IBM FlashSystem 840

Firmware Version 1.2.1.10

Release Notes

July 5, 2016

Contents

1.0 Applicable systems

This release is recommended for the following systems:
— IBM FlashSystem® 840, machine type 9840, model AE1
— IBM FlashSystem 840, machine type 9843, model AE1

2.0 Product resources

IBM FlashSystem 840 product information resources guide users through the various features and components of the storage system, including usage and troubleshooting guides. To read about this storage system and learn how to use or troubleshoot, see the IBM Knowledge Center for IBM FlashSystem 840 at www.ibm.com/support/knowledgecenter/ or visit the IBM Redbooks® website at www.redbooks.ibm.com for the *IBM FlashSystem 840 Product Guide*.

3.0 Bug severity legend

The following explains the bug severity ranking used in Section 4.2 for key fixes, as well as Section 7.0 for the release history:

S1: Highest   Recommend upgrade for all users as soon as possible.
S2: Medium   Recommend upgrade for all users at the next scheduled maintenance window.
S3: Average   Recommend upgrade at the next scheduled maintenance window for users experiencing these issues. All other users may wish to upgrade at the next scheduled maintenance window.
S4: Low   Upgrade at the next scheduled maintenance window. May be performed at the discretion of the user if the issue is having a negative impact.
S5: Lowest   Upgrade is not necessary. This would include a mostly cosmetic or minor annoyance fix.

4.0 Latest changes

This release is a Program Temporary Fix (PTF) including recommended fixes for 1.2 releases. The fixes provide improved FlashSystem reliability.

After initial configuration of the hardware is complete, IBM strongly recommends that you make sure that your IBM FlashSystem firmware is up-to-date. Visit IBM Fix Central using the link below to see if any updates are available for your system.

http://www.ibm.com/support/fixcentral

4.1 Release features

The following are features of all 1.2 releases and are therefore included in the current release:
- Error isolation and detection logic throughout data path to enhance component failure identification.
- Integrity is ensured with the addition of a background continuous array sweeper.
- The ability to correct certain single drive errors from system level RAID which serves to reduce the need for flashcard replacement.
- Background trim functions to reclaim unused space.
- Support for SCSI UNMAP.
- Support for the VMware vSphere Storage APIs – Array Integration (VAAI) UNMAP action.
- The first 1MB of VDisk space is deleted upon creation to remove any old file system information.
- Support for VMware vSphere API for Storage Awareness (VASA).
- Support for a RESTful API.
- Rear system view of components is available through the management GUI.

- The multi-system monitoring tool called Neighborhood is available for use through the GUI.

4.2 Issues fixed

The following is a fix included in this release and the severity level for that fix. Use this severity level as described in Section 3.0 to aid in your decision to upgrade.

S1

FLASH-18068 - Internal error handling causes loss of access.
FLASH-18135 - PSoC issue leads to both nodes in service state.
FLASH-18133 - Issues result when the same call home manager processes run simultaneously.

S2

FLASH-18036 - Degraded components are still used in the thermal algorithm
FLASH-18063 - Fix interface error reporting.

S3

FLASH-15899 - A rare scenario finds sequential fail logic to be too aggressive.
FLASH-17843 - Error in verifying the signature of the update package.
FLASH-17932 - Inter-node communication issue causes CCU to stall.
FLASH-15958 - Internal error results when using the "-force" option to remove a VDisk via the CLI.

S4

FLASH-18149 - The CLI command "lsdumps -prefix" with an invalid directory causes a node failover.

S5

FLASH-16723 - Update system page reports the current software version is not supported.

4.3 Known issues

The following issues have not been addressed in this release:
- Currently, there is a known issue (FLASH-11468) fixed in version 1.3 where the GUI could show that a canister is offline when the CLI indicates the canister is online. This is a cosmetic issue which can be resolved by performing a node failover issuing the `satask startservice -force` command on the configuration node followed by `satask stopservice` to remove that node from service state. Contact IBM Support for any questions regarding this issue.
- Another known issue (FLASH-15983) exists for those upgrading from earlier 1.2 versions which may not be noticed. You may see an "Update process failed" event when the GUI upgrade status doesn't show "stalled," and the upgrade is still progressing. The event should be ignored and will automatically clear upon completion of the upgrade.

4.4 Currently supported specifications

SCSI-SAM-3   SCSI Architecture Model – v3
SCSI-SPC-3   SCSI Primary Commands – v3
SCSI-SBC-2   SCSI Block Commands – v2
SCSI-FCP-3   Fibre Channel Protocol – v3
SCSI-SRP   SCSI RDMA Protocol – v1
FC-PH-3   Fibre Channel Physical and Signaling Interface – v3
FC-AL-2   Fibre Channel Arbitrated Loop – v2
IBTA-1.2   InfiniBand Trade Association Architecture Specification – v1.2

Note: In order to test or demonstrate concurrent maintenance on canisters and batteries, use the following link to access the featured document, which describes the recommended process for concurrent maintenance: http://www.ibm.com/support/docview.wss?uid=ssg1S7005077

5.0 Upgrading firmware

Use the following sections to perform code upgrades for your systems to the current release.

Warning: Please read all the instructions below before upgrading.

5.1 Release overview

If you are upgrading to this release and your system is healthy, you can perform a Concurrent Code Load (CCL) upgrade. A CCL upgrade is a non-disruptive upgrade and is the preferred upgrade method. For general instructions on performing upgrades, refer to the FlashSystem Knowledge Center using the following URL: http://www.ibm.com/support/knowledgecenter/

From this link, you can access the appropriate FlashSystem page through the following path:

System Storage → Flash Storage → Flash high availability systems →IBM FlashSystem 840 → Upgrading

5.2 Supported upgrade paths

The following upgrade paths are supported for this release:

1.1.0.3   → 1.1.2.7   → 1.1.3.8 → 1.2.1.10
1.1.0.7   → 1.1.2.7   → 1.1.3.8 → 1.2.1.10
1.1.1.1   → 1.1.3.8   → 1.2.1.10
1.1.1.2   → 1.1.3.8   → 1.2.1.10
1.1.1.3   → 1.1.3.8   → 1.2.1.10
1.1.1.4   → 1.1.3.8   → 1.2.1.10
1.1.2.2   → 1.1.3.8   → 1.2.1.10
1.1.2.5   → 1.1.3.8   → 1.2.1.10
1.1.2.6   → 1.1.3.8   → 1.2.1.10
1.1.2.7   → 1.1.3.8   → 1.2.1.10
1.1.3.2   → 1.1.3.8   → 1.2.1.10
1.1.3.6   → 1.1.3.8   → 1.2.1.10
1.1.3.7   → 1.2.1.10
1.1.3.8   → 1.2.1.10
1.2.0.11   → 1.2.1.10
1.2.0.12   → 1.2.1.10
1.2.1.4   → 1.2.1.10
1.2.1.5   → 1.2.1.10
1.2.1.6   → 1.2.1.10
1.2.1.7   → 1.2.1.10
1.2.1.8   → 1.2.1.10
1.2.1.9   → 1.2.1.10

5.3 Preparing to upgrade

CCL is a non-disruptive upgrade, which means that the system remains online throughout the process and that you can continue to access data normally. As a precaution, it is recommended that the upgrade occur during a time of reduced traffic. During the upgrade, the interface adapters in each canister are taken offline temporarily in order to be upgraded. This might impact performance or throughput. The impact is more noticeable under heavy load conditions. With a properly configured multi-path configuration, access to your data is maintained at all times.

In order to ensure a successful, non-disruptive upgrade, you should verify that your interface ports are all online and all the system hardware is functioning normally. Ideally, you should have the following:

- All host interfaces should be online. An active multi-path configuration is required to ensure no loss of access during the upgrade.
- Both batteries should be online and charged at least 85%. Use the CLI command `lsenclosurebattery` or the management GUI under Monitoring → Systems to verify battery charge.
- If using encryption, ensure that both USB keys are inserted during CCL.
- All hardware should be online and functioning normally. There should be no unfixed alerts in the event log (see the exceptions below).

Important: Before you begin the upgrade, we recommend that you perform a backup of your data and a backup of the FlashSystem configuration. To back up the configuration, log into the cluster management IP address and issue the following command using admin-level authority:

```
svcconfig backup
```

Optionally, you can copy the configuration backup file from the FlashSystem to your workstation using secure copy (scp) on Linux or PuTTY secure copy (pscp.exe) on Windows as in the following examples:

(Using Linux)

```
scp superuser@cluster_ip:/dumps/svc.config.backup.* .
```

(Using Windows)

```
pscp -unsafe superuser@cluster_ip:/dumps/svc.config.backup.* .
```

Note: Do not ignore the periods shown above at the end of each command. In addition, replacement of italicized descriptions with appropriate information is required.

5.4 Performing the upgrade

It is highly recommended that the upgrade be performed using the web-based cluster management interface known as the management GUI. Access this option under the **Settings** tab in the GUI. Using the management GUI, you will be prompted to install and run the latest version of the software upgrade test utility, which is designed to detect and warn of various conditions that prevent a successful upgrade. Currently, the upgrade test utility is at version 1.8. For more detailed instructions and information on using the upgrade utility from the CLI or the GUI, visit the following website or see the upgrade utility release notes available on Fix Central:

http://www.ibm.com/support/docview.wss?uid=ssg1S4001181

The upgrade can proceed successfully without the Call Home feature enabled, but IBM highly recommends that the feature be enabled. The upgrade can also be performed using the `applysoftware` command using the CLI. This requires that you manually upload the latest release to the `/upgrade` directory on the cluster management node.

5.5 Array validation

Releases with firmware version 1.2.x.x include a constant array scrubber which scans the array attempting to detect errors and then subsequently correcting those errors. While this scan typically takes 7 days to complete one cycle, there is a faster scan available which completes array validation in 2-4 hours, significantly affecting system I/O performance. A faster array validation may be useful for users who have a maintenance window or SAN configuration which allows the significant performance impact.

To initiate this faster array validation, issue `recoverarray -validate` from the CLI. You can monitor the progress of array validation through the Event log by issuing `lseventlog` from the CLI or navigating to the GUI Event log via Monitoring → Events where messages appear indicating when the array validation has started and when it has finished, as shown in the figures below.

Error Code	Last Time Stamp	Status	Description	Object Type	
	7/28/15 10:34:53 AM	Message	Array validation started	mdisk	0

Figure 1. Viewing that the array validation has started in the GUI Event log

Check Log Off	Refresh	Actions	Show All	Filter		
Error Code	**Last Time Stamp**	**Status**	**Description**		**Object Type**	
	7/28/15 11:12:28 AM	Message	Array validation complete		mdisk	

Figure 2. Viewing that the array validation process has completed in the GUI Event log

Array validation percentage of completion can also be determined via the CLI by issuing `lsarray 0` and viewing the "scrub_progress" field's value. Once the array validation progress reaches 100%, this value goes back to 0 and the slow validation process continues automatically.

5.6 Troubleshooting

Use the following sections to troubleshoot problems that may occur during the upgrade process.

5.6.1 Stalled upgrade

If the upgrade takes more than two hours to complete, it may have stalled. Upgrade status is viewed by issuing `lsupdate` CLI command or by going to Settings → System → Update System in the GUI. Both show a "Stalled" status. In most cases, this can be resolved by aborting the upgrade and reattempting the upgrade after the system downgrades to its original level. To abort the upgrade, issue the `applysoftware -abort` CLI command or click the "Stop Upgrade" button in the GUI, as seen in Figure 1 below.
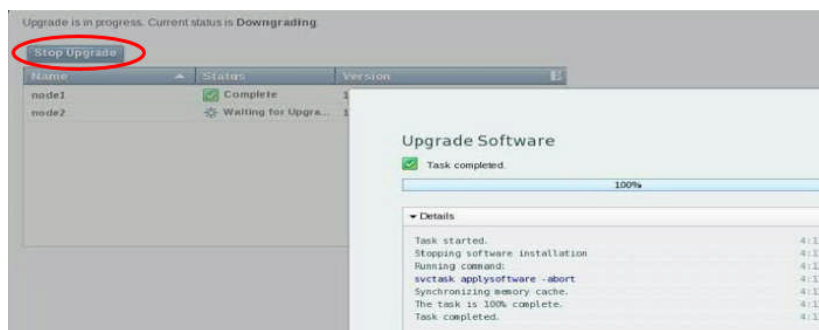
Figure 3. Aborting the upgrade

After the system is downgraded, you can reattempt your upgrade from the GUI or CLI. If the upgrade stalls repeatedly or if you have alerts which cannot be cleared, contact IBM Support. Support contact information is provided in Section 6.0 of this document.

5.6.2 Failures during upgrade

You may get a battery or quorum alert during upgrade due to required reconfiguration. These alerts should be automatically cleared when the upgrade is completed. They may be visible from the Events view of the management GUI if the filter is set to "Show All," but they should no longer appear in the Recommended Actions, Unfixed Messages, or Alerts views. If you see unfixed battery or quorum alerts after an upgrade is complete, contact IBM Support.

If the upgrade has failed or stopped due to a hardware failure, you will see the "Hardware Failed" status as presented in Figure 2 below.
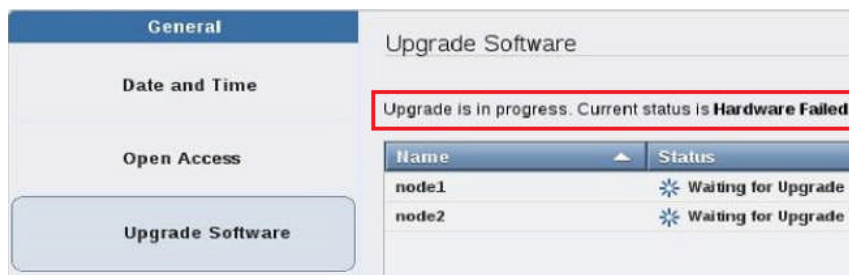

Figure 4. Viewing the upgrade status

If you suspect a hardware failure, issue the `lsupdate` command to confirm the state of your system. This command shows that the system is in a `hardware_failed` state and the event log contains a "System upgrade suspended" event. You may resume the upgrade by issuing the command `applysoftware -resume –force` for the following conditions:

- PSU unsupported events
- Battery fault type 1 events that are fixed and online according to the CLI command `lsenclosurebattery`
- Fan events

If the upgrade cannot be resumed or you have other alerts which cannot be cleared, contact IBM Support. The battery reconditioning feature calibrates the gauge that reports the amount of charge on the batteries. On systems that have been installed for 10 months or more or systems that have experienced several power outages, the recommendation to run "battery reconditioning" will appear in the event log shortly after upgrading. This is normal. Use the management GUI to run a DMP for this error or see the FlashSystem Knowledge Center to view how to properly issue the `chenclosureslot` command in reference to this issue. Use the following link to access the Knowledge Center page for battery reconditioning:

http://www.ibm.com/support/knowledgecenter/

6.0 Contact information

Call IBM at 1-800-IBM-SERV (1-800-426-7378). To find contact information for a specific region, visit the IBM directory of worldwide contacts at http://www.ibm.com/planetwide/.

7.0 Release history

The following sections include a list of all fixes and improvements for previous releases.

Release 1.2.1.9

The following issues were fixed in release 1.2.1.9:
FLASH-15935 - Add Pass 5 CPLD support. (S4)
FLASH-13429 - Remediate a vulnerability in nss-softokn (CVE-2015-2730).
FLASH-13794 - Remediate multiple vulnerabilities related to Apache Struts (CVE-2015-5209).
FLASH-14847- Remediate a vulnerability in PAM (CVE-2015-3238).
FLASH-14848 - Remediate a vulnerability in Java™ (CVE-2015-4842).
FLASH-15061 - Remediate NSS-related vulnerabilities (CVE-2015-7181, CVE-2015-7182, CVE-2015-7183).
FLASH-15836 - Remediate a vulnerability in OpenSSL (CVE-2015-3194).

Release 1.2.1.8

The following issues were fixed in release 1.2.1.8:
FLASH-13527, 13528 - Vulnerabilities in OpenSSL (CVE-2015-1788, CVE-2015-1789, CVE-2015-1791, and CVE-2015-3216).
FLASH-13000 - A vulnerability in SSL/TLS also known as "Bar Mitzvah Attack" (CVE-2015-2808).
FLASH-12502, 13526 - Vulnerabilities in Java™ CPU (CVE-2015-1931, CVE-2015-2601, CVE-2015-2613, and CVE-2015-2625).
FLASH-13706, 13075 - HIPER (highly pervasive): Potential undetected data corruption may occur due to a low probability race condition. The race condition has been observed on a system with a specific workload that is doing 1 to 2 GB/s of read operations with 250 MB/s of write operations. The write operations were less than 4K in size. (S1)
FLASH-10119, 13429 - HIPER: Potential undetected data corruption may occur from interface error. FlashSystem 840 and 900 products can write inconsistent data to a host. This is considered a highly pervasive problem involving firmware versions 1.1.x.x and 1.2.x.x. (S1)
FLASH-13075, 10534 - Improve WRITE SAME command usage in periods of heavy data Input/Output to prevent potential data issues. (S1)
FLASH-15207, 15208 - Repeated interface panics due to a bad interface cable can cause unnecessary component failures. (S2)
FLASH-14793, 15286 - A flashcard can become unresponsive when array certify is running while hardware errors are being found. (S2)
FLASH-12271, 12757 - The RAID controller was falsely marked as "failed" instead of a flashcard in a particular double flashcard failure scenario. (S2)
FLASH-15254 - Improve signal integrity between canisters. (S3)
FLASH-12758, 11567 - Latency spikes caused by encryption key validation. (S3)
FLASH-15315 - Telephone field length in the GUI does not match the length in other SVC products. (S5)

Release 1.2.1.7

The following issues were fixed in release 1.2.1.7:
FLASH-11718 - Security vulnerabilities in both Apache Struts (CVE-2015-1831) and Java™ (CVE-2015-0204, CVE-2015-0488, and CVE-2015-1916). (S1)
FLASH-11722 - Issue with multiple panics affecting 1.2.x.x firmware versions causing one canister to go into Service state. (S2)
FLASH-11657 - Array in rebuilding state may become offline instead of degraded on sequential fails for systems with 1.2.x.x firmware versions. (S2)

FLASH-11709 - Encryption enabled systems may result in a node assert upon upgrade. (S3)

FLASH-11659 - During the upgrade from firmware versions 1.1.x.x to 1.2.x.x, the system could incorrectly fail flash on a correctable error. (S3)

FLASH-11656 - For firmware versions 1.2.x.x, uninitialized variable can cause the stopsystem command to behave incorrectly in some scenarios. (S3)

FLASH-11658, FLASH-11897 - Rather than taking the system offline for uncorrectable errors, the system validation tool raises an event. (S3)

FLASH-11655, FLASH-11660 - Added recovery tools to assist in array recovery. (S5)

Release 1.2.1.6

The following issue was fixed in release 1.2.1.6:

FLASH-11293 - This fix addresses an array rebuild omission issue found in the IBM FlashSystem V9000 for 5.7 TB flash modules. This does not affect FlashSystem 840 or any other FlashSystem products aside from IBM FlashSystem V9000. (S5)

Release 1.2.1.5

The following issue was fixed in release 1.2.1.5:

FLASH-11051, 11108, 11184 - The neighborhood feature has been disabled due to an intermittent issue that, in some cases, causes the management GUI to hang. Disabling this feature also prevents an issue where it could cause Ethernet connectivity issues on the user's network (S2)

Release 1.2.1.4

The following were fixed in release 1.2.1.4:

FLASH-9995   - Remediated vulnerability in SSL/TLS (CVE-2015-2808).

FLASH-8991   - Remediated vulnerability in Java (CVE-2014-6593 and CVE-2015-0410).

FLASH-9913   - Fixed Fibre Channel (FC) interface data reporting on double XBAR failure before the system takes the links down. (S1)

FLASH-10156 - Canisters no longer go into an error state after failover in combination with adding or removing a host. (S1)

FLASH-10391 - Cards will not fault after a CCU from 1.1.3.2 to 1.2.0.11 and a reboot. (S2)

FLASH-10599 - Improved handling of canister failover during a CCU for canisters at different firmware levels. (S2)

FLASH-10164, 9862, 9861, 8766, 8763, 7491, 9486 – Improvements have been made to iSCSI behavior during cable pulls and host connects and disconnects. (S2)

FLASH-10102, 10091 - T3 recovery failure with an encrypted array has been fixed. (S2)

FLASH-9923   - `charray -encryption yes` put nodes into service state when the user created keys, didn't encrypt, upgraded system, and then tried to encrypt. (S2)

FLASH-9824   - Improved sustained write behavior after changes in work load. (S2)

FLASH-9661   - Improved interface tag checking on read data packets. (S2)

FLASH-10248 - Fixed checks on LUN extents. (S2)

FLASH-10535 - Fixed XBAR issues caused by trim stripes and writes to the same location. (S2)

FLASH-10126 - Fixed a problem with canisters going into service state after failing battery_power. (S3)

FLASH-9864   - Fixed assertion list issue on Infiniband (IB) interface. (S3)

FLASH-9715   - Resolved the Input/Output termination issue for canister whose persistent reservation keys are preempted. (S3)

FLASH-9259   - Improved interface to RAID controller faulty packet error rejection. (S3)

FLASH-10265 - XBAR CCE now cleared out on reset-recovery. (S3)

FLASH-10135 - GET call_home added for RESTful API to display Call home details. (S3)

FLASH-9867   - Added ability to retrieve enclosure serial number for RESTful API. (S3)

FLASH-10541 - Fixed Flash errors due to snap run in a 5 minute window of 1 week of stats init. (S3)
FLASH-9429 - Changed default snap to not include historical stats to their reduce size. (S4)
FLASH-9705 - Call home unexpected timeout when changing system time fixed. (S4)
FLASH-10154, 10152, 10032 - Call home event spamming on successful read retries fixed. (S4)
FLASH-9631 - CCU time out after snap on boot resolved. (S4)
FLASH-10565 - Interface DRAM ECC failure incorrectly flagging flash failure fixed. (S4)
FLASH-9377 - Fixed issue where the DMP for error code 1689 did not transition to 1690 (array spare).
            (S4)
FLASH-9309 - Memory freeing issue with init code fixed. (S4)
FLASH-9294 - `lsenclosurechasis` CLI command is now completely disabled. (S4)
FLASH-9138 - Fixed the DMP for error code 1707 that was not completing. (S4)
FLASH-10150 - Simultaneous flash and interface failure not bringing the array offline is resolved. (S4)
FLASH-9595 - False reporting on flash fixed. (S5)
FLASH-10070, 10003 - Improved interface BW statistics reporting. (S5)
FLASH-9869 - Bad link fixed for upgrade URL heading from `sainfo lssaguicapabilities`. (S5)
FLASH-9840 - Call home heartbeat data XML improved. (S5)
FLASH-9773 - Missing core.ccelog restored to storage report. (S5)
FLASH-9655 - Fixed incorrect time given in export CSV file for GUI performance charts. (S5)
FLASH-9440 - `lsdrive` command not showing rekey state has been fixed. (S5)
FLASH-9375 - Performance panel hover text on the GUI has been fixed. (S5)
FLASH-9337 - Fixed port logging to spam on interface. (S5)
FLASH-9323 - Help examples for `lsmdiskgrp` have been improved. (S5)
FLASH-9158 - DMP for error code 1061 fixed to identify the appropriate port. (S5)
FLASH-9156 - GUI improved to identify the correct port. (S5)
FLASH-9066 - Wording error on the DMP screen for event 085092, error code 1803 has been fixed.
            (S5)
FLASH-8987 - Encryption page in Settings $\rightarrow$ Security now auto-refreshes. (S5)
FLASH-10337 – Improved Flash testing on reboots. (S5)

Release 1.2.0.12

The following was fixed in release 1.2.0.12:
35462 - Improved interface tag checking on read data packets. (S2)

Release 1.2.0.11

The following issues were fixed in release 1.2.0.11:
32697, 32603, 33296, 34905 - Added sector checking for Flash. (S1)
34437 - Fixed behavior of controller after failing sequential flashcards. (S1)
34944 - Fixed issue with single interface DMA timeouts after 248. (S1)
32649 - Fixed issue with undetected write errors on flash. (S1)
29949 - Fixed failure to report loss of control path to battery. (S2)
32703 - Fixed gas gauge corruption event during upgrade to Service Pack 3. (S2)
34150 - Fixed battery upgrade issue after battery degraded. (S2)
34792 - Non-configuration node should update born-on-date on battery creation. (S2)
32539 - Changed VDisk command allows rename to existing VDisk. (S2)
29590 - Added ability to zero-out host-seen LUN header. (S3)
31741 - InfiniBand (IB) interfaces improved to handle non-aligned buffer sizes. (S3)
32617 - Canister failure error code 1039 triggered after upgrading to iSCSI adapters. (S3)
34220 - IB performance improvements. (S3)
32502 - IB: Update Mellanox Firmware to 2.31.5050. (S3)
32812 - Fixed encryption key verification during flash module replacement DMP. (S3)

28865 - The `chenclosure -encrypt` command now puts keys on both canisters. (S3)
29097 - Periodic key validate now checks non-configuration canister also. (S3)
31149 - Battery charge issue fixed. (S3)
31068 - Running a CCL upgrade repeatedly fills up partition when CCL fails. (S3)
32163 - Array creation succeeds when unresponsive flashcards are present. (S3)
32913 - Open Access: changing the SCSI ID of a drive leaves a phantom on the interface. (S3)
32642 - The `chvdisk` command allows VDisk with duplicate names. (S3)
34620 - Battery at pre 19.6 failed to boot upgrade. (S4)
30536 - Improved interface patching. (S4)
30734 - Improved boot upgrade for FPGA. (S4)
30940 - Fixed boot upgrade to upgrade a failed battery during reboot. (S4)
32036 - Improved flashcard patching. (S4)
32957 - Flashcard in Golden Image fails to boot upgrade. (S4)
31989 - Modified Call Home usertype description to be more verbose, especially related to Support usertype. (S4)
31007 - Improved fan behavior during certain bad scenarios. (S4)
31765 - Improved PSU comm errors. (S4)
32580 - Fixed battery issue on upgrade to version 1.1.2.7. (S4)
32650 - Removed email notification spamming for drive and temperature events. (S4)
33119 - On a system with two PSUs, PSU fan speed fluctuates when applying 110V to one PSU and 100V to the other PSU. (S4)
33486 - Fixed RAID status to distinguish the type of error. (S4)
31739 - Flashcards now return failure status on invalid offset/count accesses. (S4)
32084 - Displays have been fixed for flashcard failover caused by CPU sleep. (S4)
34367 - Can now disable low power mode on a single flashcard. (S4)
32142 - Non-default SNMP community now preserved when turning agent off and on again. (S4)
27503 - Interface cards now implement a timeout watchdog for unresponsive management complex. (S4)
31303 - Improved Fibre Channel (FC) interface reports. (S4)
32102 - Updated company IDs. (S4)
32157 - For IB, updated node description and vendor ID. (S4)
29600 - SVC can now handle quick service state transitions. (S4)
33866 - Node failover during `mkarray/recoverarray -format` formats more drives. (S4)
33606 - Event log improved for battery reconditioning expiration. (S4)
32959 - Resolved fan status in `lsenclosurecanister`. (S4)
30134 - Management GUI improved to allow users to reboot the system or canister. (S5)
30415 - Battery reconditioning fixed for `lsenclosurebattery` when that battery is not in the system. (S5)
30646 - Event message for unexpected node failovers now generated. (S5)
30964 - Snap now captures audit log file from non-configuration node in partner snap. (S5)
32360 - Fixed log errors for DMAs in RAID 0. (S5)
32966 - Added support for InfiniBand Mellanox register dumps. (S5)
30838 - Improved the timing for the update test utility 'read me' screen. (S5)
32629 - Improved battery reconditioning information. (S5)
32670 - Flashcard power and health stats are now monitored. (S5)
34461 - Fixed LED behavior when USB from inittool is inserted. (S5)
31499 - Fixed error messages retrieval during battery learning. (S5)

Release 1.1.3.8

The following were fixed in release 1.1.3.8:
33931 - Remediate vulnerabilities for NSS. (S2)

35503 - Remediate vulnerability for SSL/TLS. (S2)
33394 - Remediate Apache struts security vulnerabilities. (S2)
33479 - Remediate Java security vulnerabilities. (S2)

Release 1.1.3.7

The following were fixed in release 1.1.3.7:

33931 - Update to newer OpenSSL to remediate PSIRT Advisories 2500 & 2697 on SP3c. (S1)
34551 - Update Tomcat to remediate PSIRT Advisory 2818 on SP3c. (S1)
34958 - Interface DMA timeouts after 248 days results in failing drives due to timer wrap. (S1)
34916 - 1.1.3.x code version flash Field Replaceable Units (FRUs) inserted into 1.1.2.x code version systems followed by system upgrade to 1.1.3.x code version can lead to encryption key loss. (S2)
34967 - Failing sequential flashcards does not fail RAID controller, resulting in array going offline. (S2)
34744 - FRU battery incorrectly reaches end of life right after insertion and after node failover. (S3)
34788 - Battery expiration and Expiration warn never get cleared after the issue is corrected. (S3)
34806 - Battery gas gauge upgrade fails to complete if an error is encountered on the other battery during the upgrade. (S3)
34932 - iSCSI controller crashes during cable pull. (S3)

Release 1.1.3.6

The following were fixed in release 1.1.3.6:

33113 - Unresponsive interfaces are not failed or recovered. (S2)
32886 - Faulty input power reading at < 100VAC causes data access loss. (S3)
33115 - Insufficient voltage on non-redundant PSU causes system to go in and out of service state. (S3)
33240 - Long cable pulls with iSCSI can cause the affected interface controller to hang. (S3)
33573 - Add power supply consumption to heartbeat (1300W power supply only). (S5)

Release 1.1.3.2

The following were fixed in release 1.1.3.2:

31171 - Possible data corruption on flash fail due to sub-4k accesses being allowed to coalesce on two lanes of a stripe. (S1)
31112 - Ethernet network loop storm causes both nodes to go into Service State 578. (S1)
32242 - Read Sweeper "page is used" check not always correct. (S2)
32257 - Gateway node timeout is less than XBAR timeout, causing unexpected flash fail. (S2)
31177 - Illegal read/write access sometimes allowed with persistent reservations. (S2)
31898 - IB: Detect unaligned RDMA accesses. (S2)
31523 - Panic with fast node reset after slow email notifications. (S2)
30705 - Node is offline due to logs running out of memory. (S3)
31419 - Race condition with XBAR switching in driver can cause soft lockup. (S3)
31088 - PSU: i2c problems on the PSU are never reported to the user. (S3)
30982 - Clear BCAST bit on the batteries. (S3)
31011 - Add mechanism to report gas gauge corruption. (S3)
31193 - Maintenance reset failure may leave interface in service. (S3)
27936 - Protocol: Target does not abort active tasks upon entering ACA as directed by QErr flag. (S3)
27970 - Protocol: Drop PLOGI received before a FLOGI_ACC. (S3)
30327 - Modify Target Reset to only reset LUNS associated with the initiator. (S3)
30927 - Orphaned DMA tracker if a write DMA completion status is missed. (S3)
31561 - LU Reset with heavy write IO can result in multiple release calls for the same tracker. (S3)
31563 - iSCSI: Running out of buffer on login response will mangle response. (S3)
31564 - iSCSI: During login negotiation, return transition bit when no more keys pending. (S3)
31693 - Bad sanity check in get_target_name can cause memory corruption or bad response. (S3)

31776 - USIC: Fix broken VPD page length for block limits (0xB0). (S3)

31527 - T4 Recovery fails to recover LDAP server names. (S3)

31087 - T4 not restoring VDisks UIDs; need to support `mkvdisk -instance`. (S3)

31256 - Spare flashcards sometimes certify when joining the array. (S3)

31482 - `stopsystem -node X -reboot` to power on a powered off node produces error code 1039. (S3)

32070 - Array parity_compromised is not always saved. (S3)

30725 - Call home test messages sent that are not initiated by the customer. (S3)

29672 - Removing a flashcard while boot upgrading does not remove drive from state machines. (S4)

29925 - CCL allowed with array offline and no drives. (S4)

30290 - SVM fails to upgrade PSoC in golden image. (S4)

30688 - Boot upgrade fails on drive if a canister is missing. (S4)

30752 - Node failover during CCL will incorrectly allow boot upgrade. (S4)

31991 - IB: Change patching order to prevent card "bricking" on patch failures. (S4)

31688 - Documentation for `lsenclosurestats`, `lssystemstats`, and `lsnodecanisterstats` (`lsnodestats`) is present, but commands are not supported. (S5)

32048 - A window to select interface speed doesn't come up in DBCS environment. (S5)

30700 - Add system reboot required event after non-concurrent upgrade. (S5)

Release 1.1.2.7

The following were fixed in 1.1.2.7:

31892 - Remediate PSIRT Advisory 2106: MCP affected by Open Source - 7 issues for openssl (S1)

31893 - Remediate PSIRT Advisory 2093: MCP affected by Open Source - 2 issue(s) for glibc (S1)

31975 - Remediate PSIRT Advisories 2209 and 2211 ("bash bug" vulnerability) (S1)

31666 - T3 attempts to restore iSCSI host twice and fails. (S3)

Release 1.1.2.2

The following were fixed in release 1.1.2.2:

29687, 29694, 30973, 30992 - Improved Robustness of Hot Canister Pulls. (S1)

29124 - PMOM: Add mask bits for PSU error reporting to software. (S2)

30806 - `chsystem -alias` command does not work, causing incorrect UUIDs after T3. (S2)

30937 - T3 does not recover VDisk mapping SCSI IDs (LUN). (S2)

30143 - System report with canister powered off can crash remaining canister. (S2)

30740 - Changing flashcard positions while the system is powered off leads to data loss. (S2)

29508 - Interface's PCI links have issues while data running, should fail interface not both xbars. (S2)

29917 - Fixed issue with FRU replacement upgrades causing nodes to come up with 841 error. (S2)

26338 - Fixed DMA stall due to wear leveling moves. (S2)

30754 - Fixed erroneous interface timeout that can occur approximately 497 days after boot. (S2)

30920 - Interface with PCI errors can incorrectly take down access to entire system. (S2)

29515 - Fixed issue that caused a RAID controller failure on canister when hot removing the other canister while running and replacing it within 15 seconds. (S2)

29539 - ftdc - system report - seeing samnet issues in certain cases. (S3)

29970 - `lsibportcandidate` does not show any IB ports. (S3)

30448 - `svctask chnodehw` asserts when used to fix node error 841. (S3)

30872 - `lsiogrphost` command caused a node restart on non-config node. (S3)

29819 - Non-config Intel complex dies during satask snap. (S3)

29946 - Concurrent replacement of Canister 2 caused Event ID=085071 error 1039. (S3)

29822 - Fan failure not cleared on node failover. (S3)

30323 - Fixed canister power off issues during battery concurrent upgrades. (S3)

29705, 30140, 30261 - Fixed drive encryption issues after a concurrent update. (S3)

29534 - Improved automatic reset recovery of interfaces. (S3)

29818 - Improved error handling of interfaces during automatic internal hardware upgrades. (S3)

29848 - Improved error handling of RAID Controllers during automatic hardware upgrades. (S3)

29957 - Improved software upgrade test utility to check drives and PSU states. (S3)

30051 - Fixed quorum communication timeouts during concurrent updates. (S3)

30119 - Improved checks for interface failures during RAID Controller concurrent updates. (S3)

30135 - Handle batteries with bad manufacturing set up during upgrades. (S3)

30240 - Add better handling of single canister upgrades. (S3)

30284 - Improve handling of PSoC upgrade failures. (S3)

28487 - ecmon kills volman sometimes on boot, killing node during CCL. (S3)

25822 - Write CPLD mask register on PMOM to prevent canister power off during CCL. (S3)

29505 and 29979 - Fix I2C issues on battery module. (S3)

29833 - Increase fault tolerance on reads to the battery module. (S3)

30350 - Fix issue with not high charging current when both batteries are offline. (S3)

29472 - Added support for untagged task attribute. This had been removed in a previous release as obsolete, but is needed for interoperability support. (S3)

29628 - Fixed interface cards failure when both batteries are pulled out and replaced while data is running. (S3)

30259 - A resolve transport ID conflicts with certain versions of SVC. (S3)

29712 - Fixed issue with sending FLOGI requests with non-zero S_ID values when moving Fibre Channel cables between switch ports. (S3)

29864 - XBAR link failure to GBE or Interface following CCL of XBAR can cause Interface heartbeat failure. (S3)

24802 - The PTPL_A bit in the PERSISTENT RESERVE IN command is now reported correctly with the REPORT CAPABILITIES service action. (S3)

29651 - Quick (< 1 second) battery reseat caused quorum error. (S4)

30416 - 2 instances of rsyslogd running on Texan. (S4)

29545 - Fix packet to orca FPGAs times out during canister insertion. (S4)

30444 - Flashcard log messages not being serviced from log buffer. (S4)

30704 - Reseating canisters one after another cause samnet timeouts. (S4)

29427 - Made upgrade more resilient to node failovers. (S4)

29729, 29787 - Improved battery state checking during concurrent updates. (S4)

30295 - Flashcard "CCE" - Enable the SEM core to check and, with FW assist, correct configuration memory. (S4)

30219 - Fix issue with system not getting out of service 657 state when both batteries are removed from system. (S4)

30575 - Panel name renames as serial number when clustered. (S5)

29645 - Allow CLI access from the serial port user. (S5)

29838 - `svcinfo lsnode` shows partner node status is 'offline' instead of 'service' preventing obtaining partner snap. (S5)

29639 - `sainfo lsservicenodes` "error_data" column showing incorrect string. (S5)

29274 - Status of Ethernet port does not get updated in `lsportip`. (S5)

29829 - HWERRLOG fills up and stops rather than rotates. (S5)

30159 - System will generate Call Home PMR but will NOT heartbeat. (S5)

29891 - Added new events for automatic internal hardware upgrades during boot. (S5)

30023 - Added a manual way to bypass the 30 min multipath wait during upgrades. (S5)

29386 - Fixed issue with concurrent upgrade `lssoftwareupgradestatus` command "percent_complete" field decreasing. (S5)

29120 - Improved support maintenance command. (S5)

29342 - Improved PSoC error handling during upgrades. (S5)

24943 - Persist flash program erase count across flashcard initialization. (S5)

26915 - Correctly calculate the amount of time required for a battery to charge when using `sainfo lsservicestatus`. (S5)

29525 - Add system power statistics to call home data. (S5)

29538 - GUI stat "Latency" renamed "Internal Latency" to correctly represent the statistic. (S5)

30004 - `svc_snap -dumpall` returns" CMMVC5741E The filter value [] is not valid." (S5)

Release 1.1.1.3

The following were fixed in release 1.1.1.3:

30117 - Need to port SVC's remediation of the Heartbleed vulnerability. (S1)

29969 - Error 1111 "Batteries have insufficient charge." (S2)

25822 - Write CPLD mask register on PMOM to prevent canister power off during CCL. (S2)

30143 - System report with canister powered off can crash remaining canister. (S2)

29935 - Spurious Samnet from 0x2b with the tag from 0x2a. (S3)

29694 - Pulling a canister while only reading can put interface in an error state. (S3)

29353 - SVM should check for foreign canister before attempting to perform remote acquiesce. (S4)

30172 - One node is cluster and the other in service during the first boot upgrade. (S5)

30171 - Removed unnecessary information from battery VPD writing. (S5)

Release 1.1.1.2

The following were fixed in release 1.1.1.2:

29814 - Intermittent 114 Enclosure Battery fault type 1. (S2)

29881 - MGMT to XBAR link integrity improvement. (S2)

29894 - Management FPGA is not always patched on boot. (S4)

29893 - Displayed battery charge percentage calculation not correct. (S5)

Release 1.1.1.1

The following were fixed in release 1.1.1.1:

29021 - System is now resilient to canister failures during a rebuild. (S2)

28767 - Battery inlet temperature sensor no longer reports impossible values. (S2)

27191 - Correctly read Power Supply's VPD which fixes an un-clearable error in the event log. (S3)

29028 - Added hysteresis to temperature monitoring to avoid strong reactions to temporary temperature spikes due to sensor inexactness. (S3)

29443 - Only an active management node can power off flashcards; previously the redundant node could cause a power off if it detected bad batteries, unfortunately the user may not be properly notified of the power off since it was being sourced by the redundant node. (S3)

28698 - Concurrent code updates are more resilient to interface programming errors. (S3)

28924 - Interface connectivity alerts greatly improved and clarified. (S3)

27922 - Power supply temperature notices no longer flood system logs. (S3)

28622 - Flash data retention logic now correctly notes system power off time to better correct for stored data on flash cards powered off for extended periods of time. (S3)

29036 - Can now recover an offline array into a degraded state; for example if you powered off a system and removed the spare and a data flashcard, you can now add a single card and recover the array. (S4)

27761 - FC link breaks will now wait 10 seconds before cancelling all open exchanges and logging out all connected initiators for that port. (S4)

27664 - InfiniBand interface repair procedure no longer references Fibre Channel. (S4)

27548 - InfiniBand status LEDs now illuminate correct components. (S4)

29549 - Power controller monitoring no longer result in false battery failures. (S4)

29451 - Average latency performance shown in GUI no longer averages unused links (which report "0" and cause better latency numbers when averaged). (S4)

29020 - Temperature statistics now being collected. (S4)

29392 - Battery goes to "fault type 1" temporarily due to issues with battery gas gauge communication. (S4)

28978 - Now correctly detect failed RAID controller instead of incorrectly failing flashcards. (S4)

29012 - Battery charge voltage doesn't get set properly due to issues with battery gas gauge communication. (S4)

28823 - Canister concurrent maintenance now supported. (S4)

28948 - Repeated SCSI RESERVE6 commands no longer cause failures. (S4)

28818 - When system is powered off, but plugged in, power supply fans will only ramp up when the batteries are charging. (S4)

28760 - Non-concurrent upgrades done via CLI now are correctly represented by the GUI. (S4)

28902 - Interface "Links Degraded" messages can now be correctly cleared. (S4)

29186 - Corrected a variety of displayed URLs to point to valid web sites; in particular, the code upgrade check tool can now be downloaded using the embedded URL link. (S4)

28960 - Upon power-on, flashcard now correctly report power status, thus preventing initial flashcard arrays being incorrectly created without all members. (S4)

28903 - Interface "Links Degraded" message downgraded from "alert" to "warning". (S4)

8.0 Copyright notice

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of IBM Corporation in the United States, other countries, or both. These and other IBM trademarked terms are marked on their first occurrence in this information with the appropriate symbol (® or ™), indicating US registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at http://www.ibm.com/legal/copytrade.shtml.

The following terms are trademarks of other companies:

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.