



**Hewlett Packard**  
Enterprise

# **HPE 3PAR OS 3.3.1 MU2 Patch 32**

## **Release Notes**

### **Abstract**

This release notes document is for Patch 3.3.1 MU2 P32.

Part Number: QL226-99918  
Published: July 2018  
Edition: 1

## Notices

© 2014-2018, Hewlett Packard Enterprise Development LP

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.

Export of the information contained in this publication may require authorization from the U.S. Department of Commerce.

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.

## Acknowledgements

Microsoft and Windows are U.S. registered trademarks of Microsoft Corporation.

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

Java and Oracle are registered trademarks of Oracle and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

Intel®, Itanium®, Pentium®, Intel Inside®, and the Intel Inside logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

# Purpose

The HPE 3PAR OS 3.3.1 MU2 Patch 32 provides several critical quality improvements.

---

❗ **IMPORTANT:** See the [HPE 3PAR OS and Service Processor Software Update Guide \(HPE 3PAR OS 3.3.1 HPE 3PAR Service Processor 5.x\)](#) for instructions on updating your specific software.

---

## Guidance

This is a critical patch.

## Prerequisites

- Minimum Service Processor required: SP-5.0.3+latest SP patch
- Base OS: See the Requires field in the Patch details.

## Patch details

Patch ID: P32

Synopsis: Provides several critical quality improvements

Date: June 28, 2018, 17:30:02 PDT

Description: See the Release Notes for details about this patch

Affected Packages: tpd-adlc, tpd-cachesvr, tpd-kernelpatch, tpd-sysmgr, tpd-utils, tpd-libtpdtcl, libkrb5-3, libgssapi-krb5-2, libk5crypto3, libkrb5support0, tpd-prerevert

Obsoletes: None

Requires: OS-3.3.1.410-MU2, OS-3.3.1.410-P30

Patches Partially Superseded: OS-3.3.1.410-P30

Patches Included: None

Patches Obsolete by Combination: None

Supports Revert: Yes

Build Version: **3.3.1.439**

Notes:

---

## NOTE:

Hewlett Packard Enterprise recommends installing patches in the same sequence as they are released, unless instructed otherwise.

---

# Modifications

HPE 3PAR Patch 32 addresses the following issues:

---

**Issue ID:** 157989, 233586

**Issue summary:** An `unmap` command immediately followed by writes to the same blocks of a TPVV results in an unsuccessful I/O.

**Platforms affected:** All StoreServ

**Affected software versions:** 3.2.2, 3.3.1 GA - MU2

**Issue Description:** When a TPVV is full, if the host sends `unmap` commands, the `unmap` completion is sent to the host, but the VV space is not immediately freed. If the host then attempts to write the unmapped blocks, this will result in an unsuccessful write operation even though the free space exists within the CPG.

**Symptoms:** A TPVV appears to be read-only by the host.

Allocation failure messages are seen in event logs.

**Conditions of occurrence:** A TPVV is fully used and the host has issued `unmap` commands to the TPVV.

**Impact:** High

**Customer circumvention:** None.

**Customer recovery steps:** None.

---

---

**Issue ID:** 208350, 236719

**Issue summary:** LDAP connections do not successfully bind when using Simple Authentication and Security Layer (SASL) as a binding mechanism.

**Platforms affected:** All StoreServ

**Affected software versions:** 3.2.2, 3.3.1 GA - MU2

**Issue Description:** LDAP connections do not successfully bind through Simple Authentication and Security Layer (SASL) due to a Kerberos error, resulting in the binding not completing which causes the `auth_helper` process to never exit.

**Symptoms:** Multiple `auth_helper` processes never complete leading to near 100% CPU utilization.

**Conditions of occurrence:** LDAP is configured with a binding type of SASL.

**Impact:** Medium

**Customer circumvention:** Set the binding type to simple.

**Customer recovery steps:** None.

---

---

**Issue ID:** 237529, 229448, 214454

**Issue summary:** During the controller node integration process, the controller node may unexpectedly restart.

**Platforms affected:** All StoreServ

**Affected software versions:** 3.3.1 GA - MU2

**Issue description:** If a large amount of deduplication accounting is required during a controller node integration and the array is experiencing a heavy write workload, the process may time out. When this timeout occurs, the controller node will restart unexpectedly.

**Symptoms:** Unexpected controller node or array restart.

**Conditions of occurrence:** During controller node integration.

**Impact:** High

**Customer circumvention:** None.

**Customer recovery steps:** None.

---

**Issue ID:** 223994, 226499

**Issue summary:** Hosts may temporarily lose connection to VLUNs or experience high service times to VLUNs during an `upgraded` operation.

**Platforms affected:** All StoreServ

**Affected software versions:** 3.3.1 GA - MU2

**Issue description:** When the upgrade firmware operation on the physical disks takes place with high write operations occurring at the same time, access to the data may be delayed several seconds. This delay can result in some host operating environments experiencing a disconnect from the VLUNs they are accessing.

**Symptoms:** Long service times to access VLUNs and possibly a temporary host disconnect from the VLUN.

**Conditions of occurrence:** Upgrading physical disk firmware during periods of high I/O.

**Impact:** High

**Customer circumvention:** Perform physical disk firmware operations in a period of low I/O.

**Customer recovery steps:** None.

---

---

**Issue ID:** 226073

**Issue summary:** AREA model Self-Encrypting Drives in an unencrypted array report being `LOCKED` and the `fipsvr` process sees an unrecognized encryption key.

**Platforms affected:** All StoreServ

**Affected software versions:** 3.3.1 GA - MU2

**Issue description:** Certain FIPs Self-Identifying drives (SID) in an unencrypted array report a `LOCKED` status and the `fipsvr` process receives an unrecognized encryption key. This occurs due to Automatic Drive Log Collection (ADLC).

**Symptoms:** One of the affected drives fail to admit.

**Conditions of occurrence:** When ADLC runs with following combinations of drive model and firmware installed on the array.

Drive model	Drive Firmware
AREA0920S5xnFTRI	3P00
AREA1920S5xnFTRI	3P00
AREA3840S5xnFTRI	3P00
AREA7680S5xnFTRI	3P01 or lower
AREA15T4S5xnFTRI	3P01 or lower

**Impact:** High

**Customer circumvention:** None.

**Customer recovery steps:** None.

---

**Issue ID:** 228035

**Issue summary:** A single controller node or the array unexpectedly restarts due to an internal log exception.

**Platforms affected:** All StoreServ

**Affected software versions:** 3.2.2, 3.3.1 MU1 - MU2

**Issue description:** The virtual volume master node restart followed by the cluster reboot when meta log page processing thread encounters an invalid log page exception entry that points to the page beyond the grown admin virtual volume size.

**Symptoms:** Node restart.

Cluster restart.

**Conditions of occurrence:** Meta log page processing.

**Impact:** Low

**Customer circumvention:** None.

**Customer recovery steps:** None.

---

---

**Issue ID:**233919

**Issue summary:** The `cachesvr` process does not release used memory resources.

**Platforms affected:** All StoreServ

**Affected software versions:** 3.2.2, 3.3.1 GA - MU2

**Issue description:** In some environments, the `cachesvr` process memory consumption grows unbounded over time which may, in turn, cause other processes to unexpectedly restart.

**Symptoms:** The array becomes unresponsive. Some processes may unexpectedly restart and the event log indicates an out of memory condition.

**Conditions of occurrence:** Environments with increased levels of PD chunklet failure recovery, PD chunklet relocation, or PD maintenance operations.

**Impact:** Medium

**Customer circumvention:** None.

**Customer recovery steps:** None.

---

**Issue ID:** 235662

**Issue summary:** Unexpected controller node restarts when an internal system map is not in a consistent state.

**Platforms affected:** All StoreServ

**Affected software versions:** 3.2.2, 3.3.1 MU1 - MU2

**Issue description:** An internal inconsistency is encountered during a memory page allocation which causes the controller node to unexpectedly restart.

**Symptoms:** Controller nodes unexpectedly restart.

**Conditions of occurrence:** A space allocation takes place.

**Impact:** Low

**Customer circumvention:** None.

**Customer recovery steps:** After the controller node restart completes, run `checkvv` on the affected VV.

---

**Issue ID:** 236286

**Issue summary:** Hosts may lose access to VLUNs when large numbers of snapshots are being created by Recovery Manager Central (RMC).

**Platforms affected:** All StoreServ

**Affected software versions:** 3.2.2, 3.3.1 MU1 - MU2

**Issue description:** During snapshot processing between controller nodes, a deadlock condition can be encountered. This can result in the host I/O being delayed and the array may become unresponsive.

**Symptoms:** Hosts cannot access VLUNs and the array may become unresponsive.

**Conditions of occurrence:** Creating many snapshots using RMC.

**Impact:** High

**Customer circumvention:** None.

**Customer recovery steps:** None.

---

---

**Issue ID:** 237098

**Issue summary:** VMware initiated snapshots on VVols taking approximately eight seconds to complete.

**Platforms affected:** All StoreServ

**Affected software versions:** 3.2.2, 3.3.1 GA - MU2

**Issue description:** Commands processed during the creation of a VMware initiated snapshot on a VVol have a long response time. The longer response time results in VMware virtual machines being suspended for that period of time.

**Symptoms:** Delay in VMware snapshot completion on VVOLS.

**Conditions of occurrence:** VMware snapshots taken when using VVols.

**Impact:** High

**Customer circumvention:** None.

**Customer recovery steps:** None.

---

---

**Issue ID:** 237546

**Issue summary:** Unexpected controller node restarts occur while using compressed volumes.

**Platforms affected:** StoreServ 8000, StoreServ 9000, StoreServ 20000, StoreServ 20000 R2

**Affected software versions:** 3.3.1 GA - MU2

**Issue description:** Unexpected controller node restarts occur when inconsistent metadata entries for compression volumes are encountered and a subsequent partial page write happens

**Symptoms:** Unexpected controller node restarts occur.

**Conditions of occurrence:** Presence of compression volumes.

**Impact:** Medium

**Customer circumvention:** None.

**Customer recovery steps:** None.

---

## Affected components

---

Component	Version
System Manager	3.3.1.439 (P32)
TPD Kernel Patch	3.3.1.439 (P32)

---

**NOTE:** Applying an HPE 3PAR OS patch can cause a restart of the affected OS components. This restart is an expected behavior, which will generate events and alerts. The system continues to serve data, but existing CLI or SSMC sessions could be interrupted.

---

## Verification

The installation of Patch 32 can be verified from an interactive CLI session. Issue the CLI command `showversion -a -b` to verify that Patch 32 is listed:



---

Release version 3.3.1.410 (MU2)

Patches: P30,P32

Component Name	Version
CLI Server	3.3.1.410 (MU2)
CLI Client	3.3.1.410
<b>System Manager</b>	<b>3.3.1.439 (P32)</b>
Kernel	3.3.1.410 (MU2)
TPD Kernel Code	3.3.1.410 (MU2)
<b>TPD Kernel Patch</b>	<b>3.3.1.439 (P32)</b>
CIM Server	3.3.1.410 (MU2)
WSAPI Server	3.3.1.410 (MU2)
Console Menu	3.3.1.410 (MU2)
Event Manager	3.3.1.410 (MU2)
Internal Test Tools	3.3.1.410 (MU2)
LD Check Tools	3.3.1.410 (MU2)
Network Controller	3.3.1.410 (MU2)
Node Disk Scrubber	3.3.1.410 (MU2)
PD Scrubber	3.3.1.410 (MU2)
Per-Node Server	3.3.1.410 (MU2)
Persistent Repository	3.3.1.410 (MU2)
Powerfail Tools	3.3.1.410 (MU2)
Preserved Data Tools	3.3.1.410 (MU2)
Process Monitor	3.3.1.410 (MU2)
Software Updater	3.3.1.410 (MU2)
TOC Server	3.3.1.410 (MU2)
VV Check Tools	3.3.1.410 (MU2)
Upgrade Check Scripts	180507.U013
File Persona	1.4.2.40-20171006 (MU2)
SNMP Agent	1.10.0
SSH	6.0p1-4+deb7u5
VASA Provider	3.0.17 (MU2)
Firmware Database	3.3.1.410 (MU2)
Drive Firmware	3.3.1.410 (MU2)
UEFI BIOS	05.02.54 (MU2)
MCU Firmware (OKI)	4.8.60 (MU2)
MCU Firmware (STM)	5.3.17 (MU2)
Cage Firmware (DC1)	4.44 (MU2)
Cage Firmware (DC2)	2.64 (MU2)
Cage Firmware (DC3)	08 (MU2)
Cage Firmware (DC4)	2.64 (MU2)
Cage Firmware (DCN1)	4082 (MU2)
Cage Firmware (DCN2)	4082 (MU2)
Cage Firmware (DCS1)	4082 (MU2)
Cage Firmware (DCS2)	4082 (MU2)
Cage Firmware (DCS5)	2.79 (MU2)
Cage Firmware (DCS6)	2.79 (MU2)
Cage Firmware (DCS7)	4082 (MU2)
Cage Firmware (DCS8)	4082 (MU2)
QLogic QLA4052C HBA Firmware	03.00.01.77 (MU2)
QLogic QLE8242 CNA Firmware	04.15.27
QLogic 260x HBA FC Firmware	174.03.70
QLogic 27xx/268x HBA FC Firmware	174.03.70

QLogic 83xx HBA FCoE Firmware	08.01.05
QLogic 8300 HBA iSCSI Firmware	05.07.35
Emulex LP11002 HBA Firmware	02.82.x10
Emulex LPe12002 HBA Firmware	02.10.x03
Emulex LPe12004 HBA Firmware	02.10.x03
Emulex LPe16002 HBA Firmware	11.1.220.10
Emulex LPe16004 HBA Firmware	11.1.220.10
3PAR FC044X HBA Firmware	200A8
LSI 9201-16e HBA Firmware	17.11.03
LSI 9205-8e HBA Firmware	17.11.03
LSI 9300-8e HBA Firmware	10.10.01

---

**NOTE:** When displaying the `showversion` command output from the SP, the CLI Client version is static in the SP code and may differ from the output from any other system.

---

# Websites

## **General websites**

**Hewlett Packard Enterprise Information Library**

**[www.hpe.com/info/EIL](http://www.hpe.com/info/EIL)**

**Single Point of Connectivity Knowledge (SPOCK) Storage compatibility matrix**

**[www.hpe.com/storage/spock](http://www.hpe.com/storage/spock)**

**Storage white papers and analyst reports**

**[www.hpe.com/storage/whitepapers](http://www.hpe.com/storage/whitepapers)**

For additional websites, see **[Support and other resources](#)**.

# Support and other resources

## Accessing Hewlett Packard Enterprise Support

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

### Information to collect

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

## Accessing updates

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

### Hewlett Packard Enterprise Support Center

[www.hpe.com/support/hpesc](http://www.hpe.com/support/hpesc)

### Hewlett Packard Enterprise Support Center: Software downloads

[www.hpe.com/support/downloads](http://www.hpe.com/support/downloads)

### Software Depot

[www.hpe.com/support/softwaredepot](http://www.hpe.com/support/softwaredepot)

- To subscribe to eNewsletters and alerts:  
[www.hpe.com/support/e-updates](http://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:

- 
- ❗ **IMPORTANT:** Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HPE Passport set up with relevant entitlements.
- 

## Customer self repair

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

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

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

## Remote support

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

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

### Remote support and Proactive Care information

#### HPE Get Connected

[www.hpe.com/services/getconnected](http://www.hpe.com/services/getconnected)

#### HPE Proactive Care services

[www.hpe.com/services/proactivecare](http://www.hpe.com/services/proactivecare)

#### HPE Proactive Care service: Supported products list

[www.hpe.com/services/proactivecaresupportedproducts](http://www.hpe.com/services/proactivecaresupportedproducts)

#### HPE Proactive Care advanced service: Supported products list

[www.hpe.com/services/proactivecareadvancedsupportedproducts](http://www.hpe.com/services/proactivecareadvancedsupportedproducts)

### Proactive Care customer information

#### Proactive Care central

[www.hpe.com/services/proactivecarecentral](http://www.hpe.com/services/proactivecarecentral)

#### Proactive Care service activation

[www.hpe.com/services/proactivecarecentralgetstarted](http://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

[www.hpe.com/support/ProLiantServers-Warranties](http://www.hpe.com/support/ProLiantServers-Warranties)

### HPE Enterprise and Cloudline Servers

[www.hpe.com/support/EnterpriseServers-Warranties](http://www.hpe.com/support/EnterpriseServers-Warranties)

## HPE Storage Products

[www.hpe.com/support/Storage-Warranties](http://www.hpe.com/support/Storage-Warranties)

## HPE Networking Products

[www.hpe.com/support/Networking-Warranties](http://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:

[www.hpe.com/support/Safety-Compliance-EnterpriseProducts](http://www.hpe.com/support/Safety-Compliance-EnterpriseProducts)

## Additional regulatory information

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

[www.hpe.com/info/reach](http://www.hpe.com/info/reach)

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

[www.hpe.com/info/ecodata](http://www.hpe.com/info/ecodata)

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

[www.hpe.com/info/environment](http://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](mailto: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.