Hewlett Packard Enterprise

HPE 3PAR OS 3.3.1 MU3 Patch 58 Release Notes

Abstract

This release notes document is for 3.3.1 MU3 P58.

Part Number: QL226-10023
Published: March 2019
Edition: 1

© Copyright 2019 Hewlett Packard Enterprise Development LP

© 2014-2019, 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 MU3 Patch 58 delivers 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.

IMPORTANT: Do not install this patch on arrays where File Persona is in use. For those systems, install a future File Persona patch, which will include this patch.

Prerequisites

- Minimum Service Processor required: SP-5.0.4 + latest SP Patch.
- Base OS: 3.3.1 MU3. See the Requires field in the Patch details.

Patch details

Patch ID: P58

Synopsis: Delivers critical quality improvements

Date: March 01, 2019, 15:10:13 PST

Description: See the Release Notes for details about this patch

Affected Packages: tpd-adlc, tpd-api, tpd-cli, tpd-enclmgmt, tpd-evt, tpd-fipsvr, tpd-kernelpatch, tpd-libauth, tpd-libcli, tpd-libtpdapi, tpd-libtpdtcl, tpd-motd, tpd-nodesvr, tpd-qw, tpd-sysmgr, tpd-wsapi, tpd-prerevert

Obsoletes: OS-3.3.1.460-P53

Requires: OS-3.3.1.460-MU3

Build Version: 3.3.1.522

Patches Included: None.

Patches Partially Superseded: None.

Patches Obsolete by Combination: None.

Supports Revert: Yes

Notes: Description of the obsoleted patches:

Patch ID: P53

Synopsis: Further improves error handling for certain drive models

Date: January 25, 2019, 19:47:08 PST

Description: See the Release Notes for details about this patch

Affected Packages: tpd-kernelpatch, tpd-libcli, tpd-sysmgr, tpd-prerevert

Obsoletes: None

Requires: OS-3.3.1.460-MU3

Build Version: 3.3.1.506

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 MU3 Patch 58 addresses the following issues:

Issue ID: 253562

Issue summary: An incorrect `Cage interface card max daisy chain violation` alert displayed on 8400 and 8440 platforms that have a daisy chain deeper than 5.

Platforms affected: StoreServ 7000, StoreServ 8000

Affected software versions: 3.3.1 MU3

Issue description: An incorrect configuration in enclosure management causes the alert `Cage interface card max daisy chain violation` to appear on platforms that have a daisy chain deeper than 5.

Symptoms: A `Cage interface card max daisy chain violation` is displayed.

Conditions of occurrence: A 7440c, 8400, or 8440 series array with a daisy chain deeper than five cages.

Impact: Low

Customer circumvention: None.

Customer recovery steps: None.

Issue ID: 257270, 257269

Issue summary: CBC cipher changes for WSAPI and CIM connections.

Platforms affected: All StoreServ

Affected software versions: 3.2.2, 3.3.1

Issue description: WSAPI and CIM CBC cipher changes for both `tls_strict` and `no_tls_strict` modes:

Supported: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 - ECDHE-RSA-AES128-GCM-SHA256

Previously supported and no longer supported: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA - ECDHE-RSA-AES256-SHA, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 - ECDHE-RSA-AES256-SHA384

Symptoms: WSAPI and CIM are no longer able to connect.

Conditions of occurrence: A non-supported cipher is being used with HPE 3PAR OS version 3.2.2 or 3.3.1.

Impact: Medium

Customer circumvention: None.

Customer recovery steps: If connectivity issues occur, reconfigure the clients to use currently supported cipher from the above list.

Issue ID: 247827

Issue summary: WSAPI process restarts.

Platforms affected: All StoreServ

Affected software versions: 3.3.1

Issue description: The WSAPI process has a segment fault, resulting in a restart. Existing requests are terminated.

Symptoms: The WSAPI process restarts and existing requests are terminated.

Conditions of occurrence: A port scanner for security checks is running on the array.

Impact: Medium

Customer circumvention: Avoid port scanner for security checks on ports 8008/8080.

Customer recovery steps: None.

Issue ID: 247837

Issue summary: The WSAPI returns a **`500 Internal Server Error`** when there is no Remote Copy license on the system.

Platforms affected: All StoreServ

Affected software versions: 3.3.1

Issue description: `getrcopy()` inside of `getvv_int()` does not succeed if there is no Remote Copy license on the system. The operation returns a `500 Internal Server Error` message.

Symptoms: An **`HTTP GET`** request returns `500 Internal Server Error` instead of the volume properties.

Conditions of occurrence: There is no remote copy license install on the array.

Impact: Medium

Customer circumvention: None.

Customer recovery steps: None.

Issue ID: 247848

Issue summary: WSAPI process does not execute successfully.

Platforms affected: All StoreServ

Affected software versions: 3.3.1

Issue description: The session is not marked `in use` when a WSAPI request is received by the WSAPI server. Another WSAPI request or CLI command requests the session key to be removed. This condition causes WSAPI to stop responding.

Symptoms: WSAPI process does not execute successfully,

Conditions of occurrence: A WSAPI or CLI command requests a session key to be removed while another request has the session key locked.

Impact: Medium

Customer circumvention: None.

Customer recovery steps: None.

Issue ID: 250657

Issue summary: WSAPI process terminates unexpectedly.

Platforms affected: All StoreServ

Affected software versions: 3.2.2, 3.3.1

Issue description: WSAPI process terminates unexpectedly. This occurs when there are concurrent HTTP GET requests made with **`sampleTime`** query filter to System Reporter objects (**`srspacecpg`**, **`srspacepd`**, **`srspacevv`**, **`srstatcmp`**, **`srstatcpg`**, **`srstatcpu`**, **`srstatpd`**, **`srstatport`**, **`srstatqos`**, **`srstatrcopy`**, **`srstatrcvv`**, **`srstatvlun`**).

Symptoms: WSAPI process terminates unexpectedly.

Conditions of occurrence: Concurrent HTTP GET requests with **`sampleTime`** query filter on System Reporter objects.

Impact: Medium

Customer circumvention: Avoid using the **`sampleTime`** query filter.

Customer recovery steps: None.

Issue ID: 233906, 243541

Issue summary: Adds support for internal drive log collection for the ARFX drive model family.

Platforms affected: All StoreServ

Affected software versions: All

Issue description: Adds the required support for internal log collection from the ARFX drive models. The following table shows the affected drives.

Drive	Category	Capacity	Speed	StoreServ 10000	StoreServ 7000	StoreServ 20000	StoreServ 8000	FW
ARFX0920S5xnNTRI	SSD	920GB	150K	No	Yes	Yes	Yes	3P00
ARFX1920S5xnNTRI	SSD	1.92TB	100K	Yes	Yes	Yes	Yes	3P00
ARFX3840S5xnNTRI	SSD	3.84TB	100K	No	Yes	Yes	Yes	3P00
ARFX7680S5xnNTRI	SSD	7.68TB	100K	No	No	Yes	Yes	3P00
ARFX15T4S5xnNTRI	SSD	15.3TB	100K	No	No	Yes	Yes	3P00

Symptoms: Internal log collection does not occur for ARFX drive models.

Conditions of occurrence: ARFX drive models are installed.

Impact: High

Customer circumvention: None.

Customer recovery steps: None.

Issue ID: 234631, 245130

Issue summary: Adds support of Automatic Drive Log Collection (ADLC) for the ARFX physical disk drive series.

Platforms affected: All StoreServ

Affected software versions: 3.2.2, 3.3.1 GA - MU2

Issue description: Adds support of Automatic Drive Log Collection (ADLC) for the ARFX physical disk drive series. The following drive table shows the affected drives.

Drive	Category	Capacity	Speed	StoreServ 10000	StoreServ 7000	StoreServ 20000	StoreServ 8000	FW
ARFX0920S5x nNTRI	SSD	920GB	150K	No	Yes	Yes	Yes	3P00
ARFX1920S5x nNTRI	SSD	1.92TB	100K	Yes	Yes	Yes	Yes	3P00
ARFX3840S5x nNTRI	SSD	3.84TB	100K	No	Yes	Yes	Yes	3P00
ARFX7680S5x nNTRI	SSD	7.68TB	100K	No	No	Yes	Yes	3P00
ARFX15T4S5x nNTRI	SSD	15.3TB	100K	No	No	Yes	Yes	3P00

Symptoms: Drive log collection does not occur for ARFX drive models.

Conditions of occurrence: ARFX drive models are installed, but ADLC does not occur.

Impact: High

Customer circumvention: None.

Customer recovery steps: None.

Issue ID: 205028, 244217

Issue summary: HPE support cannot automatically collect **InSplore** data following a System Manager restart.

Platforms affected: All StoreServ

Affected software versions: 3.3.1 GA - MU2

Issue description: If System Manager restarts during **controlinsplore** execution, a new **controlinsplore** cannot be started until the previous operation releases the **controlinsplore** lock. This may take up to ten minutes.

Symptoms: Collection of **InSplore** does not start when a previous instance of an **InSplore** has not completed successfully.

Task detailed status shows `A controlinsplore task is already running.`

Conditions of occurrence: An **InSplore** collection process does not complete successfully due to a System Manager restart, and another **InSplore** process is initiated.

Impact: Medium

Customer circumvention: Do not restart System Manager when **controlinsplore** execution is in progress.

Customer recovery steps: Wait for the previous **InSplore** operation to release the **controlinsplore** lock.

Issue ID: 257937, 242378, 244543

Issue summary: Data Inconsistencies may be seen during volume migration of non-ALUA hosts if proper migration procedure is not followed.

Platforms affected: All StoreServ

Affected software versions: 3.3.1 MU1 - MU3

Issue description: When migrating volumes that are exported to non-ALUA hosts, if unzoning the source array as required by the proper migration procedure is not followed, then Data Inconsistencies may be seen on the volumes being migrated. Note that failure to perform the unzoning operation is not a supported procedure. The migration tools clearly prompt with the message to perform unzone operation, perform the same before proceeding with the subsequent migration steps.

Symptoms: The hosts or the applications at the hosts may not function as expected due to Data Inconsistency on the volumes.

Conditions of occurrence: Non-ALUA hosts are migrated and the proper procedure of unzone operation is not followed.

Impact: Medium

Customer circumvention: Follow the proper migration procedure by following the prompts from migration tools for the unzone operation when migrating non-ALUA hosts.

Customer recovery steps: None.

Issue ID: 257778, 228811, 243914

Issue summary: An unexpected controller node restart occurs under specific workloads (combined with **`updatevv`** operations) on a thinly deduplicated virtual volume (TDVV), when a cache page ends up being shared by both the base and snap VV, but the dedup is initiated for the snapshot.

Platforms affected: All StoreServ

Affected software versions: 3.3.1 GA - MU2

Issue description: When a previously written data pattern is written for the second time, the deduplication store (DDS) triggers a conversion request to the original data block to convert its exception entry from the deduplication client (DDC) to DDS. In specific workloads (combined with **`updatevv`** operations), the original DDC entry belongs to a snapshot but the cache page belonging to this DDC block is shared with the base VV. In this condition the dedupe handler wrongly processes the base VV and updates the base VV's counters causing the panic.

Symptoms: An unexpected controller node restart occurs while running dedup on snapshots.

Conditions of occurrence: VVs with dedup data where snapshots are present and **`updatevv`** operations happen. This happens in some very peculiar (and infrequent) I/O workloads.

Impact: High

Customer circumvention: Stop **`updatevv`** operations.

Customer recovery steps: None.

Issue ID: 257759, 200337, 244954

Issue summary: Insufficient free space causes dedup conversion to not complete successfully.

Platforms affected: All StoreServ

Affected software versions: 3.3.1 GA - MU2

Issue description: Insufficient free space causes dedup conversion to not complete successfully.

Symptoms: **`tunevv`** conversion tasks do not complete successfully, and consume double the amount of space.

Conditions of occurrence: Running TDVV conversion with insufficient free space in the system.

Impact: High

Customer circumvention: Check required space before starting conversion.

Customer recovery steps: Roll back the **`tunevv`** conversion task that did not complete successfully.

Issue ID: 257931, 257658, 232936, 238410, 244941, 244949

Issue summary: A shortage of XOR engine resources may cause an unexpected array restart when compression is in use.

Platforms affected: StoreServ 8000, StoreServ 9000, StoreServ 10000, StoreServ 20000, StoreServ 20000 R2

Affected software versions: 3.3.1 GA - MU2

Issue description: If XOR operations request more resources than are available to the hardware, a temporary memory page is allocated. Depending on the location of that memory page, it could lead to an unexpected array restart. This occurs on arrays running with compression volumes.

Symptoms: Host I/O operations stall, eventually causing timeouts.

Conditions of occurrence: Using compression and large set sizes in RAID sets.

Impact: High

Customer circumvention: Use set sizes less than 9 and/or disable compression.

Customer recovery steps: None.

Issue ID: 255650, 239621, 244596

Issue summary: iSCSI target ports wrongly set a field which can lead to I/O stalls.

Platforms affected: All StoreServ

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

Issue description: Under high CPU load, iSCSI target ports might return an incorrect value to the initiator iSCSI protocol data unit (PDU) causing I/O stalls.

Symptoms: Host I/O stalls and/or LUN disconnects.

Conditions of occurrence: High controller node CPU utilization.

Impact: Medium

Customer circumvention: None.

Customer recovery steps: None.

Issue ID: 249429, 236682

Issue summary: **`startrcopygroup`** issued from the primary reverse role side of a Remote Copy group can take up to three minutes before it stops responding.

Platforms affected: All StoreServ

Affected software versions: 3.3.1GA - MU2

Issue description: After remote copy group failover, **`startrcopygroup`** from pri-rev side can take up to three minutes and does not succeed.

Symptoms: **`startrcopygroup`** does not complete successfully when attempted from the primary reverse role array.

Conditions of occurrence: The primary is running HPE 3PAR OS 3.2.2, and the secondary is running HPE 3PAR OS 3.3.1.

Impact: Medium

Customer circumvention: None.

Customer recovery steps: None.

Issue ID: 257406, 252739, 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 cluster.

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 -l <port number>`** command, and reboot the controller node.

Issue ID: 258319, 258320, 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 controller node restarts unexpectedly.

Conditions of occurrence: Presence of compression volumes.

Impact: Medium

Customer circumvention: None.

Customer recovery steps: None.

Issue ID: 257435, 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: 258127, 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: 3.2.2 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: 247949, 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: 257776, 224669, 247016, 247017

Issue summary: Control cache memory fragmentation leads to an unexpected controller node restart.

Affected platforms: All StoreServ

Affected software versions: 3.2.2, 3.3.1 GA - MU3

Issue description: Controller nodes may unexpectedly restart due to memory fragmentation even when unallocated memory is available.

Symptoms: Controller nodes restart abruptly.

Conditions of occurrence: Memory is highly fragmented.

Impact: Medium

Customer circumvention: None.

Customer recovery steps: None.

Issue ID: 257777, 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 Adaptive Optimization (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: 257761, 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/or online copy activities.

Customer recovery steps: None.

Issue ID: 257941, 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: I/O from a host may become blocked when the target volume or its first snapshot child state is not marked `normal`.

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: 247179, 243618, 247179, 247180

Issue summary: Array restarts can occur due to an inconsistent view of the 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: An unexpected array restart occurs.

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: 257797, 237034, 257796

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: 254138, 257741, 257742

Issue summary: The array unexpectedly restarts while processing an inter-node link error.

Platforms affected: All StoreServ

Affected software versions: 3.2.2, 3.3.1 GA - MU3

Issue description: The controller node is unable to participate in cluster validation when an inter-node link error occurs. This condition leads to an unexpected array restart.

Symptoms: Unexpected controller node restart.

Conditions of occurrence: Normal operation.

Impact: High

Customer circumvention: None.

Customer recovery steps: None.

Issue ID: 250237, 258323, 258324

Issue summary: Controller node restarts due to a race condition between two processes.

Platforms affected: All StoreServ

Affected software versions: 3.3.1 GA - MU2

Issue description: Unplanned controller node restarts occur upon race condition between two processes. These restarts occur in the presence of compressed deduplicated volumes with Read Only (RO) or Read Write (RW) snaps which have had the **updatevv** operation run on them.

Symptoms: Controller node unexpectedly restarts.

Conditions of occurrence: Presence of compressed deduplicated volumes with snapshots and **updatevv** operation performed on them anytime prior.

Impact: Medium

Customer circumvention: None.

Customer recovery steps: None.

Issue ID: 230407, 234150, 183091, 154837, 258051, 256806

Issue summary: The array restarts unexpectedly if Flash Cache simulation is enabled during an upgrade, or while the System Manager restarts.

Platforms affected: All StoreServ

Affected software versions: 3.3.1 MU1 - MU2

Issue description: If Flash Cache simulation is enabled either during upgrade, or if System Manager restarts, there is an unwanted increase in memory usage. This increase leads to array `Out of Memory` situation and eventually the array restarts.

Symptoms: Array physical memory (RAM) usage increases in an incremental fashion. Each time System Manager is restarted, or during an upgrade, approximately 800 MB of memory space is consumed, which is not reclaimed. After several restarts, the array reaches its full memory capacity and restarts.

Conditions of occurrence: Flash Cache simulation is enabled. Either System Manager restarts, or an upgrade is performed.

Impact: High

Customer circumvention: Disable Flash Cache simulation before performing an upgrade.

Customer recovery steps: None.

Issue ID: 259070, 226214, 250186, 250189, 227826, 225250, 239105

Issue summary: Slow management response times during `InSplore` collection.

Platforms affected: All StoreServ

Affected software versions: 3.3.1 GA - MU2

Issue description: In version 3.3.1, with Service Processor (SP) version 5.x.x, `InSplore` data is collected internally to the array before being copied off by the SP. The data gathering process can be time consuming and affect other array processes.

Symptoms: Slow management response times during `InSplore` collection.

Conditions of occurrence: `InSplore` collection is being done during heavy usage times.

Impact: Low

Customer circumvention: Avoid `InSplore` collection during heavy array usage times.

Customer recovery steps: None.

Issue ID: 243157, 243105, 257932, 257933

Issue summary: When all Remote Copy links are down, virtual volumes belonging to synchronous Remote Copy groups are temporarily put in an Asymmetric Logical Unit Access (ALUA) transition state.

Platforms affected: All StoreServ

Affected software versions: 3.2.2 MU2 - MU6, 3.3.1 MU1 - MU3

Issue description: When all Remote Copy links are down, virtual volumes (VVs) belonging to synchronous Remote Copy groups are temporarily put in an Asymmetric Logical Unit Access (ALUA) transition state. If System Manager restarts, the VVs may remain in a transition state, resulting in data becoming unavailable. VVs will no longer be in transition state.

Symptoms: Data becomes unavailable.

Conditions of occurrence: System Manager and controller node restart after all Remote Copy links are down and VVs belong to Remote Copy sync group are in transition state.

Impact: High

Customer circumvention: None.

Customer recovery steps: Check the VVs that are in transition state. **`showvlun`** will show them, if the exported host is online. Ensure that the affected groups are not in failed-over/failsafe state. For each VV/VLUN that is stuck at ALUA transition state which is part of Remote Copy group, run the **`setvv -setalua 0 <vv_name>`** command.

Issue ID: 234624, 243677, 257934, 257935

Issue summary: During Peer Persistence target failure check, a transient Quorum Witness communication error is received. This error results in failsafe action causing data to become unavailable.

Platforms affected: All StoreServ

Affected software versions: 3.2.2 GA - MU6, 3.3.1 GA - MU4

Issue description: In a system configured with Peer persistence, a target failure check transient Quorum Witness communication error is received. This condition results in failsafe action, causing data to become unavailable.

Symptoms: Virtual volumes affected by failsafe experience data unavailability.

Conditions of occurrence: The array is configured with peer persistence and Quorum Witness.

Impact: High

Customer circumvention: None.

Customer recovery steps: Use the override option to bring volumes out of failsafe state.

Issue ID: 245261, 258483, 258484

Issue summary: Communication with External Key Management servers (EKMs) does not work correctly if more than two EKMs are defined.

Platforms affected: All StoreServ

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

Issue description: When more than two External Key Management servers are defined, the array will only successfully communicate with the first configured EKM. This situation will result in the array being unable to retrieve a key when the primary EKM is unreachable, and rekey operations will not successfully complete.

Symptoms: Encryption keys will not be retrieved if the more than two EKMs are defined and the primary EKM is unreachable.

Encryption rekey operations will not successfully complete if more than two EKMs are defined.

Conditions of occurrence: More than two EKMs are defined.

Impact: High

Customer circumvention: Reduce the number of configured EKMs to two.

Customer recovery steps: Restore connection to primary EKM or contact support to provide a backup file with different EKMs defined.

Issue ID: 250806, 237618, 258025, 258026

Issue summary: Accessing stale metadata causes the controller node to restart.

Platforms affected: All StoreServ

Affected software versions: 3.3.1 GA - MU2

Issue description: Accessing stale metadata creates a race condition between two different I/O requests. This condition leads to a controller node restarting.

Symptoms: Controller node restarts.

Conditions of occurrence: Normal operation.

Impact: Medium

Customer circumvention: None.

Customer recovery steps: None.

Issue ID: 253308, 236286, 257945,257946

Issue summary: Input/output commands time out due to collision of the SCSI **GET_VVMAP** command and creation of the snapshot.

Platforms affected: All StoreServ

Affected software versions: 3.2.2, 3.3.1 GA - MU3

Issue description: A Recovery Manager incremental backup job hangs due to inter-node deadlock when a **GET_VVMAP** command interrupts before snapshots have been fully defined.

Symptoms: Input/output commands time out. The array becomes unresponsive to commands, and hosts can experience data unavailability.

Conditions of occurrence: Reading the allocation map of the virtual volume while running the **GET_VVMAP** command.

Impact: High

Customer circumvention: None.

Customer recovery steps: None.

Issue ID: 254203, 247571, 233388, 254202, 257633

Issue summary: A Fibre Channel Discover Address (**ADISC**) request does not respond, creates an unwanted callback invocation, and leads to an unexpected controller node restart.

Platforms affected: All StoreServ

Affected software versions: 3.2.2 MU4 - MU6, 3.3.1 GA - MU3

Issue description: Utility for orphaning Extended Link Services (ELS) request bypasses a `Dev Lost` scenario. This results in an unwanted callback invocation from a timed out **ADISC** request.

Symptoms: Single controller node restart.

Conditions of occurrence: 16G/32G Fibre Channel driver is being used.

Impact: Medium

Customer circumvention: None.

Customer recovery steps: None.

Issue ID: 255132, 255133, 248022, 247631

Issue summary: Duplicate session alerts cause unexpected controller node restarts.

Platforms affected: All StoreServ

Affected software versions: 3.2.2 MU6, 3.3.1 GA - MU3

Issue description: Duplicate logins from the iSCSI initiators cause duplicate session alerts. The event logging subsystem allocates memory for these alerts and eventually runs out of memory.

Symptoms: Controller node unexpectedly restarts.

Conditions of occurrence: Duplicate sessions from the initiators.

Impact: Medium

Customer circumvention: None.

Customer recovery steps: None.

Issue ID: 252554, 247254, 246894, 258525, 252553

Issue summary: **`setsys DisableCompr no`** cannot be used to enable compression after it has been disabled.

Platforms affected: StoreServ 8000, StoreServ 9000, StoreServ 20000

Affected software versions: 3.3.1 GA - MU3

Issue description: **`setsys DisableCompr no`** cannot be used to enable compression after it has been disabled without re-initializing the array.

Symptoms: Unable to turn on compression using **`setsys`**.

Conditions of occurrence: CLI command **`setsys DisableCompr yes`** has been issued

Impact: Medium

Customer circumvention: Do not disable compression with **`setsys DisableCompr yes`**.

Customer recovery steps: None.

Issue ID: 252572, 252564, 247853, 212271, 252571, 258088

Issue summary: Quorum Witness configured with an IPV6 address gets reset by System Manager if the network connection between the administrative controller node and the Quorum Witness is less than optimal.

Platforms affected: All StoreServ

Affected software versions: 3.3.1 GA - MU3

Issue description: When configured with IPV6 addresses, if the network latencies between the administrative controller node and the Quorum Witness are high, bursts of connection issues force System Manager to reset Quorum Witness. A quorum reset can be disruptive because it cannot be used to inform an automatic failover decision if the RC target happens to fail at the same time.

Symptoms: Bursts of Quorum Witness unreachable events.

Conditions of occurrence: Quorum Witness is configured with IPV6 addresses.

Impact: High

Customer circumvention: Avoid high latencies between array controller nodes and Quorum Witness.

Customer recovery steps: None.

Issue ID: 259594, 237143, 251700, 251701

Issue summary: Data becomes unavailable during controller node down recovery.

Affected platforms: All StoreServ

Affected software versions: All

Issue description: When one controller node is in controller node down recovery, one of the other controller nodes tries an interprocess communication (IPC) request and does not succeed. This causes all the controller nodes to unexpectedly restart resulting in data unavailability.

Symptoms: Data becomes unavailable during controller node down processing.

Conditions of occurrence: During a controller node down recovery, one of the other controller nodes retries an IPC request. A response is received before the send request is completed.

Impact: High

Customer circumvention: None.

Customer recovery steps: None.

Issue ID: 259637, 259636, 244667

Issue summary: Peer Motion Migrations for Windows Clusters may result in data becoming unavailable.

Platforms affected: All StoreServ

Affected software versions: 3.3.1 GA - MU3

Issue description: During Windows Cluster Peer Motion Migrations on 3.3.1, data may become unavailable when I/O from the Windows Cluster encounters a SCSI-3 reservation conflict from the source array.

Symptoms: Data unavailable.

Conditions of occurrence: Peer Motion Migration of Windows Cluster storage when array is running HPE 3PAR OS 3.3.1.

Impact: High

Customer circumvention: Perform Peer Motion during downtime for Windows Cluster.

Customer recovery steps: None.

Issue ID: 259592, 259591, 160853, 198379, 214647, 217390, 226158

Issue summary: A single controller node restarts.

Platforms affected: All StoreServ

Affected software versions: 3.2.2 MU1 - MU6, 3.3.1 GA - MU3

Issue description: Two threads working on the same cache memory page cause a single controller node to restart.

Symptoms: A single controller node restarts.

Conditions of occurrence: Normal operation.

Impact: Medium

Customer circumvention: None.

Customer recovery steps: None.

Affected components

Component	Version
CLI Server	3.3.1.522 (P58)
System Manager	3.3.1.522 (P58)
TPD Kernel Patch	3.3.1.522 (P58)
CIM Server	3.3.1.522 (P58)
WSAPI Server	3.3.1.522 (P58)
Event Manager	3.3.1.522 (P58)
Per-Node Server	3.3.1.522 (P58)

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 58 can be verified from an interactive CLI session. Issue the CLI command `showversion -a -b` to verify that Patch 58 is listed:

```
$ showversion -a -b
Release version 3.3.1.460 (MU3)
Patches:  P58

Component Name                  Version
CLI Server                      3.3.1.522 (P58)
CLI Client                      3.3.1.522
System Manager                  3.3.1.522 (P58)
Kernel                          3.3.1.460 (MU3)
TPD Kernel Code                 3.3.1.460 (MU3)
TPD Kernel Patch                3.3.1.522 (P58)
CIM Server                      3.3.1.522 (P58)
WSAPI Server                    3.3.1.522 (P58)
Console Menu                    3.3.1.460 (MU3)
Event Manager                   3.3.1.522 (P58)
Internal Test Tools             3.3.1.460 (MU3)
LD Check Tools                  3.3.1.460 (MU3)
Network Controller              3.3.1.460 (MU3)
Node Disk Scrubber              3.3.1.460 (MU3)
PD Scrubber                     3.3.1.460 (MU3)
Per-Node Server                 3.3.1.522 (P58)
Persistent Repository           3.3.1.460 (MU3)
Powerfail Tools                 3.3.1.460 (MU3)
Preserved Data Tools            3.3.1.460 (MU3)
Process Monitor                 3.3.1.460 (MU3)
Software Updater                3.3.1.460 (MU3)
TOC Server                      3.3.1.460 (MU3)
VV Check Tools                  3.3.1.460 (MU3)
Upgrade Check Scripts           181211.U018
File Persona                    1.5.2.8-20180817 (MU3)
SNMP Agent                      1.13.0
SSH                             7.5p1-5
VASA Provider                   3.0.18 (MU3)
Legacy FW Database              3.3.1.460 (MU3)
Legacy Drive FW                 3.3.1.460 (MU3)
Emulex Drive FW                 3.3.1.460 (MU3)
Legacy HGST Drive FW            3.3.1.460 (MU3)
Samsung FIPS Drive FW           3.3.1.460 (MU3)
Samsung nonFIPS FW              3.3.1.460 (MU3)
Seagate FIPS Drive FW           3.3.1.460 (MU3)
Seagate nonFIPS FW              3.3.1.460 (MU3)
WDC FIPS 10K Drive FW           3.3.1.460 (MU3)
WDC FIPS 15K Drive FW           3.3.1.460 (MU3)
WDC FIPS SSD FW                 3.3.1.460 (MU3)
WDC nonFIPS 10K FW              3.3.1.460 (MU3)
WDC nonFIPS 15K FW              3.3.1.460 (MU3)
WDC nonFIPS 7.2K FW             3.3.1.460 (MU3)
WDC nonFIPS SSD FW              3.3.1.460 (MU3)
UEFI BIOS                       05.04.04 (MU3)
MCU Firmware (OKI)              4.9.01 (MU3)
MCU Firmware (STM)              5.4.00 (MU3)
Cage Firmware (DC1)             4.44 (MU3)
Cage Firmware (DC2)             2.64 (MU3)
Cage Firmware (DC3)             08 (MU3)
```

```
Cage Firmware (DC4)              2.64 (MU3)
Cage Firmware (DCN1)             4082 (MU3)
Cage Firmware (DCN2)             4082 (MU3)
Cage Firmware (DCS1)             4082 (MU3)
Cage Firmware (DCS2)             4082 (MU3)
Cage Firmware (DCS5)             2.88 (MU3)
Cage Firmware (DCS6)             2.88 (MU3)
Cage Firmware (DCS7)             4082 (MU3)
Cage Firmware (DCS8)             4082 (MU3)
QLogic QLA4052C HBA Firmware     03.00.01.77 (MU3)
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   05.07.36
Emulex LP11002 HBA Firmware      02.82.x10
Emulex LPe12002 HBA Firmware     02.10.x08
Emulex LPe12004 HBA Firmware     02.10.x08
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         10.10.03
```

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.