DiffBI Report

BASELINE SELECTOR 1: SAS3FW_Phase16.0-2018-04-26-16.00.01.00_REL_1524803145@\SAS_CTRL_FW
BASELINE SELECTOR 2: SAS3FW_Phase16.0-2019-08-01-16.00.10.00_REL_1564646639@\SAS_CTRL_FW

Change Summary (9)

(SCGCQ01823844) - Point Release Version 16.00.02.00 - SAS3FW_Phase16.0 (7)

SCGCQ01793093 - (Defect) - [MCTP] Invalidate the incoming MCTP packet if packet sequence count out of range.

SCGCQ01749157 - (Defect) - PL: (SATA only) After FORMAT Operation, WRITE POINTER LBA is Not set to ZONE START LBA When Issued REPORT ZONES Command

SCGCQ01823793 - (BaseCMActivity) - Invader/Fury: Phase point Release 16.00.02.00

SCGCQ01823797 - (BaseCMActivity) - Invader/Fury: Update summary release note

SCGCQ01801163 - (CSETActivity) - PL: (SATA only) Proper Sense key not set to failed read/write command while handling NCQ error

SCGCQ01714694 - (CSETActivity) - Data NAK of large master TX packet can stop I2C out of band

SCGCQ00907366 - (CSETActivity) - Cutlass A1: 0xC002 fault while doing Cable breaking on I/T Switching

ACTIVITY ID: SCGCQ01793093
RECORD TYPE: Defect
HEADLINE: [MCTP] Invalidate the incoming MCTP packet if packet sequence count out of range.
DESCRIPTION OF ISSUE: If Packet Sequence Count is out of range we are not intimating to applications about it.
DESCRIPTION OF CHANGE: When Packet Sequence Count goes out of range intimate to Strolib application.
STEP TO REPRODUCE: 1) Pump large MCTP packets with packet size set to minimum.
2) From logs we can observe for this transaction Packet Application Message Tag remains same but Sequence Count should be incremented.

ACTIVITY ID: SCGCQ01749157
RECORD TYPE: Defect
HEADLINE: PL: (SATA only) After FORMAT Operation, WRITE POINTER LBA is Not set to ZONE START LBA When Issued REPORT ZONES Command
DESCRIPTION OF ISSUE: After format operation on SMR drive, Reset write pointer command was not triggered due to wrong enum comparison and wrong HW state.
Hence WRITE POINTER LBA is Not set to ZONE START LBA
DESCRIPTION OF CHANGE: Change done in PL to trigger reset write pointer command at the end of format.
STEP TO REPRODUCE: Issue format command to SMR SATA drive
Wait for format to complete
Send report zone command.
WRITE POINTER LBA is Not set to ZONE START LBA and zone condition full

---

ACTIVITY ID: SCGCQ01823793
RECORD TYPE: BaseCMActivity
HEADLINE: Invader/Fury: Phase point Release 16.00.02.00

ACTIVITY ID: SCGCQ01823797
RECORD TYPE: BaseCMActivity
HEADLINE: Invader/Fury: Update summary release note

ACTIVITY ID: SCGCQ01801163
RECORD TYPE: CSETActivity
PORT OF: Defect - SCGCQ01763871
HEADLINE: PL: (SATA only) Proper Sense key not set to failed read/write command while handling NCQ error
DESCRIPTION OF ISSUE: In SATA NCQ error handling scenario, there's one IO that hit the error, and the others are "collateral aborts", meaning they did not hit an error, but must be aborted anyway.
PL uses the NCQ Tag value in the NCQ error log to determine which IO actually hit the error. There's a Broadcom Gen3 expander hardware bug which can cause Tag to be incorrect.
Ultimately, controller reporting wrong sense
key for the IO which actually hit error.
This can only happen if SATA drive attached behind EDFB (DataBolt) enabled Broadcom Gen3 expander.
STEP TO REPRODUCE: Connect Host managed SATA SMR drive behind EDFB (DataBolt) enabled Broadcom Gen-3 expander.
Trigger sequential write on one zone and trigger random write on another zone to trigger write pointer not aligned error.
Drive aborts command with abort error and controller reports incorrect sense key to the command on which error occurred.

ACTIVITY ID: SCGCQ01714694
RECORD TYPE: CSETActivity
PORT OF: Defect - SCGCQ01713685
HEADLINE: Data NAK of large master TX packet can stop I2C out of band
DESCRIPTION OF ISSUE: The firmware, when configured as an I2C master-slave (master for message transmission and slave for message reception), has an error case where the controller sees an error transmitting a packet, which incorrectly causes the next packet to be sent to fail (checking stale data from the hardware), and then the firmware fails to reconfigure for slave reception. This causes the I2C out of band
communication stops working, and all packets sent to the controller are not ACKed.

The reason for the missing ACKs on a data byte is system dependent, but asynchronous I2C mux switching and slow software bit-bang I2C slave code on the BMC are possibilities.

STEP TO REPRODUCE: Configure the controller as MCTP I2C master-slave for the out of band feature. Configure a large packet support (MaxPacketSize) such as 256 bytes.
Send a request from a BMC over I2C that generates multiple response packets.
Before the second to last response packet is sent out (like the first response packet), NAK a data byte that is late in the packet, such as byte 174 (not including the I2C
address byte and using 1-indexing).

ACTIVITY ID: SCGCQ00907366 ↑
RECORD TYPE: CSETActivity
PORT OF: Defect - SCGCQ00904531
HEADLINE: Cutlass A1: 0xC002 fault while doing Cable breaking on I/T Switching
DESCRIPTION OF ISSUE: Firmware incorrectly setting status of an internal IoIndex to invalid value after cleaning it up. As a result, when the Ioindex is being re-used, firmware detects bad io status and faults with 0xC002.
STEP TO REPRODUCE: Set up four Cutlass HBAs in four systems all running Initiator and Target mode with 16 LUNs each.
Each HBA is connected to a different Cobra expander cascaded together.
While Running IO to all HBAs from each HBA, sequentially break the cables between two different HBAs and their respective cobras.

(SCGCQ01840265) - Phase16 Point Release Version 16.00.03.00 - SAS3FW_Phase16.0 (2)

SCGCQ01792419 - (Defect) - PL Enclosure Management: 0x7C41 or 0x265E Fault During Bootup of Customer System

SCGCQ01840048 - (BaseCMActivity) - New Build Version 16.00.03.00

ACTIVITY ID: SCGCQ01792419
RECORD TYPE: Defect
HEADLINE: PL Enclosure Management: 0x7C41 or 0x265E Fault During Bootup of Customer System
DESCRIPTION OF ISSUE: As part of a customer requested feature added for SAS3 Phase 16, code was added in PL to internally generate a SEP request for reading/writing slot status. This requires allocating a resource frame. The resource frame was marked as an internal IO, but the flag was not cleared when the internal request finished. Later, the resource frame was re-used for a SCSI IO request started via MCTP. When this request went to complete, it went down the wrong completion path, due to the internal IO flag being set, resulting in a 265E or 7C41 fault.
DESCRIPTION OF CHANGE: In enclosure management code, always clear the FW context before completing the request or freeing the frame.
STEP TO REPRODUCE: Boot up customer system with large topology.

ACTIVITY ID: SCGCQ01840048
RECORD TYPE: BaseCMActivity
HEADLINE: New Build Version 16.00.03.00

(SCGCQ01882392) - Phase16 Point Release Version 16.00.04.00 - SAS3FW_Phase16.0 (2)

SCGCQ01876881 - (Defect) - PL Enclosure Management: Vendor Specific Fields in Enclosure Page 0 Sometimes Incorrect

SCGCQ01882245 - (BaseCMActivity) - New Build Version 16.00.04.00

ACTIVITY ID: SCGCQ01876881
RECORD TYPE: Defect
HEADLINE: PL Enclosure Management: Vendor Specific Fields in Enclosure Page 0 Sometimes Incorrect
DESCRIPTION OF ISSUE: With certain vendor specific enclosure configurations, vendor specific fields in Enclosure Page 0 are filled out incorrectly by PL firmware. This was ultimately caused by one field in a PL data structure having fewer bits than were needed.
DESCRIPTION OF CHANGE: Made a correction so that the relevant field has the necessary number of bits to represent all potential values.
STEP TO REPRODUCE: Attach vendor enclosure with drives in all backplanes. Perform port enable and read enclosure page 0. Certain vendor specific fields will be filled incorrectly.

ACTIVITY ID: SCGCQ01882245
RECORD TYPE: BaseCMActivity
HEADLINE: New Build Version 16.00.04.00

(SCGCQ01952464) - Phase16 Point Release Version 16.00.05.00 - SAS3FW_Phase16.0 (3)

SCGCQ01940668 - (Defect) - PL: SSP Open Address frame uses wrong Destination SAS Address

SCGCQ01952437 - (BaseCMActivity) - New Build Version 16.00.05.00

SCGCQ01898054 - (CSETActivity) - (SATA Only) SCSI Start Stop Unit command with power condition set to standby may fail for SATA drives.

ACTIVITY ID: SCGCQ01940668
RECORD TYPE: Defect
HEADLINE: PL: SSP Open Address frame uses wrong Destination SAS Address
DESCRIPTION OF ISSUE: Firmware enters the Auto-port configuration process when links come up. During this process it is determined which PHYs belong together and create a wide port. There is a small window of opportunity where it is possible for two PHYs with different SAS addresses to be assigned to port 0. This situation ends up being corrected when this process runs again. However, during this small window where both PHYs are assigned to port 0, an I/O can potentially start and the command might go out to the wrong PHY. It is rejected by the SAS target device with an OPEN_REJECT (Wrong Destination). Firmware will handle this by aborting the task for this I/O.
DESCRIPTION OF CHANGE: When the Auto-port configuration process detects that two PHYs are assigned to the same port but have different SAS addresses, it will immediately change the Link Alias (Port number) in hardware. The small window of opportunity is greatly reduced by firmware because re-assigning a port number no longer involves waiting on a link reset and the link coming up again.
STEP TO REPRODUCE: Enable Auto-port configuration on all PHYs. Attach two target devices on controller PHYs 0 and 1. After port enable, power on the target device on PHY 1 first (this ensures it is assigned to port 0) and then the target device on PHY 0. Run heavy I/O to the target device on PHY 1. Perform a link reset on PHY 0. PHY 0 will temporarily be assigned to port 0 when it comes up (same as PHY 1). There is a chance an I/O meant for the target device on PHY 1 can go out PHY 0, since they are the same port and PHY 0 is the lower PHY. This behavior is hard to reproduce. The firmware ringbuffers show that a PHY can temporarily be assigned the wrong port number.

ACTIVITY ID: SCGCQ01952437
RECORD TYPE: BaseCMActivity
HEADLINE: New Build Version 16.00.05.00

ACTIVITY ID: SCGCQ01898054
RECORD TYPE: CSETActivity
PORT OF: Defect - SCGCQ01833392
HEADLINE: (SATA Only) SCSI Start Stop Unit command with power condition set to standby may fail for SATA drives.
DESCRIPTION OF ISSUE: For translating Start Stop Unit command with power condition standby to SATA Drives supporting Extended Power Conditions feature set, firmware sends multiple ATA commands as per SATL spec. While sending one of the ATA command the reserved fields were being set which some drive will abort.
STEP TO REPRODUCE: 1. Attach a drive that supports Extended Power Conditions feature set.
2. Send SCSI Start Stop Unit command with power condition to standby.
3. Observe that the command fails.

(SCGCQ01994263) - Point Release Version 16.00.06.00 - SAS3FW_Phase16.0 (2)

SCGCQ01993821 - (BaseCMActivity) - Invader Point Release version 16.00.06.00

SCGCQ01993172 - (CSETActivity) - PL : Task management timeout is observed if the task management type is invalid

ACTIVITY ID: SCGCQ01993821
RECORD TYPE: BaseCMActivity
HEADLINE: Invader Point Release version 16.00.06.00

ACTIVITY ID: SCGCQ01993172
RECORD TYPE: CSETActivity
PORT OF: Defect - SCGCQ01969521
HEADLINE: PL : Task management timeout is observed if the task management type is invalid
DESCRIPTION OF ISSUE: Server hang and reboot observed if the task management type is invalid
STEP TO REPRODUCE: Issue task management with invalid task management type to SAS drive

---

(SCGCQ02078004) - Phase16 Point Release Version 16.00.07.00 - SAS3FW_Phase16.0 (3)

SCGCQ02066816 - (Defect) - IOP: Interrupts to Host Are Incorrectly Masked Leading to IO and TM Timeouts

SCGCQ02077881 - (BaseCMActivity) - New Build Version 16.00.07.00

SCGCQ02053572 - (CSETActivity) - PL SATA: Repeating Internal Target Resets with Loginfo Code 0x31110e03

ACTIVITY ID: SCGCQ02066816
RECORD TYPE: Defect
HEADLINE: IOP: Interrupts to Host Are Incorrectly Masked Leading to IO and TM Timeouts
DESCRIPTION OF ISSUE: Phase 16 implemented a FW workaround for a HW issue with handling Function Level Resets (FLR). The implementation had a hole whereby it could falsely detect an FLR request. As part of the FLR process, FW disables interrupts which will be re-enabled on FLR completion. Since this is a false detection, no FLR occurs thus interrupts are never re-enabled. This results in IO/Task Management timeouts, and propagated error recovery of the HBA.
DESCRIPTION OF CHANGE: In the config trap code for the PCIe Device Status and Control register, when checking the InitiateFunctionLevelReset bit, qualify on the byte-enable bit for that byte.
STEP TO REPRODUCE: Perform a PCI config write directed at the HBA as follows:
- Offset 0x70 (PCIe Device Status and Control)
- Byte enable bits set only for the two upper bytes (Status)
- Bit 15 set (InitiateFunctionLevelReset)

Interrupts to the host will be masked, causing all outstanding requests to timeout from the host perspective.

ACTIVITY ID: SCGCQ02077881
RECORD TYPE: BaseCMActivity
HEADLINE: New Build Version 16.00.07.00

ACTIVITY ID: SCGCQ02053572
RECORD TYPE: CSETActivity
PORT OF: Defect - SCGCQ01955681
HEADLINE: PL SATA: Repeating Internal Target Resets with Loginfo Code 0x31110e03
DESCRIPTION OF ISSUE: After a target reset to a SATA drive, there's a chance that the host may immediately send an IO to the drive and SATA initialization may run before discovery code runs and processes the re-discovery of the drive. When discovery runs, it sets a SATA initialization needed state for the drive. If there are outstanding IOs at this point, code in the timer callback may start a target reset with loginfo
code 0x31110e03, due to outstanding IOs with SATA initialization needed. At this point, the cycle can begin over again, and may repeat many times, causing a target reset with loginfo code 0x31110e03 every time.
STEP TO REPRODUCE: This is only applicable to SATA drives, and requires a host or other software/firmware above PL to immediately send IOs after a target reset to the SATA drive. To potentially kick off the repeated resets, there has to be an initial target reset due to a hardware error or sent by the host.

(SCGCQ02093660) - Phase16 Point Release Version 16.00.08.00 - SAS3FW_Phase16.0 (5)

SCGCQ02063754 - (Defect) - IR : drive(part of volume) becomes inaccessible after drive removal and insertion back to same port

SCGCQ02082743 - (EnhancementRequest) - IOP: Add Additional Prints for PCIe Configuration Request Trapping

SCGCQ02093609 - (BaseCMActivity) - New Build Version 16.00.08.00

SCGCQ02080388 - (CSETActivity) - PL: FPE IO Timeout Following SCSI ATA Passthrough Command for Same Device

SCGCQ02080386 - (CSETActivity) - PL: SCSI ATA Passthrough command hangs with higher than expected DataLength

ACTIVITY ID: SCGCQ02063754
RECORD TYPE: Defect
HEADLINE: IR : drive(part of volume) becomes inaccessible after drive removal and insertion back to same port
DESCRIPTION OF ISSUE: Drive(part of volume) becomes inaccessible after drive removal and insertion back to same port because IR fails the commands to the drive as the drive is not mapped.
When the drive was inserted back, it was marked as not mapped due to a buggy code
DESCRIPTION OF CHANGE: Removed the buggy code that was marking the drive as not mapped
STEP TO REPRODUCE: 1. Creating RAID0 volume with 2 drives
2. Remove one drive
3. Insert it back to same slot
4. Drive on the other slot is not accessible.

ACTIVITY ID: SCGCQ02082743
RECORD TYPE: EnhancementRequest
HEADLINE: IOP: Add Additional Prints for PCIe Configuration Request Trapping
DESCRIPTION OF CHANGE: Extended the existing PCIe Configuration Request trap print to show the write data pulled from hardware, and added another print to show the data that firmware wrote back to hardware to complete the config trap.

ACTIVITY ID: SCGCQ02093609
RECORD TYPE: BaseCMActivity
HEADLINE: New Build Version 16.00.08.00

ACTIVITY ID: SCGCQ02080388
RECORD TYPE: CSETActivity
PORT OF: Defect - SCGCQ01965930
HEADLINE: PL: FPE IO Timeout Following SCSI ATA Passthrough Command for Same Device
DESCRIPTION OF ISSUE: Although not typical, it's possible to submit an ATA passthrough command with a count specified in bytes, rather than sectors. PL firmware was just passing this byte count to SAS HW, which was expecting a sector count. If the count is a high value, say 512, the HW gets messed up and a future NCQ read command to the drive hangs (never completed in SAS core).
STEP TO REPRODUCE: Send a SCSI ATA pass through data in command with a count of 512. Send other ATA passthrough commands after, and then read commands. A future read command should timeout.

ACTIVITY ID: SCGCQ02080386
RECORD TYPE: CSETActivity
PORT OF: Defect - SCGCQ02030158
HEADLINE: PL: SCSI ATA Passthrough command hangs with higher than expected DataLength
DESCRIPTION OF ISSUE: For ATA passthrough PIO data in commands, firmware processes all received data. The current code looks at DataLength in the IO request to see how much data is expected, and will keep waiting for more data until DataLength is satisfied. If, for example, the command only returns 512 bytes of data, but DataLength is 4096, the command will effectively hang as firmware continues waiting for more data
that will never come.
STEP TO REPRODUCE: Send an ATA passthrough that will return 512 bytes of data and set DataLength to greater than 512.

(SCGCQ02154758) - Point Release Version 16.00.09.00 - SAS3FW_Phase16.0 (3)

SCGCQ02105319 - (Defect) - MCTP I2C: Fault 0x26a4 observed during power cycle test

SCGCQ02154619 - (BaseCMActivity) - Bld : Update Invader/Fury phase 16 point release version to 16.00.09.00

SCGCQ02122434 - (CSETActivity) - Ventura B0: StorCLI does not list 'Model' information for SATA drives

ACTIVITY ID: SCGCQ02105319
RECORD TYPE: Defect
HEADLINE: MCTP I2C: Fault 0x26a4 observed during power cycle test
DESCRIPTION OF ISSUE: During power cycle testing, devices are lost behind controller.
The controller is acting as an I2C slave responding to an I2C Read and
fault 0x26a4 is observed.
DESCRIPTION OF CHANGE: Refined the HW workaround added as part of SCGCQ01394463.
When there is I2C timeout, added additional condition checks during which I2C DMA can be reset.
STEP TO REPRODUCE: Reboot system in loop.
Issue seen after 20-30 reboots.

ACTIVITY ID: SCGCQ02154619
RECORD TYPE: BaseCMActivity
HEADLINE: Bld : Update Invader/Fury phase 16 point release version to 16.00.09.00

ACTIVITY ID: SCGCQ02122434
RECORD TYPE: CSETActivity
PORT OF: Defect - SCGCQ02097328
HEADLINE: Ventura B0: StorCLI does not list 'Model' information for SATA drives
DESCRIPTION OF ISSUE: StorCLI does not list 'Model' information for direct attached or expander attached SATA drives.
STEP TO REPRODUCE: Connect DA and Expander attached SATA drives and sent storcli show command

---

(SCGCQ02185856) - Phase16 Point Release Version 16.00.10.00 - SAS3FW_Phase16.0 (2)

SCGCQ02181554 - (Defect) - SATA: Pended command not starting after sata passthrough command completed with fail status.

SCGCQ02185744 - (BaseCMActivity) - Invader/Fury: Phase16 Point Release 16.00.10.00

ACTIVITY ID: SCGCQ02181554
RECORD TYPE: Defect
HEADLINE: SATA: Pended command not starting after sata passthrough command completed with fail status.
DESCRIPTION OF ISSUE: Customer hit this issue where they have utility running in background for SATA drive to collect SMART data while normal IO load is in progress.

When SATA pass-through command was in progress, new commands got pended. But if existing SATA pass-through command completed with a fail status, the pended IOs never started resulting in command timeout.
DESCRIPTION OF CHANGE: When an IO completes through the PL SCSI error reply path for a SATA drive, set the global flag to check for and start pending IOs.
STEP TO REPRODUCE: Run IOs to SATA drive.
In parallel, use script to issue sata pass through command which may get fail status.

ACTIVITY ID: SCGCQ02185744
RECORD TYPE: BaseCMActivity
HEADLINE: Invader/Fury: Phase16 Point Release 16.00.10.00
