Hewlett Packard Enterprise

HPE 3PAR OS 3.3.1 MU1 Patch 19 Release Notes

Abstract

This release notes document describes the HPE 3PAR OS 3.3.1 MU1 Patch 19. This patch must be applied to all systems running 3.3.1 MU1 when using or planning to use File Persona. Attempting to manage File Persona on 3.3.1 MU1 without this patch installed will lead to unexpected results.

Part Number: QL226-99749
Published: October 2017
Edition: 1

Notices

Acknowledgements

Purpose

This document describes the HPE 3PAR OS 3.3.1 MU1 Patch 19.

Caution

This patch **must** be applied to all systems running HPE 3PAR OS 3.3.1 MU1 when using or planning to use File Persona. Do not perform file services related tasks or administrative operations until this patch is installed.

Note

HPE 3PAR Deduplication and compression are resource intensive operations, and as loads increase to these volumes, File Persona volume performance can decrease significantly. The load applied to volumes with these services enabled may need to be controlled in order to manage the impact to other volumes, specifically volumes that are used by the File Persona feature set as part of a File Provisioning Group.

Prerequisites

- SP prerequisite: SP-5.0.2.0 + latest SP patch
- OS prerequisites: OS-3.3.1 MU1

Patch details

Patch ID:	P19
Synopsis:	Required patch to support File Persona version 1.4.2 with 3.3.1 MU1
Date:	October 09, 2017, 14:27:52 PDT
Description:	See the Release Notes for details about this patch
Affected Packages:	`tpd-fs, tpd-prerevert`
Obsoletes:	OS-3.3.1.269-P08
Requires:	OS-3.3.1.269-MU1
Build Version:	3.3.1.298
Supports Revert:	No
Patches Partially Superseded:	None
Patches Obsolete by Combination:	None
Notes:	Description of the incorporated patches: Patch ID: P08

Table Continued

Synopsis: Required patch to support File Persona version 1.4.1 with 3.3.1 MU1

Date: September 02, 2017, 10:53:21 PDT

Description: See the Release Notes for details about this patch

Affected Packages: `tpd-fs, tpd-prerevert`

Obsoletes: OS-3.3.1.269-P07

Requires: OS-3.3.1.269-MU1

Build Version: 3.3.1.280

Notes: Description of the incorporated patches:

Patch ID: P07

Synopsis: Required patch to support File Persona version 1.4 with 3.3.1 MU1

Date: August 11, 2017, 18:42:29 PDT

Description: FPv1.4 See the Release Notes for details about this patch

Affected Packages: `tpd-fs, tpd-prerevert`

Obsoletes: None

Requires: OS-3.3.1.269-MU1

Build Version: 3.3.1.270

Notes:

NOTE:

- Applying this patch to the 3PAR OS might restart the affected OS components. With these restarts, events and alerts might be generated and this is an expected behavior. The system continues to serve data, but existing CLI or SSMC sessions might be interrupted.
- Hewlett Packard Enterprise recommends installing patches in the same sequence as they are released, unless instructed otherwise.
- When displaying the `showversion` command output from the SP, the CLI Client version is fixed in the SP code and might differ from the output displayed from any other system.

Modifications

HPE 3PAR OS 3.3.1 MU1 Patch 19 addresses the following issues:

Issue ID: 72021
Issue summary: Corrects an issue where an alert indicating a temporary failure is received, while other CLI commands are failing repeatedly.
Affected platforms: StoreServ 7000c, 8000, 9000, 20000, 20000 R2
Affected software versions: All versions earlier than 3.3.1 MU1 P07
Issue description: If there is an issue with the operation of the node listed as `Active` by the `showfs` command, the other nodes may report one or more alerts indicating a temporary failure condition. Once the node listed as Active is healthy again, this issue will be automatically resolved.
Symptoms: Alert indicating a temporary failure is retrieved while other CLI commands are failing repeatedly.
Conditions of occurrence: The node listed as Active in the `showfs` command is in an abnormal state.
Impact: Medium
Customer circumvention: None
Customer recovery steps: Use the "`stopfs <node>`" command to stop the active node that is in an abnormal state and allow one of the other nodes to become Active.

Issue ID: 91629
Issue summary: Node for File Services restarts after upgrade to 3.2.2 MU3
Affected platforms: StoreServ 7000c, 8000, 9000, 20000, 20000 R2
Affected software versions: All versions earlier than 3.3.1 MU1 P07
Issue description: An application that sets and cancels Directory Change Notification many times for each file during open/read/write/close file access pattern can trigger inefficient memory usage by the file services SMB server. Over time this memory usage can cause the file services to restart, which migrates the FPGs to their alternate node.
Symptoms: After several weeks of running, the file services for a node restart, causing the FPGs to be migrated to their alternate node.
Conditions of occurrence: Custom SMB application that uses an unusual pattern of Directory Change Notifications (set/cancel/set/…) while doing high I/O loads.
Impact: High
Customer circumvention: None
Customer recovery steps: Cluster automatically fails the file systems over to HA node. Customer must migrate the FPGs back to the original node.

Issue IDs: 94268
Issue summary: Corrects an issue when snapshot operations fail and the snapshot component is not functional.
Affected platforms: StoreServ 7000c, 8000, 9000, 20000, 20000 R2
Affected software versions: All versions earlier than 3.3.1 MU1 P07
Issue description: The issue occurs when snapshot reclamation operations such as snapshot creation, deletion or listing are running. An error message or exception "`Cannot get actor reference. Actor system is down`" could be seen.
Symptoms: Snapshot operations failing with an internal exception stating "`Cannot get actor reference. Actor system is terminated`".
Conditions of occurrence: 1. The file snapshot functionality is sensitive to system load, and could produce unexpected results under heavy snapshot operations 2. File services for a node could become unresponsive when reclamation operations are running.
Impact: High
Customer circumvention: Avoid running reclamation operations during peak hours. When reclamation is running, avoid running other snapshot operations.
Customer recovery steps: Restart the File Persona file system services using the `stopfs` and `startfs` CLI commands.

Issue ID: 96032/99297
Issue summary: When using the Open Files functionality in Microsoft Management Console (MMC), "`Error 6: The handle is invalid`" is often returned.
Affected platforms: StoreServ 7000c, 8000, 9000, 20000, 20000 R2
Affected software versions: All versions earlier than 3.3.1 MU1 P07
Issue description: Customers monitoring open file count with MMC will not receive "`Error 6`" on shares with frequent open/close/delete operations.
Symptoms: In-accurate open file count and "`Error 6: The handle is invalid`"
Conditions of occurrence: Attempting to use the "`Open Files`" functionality of the 'Shared Folders' plugin in MMC. Due to the active nature of their file system, file handles are closed in the time period between when the MMC client asks our server for the file list and when that list is returned. If this occurs "Error 6: The handle is invalid" is returned to the MMC an no file list is displayed.
Impact: High

Table Continued

Customer circumvention: Reduce the frequency of create/delete cycles on MMC monitored shares.
Customer recovery steps: Reducing the frequency of MMC polling, or reducing the open/close/delete frequency are the only actions (without the patched code) to avoid the "Error 6" issue.

Issue ID: 97041
Issue summary: A failover request can be unsuccessful when an SMB connection request comes in after a failover request has been made and SMB is still closing existing connections.
Affected platforms: StoreServ 7000c, 8000, 9000, 20000, 20000 R2
Affected software versions: All versions earlier than 3.3.1 MU1 P07
Issue description: Request for a manual failover is unsuccessful.
Symptoms: Requested file system failover is unsuccessful, and file system remains presented for original node.
Conditions of occurrence: SMB clients requesting new connections after a failover request was made, but not yet completed.
Impact: Medium
Customer circumvention: Do not allow new connections to the SMB server while failover is in progress.
Customer recovery steps: Retry of the failover after the initial failover will succeed unless new clients continue to try to make new connections.

Issue ID: 97354
Issue summary: Under some rare conditions, when a directory has a large number of sub-directories or files, `create` or `rename` operations in that directory may result in the disappearance of some files.
Affected platforms: StoreServ 7000c, 8000, 9000, 20000, 20000 R2
Affected software versions: All versions earlier than 3.3.1 MU1 P07
Issue description: Using `create` or `rename` operations on directories whose index was removed can cause some files in that directory to no longer be visible.
Symptoms: Some files in the affected directory will not be visible.
Conditions of occurrence: • When offline FSCK is run on an FPG and when FSCK ends up detaching the directory index when correcting the directory entry in one of the directory pages where the directory has more than one 8K page. • When a Snapshot Purge operation directory index is closed prematurely.

Table Continued

Impact: High

Customer circumvention: Perform one of the following actions:

- Upgrade to 3.2.2 MU4 with P85.
- Upgrade to 3.3.1 MU1 with P19.

Customer recovery steps:

1. Upgrade to one of the releases mentioned above.
2. Have Support run FSCK.

Issue ID: 97551

Issue summary: Offline FSCK reconnected lost+found directory names could not be renamed if the FPG had taken a snapshot.

Affected platforms: StoreServ 7000c, 8000, 9000, 20000, 20000 R2

Affected software versions: All versions earlier than 3.3.1 MU1 P07

Issue description: Each snapshot is associated with an epoch. Each file which is visible in a snapshot has an epoch range. Using the epoch range, the system is able to determine which file belongs to which snapshot, along with the changes that exist in that file which are different in different snapshots. When these files were lost FSCK brought them back as LOST + FOUND entries, but it did not update their epochs (different for each snapshot taken). This made them visible across all snapshots, causing the file rename operation to not succeed.

Symptoms: Rename operation does not complete on lost+found files.

Conditions of occurrence: When directory entries become inconsistent, FSCK tries to bring them back with the help of disk data as lost and found entries in the same folder where they were originally previous to the inconsistency. If they cannot be linked to their parent directory, they are placed in the Lost+Found folder in the root directory .

In the case of snapshots, directory entries with the same name can be part of different snapshots based on their birth and death epochs. If the directory entries have the same epoch, then all files will be visible to all snapshots, and the effect of different directory entries visible to different snapshots will no longer be possible. Hence renaming will not succeed.

Impact: Medium

Customer circumvention: N/A

Customer recovery steps: If the epochs have already been updated and lost+found files have been generated, the latest changes will not be able to bring back the correct epochs for the lost files/dentries. Otherwise with new changes, the lost files should be recovered with correct epochs.

Issue ID: 97565
Issue summary: Correct an issue where NFS Share is inaccessible after failover/ failback.
Affected platforms: StoreServ 7000c, 8000, 9000, 20000, 20000 R2
Affected software versions: All versions earlier than 3.3.1 MU1 P07
Issue description: The issue occurs after upgrade to 3.2.2 MU4 P51, during failover File Persona node has been powered off. After this operation, NFS Shares are not accessible. This causes /etc/export entry for the NFS shares to vanish. This issue occurs when the NFS Share path has been removed without removing the share. NFS Manageability component stops re-exporting NFS shares if it encounters any issue during the re-export of NFS Shares.
Symptoms: Inaccessible NFS share after failover/ failback operation.
Conditions of occurrence: Upgrade to version 3.2.2 MU4 P51 followed by Failover/Failback causes an NFS Share access issue. If any of the NFS share directory is deleted without removing the NFS share, re-export of NFS shares fails for that NFS share and it will not proceed to add other NFS shares. Due to this, not all NFS shares may be exported.
Impact: Medium
Customer circumvention: Do not remove any directory exported over NFS without removing the NFS Share.
Customer recovery steps: Recreate the removed directory and failover and failback fpg. A fix has been provided in NFS manageability component to continue processing other NFS export entries by skipping exports with non-existing directories.

Issue ID: 97762
Issue summary: Windows 10 client backup to a File Persona SMB share does not complete and returns the message "The sector size of the physical disk on which the virtual disk resides is not supported."
Affected platforms: StoreServ 7000c, 8000, 9000, 20000, 20000 R2
Affected software versions: All versions earlier than 3.3.1 MU1 P07

Issue description: The Windows 10 version of Windows backup utility displays the following message:
`Cannot create a file when that file already exists.`
`Details: The sector size of the physical disk on which the virtual disk resides is not supported.`

Symptoms: • Windows 10 backup to File Persona SMB share is unsuccessful. • Mount of ISO by Windows 10 from a File Persona SMB share is unsuccessful.

Table Continued

Conditions of occurrence: Using Windows 10 client to backup to a File Persona Share, or mount and ISO file from a File Persona share.
Impact: High
Customer circumvention: Using Windows client version earlier than Windows 10 works successfully.
Customer recovery steps: None

Issue ID: 98767
Issue summary: Delete operation is unsuccessful and no error is returned when the directory in question contains an Alternate Data Stream (ADS).
Affected platforms: StoreServ 7000c, 8000, 9000, 20000, 20000 R2
Affected software versions: All versions earlier than 3.3.1 MU1 P07
Issue description: Customer cannot remove a directory that appears to be empty after renaming a file to which an Alternate Data Stream was attached.
Symptoms: Deletion of a directory is unsuccessful without an error message.
Conditions of occurrence: When you rename a file that has an Alternate Data Stream to an existing file name which also has an Alternate Data Stream, delete the target file and its associated ADS, then attempt to remove the empty directory.
Impact: Medium
Customer circumvention: Before renaming a file, verify that the destination file name does not already exist.
Customer recovery steps: None

Issue ID: 98778
Issue summary: In certain rare case scenarios, where case-insensitive lookups for files are involved over a CIFS client, a file services failover can be observed. It leads to data unavailability for the period of failover. This situation can be caused by multiple file operations such as `stat`, `create`, and so on, in parallel on the client under a heavy load.
Affected platforms: StoreServ 7000c, 8000, 9000, 20000, 20000 R2
Affected software versions: All versions earlier than 3.3.1 MU1 P07
Issue description: This issue is observed when in-memory inconsistency in the dentry cache triggered by parallel modifications of the entry cache results in accessing illegal memory addresses. This leads to a file services failover.
Symptoms: FPGs in a degraded state due to being activated on their backup node and an alert indicating a failure of file services on the primary node for the FPGs.

Table Continued

Conditions of occurrence:

1. When files accessed over CIFS client trigger case-insensitive lookups in the file persona file services software.
2. Multiple parallel operations on the same FPG to create/delete/modify directory entries.
3. FPG node under heavy load triggers shrinking of the entry cache.

Impact: High

Customer circumvention: The issue can be avoided if the file names are unique irrespective of the letter case.

Customer recovery steps: None. This issue leads to temporary unavailability of file services data only for the duration of file services failover. The file services failover is automatic and does not need customer intervention.

Issue ID: 99998

Issue summary: Archive-bit on File Persona SMB-share not set when Microsoft Word modifies a file.

Affected platforms: StoreServ 7000c, 8000, 9000, 20000, 20000 R2

Affected software versions: All versions earlier than 3.3.1 MU1 P07

Issue description: After creating a file with Microsoft Word, the file does not have the archive bit set.

Symptoms: Backup utilities that rely on the archive bit, like Windows Backup Utility, will not back up files that were created by Microsoft Word or similarly behaving applications.

Conditions of occurrence: The DOS archive bit is not set on a files created by any application, like Microsoft Word, that keeps a temporary copy of a file while it is being modified, and then renames the file to the final name when the file is saved.

Impact: Medium

Customer circumvention: None

Customer recovery steps: Set the archive bit manually using the Powershell command line.

Issue ID: 100166

Issue summary: SMB service self-restart causes momentary interruption in SMB share access.

Affected platforms: StoreServ 7000c, 8000, 9000, 20000, 20000 R2

Affected software versions: All versions earlier than 3.3.1 MU1 P07

Issue description: When the SMB service restarts, access to the SMB share is interrupted for less than a minute while the service comes backup.

Table Continued

Symptoms:

- New share mapping cannot complete.
- I/O on existing mapped shares cannot complete

Conditions of occurrence: System under high authentication loads can, in rare circumstances, encounter this issue.

Impact: Medium

Customer circumvention: None

Customer recovery steps: None. System self-heals.

Issue ID: 101057

Issue summary: When SMB shares are created under fstore level on File Persona, the permissions (ACLS) inherited should be converted to explicit to match Windows Server behavior. As the default ACL at the root of a share is server specific, and in File Persona it has inherited ACES (from the parent), the user should be cautious when modifying ACLs at the root of the share from a Windows Client.

Affected platforms: StoreServ 7000c, 8000, 9000, 20000, 20000 R2

Affected software versions: All versions earlier than 3.3.1 MU1 P07

Issue description: A warning pop-up message is showing regarding inherited permissions when modifying permissions on an existing directory or file that is a child object of a directory that was shared after being populated with files and directories.

Symptoms: Warning pop-up message regarding inherited permissions when modifying permissions on an existing directory or file.

Conditions of occurrence: Depending on the Windows version and the default Windows configuration, when using some Windows tools to modify the ACL at the root of the share, the Windows client might also request the server to modify/delete some of the inherited ACES on the share folder and its children (if children exist). PLEASE NOTE that this behavior is different from a Windows Server, where the ACL at the root of a share does not have inherited ACES.

Impact: Low

Table Continued

Customer circumvention: None

Customer recovery steps:

Different windows versions and Windows Explorer GUI versions will display pop-ups with warnings and/or options to avoid this by converting the inherited ACES on the folder to explicit ACES. For example, in Windows 2008R2, to allow permissions to be added to a File Persona SMB share folder from Windows without losing the existing permissions perform the following workaround:

1. Right-click the share folder.
2. Select **Properties > Advanced > Disable Inheritance > Convert inherited permissions into explicit permissions on this object**.
3. Click **OK**.
4. Add the user(s) or group (s) in the security tab.

An alternative is to use the File Persona 3PAR CLI:

```
setfshare smb - acl + | <permlist>
```

The specified ACES in `<permlist>` will be pre-pended to the other existing ACES in the share folder for ACL without affection the attributes of the other ACE and without affecting the ACLS of the children directories.

```
setfshare smb -acl <permlist>
```

The specified ACL will be applied (replacing the existing ACL) to the share folder, but any existing children directories will keep their existing ACL. Child directories created after the share folder ACL is modified will inherit from the new share folder ACL.

Issue ID: 102753

Issue summary: When using SSMC to update the File Persona configuration, the task fails even though the configuration was changed successfully.

Affected platforms: StoreServ 7000c, 8000, 9000, 20000, 20000 R2

Affected software versions: 3.3.1-MU1 P07

Table Continued

Issue description: Sometimes when SSMC is used to update the File Persona configuration, the task may unexpectedly fail even though the configuration change has processed successfully. The following areas may area affected:

- Active Directory
- LDAP
- Local Users & Groups
- User Mapping
- NFS v4 ID Mapping
- SMB Global Settings
- Antivirus Definitions
- FTP Global Settings
- NDMP

When the issue occurs, the task details may show something similar to the following:

```
Jul 19, 2017 6:39:30 AM MDT Checking for object to update in the cache
Jul 19, 2017 6:41:01 AM MDT Exception
Jul 19, 2017 6:41:01 AM MDT Failed: Failed
```

If this occurs, you should check the configuration using CLI, and if SSMC and CLI do not report the same information, restart the SSMC to synchronize the cache.

Symptoms: Configuration update task fails unexpectedly, even though the configuration has been changed (as seen via the CLI).

Conditions of occurrence: A configuration update is made using SSMC, where the event confirming the configuration change does not contain any variable parameters (like the name of an object).

Impact: Medium

Customer circumvention: Use the CLI to make these configuration changes and then restart SSMC, to get its cache synchronized.

Customer recovery steps: Restart SSMC to synchronize the cache

Issue ID: 102630

Issue summary: When making updates to the share folder ACLs in a sequence, File Persona manageability operations are temporarily unavailable.

Affected platforms: StoreServ 7000c, 8000, 9000, 20000, 20000 R2

Affected software versions: 3.3.1 MU1 P07

Table Continued

Issue description: When using the "`setfshare {smb|nfs|obj|ftp} -acl…`" command to update the ACLs for a share folder, if the command is issued many times in succession (for instance in a script), all manageability operations could become unavailable for a few minutes. The failing request may return an error message such as "`File Services server error: 401`". After the error occurs, the "`showfs`" command may show all nodes in a starting state for a period of time.

Symptoms: A command returns an error such as "`File Services server error: 401`" and the `showfs` command lists all the nodes as `starting`.

Conditions of occurrence: Frequent updates to share folder ACLs via CLI or SSMC.

Impact: Medium

Customer circumvention: Avoid making several share folder ACL updates with the means of a script in close succession.

Customer recovery steps: Wait for the `showfs` command to report all nodes as `running`, and then avoid making several share folder ACL updates with a script in close succession.

Issue ID: 105417

Issue summary: Duplicate files are being listed in the directory.

Affected platforms: StoreServ 7000c, 8000, 9000, 20000, 20000 R2

Affected software versions: 3.3.1-MU1 P07 and 3.3.1-MU1 P08

Issue description: Access to certain files is lost and deleting the directories containing those files is failing when the file/directory names contain multi-byte UTF-8 encoded characters. Additionally, two files with the exact same names are seen in some directories and access to those files is failing as well.

Symptoms: Loss of access to certain files or directories and duplicate file entries in a directory.

Conditions of occurrence: The two possible conditions the issue occurs are the following:

- If a file is created by an SMB client on a File Share exported under a File Store and the filename contains multi-byte UTF-8 encoded characters.
- If a file is created by an NFS client on a File Share exported under a File Store which has security mode set to NTFS and the filename contains multi-byte UTF-8 encoded characters.

Impact: High

Customer circumvention: None.

Customer recovery steps: Duplicate file names should be renamed to unique names.

Issue ID: 105472
Issue summary: Some space was not properly reclaimed during a snapshot reclamation operation after snapshots were deleted.
Affected platforms: StoreServ 7000c, 8000, 9000, 20000, 20000 R2
Affected software versions: 3.3.1-MU1 P07 and 3.3.1-MU1 P08
Issue description: Snapshot objects referred in the snapshot reclamation logs were never removed from the File Store and were non-reclaimable. This means that the space consumed by these directories was being leaked.
Symptoms: Used space for an FPG is higher than expected after running a snapshot reclamation operation.
Conditions of occurrence: If a directory was created and removed after a snapshot was taken on the File Store, that is, a directory was created after taking a snapshot and removed before taking a subsequent snapshot on the File Store, then the directory would remain in the File Store even after the snapshot has been deleted and snapshot reclamation has been run on the FPG.
Impact: Low
Customer circumvention: None.
Customer recovery steps: Contact support for assistance.

Affected components

Component	Version
File Persona	1.4.2.40-20171006 (P19)

Verification

The installation of P19 can be verified from an interactive CLI session. Issue the CLI command `showversion -a -b` to verify that P19 is listed:

```
cli% showversion -a -b
Release version 3.3.1.269 (MU1)
Patches:  P11,P14,P19

Component Name                    Version
CLI Server                        3.3.1.269 (MU1)
CLI Client                        3.3.1.269
System Manager                    3.3.1.288 (P14)
Kernel                            3.3.1.269 (MU1)
TPD Kernel Code                   3.3.1.269 (MU1)
TPD Kernel Patch                  3.3.1.288 (P14)
CIM Server                        3.3.1.269 (MU1)
WSAPI Server                      3.3.1.269 (MU1)
Console Menu                      3.3.1.269 (MU1)
Event Manager                     3.3.1.269 (MU1)
Internal Test Tools               3.3.1.269 (MU1)
LD Check Tools                    3.3.1.269 (MU1)
Network Controller                3.3.1.269 (MU1)
Node Disk Scrubber                3.3.1.269 (MU1)
PD Scrubber                       3.3.1.269 (MU1)
Per-Node Server                   3.3.1.269 (MU1)
Persistent Repository             3.3.1.269 (MU1)
Powerfail Tools                   3.3.1.269 (MU1)
Preserved Data Tools              3.3.1.269 (MU1)
Process Monitor                   3.3.1.269 (MU1)
Software Updater                  3.3.1.269 (MU1)
TOC Server                        3.3.1.269 (MU1)
VV Check Tools                    3.3.1.269 (MU1)
Upgrade Check Scripts             170825.U009
File Persona                      1.4.2.40-20171006 (P19)
SNMP Agent                        1.10.0
SSH                               6.0p1-4+deb7u5
VASA Provider                     3.0.14 (MU1)
Firmware Database                 3.3.1.269 (MU1)
Drive Firmware                    3.3.1.269 (MU1)
UEFI BIOS                         05.02.54 (MU1)
MCU Firmware (OKI)                4.8.60 (MU1)
MCU Firmware (STM)                5.3.17 (MU1)
Cage Firmware (DC1)               4.44 (MU1)
Cage Firmware (DC2)               2.64 (MU1)
Cage Firmware (DC3)               08 (MU1)
Cage Firmware (DC4)               2.64 (MU1)
Cage Firmware (DCN1)              4082 (MU1)
Cage Firmware (DCN2)              4082 (MU1)
Cage Firmware (DCS1)              4082 (MU1)
Cage Firmware (DCS2)              4082 (MU1)
Cage Firmware (DCS5)              2.79 (MU1)
Cage Firmware (DCS6)              2.79 (MU1)
Cage Firmware (DCS7)              4082 (MU1)
Cage Firmware (DCS8)              4082 (MU1)
QLogic QLA4052C HBA Firmware      03.00.01.77 (MU1)
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     11.1.220.9
Emulex LPe16004 HBA Firmware     11.1.220.9
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
```

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**.

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:

  http://www.hpe.com/assistance

- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:

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

Information to collect

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

Accessing updates

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

  Hewlett Packard Enterprise Support Center

  www.hpe.com/support/hpesc

  Hewlett Packard Enterprise Support Center: Software downloads

  www.hpe.com/support/downloads

  Software Depot

  www.hpe.com/support/softwaredepot

- To subscribe to eNewsletters and alerts:

  www.hpe.com/support/e-updates

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

  www.hpe.com/support/AccessToSupportMaterials

IMPORTANT:

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

Customer self repair

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

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

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

Remote support

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

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

Remote support and Proactive Care information

HPE Get Connected

www.hpe.com/services/getconnected

HPE Proactive Care services

www.hpe.com/services/proactivecare

HPE Proactive Care service: Supported products list

www.hpe.com/services/proactivecaresupportedproducts

HPE Proactive Care advanced service: Supported products list

www.hpe.com/services/proactivecareadvancedsupportedproducts

Proactive Care customer information

Proactive Care central

www.hpe.com/services/proactivecarecentral

Proactive Care service activation

www.hpe.com/services/proactivecarecentralgetstarted

Warranty information

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

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

Additional warranty information

HPE ProLiant and x86 Servers and Options

www.hpe.com/support/ProLiantServers-Warranties

HPE Enterprise Servers

www.hpe.com/support/EnterpriseServers-Warranties

HPE Storage Products

www.hpe.com/support/Storage-Warranties

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.