



Hewlett Packard
Enterprise

HPE 3PAR OS 3.3.1 MU2 Patch 45

Release Notes

Abstract

This release notes document is for 3.3.1 MU2 Patch 45.

Part Number: QL226-10576
Published: November 2018
Edition: 1

© 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 P45 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: OS-3.3.1 MU2. See the Requires field in the Patch details.

Patch details

Patch ID: P45

Synopsis: Provides several critical quality improvements

Date: October 12, 2018, 15:08:13 PDT

Description: See the Release Notes for details about this patch

Affected Packages: tpd-sysmgr, tpd-libcli, tpd-kernelanalysis, tpd-nodesvr, tpd-kernelpatch, tpd-cli, tpd-libtpdtcl, tpd-evt, tpd-prerevert

Obsoletes: None

Requires: OS-3.3.1.410-MU2,OS-3.3.1.410-P30,OS-3.3.1.410-P32,OS-3.3.1.410-P40

Build Version: 3.3.1.482

Patches Included: None.

Patches Partially Superseded: OS-3.3.1.410-P32,OS-3.3.1.410-P40

Patches Obsolete by Combination: None.

Supports Revert: Yes

Notes:

NOTE:

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

Modifications

HPE 3PAR OS 3.3.1 MU2 Patch 45 addresses the following issues:

Issue ID: 155807, 247725, 246140

Issue summary: A controller node restart occurs during Port Persistent failback when a loss of a SCSI initiator occurs at the same time on the same vPort that is disappearing.

Affected platforms: All StoreServ

Affected software versions: 3.2.1 GA - MU5, 3.2.2 GA - MU6, 3.3.1 GA - MU2

Issue description: An unexpected controller node restart occurs during Port Persistence failback when a loss of a SCSI initiator occurs at the same time on the vPort that is being failed back.

Symptoms: A controller node restarts.

Conditions of occurrence: A SCSI initiator is lost on the network by the vPort that is being failed back.

Impact: Medium

Customer circumvention: None.

Customer recovery steps: None.

Issue ID: 202616, 247902, 247901

Issue summary: Firmware creates diagnostic files, and the port is reset.

Affected platforms: All StoreServ

Affected software versions: 3.2.2 GA - MU6, 3.3.1 GA - MU3

Issue description: Hosts ports may experience a Converged Network Adapter (CNA) port reset due to an outstanding exchange in the CNA firmware. This reset leads to host aborts or I/Os not completing. The affected port may also fail over to another port.

Symptoms: Port reset occurs.

Conditions of occurrence: Host connected to CNA ports are under high load, or high service time.

Impact: Medium

Customer circumvention: None.

Customer recovery steps: None.

Issue ID: 213894, 239147, 248306, 248305

Issue summary: System Manager stops responding.

Platforms affected: All StoreServ

Affected software versions: 3.2.2, 3.3.1 GA - MU3

Issue description: A VV block operation triggered by AO region moves is delayed. This delay leads to the System Manager becoming unresponsive. A subsequent restart of System Manager leads to the array unexpectedly restarting.

Symptoms: The array unexpectedly restarts.

Conditions of occurrence: Adaptive Optimization is being used.

Impact: High

Customer circumvention: None.

Customer recovery steps: None.

Issue ID: 232101, 247924, 247923

Issue summary: Invalid iSCSI Protocol Data Units (PDUs) from the initiator can cause the host port to go offline.

Affected platforms: All StoreServ

Affected software versions: 3.2.1 GA - MU6, 3.2.2 GA - MU6, 3.3.1 GA - MU2

Issue description: Invalid iSCSI Protocol Data Units (PDUs) from the initiator can cause the host port to go offline.

Symptoms: iSCSI host ports go offline.

Diagnostic files are generated.

Conditions of occurrence: Initiator sends invalid iSCSI PDUs.

Impact: Medium

Customer circumvention: None.

Customer recovery steps: None.

Issue ID: 237034

Issue summary: SAS port resets when `admithw` is executed on an array.

Affected platforms: StoreServ 7000

Affected software versions: 3.3.1 GA - MU3

Issue description: SAS port hard resets are initiated when `admithw` is executed on an array with non-9300 SAS Host Bus Adapter (HBA) cards. This reset occurs even when the firmware is up-to-date and in check-only mode.

Symptoms: SAS port resets.

Conditions of occurrence: `admithw` is run on an array running 3PAR OS 3.3.1 with non-9300 SAS Host Bus Adapter (HBA) cards.

Impact: Medium

Customer circumvention: Avoid running `admithw`.

Customer recovery steps: None.

Issue ID: 237299, 231715, 240062, 248623, 248622

Issue summary: No alerts are raised for faulty Active Optical Cables (AOC).

Affected platforms: All StoreServ

Affected software versions: 3.3.1 GA - MU2

Issue description: No alerts are raised for faulty AOC, despite `TxFault` being set and reported in diagnostic checks.

Symptoms: None.

Conditions of occurrence: A faulty AOC is present.

Impact: Medium

Customer circumvention: None.

Customer recovery steps: None.

Issue ID: 238127, 241832, 247043, 247042

Issue summary: Host I/O stalls while snapshots are being created.

Affected platforms: All StoreServ

Affected software versions: 3.3.1 MU1 - MU2

Issue description: A change blocks I/O from the host when the target volume or its first snapshot child is not marked normal. This causes host I/O to not complete when snapshots are being created.

Symptoms: Host I/O stalls or does not complete.

Conditions of occurrence: Snapshots are being created.

Impact: High

Customer circumvention: Avoid creating snapshots including Remote Copy snapshots.

Customer recovery steps: None.

Issue ID: 240493, 247515, 247514

Issue summary: System Manager consumes memory in an unconstrained manner and does not return released memory.

Affected platforms: All StoreServ

Affected software versions: 3.3.1 GA - MU1

Issue description: The System Manager calculate system capacity utility does not release memory (fail_ids).

Symptoms: System Manager consumes memory in an unconstrained manner and does not return released memory.

Conditions of occurrence: `showsys -space` can cause System Manager to consume memory in an unconstrained manner and not return released memory.

Impact: Medium

Customer circumvention: Avoid running `showsys -space`.

Customer recovery steps: None.

Issue ID: 242656, 243675

Issue summary: Data Integrity Field (DIF) recovery on compressed volumes leads to an unexpected controller node restart.

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

Affected software versions: 3.3.1 GA - MU3

Issue description: Controller node may unexpectedly restart due to DIF recovery attempting to write an already cleaned internal system area from a compressed volume.

Symptoms: The array restarts unexpectedly.

Conditions of occurrence: Presence of compression volumes.

Impact: Medium

Customer circumvention: None.

Customer recovery steps: None.

Issue ID: 243618, 247179,247180

Issue summary: Array restarts can occur due to an inconsistent view on virtual volume (VV) metadata.

Platforms affected: All StoreServ

Affected software versions: 3.2.2, 3.3.1 GA - MU3

Issue description: Unexpected array restarts occur due to an inconsistent view of the virtual volume (VV) master controller node following the restarting of a controller node which was the master of a Virtual Volume.

Symptoms: Array restart.

Conditions of occurrence: A controller node is rebooted or restarted either intentionally or due to an unexpected condition on the controller node.

Impact: High

Customer circumvention: None.

Customer recovery steps: None.

Issue ID: 245154, 248221, 248222

Issue summary: The System Manager restarts due to memory resources being unavailable.

Affected platforms: All StoreServ

Affected software versions: 3.3.1 GA - MU3

Issue description: Excessive memory usage by the System Manager process due to execution of a large amount of import VV operations and/or online copy can eventually lead to the process running out of memory, which triggers an unexpected System Manager restart.

Symptoms: System Manager process restarts abruptly.

Conditions of occurrence: Performing a large amount of import VV and/or online copy activities.

Impact: High

Customer circumvention: Avoid running `importvv` and online copy activities.

Customer recovery steps: None.

Issue ID: 245417, 246544

Issue summary: If a controller node is restarted, as is the case during an online upgrade, the controller node does not rejoin the cluster if an FCoE port reset does not succeed.

Affected platforms: All StoreServ

Affected software versions: 3.2.2 GA - MU6, 3.3.1 GA - MU3

Issue description: The Host Bus Adapter (HBA) FCoE port does not reset successfully which prevents the controller node from rejoining the array.

Symptoms: FCoE port resets.

Conditions of occurrence: Online upgrade is being performed.

Impact: Medium

Customer circumvention: None.

Customer recovery steps: Perform a hard reset of the port using the `controlport rst -1 <port number>` command, and reboot the controller node.

Issue ID: 246720, 247885, 247884

Issue summary: Allowing recovery to continue when Remote Copy groups on the target arrays are still enabled causes controller node to unexpectedly restart.

Affected platforms: All StoreServ

Affected software versions: 3.3.1 GA - MU2

Issue description: Allowing a recovery operation to continue while Remote Copy groups on some targets are still enabled causes an unexpected controller node restart.

Symptoms: Controller node restarts.

Conditions of occurrence: Perform failover, recover, or restore on periodic target while the groups on sync target are still enabled.

Impact: Medium

Customer circumvention: Stop groups on all targets before executing the `failover` command.

Customer recovery steps: None.

Affected components

Component	Version
CLI Server	3.3.1.482 (P45)
System Manager	3.3.1.482 (P45)
TPD Kernel Patch	3.3.1.482 (P45)
Event Manager	3.3.1.482 (P45)
Per-Node Server	3.3.1.482 (P45)

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 45 can be verified from an interactive CLI session. Issue the CLI command `showversion -a -b` to verify that Patch 45 is listed:

Release version 3.3.1.410 (MU2)

Patches: P32,P36,P39,P40,P45

Component Name	Version
CLI Server	3.3.1.482 (P45)
CLI Client	3.3.1.482
System Manager	3.3.1.482 (P45)
Kernel	3.3.1.410 (MU2)
TPD Kernel Code	3.3.1.410 (MU2)
TPD Kernel Patch	3.3.1.482 (P45)
CIM Server	3.3.1.410 (MU2)
WSAPI Server	3.3.1.410 (MU2)
Console Menu	3.3.1.410 (MU2)
Event Manager	3.3.1.482 (P45)
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	3.3.1.482 (P45)
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	3.3.1.467 (P40)
TOC Server	3.3.1.410 (MU2)
VV Check Tools	3.3.1.410 (MU2)
Upgrade Check Scripts	181001.U016
File Persona	1.5.1.900-20180914 (P39)
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

Single Point of Connectivity Knowledge (SPOCK) Storage compatibility matrix

www.hpe.com/storage/spock

Storage white papers and analyst reports

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

Hewlett Packard Enterprise Support Center: Software downloads

www.hpe.com/support/downloads

Software Depot

www.hpe.com/support/softwaredepot

- To subscribe to eNewsletters and alerts:

www.hpe.com/support/e-updates

- To view and update your entitlements, and to link your contracts and warranties with your profile, go to the Hewlett Packard Enterprise Support Center **More Information on Access to Support Materials** page:

www.hpe.com/support/AccessToSupportMaterials

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

Customer self repair

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

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

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

Remote support

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

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

Remote support and Proactive Care information

HPE Get Connected

www.hpe.com/services/getconnected

HPE Proactive Care services

www.hpe.com/services/proactivecare

HPE Proactive Care service: Supported products list

www.hpe.com/services/proactivecaresupportedproducts

HPE Proactive Care advanced service: Supported products list

www.hpe.com/services/proactivecareadvancedsupportedproducts

Proactive Care customer information

Proactive Care central

www.hpe.com/services/proactivecarecentral

Proactive Care service activation

www.hpe.com/services/proactivecarecentralgetstarted

Warranty information

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

HPE ProLiant and IA-32 Servers and Options

www.hpe.com/support/ProLiantServers-Warranties

HPE Enterprise and Cloudline Servers

www.hpe.com/support/EnterpriseServers-Warranties

HPE Storage Products

www.hpe.com/support/Storage-Warranties

HPE Networking Products

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

Additional regulatory information

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

www.hpe.com/info/reach

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

www.hpe.com/info/ecodata

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

www.hpe.com/info/environment

Documentation feedback

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