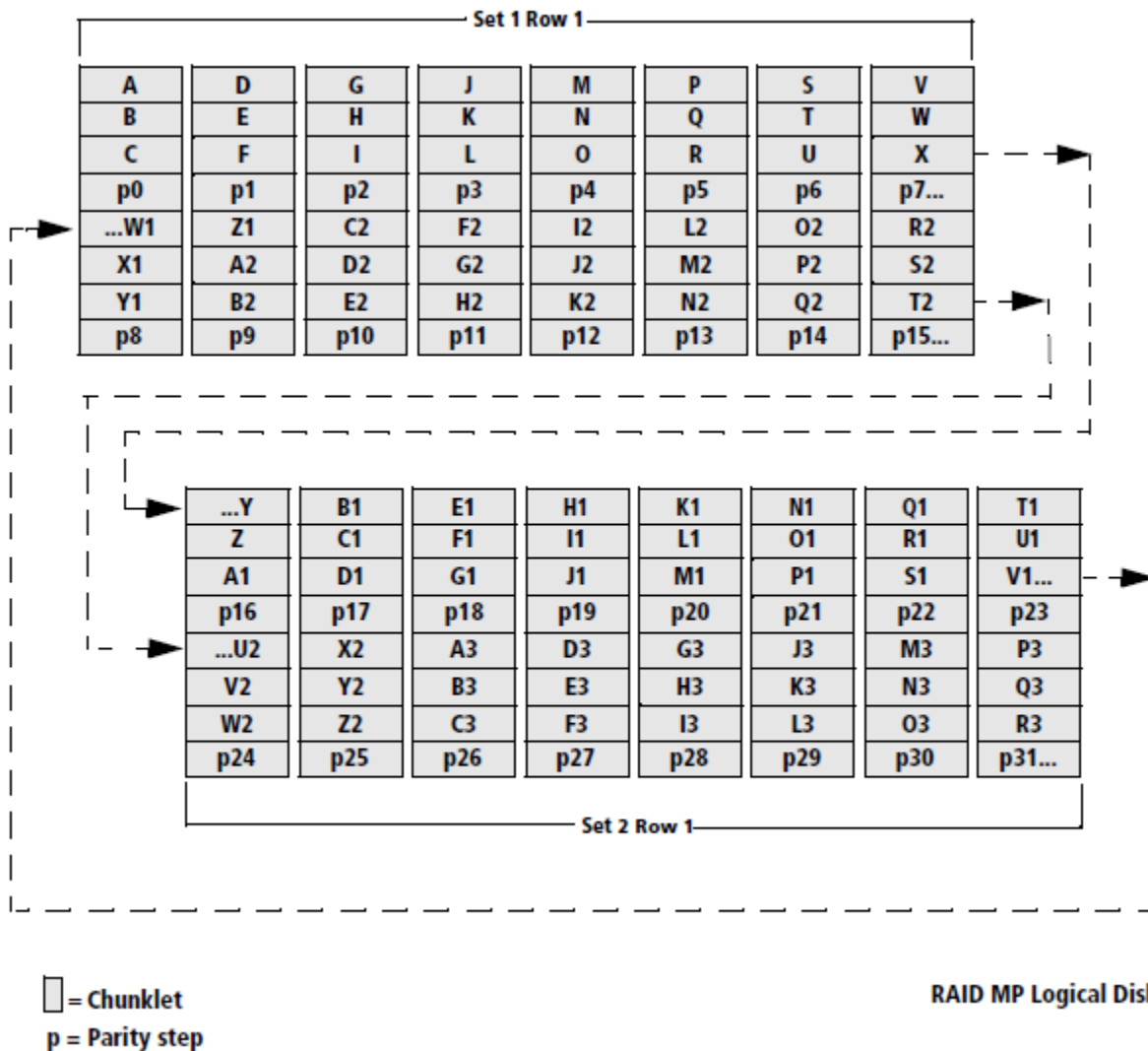


Figure 9: Data striped across RAID MP sets on a RAID MP LD

Logical disk size and RAID types

All systems round up so that the LD size is divisible by the size of one chunklet, 1 GiB. 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 GiB.

Common Provisioning Groups

A CPG creates a virtual pool of Logical Disks (LD) that allows virtual volumes (VV) to share CPG resources and allocates 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, 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.

More information

Virtual Volumes

CPG precautions, planning, and guidelines



CPG precautions, planning, and guidelines

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. Any 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.

Setting up overprovisioning parameters can help limit warnings. For example, you can set up:

- Overprovisioning ratio limit (`OverprovRatioLimit <value>`)
- Overprovisioning ratio warning (`OverprovRatioWarning <value>`)

See the *HPE 3PAR Command Line Interface Administrator Guide* for more information.

Growth increments

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:

Number of Nodes	Default	Minimum
2	32 GB	8 GB
4	64 GB	16 GB
6	96 GB	24 GB
8	128 GB	32 GB

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.
- 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**.

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)**. For information about FPVVs, see **Fully Provisioned Virtual Volumes (FPVV)**.



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**.

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)
- Administrative Volume (created by the system and for system usage only)

FPVVs and TPVVs 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 consume 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 reclaims 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

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.

FPVVs 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. You can set snapshot space allocation limits and usage warnings to help manage the growth of snapshot space. For the maximum size limit and other limits for your specific configuration, see the *HPE 3PAR Support Matrix* on the SPOCK website: <http://www.hpe.com/storage/spock>.

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 GiB 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. For the maximum size limit and other limits for your specific configuration, go to the SPOCK website: <http://www.hpe.com/storage/spock>.

TPVVs can respond to host write requests by allocating space on demand in one chunklet increments, beginning with 1 GiB 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 GiB for each node but consumes that space in less than 60 seconds, the next allocation becomes 2 GiB for each node. However, if the initial 1 GiB is consumed more slowly, the next allocation increment remains at 1 GiB for each node.

For your SSDs, you have the option of removing duplicated data before it is written to the volume using the deduplication attribute. You can use the compression attribute on your SSDs to consolidate data that preserves the information while reducing the total amount of storage.

CAUTION:

- Use of allocation limits is recommended to prevent consumption of physical raw capacity beyond a tolerable limit. However, 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.
 - 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](#) for additional cautions and recommendations.
-

More information

- [Adaptive Data Reduction \(ADR\)](#)
- [TPVV warnings and limits](#)

Adaptive Data Reduction (ADR)

HPE 3PAR StoreServ Storage arrays offer the flexibility to selectively apply data reduction. You can choose, on a per-volume basis, which features are enabled. Applications that demand the highest levels of performance and the lowest latency levels can then meet service level agreements (SLAs) while other workloads gain the storage efficiencies that make flash affordable for all your mainstream applications.

Adaptive Data Reduction (ADR) is a collection of technologies that come standard with HPE StoreServ Storage which are designed to reduce your data footprint. When used alone or in combination, these technologies help you get the most out of the flash capacity of your system. They also reduce your total cost of storage while improving flash media endurance.

There are four stages of ADR that progressively improve the efficiency of data stored on SSDs:

- Zero Detect
- Deduplication
- Compression
- Data Packing

Each feature uses a combination of a fifth generation hardware ASIC, in-memory metadata, and efficient processor utilization to deliver optimal physical space utilization for hybrid and all-flash systems.

Zero Detect

Zero Detect is a data reduction technology that reduces the cost of storage by identifying and removing repeated data from incoming data streams. This hardware-accelerated capability reduces the amount of capacity required to store data on your SSDs without impacting performance, because operations take place at the hardware layer.

During normal operations, hosts often write an extended string of zeros to a storage array as part of a write stream. Zero Detect examines all incoming write streams, identifies extended strings of zeros, and removes them to prevent unnecessary data from being written to storage. As a result, duplicated data never consumes capacity on the array.

Since Zero Detect is performed within the HPE 3PAR ASIC, not only do all operations take place inline and at wire-speed, but they consume no CPU cycles so they do not impact system operations.

Zero Detect is considered the first level of data reduction. In addition, because it is completely autonomic and hardware-embedded, Zero Detect works independently from other data reduction technologies, meaning that savings can be made on all data and in combination with other data reduction technologies.

Deduplication

Deduplication eliminates duplicated data on your SSDs and reduces the amount of capacity required to store data.

Like Zero Detect, deduplication on HPE 3PAR StoreServ Storage uses the HPE 3PAR ASIC. The system assigns a unique "fingerprint" to write requests as they are processed by the array. The system saves these "fingerprints" for future reference. The system cross-references the "fingerprints" of the new data against previously captured data. A match reveals that the incoming request contains duplicative data, at which point the system performs a detailed verification check, and then discards the duplicative data. Instead of writing the duplicative data to storage, the system records a "pointer" to the original data.

Like Zero Detect, deduplication takes place inline. Since there are no post-process tasks to manage, duplicate data is not written to storage and then scrubbed. When paired with Express Indexing, deduplication offers substantial cost, storage footprint, power, and cooling reductions. It also improves flash media endurance by reducing data writes.

Deduplication offers reductions in the amount of flash capacity required to store data, such as virtual server and virtual desktop workloads. Deduplication works well with environments that store multiple copies of data such as, testing, development, and user acceptance testing (UAT). Using deduplication can dramatically reduce both the cost of flash and the data center footprint.



Deduplication works independently from other data reduction technologies, but increase savings can occur when combined with Zero Detect and compression.

Compression

Zero Detect and deduplication both reduce the amount of flash required to store data by eliminating unnecessary data. Compression reduces the amount of data on your SSDs by looking inside data streams for opportunities to reduce the overall size of the data set.

As with other data reduction technologies, the HPE 3PAR ASIC plays a key, although indirect, role in compression. The HPE 3PAR ASIC is used to offload other resource-intensive operations from the CPUs, thus freeing them up to perform compression operations. The system spreads these compression operations across multiple CPU cores to expedite data compression. An HPE 3PAR technology called Express Scan improves compression efficiency. Express Scan identifies incompressible streams of data and stores them in their native formats, instead of trying to attempt to compress data.

Like all HPE 3PAR data reduction operations, compression runs inline for optimal efficiency. Inline processing increases the endurance of flash, and helps ensure consistent performance by not needing to invoke resource-intensive post-process tasks.

Compression is a third method for reducing the amount of flash required to store a given amount of data. The combination of these three technologies is key to minimizing the cost of flash and making it an economical choice for nearly any application.

NOTE: The concurrent use of 3PAR Virtual Volume compression and File Persona is not supported on HPE 3PAR StoreServ 8200 and 8400 systems. Concurrent use is supported on 8440, 8450, 9450 and all 20000 systems.

Data Packing

Deduplication and compression increases storage efficiency by increasing the amount of data that can be stored on a given amount of capacity. But maintaining that efficiency systemwide over time is a much bigger challenge. To overcome this challenge, HPE 3PAR StoreServ Storage uses Data Packing that combines data reduction and flash efficiency technologies to maintain peak capacity efficiency over time.

To understand how Data Packing works, it is important to understand that once data has been deduplicated and compressed, the result is a set of odd-sized "pages" in cache that are inefficient to write to flash. Data Packing takes these random sized pages and packs them into small, fixed-size pages. This packing allows the system to attain a higher total system efficiency as compared to other all-flash platforms. The uniform, "packed" pages are set to a flash-native size, resulting in excellent efficiency and performance, as the resulting reads and writes to and from flash are performed at their internal page size. This packing also improves endurance as written data does not cross multiple internal pages, resulting in efficient use of flash pages.

Data Packing also packs together pages with good data locality, ensuring that excessive amounts of garbage are not created, in sharp contrast to many other implementations that require post-process garbage collection to tidy up the large amounts of garbage created by data overwritten by hosts. Reducing the need for resource-intensive garbage collection tasks has a positive impact on overall system performance. In addition, the use of Data Packing allows HPE 3PAR arrays to offer 100% inline data reduction with absolutely no post-processing, which is important to enterprise 24x7 environments that cannot accommodate "quiet" times for housekeeping tasks.

Due to the incredible efficiency gained through Data Packing, HPE 3PAR StoreServ arrays offer one of the highest raw-to-effective ratios among major all-flash arrays while maintaining high levels of performance.

Virtual volume online conversion

You can convert existing FPVVs to TPVVs and you can convert TPVVs to FPVVs 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 TPVVs. 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.

More information

HPE 3PAR software licensing

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 cause 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 a single physical copy.

A physical copy can 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>

NOTE: If the base volume and destination volume are both TPVVs, only the space that is actually used is copied. See **HPE 3PAR Storage concepts and terminology overview** for additional information on TPVVs.

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.

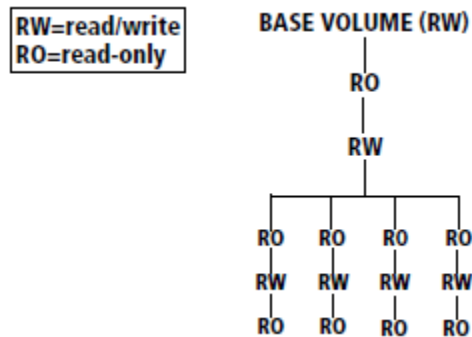


Figure 10: Alternating read-only and read/write virtual copies

See **Figure 11: Base volume and virtual copy relationships** for a more complex example of the possible relationships between a parent base volume and its virtual copies.

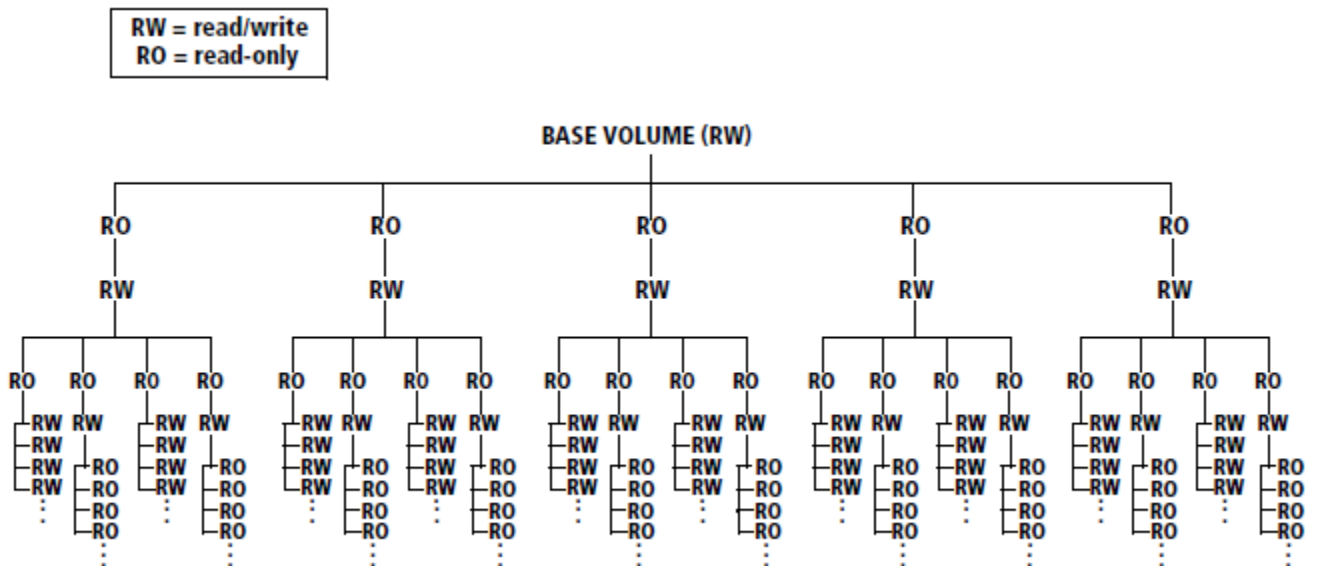


Figure 11: Base volume and virtual copy relationships

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** for an example of a sequence of snapshots.

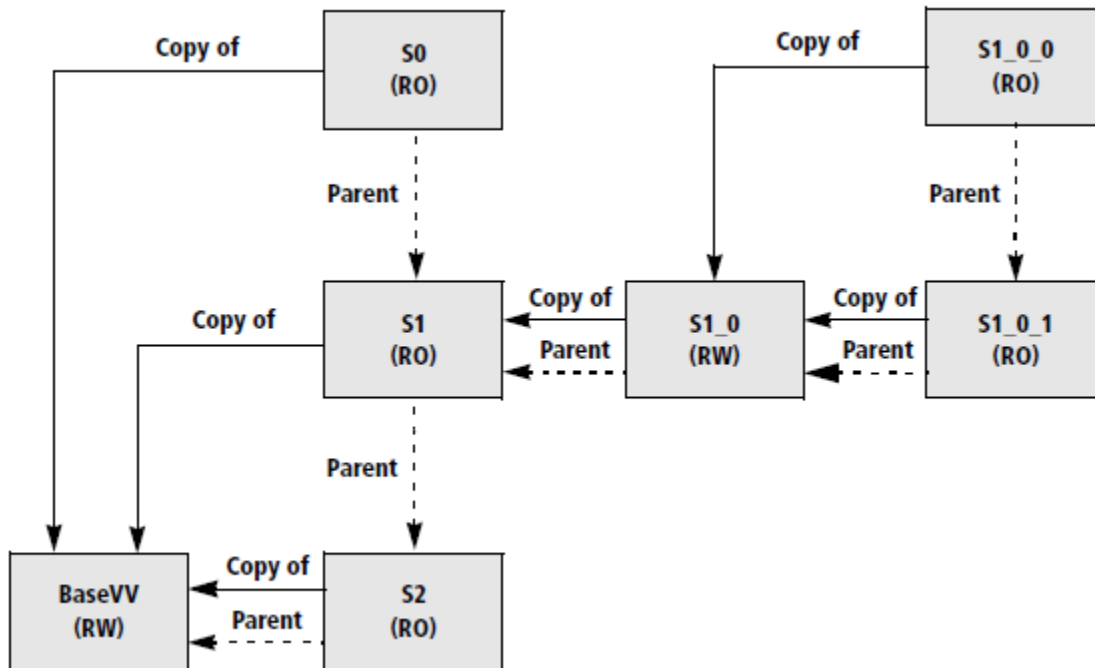


Figure 12: Snapshot tree

In **Figure 12: Snapshot tree**:

- **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**, 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**, 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.

Virtual volumes exportation

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 each host supports with your specific system configuration, go to the Single Point of Connectivity Knowledge (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.

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.

 **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*.

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.



TPVV warnings and limits

When you create a TPVV, you can set an allocation warning threshold and an allocation limit threshold. For the volume size limit and other limits for your specific configuration, go to the SPOCK website: <http://www.hpe.com/storage/spock>.

- **Allocation warning threshold**—The user-defined threshold at which the system generates an alert. For volumes capable of allocating space on demand only. This threshold is a percentage of the virtual size of the volume, the size that the volume presents to the host.
- **Allocation limit threshold**—The user-defined threshold at which writes fail, preventing the volume from consuming additional resources. For volumes capable of allocating space on demand only. This threshold is a percentage of the virtual size of the volume, the size that the volume presents to the host.

When you set TPVV allocation warnings and allocation limits, consider the space to be consumed by both the user data and the snapshot data of the volume.

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.

To determine the allocation warning and allocation limit thresholds for a TPVV, 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 warning that you require before the volume reaches its limit and writes fail.

Use the following formula to generate the allocation warning threshold:

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

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: a 1 TiB TPVV with read-only snapshots has a maximum write rate of 1 GiB per day. You want 30 days warning before that TPVV reaches the allocation limit. Use the following calculation for the allocation warning percentage:

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



Reclamation of 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](#).

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.

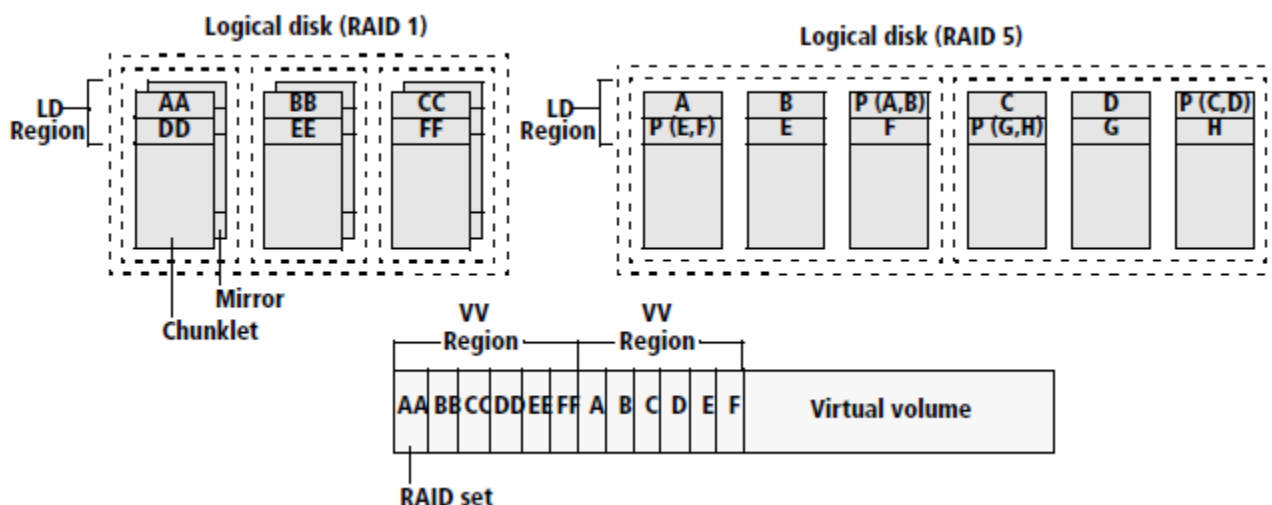


Figure 13: Mapping regions from LDs to VVs

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.

Reclamation of 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](#) 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.



Reclamation of 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 HPE 3PAR storage software](#).

Automatic reclamation of 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.

Manual reclamation of 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 GiB 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 HPE 3PAR storage software

HPE 3PAR offers several enhanced storage software 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](#).

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

HPE 3PAR File Persona

With HPE 3PAR File Persona, you can create a converged storage solution with block and file storage services. This 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, can be provisioned. 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.
- 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 PCs 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 composed of the following managed objects:

- The File Provisioning Group (FPG) is 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 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 anti-virus 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 anti-virus 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 File Persona User Guide*, the *HPE 3PAR Command Line Interface Administrator Guide*, and 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*.

NOTE: The concurrent use of 3PAR Virtual Volume compression and File Persona is not supported on HPE 3PAR StoreServ 8200 and 8400 systems. It is supported on 8440, 8450, 9450 and all 20000 systems.

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 Eight 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

HPE 3PAR Remote Copy 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

HPE 3PAR Dynamic Optimization 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 disks 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

Adaptive Flash Cache lets you 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 Adaptive Flash Cache support for NVMe Storage Class Memory Module

HPE 3PAR 750GB NVMe Storage Class Memory Module is deployed on an all-flash array and is based on the NVMe bus architecture and Storage Class Memory technology. HPE 3PAR Adaptive Flash Cache (AFC) now supports the HPE 3PAR 750GB NVMe Storage Class Memory Module.



NVMe is a standardized interface that enables accelerated transfer of data between a host and a target storage device in a solid-state drive (SSD) environment. The communication takes place over a Peripheral Component Interconnect Express (PCIe) bus. NVMe takes advantage of the parallelism in the SSDs.

Storage Class Memory is a new class of nonvolatile memory that delivers orders of magnitude faster read latency in comparison to NAND. It creates a three-dimensional matrix where memory cells are located at the intersection of word lines and bit lines, enabling cells to be addressed individually. As a result, data can be written and read in small sizes, leading to faster and more efficient read and write.

HPE 3PAR 750GB NVMe Storage Class Memory Module is ideal for shared storage where performance benefits and ultra-low latency for mixed workloads is required. HPE 3PAR 750GB NVMe Storage Class Memory Module may be added nondisruptively to any HPE 3PAR 9000 or 20000 system. HPE 3PAR's intelligent caching algorithms enable Storage Class Memory as a true extension of DRAM cache by determining when and how to move data from persistent storage into this tier. It is connected to the main memory across the NVMe (PCIe).

HPE 3PAR System Tuner

HPE 3PAR System Tuner is an optional feature that improves performance by identifying over-used 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

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

Virtual volumes with large amounts of allocated 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 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
- Unused space zeroing
- Physical copy creation

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

Data is prepared for copying by removing unnecessary data. Cleanup tasks to perform on the source volume include:

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

Unused space zeroing

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.

Physical copy creation

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

HPE 3PAR Thin Persistence is an optional feature that keeps TPVVs and read/write snapshots of TPVVs small. Thin persistence detects pages of zeros during data transfers and does not allocate 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 KiB 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

HPE 3PAR Thin Copy Reclamation is an optional feature that reclaims space when snapshots are deleted from a system. Deleting snapshots reclaims the snapshot space from a TPVV or FPVV and returns it 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](#).

HPE 3PAR Virtual Lock

HPE 3PAR Virtual Lock 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

HPE 3PAR Adaptive Optimization 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 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 SSDs 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. It 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. That is, 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:

Drive Type	Milliseconds
Solid State Drive	15 ms
Fast Class Drive	40 ms
Nearline Drive	60 ms

HPE 3PAR Peer Motion software

HPE 3PAR Peer Motion 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). Encrypted storage systems are FIPS-compliant when they are using a properly configured EKM running in FIPS mode and all drives in the array are FIPS-compliant. See the *HPE 3PAR Command Line Interface Administrator Guide* for more information.

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, if the encryption key file or the password is lost, and the HPE 3PAR StoreServ Storage system fails, the HPE 3PAR StoreServ Storage system cannot restore access to data. Ensure that backup copies of the latest encryption key file are kept and 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.

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. SED 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. 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, so 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. There is a minimal delay 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.

NOTE: The HPE 3PAR data encryption solution will help mitigate breach notifications under the Health Information Technology for Economic and Clinical Health (HITECH) Act.

Priority Optimization

Consolidation of storage systems reduces complexity of data storage and delivers 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. However, 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 input/output operations per second (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 input/output operations per second, allowing higher priority QoS rules to consume more system resources to meet their latency goals. If the System Busy level continues to increase, 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), 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 colocation 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 multitenant 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 that 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:

Name	The name of the QoS rule is the same as the name of the VVset.
State	The QoS rule can be active or disabled.
I/O	Sets the Min Goal and the Max Limit on IOPS for the target object.
Bandwidth	Sets the Min Goal and the Max Limit in bytes-per-second transfer rate for the target objective.
Priority	The limit for the target object can be set to low, normal, or high.
Latency Goal	The goals for the target object are determined in milliseconds.



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 one or more VVs 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 can provide, 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 can provide, 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 can deliver.

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 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). The type and size of drives used with a storage system vary based on the system model.

Drive types:

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

Drive sizes:



- SFF 2.5-inch drives
- LFF 3.5-inch drives

Drive Enclosure

A Drive Enclosure (Cage) is a specialized casing designed to hold and power physical 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 dense storage units that can hold many drives in a small rack space (EIA-standard rack units).

Controller Node

The Controller Node (Node) is a system component that caches and manages data in a system. It provides hosts with a coherent and virtualized view of the storage system. The Controller Nodes are located in 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 based on the model of the storage system.

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.

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).

VM Vision/VM Integration

VMVision/VM Integration is a feature of the Service Console (SC) that can be added to any StoreServ system attached to the SC.

VM Integration vCenters can be added at the time a StoreServ is added to the SC. Users can also add this feature after a StoreServ is attached to the SC by editing the StoreServ system.

To add VMWare integration to a StoreServ, the user will need to add vCenters and their associated login credentials.



After a cluster is added, it will appear in the VMWare Integration section of the **Edit System** dialog.

NOTE: Users can only add vCenter clusters to the VMWare Integration collection.

Power Distribution Unit

A Power Distribution Unit (PDU) is a device with multiple outlets to distribute electrical power to the entire rack. The PDUs can be single-phase PDU or three-phase PDU and are regionally specific.

I/O Module

The I/O Modules connect Drive Enclosures to Controller Nodes through SAS cables. (The HPE 3PAR StoreServ 10000 Storage series uses only FC drives.) These I/O Modules enable data transfer between the Controller Nodes, drives, Power Cooling Modules (PCMs), and enclosures. The I/O Modules are installed at the rear of the 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:

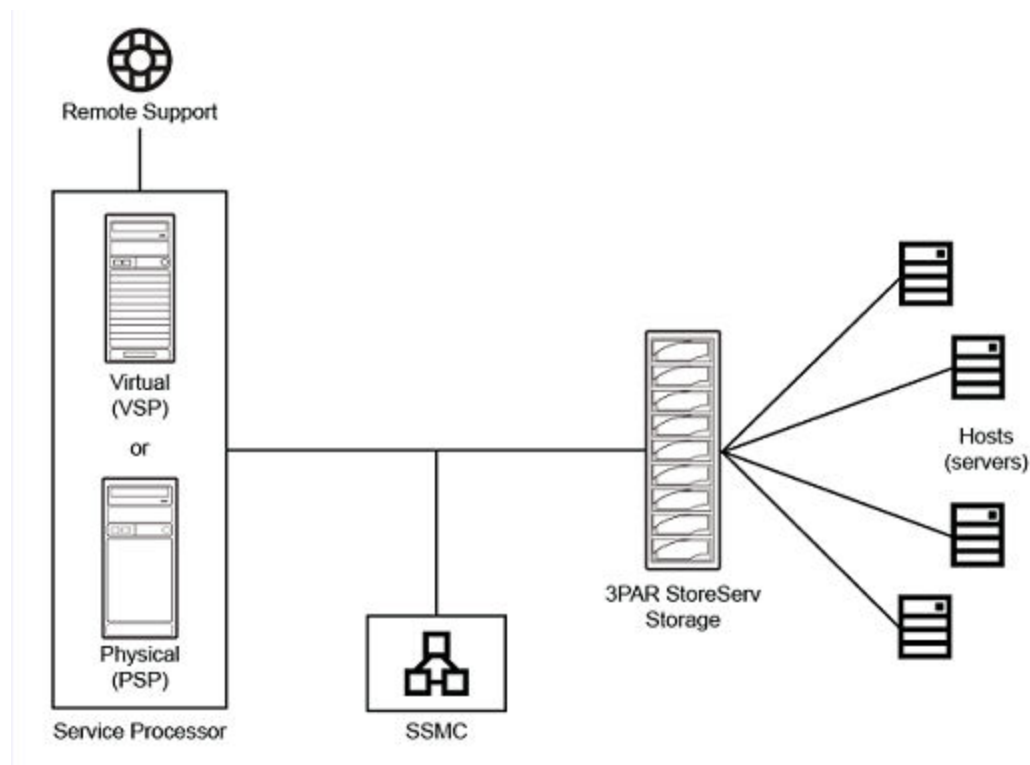


Figure 14: Configuration of an HPE 3PAR StoreServ Storage system

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 20000 Storage

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 to further optimize costs. Options include:

- True convergence of block and file protocols
- All-flash array performance
- Spinning media

HPE 3PAR StoreServ 8000 Storage offers:

- Rich, Tier-1 data services
- Quad-node resiliency
- Seamless data mobility between systems
- High availability through a comprehensive set of persistent technologies
- 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.

The HPE 3PAR StoreServ 9000 model is based on the proven 3PAR architecture built for:

- All-flash consolidation
- Delivering the performance, simplicity, and agility to support your hybrid IT environment

HPE 3PAR StoreServ 9450 is a single all-flash model 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 comprehensive set of persistent technologies
- 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 IT as a Service (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 demanding workloads with: .

- Greater than 3 million IOPS
- Sub-millisecond latencies
- A 4X density advantage
- 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. This architecture includes inline deduplication to reduce acquisition and operational costs by up to 75% without compromising performance. A choice of models provides 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 bidirectional data mobility enables nearly limitless elastic pools of storage to support the most rigorous on-demand infrastructure.



HPE 3PAR SNMP infrastructure

The HPE 3PAR OS allows you to manage a system with the StoreServ Management Console (SSMC) and the HPE 3PAR CLI. The OS also 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.



HPE 3PAR SNMP agent guidelines

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 describes critical events, are generated for every alert and alert state change issued by the system.

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.

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

Object Descriptor	Description	Access
<code>sysDescr</code>	Describes the system using the model number, system ID, serial number, and HPE 3PAR OS version of the master node.	Read-only
<code>sysObjectID</code>	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).	Read-only
<code>sysUpTime</code>	Gives the time interval (within 1/100 of a second) since the system was initialized.	Read-only
<code>sysContact</code>	User-defined name of the person or group responsible for maintaining the system.	Read/write
<code>sysName</code>	Name of the system. This helps to identify the storage system. This name cannot be set by using SNMP.	Read-only
<code>sysLocation</code>	User-defined system location. For example: Building 1, room 4, rack 3.	Read/write

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 are assigned incremental integers (2, 3, and so on). The manager uses this ID to identify products manufactured by Hewlett Packard Enterprise. The ID 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 HPE 3PAR MIB is located on the HPE 3PAR CLI and SNMP CD or ISO.

The `cpuStatsMIB` is composed 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

Object Descriptor	Description	Access
<code>component</code>	Indicates which system hardware, software, or logical component caused the alert or alert state change.	Read-only
<code>details</code>	Detailed description of the alert or alert state change, displayed as an alert string (for example: <code>PR table <table_name> is corrupt</code>). For information about system alerts, see the <i>HPE 3PAR Alerts Reference: Customer Edition</i> .	Read-only
<code>nodeID</code>	Node identification number, an integer from 0 through 7 that indicates which system controller node reported the alert or alert state change.	Read-only
<code>severity</code>	Severity level of the alert or alert state change, an integer from 0 to 7.	Read-only
<code>timeOccurred</code>	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>).	Read-only
<code>id</code>	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.	Read-only
<code>messageCode</code>	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 <i>HPE 3PAR Alerts Reference: Customer Edition</i> .	Read-only
<code>state</code>	Current alert state, which is an integer between 0 and 5. Alert states enable users to maintain detailed tracking of alerts throughout their life cycle.	Read-only
<code>serialNumber</code>	The serial-number of the HPE 3PAR StoreServ system.	Read-Only
<code>catalogKey</code>	An extension of the message code.	Read-Only
<code>detailedMessage</code>	An extension of the details component. It provides more specific details of the alerting condition.	Read-Only

Table Continued



Object Descriptor	Description	Access
tier	Indicates the event-type tier, for instance "general" or "hardware check".	Read-Only
sparePartNumber	Indicates the spare part number, if available, for events in the hardware tiers.	Read-Only

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

Table 10: Contents of the `nodeCpuStatsTable`

Component	Description	Access
<code>nodeCpuStatsIndex iso. 3.6.1.4.1.12925.1.9.3.1.1.1</code>	3PAR node ID plus 1.	Not-accessible. Index to the table.
<code>nodeCpuStatsNs iso. 3.6.1.4.1.12925.1.9.3.1.1.2</code>	Node nanoseconds when stats were read.	Read-only
<code>nodeCpuStatsNumCpus iso. 3.6.1.4.1.12925.1.9.3.1.1.3</code>	The number of CPUs in the node.	Read-only
<code>nodeCpuStatsInterrupts iso. 3.6.1.4.1.12925.1.9.3.1.1.4</code>	Total number of interrupts serviced on the node since boot time.	Read-only
<code>nodeCpuStatsContextSwitches iso. 3.6.1.4.1.12925.1.9.3.1.1.5</code>	Total number of context switches across all CPUs on the node since boot time.	Read-only
<code>nodeCpuStatsBootTime iso. 3.6.1.4.1.12925.1.9.3.1.1.6</code>	Time in the epoch when the node was booted. The epoch started at midnight on January 1, 1970 UTC.	Read-only
<code>nodeCpuStatsProcs iso. 3.6.1.4.1.12925.1.9.3.1.1.7</code>	Total number of processes created since the node was booted.	Read-only

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

Table 11: Contents of the `cpuStatsTable`

Component	Description	Access
<code>nodeCpuStatsIndex iso. 3.6.1.4.1.12925.1.9.3.1.1.1</code>	3PAR node ID plus 1.	Not-accessible. The first of the two indices to the table.
<code>cpuStatsIndex iso. 3.6.1.4.1.12925.1.9.3.2.1.1</code>	CPU number starting from 1.	Not-accessible. The second of the two indices to the table.

Table Continued



Component	Description	Access
cpuStatsUser iso. 3.6.1.4.1.12925.1.9.3.2.1.2	Total time spent executing user processes on the cpu since the node booted.	Read-only
cpuStatsSys iso. 3.6.1.4.1.12925.1.9.3.2.1.3	Total time spent executing kernel and system processes on the cpu since the node booted.	Read-only
cpuStatsIdle iso. 3.6.1.4.1.12925.1.9.3.2.1.4	Total idle time on the cpu since the node booted.	Read-only
cpuStatsNodeNs iso. 3.6.1.4.1.12925.1.9.3.2.1.5	Node nanoseconds when stats were read.	Read-only

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



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
nodeCpuStatsInterrupts.1
137572801
nodeCpuStatsInterrupts.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
```


30641
cpuStatsSys.1.1
35197
cpuStatsSys.1.2
41444
cpuStatsSys.1.3
40661
cpuStatsSys.1.4
36259
cpuStatsSys.1.5
35740
cpuStatsSys.1.6
32086
cpuStatsSys.1.7
34202
cpuStatsSys.1.8
31372
cpuStatsSys.2.1
53299
cpuStatsSys.2.2
69347
cpuStatsSys.2.3
61762
cpuStatsSys.2.4
64586
cpuStatsSys.2.5
55221
cpuStatsSys.2.6
63253
cpuStatsSys.2.7
53582
cpuStatsSys.2.8
61713
cpuStatsIdle.1.1
2167168
cpuStatsIdle.1.2
2175041
cpuStatsIdle.1.3
2166878
cpuStatsIdle.1.4
2173461
cpuStatsIdle.1.5
2169318
cpuStatsIdle.1.6
2177140
cpuStatsIdle.1.7
2168567
cpuStatsIdle.1.8
2178879
cpuStatsIdle.2.1
2146065
cpuStatsIdle.2.2
2137008
cpuStatsIdle.2.3
2138447
cpuStatsIdle.2.4
2136965
cpuStatsIdle.2.5
2144259
cpuStatsIdle.2.6



```

2142027
cpuStatsIdle.2.7
2136874
cpuStatsIdle.2.8
2140416
cpuStatsNodeNs.1.1
22651696611641
cpuStatsNodeNs.1.2
22651696611641
cpuStatsNodeNs.1.3
22651696611641
cpuStatsNodeNs.1.4
22651696611641
cpuStatsNodeNs.1.5
22651696611641
cpuStatsNodeNs.1.6
22651696611641
cpuStatsNodeNs.1.7
22651696611641
cpuStatsNodeNs.1.8
22651696611641
cpuStatsNodeNs.2.1
22651697040261
cpuStatsNodeNs.2.2
22651697040261
cpuStatsNodeNs.2.3
22651697040261
cpuStatsNodeNs.2.4
22651697040261
cpuStatsNodeNs.2.5
22651697040261
cpuStatsNodeNs.2.6
22651697040261
cpuStatsNodeNs.2.7
22651697040261
cpuStatsNodeNs.2.8

```

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)**. In addition, clear **(7)** denotes a trap that clears a current alert condition.

Table 12: Alert severity levels

Severity Level	State	Description of the Severity
0	Fatal	Indicates that an error has occurred but it is too late to take any action.
1	Critical	An action is needed immediately and scope of the error is broad.
2	Major	An action is needed, the situation is serious.
3	Minor	An action is needed, but the situation is not serious.
4	Degraded/warning	The user decides whether to take an action.

Table Continued



Severity Level	State	Description of the Severity
5	Informational	Indicates a status change that is not an error.
6	Debug	Information is logged for later analysis.
7	Clear	Indicates that the alert is cleared either by the system or by an administrator marking it acknowledged or fixed. This level is applicable only if the <code>addsnmpmgr -alertclear</code> option is <code>nodup</code> or <code>all</code> .

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

Alert state values

Table 13: Alert state values

Value	Alert State
1	New
2	Acknowledged
3	Fixed
4	Removed
5	Autofixed

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. All `alertNotify` traps have the same `snmpTrapOID` of `.1.3.6.1.1.12925.1.8`. Starting with the 3.3.1 MU1 release, you can also configure an SNMP manager to receive `storeServAlert` traps. For more information, see [storeServAlert traps](#).

The following example shows an `alertNotify` trap translated from an alert:

```
.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0: TimeTicks: 6 hours, 3 minutes, 6 seconds.:
.iso.org.dod.internet.snmpV2.snmpModules.snmpMIB.snmpMIBObjects.snmpTrap.snmpTrapOID.0: Object ID: .
1.3.6.1.4.1.12925.1.8:
.iso.org.dod.internet.private.enterprises.threepar.inserv.alertTable.alertEntry.component.1: sw_cp: 9: cpg1:
.iso.org.dod.internet.private.enterprises.threepar.inserv.alertTable.alertEntry.details.1: CPG cpg1 SD and/or
user space has reached allocation limit of 0G.:
.iso.org.dod.internet.private.enterprises.threepar.inserv.alertTable.alertEntry.nodeID.1: Gauge: 0:
.iso.org.dod.internet.private.enterprises.threepar.inserv.alertTable.alertEntry.severity.1: INTEGER: 1:
.iso.org.dod.internet.private.enterprises.threepar.inserv.alertTable.alertEntry.timeOccurred.1: 2017-06-06 15:
54: 10 PDT:
.iso.org.dod.internet.private.enterprises.threepar.inserv.alertTable.alertEntry.id.1: Gauge: 1:
.iso.org.dod.internet.private.enterprises.threepar.inserv.alertTable.alertEntry.messageCode.1: Gauge: 2555934:
.iso.org.dod.internet.private.enterprises.threepar.inserv.alertTable.alertEntry.state.1: INTEGER: 1:
.iso.org.dod.internet.private.enterprises.threepar.inserv.alertTable.alertEntry.serialNumber.1: 1999282:
.iso.org.dod.internet.private.enterprises.threepar.inserv.alertTable.alertEntry.catalogKey.1:
.iso.org.dod.internet.private.enterprises.threepar.inserv.alertTable.alertEntry.detailedMessage.1:
.iso.org.dod.internet.private.enterprises.threepar.inserv.alertTable.alertEntry.tier.1: Software check:
.iso.org.dod.internet.private.enterprises.threepar.inserv.alertTable.alertEntry.sparePartNumber.1:
```

storeServAlert traps

A storeServAlert trap contains the same varbinds as an alertNotify trap, but has a distinct snmpTrapOID that identifies the particular alert. Selected alerts generated by the system are translated into storeServAlert traps. StoreServAlert traps were added in the HPE 3PAR OS 3.3.1 MU1 release and are disabled by default. They can be enabled for an SNMP manager with the `-notify` option for the `addsnmpmgr` or `setsnmpmgr` commands. The `-notify` option can have the following values:

- `standard`—The manager wants to receive only alertNotify traps. `standard` is the default value.
- `nodup`—The manager wants to receive only storeServeAlert traps.
- `all`—The manager wants to receive both types of traps for every system 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.snmpTrapOID.0: Object ID: .
1.3.6.1.4.1.12925.1.2.0.198:
.iso.org.dod.internet.private.enterprises.threepar.inserv.alertTable.alertEntry.component.1: sw_rmm_link: 1047:
s99282_0_3_1:
.iso.org.dod.internet.private.enterprises.threepar.inserv.alertTable.alertEntry.details.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.alertEntry.nodeID.1: Gauge: 0:
.iso.org.dod.internet.private.enterprises.threepar.inserv.alertTable.alertEntry.severity.1: INTEGER: 2:
.iso.org.dod.internet.private.enterprises.threepar.inserv.alertTable.alertEntry.timeOccurred.1: 2017-06-06 16:
57: 08 PDT:
.iso.org.dod.internet.private.enterprises.threepar.inserv.alertTable.alertEntry.id.1: Gauge: 1414:
.iso.org.dod.internet.private.enterprises.threepar.inserv.alertTable.alertEntry.messageCode.1: Gauge: 3801338:
.iso.org.dod.internet.private.enterprises.threepar.inserv.alertTable.alertEntry.state.1: INTEGER: 1:
.iso.org.dod.internet.private.enterprises.threepar.inserv.alertTable.alertEntry.serialNumber.1: 1999281:
.iso.org.dod.internet.private.enterprises.threepar.inserv.alertTable.alertEntry.tier.1: General:
.iso.org.dod.internet.private.enterprises.threepar.inserv.alertTable.alertEntry.sparePartNumber.1:
```

Clearing alert traps

When an alert changes state, the manager receives a trap notification. This trap has `messageCode == 1245186`, a severity of Info (5), and details stating the “Alert <id> changed from state <prev state> to <new state>”. To find out which alert has a changed state, you must extract the alert ID from the `id` trap field.

The following information describes these alert state change events:

Message Code

1245186 (0x0130002)

Severity

Info

Type

Change in alert state

Alert String

Alert <alert_id> changed from state <old_state> to <new_state>

Operator Action

The alert has changed state, which can be used to track the state of the existing alerts in a system.

An alert state change event is not an alert. It notifies you that an alert has changed state (for example, from `New` to `Resolved` by `System`). The following example shows an `alertNotify` trap translated from an alert state change event:

```
sysUpTime.0:0 hours, 5 minutes, 26 seconds.  
snmpTrapOID 0:.iso.org.dod.internet.private.enterprises.threepar.inserv.alertNotify  
component.1:sw_alert  
details.1:Alert 647 changed from state New to Resolved by System  
nodeID.1:1  
severity.1:info(5)  
timeOccurred.1:Mon Dec 4 14:06:36 PST 2017  
id.1:647  
messageCode.1:1245186  
state.1:autofixed(5)
```

Starting with the HPE 3PAR OS 3.3.1 MU5 release, you can configure an SNMP manager to receive clearing traps that retain relevant information from the original alert. This kind of trap has the same `messageCode`, `details`, and `snmpTrapOID` as the original alert but with a severity of clear (7). Therefore, a manager can correlate an alert clearing trap with the original alert. This trap is disabled by default, but can be enabled for an SNMP manager with the `-alertclear` option for the `addsnmpmgr` or `setsnmpmgr` commands. The `-alertclear` option can have the following values:

- `standard`—The manager wants to receive only the alert state change traps. `standard` is the default value.
- `nodup`—The manager wants to receive only the alert clearing traps that have a severity of clear (7).
- `all`—The manager wants to receive both types of traps for every alert state change event.

The severity of the trap is set to clear when the state is changed to acknowledged (2), fixed (3) or autofixed (5). If the state is changed to remove (4), the `messageCode`, `details`, and `snmpTrapOID` of the original alert will not be available. The manager will receive the legacy state change `alertNotify` trap instead. For example, if an alert is removed by a user through the `removealert` CLI command, the manager will receive the legacy state change `alertNotify` trap.

The following example describes the new alert state change events:

Message Code

`messageCode` from the original alert

Severity

Clear

Type

Change in alert state

Alert String

Same text as the original alert

Operator Action

Action varies according to the original alert.

The following is an example alert and its clearing trap:

```
Original alert trap  
sysUpTime.0:0 hours, 5 minutes, 26 seconds.  
snmpTrapOID.0:.iso.org.dod.internet.private.enterprises.threepar.inserv.alertNotify  
component.1:sw_port: 0:2:1  
details.1: Port 0:2:1 Degraded (Target Mode Port Went Offline {0x3})
```

```
nodeID.1:1
severity.1:degraded(4)
timeOccurred.1: 2020-05-26 13:01:56 PDT
id.1:2
messageCode.1:196830
state.1:new(1)

Alert clear trap
sysUpTime.0:0 hours, 20 minutes, 26 seconds.
snmpTrapOID.0:.iso.org.dod.internet.private.enterprises.threepar.inserv.alertNotify
component.1:sw_port: 0:2:1
details.1: Port 0:2:1 Degraded (Target Mode Port Went Offline {0x3})
nodeID.1:1
severity.1:clear(7)
timeOccurred.1: 2020-05-26 13:16:56 PDT
id.1:2
messageCode.1:196830
state.1:autofixed(5)
```



HPE 3PAR Common Information Model API

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>



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 1.6.1.
- The HPE 3PAR CIM API passes SNIA-CTP conformance.

For additional information, see the following website:

<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 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 14: EVA and HPE 3PAR terms

EVA term	HPE 3PAR term
containers	(No equivalent)
Continuous Access	Remote Copy
controller	node, controller node
Demand allocated snapshot	Virtual copy
disk groups	CPGs
DR Group	Remote Copy Group
EVA firmware (controller software)	HPE 3PAR OS
Fully allocated snapshot	(No equivalent)
host	host
LUN	LUN
mirrorclone	physical copy
P6000 Command View	StoreServ Management Console (SSMC)
Performance Advisor	System Reporter
ports (iSCSI or FC)	ports (iSCSI or FC)
presentation (to host)	export (to host)
provisioning, thin provisioning	provisioning, full provisioning, thin provisioning
redundancy level (Vraid)	RAID
remote replication	Remote Copy

Table Continued



EVA term	HPE 3PAR term
snapclone	physical copy
snapshot	virtual copy, snapshot
thinly provisioned virtual volume (TPVV)	thinly provisioned virtual volume (TPVV)
(No equivalent)	Virtual Domains
Virtual disk (vdisk)	Virtual volume (VV)



Support and other resources

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:
<https://www.hpe.com/info/assistance>
- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:
<https://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

<https://www.hpe.com/support/hpesc>

Hewlett Packard Enterprise Support Center: Software downloads

<https://www.hpe.com/support/downloads>

My HPE Software Center

<https://www.hpe.com/software/hpesoftwarecenter>

- To subscribe to eNewsletters and alerts:
<https://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:
<https://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.

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

<https://www.hpe.com/services/getconnected>

HPE Proactive Care services

<https://www.hpe.com/services/proactivecare>

HPE Datacenter Care services

<https://www.hpe.com/services/datacentercare>

HPE Proactive Care service: Supported products list

<https://www.hpe.com/services/proactivecaresupportedproducts>

HPE Proactive Care advanced service: Supported products list

<https://www.hpe.com/services/proactivecareadvancedsupportedproducts>

Proactive Care customer information

Proactive Care central

<https://www.hpe.com/services/proactivecarecentral>

Proactive Care service activation

<https://www.hpe.com/services/proactivecarecentralgetstarted>

Warranty information

To view the warranty information for your product, see the links provided below:

HPE ProLiant and IA-32 Servers and Options

<https://www.hpe.com/support/ProLiantServers-Warranties>

HPE Enterprise and Cloudline Servers

<https://www.hpe.com/support/EnterpriseServers-Warranties>

HPE Storage Products

<https://www.hpe.com/support/Storage-Warranties>

HPE Networking Products

<https://www.hpe.com/support/Networking-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:

<https://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:

<https://www.hpe.com/info/reach>

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

<https://www.hpe.com/info/ecodata>

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

<https://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.



Glossary

A

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.

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.

ALUA

Asymmetric logical unit access.

AO

HPE 3PAR Adaptive Optimization.

API

Application program interface.

ASIC

Application-specific integrated circuit.

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 locks and unlocks the drive. The key is maintained by a local key manager or external key manager and backed up and guarded by system administrator.

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.

B**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 one of the following:

- Fully provisioned virtual volume
- Thinly provisioned virtual volume
- Thinly provisioned deduplicated virtual volume

C**CA**

Certificate authority.

CAC

Common access card used to provide two-factor authentication to a system such as SSMC.

chunklet

A block of contiguous storage space on a physical disk. On HPE 3PAR StoreServ Storage systems, all chunklets are 1 GiB.

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).

CMP

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

cluster

A group of controller nodes connected through 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.

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. In addition, 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 can allocate storage on demand.

CSR

Certificate signing request.

Customer self-repair.

D

DAR

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

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.

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.

E**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.

F**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.

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 systems.

FPVV

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

G

GB

Gigabyte.

GiB

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

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 GiB for a two-node system to 32 GiB 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.

H

HBA

Host bus adapter.

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. Those copies can then be used for disaster recovery, if necessary.

HPE 3PAR System Tuner software

A utility that enables the system to reallocate space usage 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.

I**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.

J

JSON

Javascript Object Notation.

K

KB/s

Kilobytes per second.

L

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

Lightweight Directory Access Protocol.

LFF

Large form factor.

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.

LUN

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

M

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).

MC

HPE 3PAR Management Console (formerly IMC).

message code

A keycode that identifies a system alert.

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.

MU

Maintenance update.

N

NACA

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.

NVMe

Non-volatile Memory express

O

ODM

IBM AIX Object Data Manager.

OLTP

Online transaction processing.

OSS

OpenStack Snapshot.

OU

Organizational unit.

OVF

Open Virtualization Format.

P

parent volume

A virtual volume from which a virtual or physical copy is made.

PB

Petabyte (1,000,000,000,000,000 or 10^{15}) bytes

Pct

Percent.

PD

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

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.

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)

External storage vendors 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.

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.

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

External storage vendor 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.

roles and rights

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

RTPG

Report target port group.

S

SAS

Serial attached SCSI.

SASL

Simple Authentication and Security Layer.

SC

HPE 3PAR Service Console.

SCM

Storage Class Memory.

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.

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. It will not be unlocked until the matching key from the HPE 3PAR StoreServ system is used to unlock it.

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 3PAR 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.

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.

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.

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.

SSD

Solid-state drive.

SSH

Secure Shell.

SSL

Secure Sockets Layer.

SSMC

HPE 3PAR StoreServ Management Console.

storage system

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

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

synchronous mode

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

sysmgr

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

Refers 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.

T

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.

TiB

Tebibyte [1 tebibyte = 2^{40} bytes = 1099511627776 bytes = 1024 gibibytes].

TLS

Transport Layer Security.

TPVV

Thinly provisioned virtual volume. A virtual volume that maps to logical disk space associated with a common provisioning group. Capable of growing on demand.

TUI

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

U

UDID

Unique device identifier.

UID (light)

Unit identification (light).

URI

Uniform Resource Identifier.

UTF

Uniform Transformation Format.

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, no storage is allocated to user space, so the user space represents the virtual size of the volume.

V

VAAI

VMware vStorage APIs for Array Integration.

VASA

VMware vSphere API for Storage Awareness.

VFS

Virtual file server. A VFS acts as a virtual device that controls many of the network policies for communications between 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 allocated to user space. 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 MiB.

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.

VSA

Volume set addressing.

VSP

Virtual service processor.

VV

Virtual volume.

VVol

VMware vSphere virtual volume.

W**WBEM**

Web-Based Enterprise Management.

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.

Z**zone**

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