Q4

UPTIME BULLETIN

A Newsletter from CTD, a Division of EMC

For VNX/VNXe

VOLUME 15

December 2015

Upgrading to C840 drive firmware can mitigate certain drive failures

In previous Bulletins, we shared with you information regarding EMC's first version of enhanced firmware for the 600GB VNX SAS drive, part numbers 005049675 and 005049677, and we also talked about the introduction of an enhanced proactive disk copy algorithm (PACO-R) for these drives in VNX for Block OE 05.32.000.5.217 or later, as well as VNX2 for Block OE 05.33.008.5.119 or later.   KB 195555 provides more information about this change and tells you how you can download firmware and install it using the Unisphere Service Manager's (USM's) Online Disk Firmware Upgrade (ODFU) tool.

EMC has released a second iteration of new drive firmware (version C840) for these 600GB SAS drives. This adds a `verify after write` algorithm for any occurrences of the `write same` function. The `write same` function is primarily employed by the drive during a bind operation when the storage system attempts to zero out all data in a new LUN. This new firmware will verify the integrity of each and every write before the write is deemed successfully completed. By adding a `verify after write` in just this specific instance, the potential performance impact is kept to a minimum.

Leveraging this new feature will help you achieve the highest level of protection available for these drives. Many of the outages EMC has seen would have been mitigated by an upgrade to the latest firmware.

The latest version of Unisphere Service Manager (USM) will automatically notify you when new firmware is available for your drives. USM can also be used to download and install new drive firmware as an online activity. EMC recommends running the latest available VNX for Block OE version for your VNX or VNX2 storage system as well as the latest available firmware for these 600GB SAS drives to realize the maximum potential benefit from EMC's enhanced reliability improvements.

Reviewing ETA 209725: VNX2: Solid state disk drives with firmware version 0327 may experience coherency errors after array power down

ETA 209725 was recently released and warns customers of a potential data loss situation. This issue involves certain solid state drives and can occur during planned or unplanned power down operations. EMC strongly recommends upgrading the firmware to version 0332 for those customers who have the affected drives installed and running a firmware version of 0327 on them.

The ETA provides clear instructions on how to verify your drive firmware levels and upgrade your drive firmware using either Unisphere or the Unisphere Service Manager (USM) tool.

COMMENTS? IDEAS?

WE'D LIKE YOUR FEEDBACK ABOUT THE UPTIME BULLETIN. EMAIL US YOUR IDEAS FOR FUTURE TOPICS:

UptimeforVNX@emc.com

Customer Documentation

- https://mydocuments.emc.com/VNX
- http://emc.com/vnxesupport

Search the VNX Series page for *Uptime Bulletin* here:

https://support.emc.com/products/12781

EMC²

Examining ETA 207784 more closely; An SP may panic due to an interaction with the VAAI CAS command when its peer SP reboots.

In VAAI environments with Hardware Accelerated Locking (referred to as CAS or ATS) enabled, it is possible for an SP to encounter a bugcheck and unexpectedly reboot when the peer SP is rebooted. The bugcheck can occur during any SP reboot, including a non-disruptive upgrade. It is due to a rare timing-related race condition associated with the handling of the VAAI CAS (Compare And Swap, also referred to as ATS) functionality. The issue is fully resolved in VNX2 OE R33.119 and later. In the VNX1 series, there are available hotfixes for this issue that may be applied on top of VNX Operating Environment versions R32.217, R32.218, or R32.219.

In very rare cases, this issue could occur during normal runtime. This issue has most commonly been seen during a non-disruptive code upgrade, and even then we have only seen it occur in fewer than 1% of all NDUs. The most common use case involves the peer SP already being down. An unexpected reboot of an SP while its peer SP is already down may result in a brief Data Unavailable (DU) situation, which is why EMC has called attention to this issue in the aforementioned ETA.

This issue can only occur in a VAAI enabled environment with CAS (also referred to as ATS, Atomic Test and Set) enabled. The issue is more likely to occur if you have pools that are over the user settable usage threshold. You can reduce the likelihood of experiencing this panic if you increase the size of the pool so the usage is below the threshold and perform the NDU to a "fixed" code level at a quiet time. See ETA 207784 for the latest updates and recommendations regarding this issue.

We heard you

Continuous Improvement
ENGAGE
ENABLE
TOTAL CUSTOMER EXPERIENCE
EVOLVE
We Heard You
Improvements/Initiatives based on Customer Survey Feedback

In the past year, Customer feedback responses through our product survey have increased 150% for some members of our VNX product line.

Based on this significant increase, CTD Midrange has used this Customer feedback in the following ways:

- Adopted a formal program known as Advance Business Planning to take our known customer pain points and form corresponding action plans to address those problem areas in our next generation product releases. The areas of focus pursued by the program team are derived directly from the feedback received in our customer survey results. Areas of focus include but are not limited to: Ordering, Training & Education, Tools, Ease of Use, Documentation, etc.
- To identify and mitigate customer known issues around VNX family installation, upgrade, and migration for both current and next generation products

Our Objective: Be the simplest storage product on the planet, across the entire customer experience

Stay Tuned: The Corporate Total Customer Experience team is passionate about listening to customers through our extensive product surveys as well as a structured follow-up process with customers who take the time to submit valuable feedback. We will continue our laser focus on Total Customer Experience throughout a customer's end-to-end journey with EMC.

Tips of the day

- Use of unsupported cables including but not limited to Passive TwinAx can result in unpredictable behavior including failure to reconnect to storage after a storage processor reboot and subsequent failover.
- When changing fibre-channel port speed from 4G to 8G, switches and storage systems may require you to change the "Fill Word" from IDLE to ARB(ff) or some hybrid thereof. The IDLE fill word may not maintain proper synchronization at the 8G speed, which may result in problems connecting devices at this speed as well as other headaches in long-distance replication.

VNX/VNXe target versions

EMC has established target revisions for each product to ensure stable and reliable environments. As a best practice, EMC recommends that you operate at target code levels or above to benefit from the latest enhancements and fixes available. Search using the term “adoption rates” in http://support.emc.com for current VNX/VNXe target code adoption rates.

VNXe OS VERSION	RELEASE DATE	STATUS
2.4.4.22283	08/19/15	Target
2.4.4.22283	08/19/15	Latest Release
VNXe2 OS VERSION	**RELEASE DATE**	**STATUS**
3.1.1.6207002	10/18/15	Target
3.1.1.6207002	10/18/15	Latest Release
UNIFIED VNX CODE VERSIONS (7.1 & R32)	**RELEASE DATE**	**STATUS**
7.1.79.8 (VNX for File)	05/26/15	Target
7.1.79.8 (VNX for File)	05/26/15	Latest Release
05.32.000.5.219 (VNX for Block)	09/29/15	Target
05.32.000.5.219 (VNX for Block)	09/29/15	Latest Release
UNIFIED VNX CODE VERSIONS (8.1 & R33)	**RELEASE DATE**	**STATUS**
8.1.8.121 (VNX for File)	10/19/15	Target
8.1.8.121 (VNX for File)	10/19/15	Latest Release
05.33.008.5.119 (VNX for Block)	08/10/15	Target
05.33.008.5.119 (VNX for Block)	08/10/15	Latest Release

See Product Release Notes for a full list of enhancements per new code release.

VNXe code enhancements in release 2.4.4.22283

- Fixes an MTU mismatch issue that could result in DU/DL.
- Resolves a rare blocked SMB thread issue that could cause DU/DL.

VNXe2 OE code enhancements in release 3.1.1.6207002

- Fixes a memory leak that could lead to an unplanned reboot.

VNX code enhancements in release 05.32.000.5.218/7.1.79.8

- Includes all of the fixes in 05.32.000.5.217 plus the following:
- Fixes a regression bug that could leave any storage system using FIPS in an unmanaged state after the system was upgraded to 05.32.000.5.217.
- Associated file code 7.1.79.8 fixes a regression issue in file deduplication only present in the 7.1.79.6 release.

VNX code enhancements in release 05.32.000.5.219

- Minor release that builds upon the fixes in R32.217 and R32.218 and also includes a fix for issues related to drive fallout in 60 drive enclosures during NDUs.

VNX code enhancements in release 05.33.006.5.119

- Enhanced Proactive Copy (PACO-R) for specific 600G drives to improve reliability.
- Multiple de-duplication enhancements.
- Improvements in the Savvol space reclamation area.
- Resolves an issue that prevented cache from dumping during thermal shutdowns
- Resolves a rare timing panic in VAAI environments with CAS enabled.
- Resolves some SP panics due to TCP/IP network packet storms.

File code enhancements in 8.1.8.121

- Resolves a regression issue only present in the 8.1.8.119 release that could result in a file system being inadvertently taken offline after being mistakenly marked as corrupt.
- Resolves an issue where a warm reboot of a data mover could sometimes result in a longer, more disruptive cold reboot instead.

A VNXe or VNXe2 storage processor may panic due to a memory leak after extended, uninterrupted runtime

All VNXe and VNXe2 storage systems are potentially exposed to this issue. EMC has observed a number of single SP panics due to a slow memory leak in these systems. A very small subset of these SP panics have resulted in DU due to both processors rebooting at approximately the same time period. There is no set number of days at which point EMC can say with certainty that the processor will run low enough on resources to trigger the reboot. However, the incidents that EMC has observed thus far have occurred after anywhere from 270 to 400 or more days of continuous runtime.

Fixes are being individually created for each product in the VNXe family. Please check with support or refer to knowledge base solution KB204423 for more information about fix availability for your model. As a precautionary measure, customers may check the uptime of their VNXe or VNXe2 storage array and if it is approaching 270 or more days, you can schedule a planned reboot of at least one of the storage processors to refresh the memory and ensure that they are not in synch such that if you do experience the memory leak unplanned reboot, it will not happen on both SPs simultaneously and cause data unavailability.

Common causes of outages and how to avoid them

Load balancing and fault tolerance on Unified or File-only VNX

EMC recommends that if fault tolerance is a concern, you should configure a minimum of two AV servers in the network. If one of the AV servers goes offline or cannot be reached by the VNX, having two AV servers ensures that file scanning capability is maintained. If you have more than one AV server on the network, the VNX balances workloads among the AV servers by distributing the scanning jobs in a round-robin fashion. For example, if one AV server goes offline, VNX distributes the scanning load among the other available AV servers.

You can use the CAVA Calculator and the CAVA sizing tool to help determine the number of CAVA servers the system requires. The CAVA Calculator can help you prior to installation, and you can use it to run what-if scenarios after installation. The CAVA sizing tool collects information from a running environment to give you a recommendation on the number of CAVA servers needed.

CAVA viruschecker.conf shutdown Configuration

The shutdown command in the viruschecker.conf file specifies the action CAVA will to take when no AV servers are available.

> *shutdown=no* will cause CAVA to continue retrying the list of AV servers until one becomes available.
> This is the default.
>
> *shutdown=viruschecking* will stop the virus checking if no AV servers are available (Windows clients can access VNX shares without virus checking).
>
> *Shutdown=cifs* will stop CIFS if no AV server is available (No windows clients can access any VNX share.)

If strict data security is important in the environment, you should enable this option to prevent access to the files if all AV servers are unavailable. If this option is not enabled, and all AV servers are unavailable, clients can modify files without any virus checking.
This should not be used if running fewer than two CAVA servers.

EMC to offer only most recent code versions in each product family for download from support.emc.com

In an effort to ensure that more customers are upgrading to approved “target” code releases that have achieved the highest level of uptime, EMC has decided to cut back on the number of code versions available for download at support.emc.com.

If your desired version of VNX OE code cannot be found on support.emc.com, then contact EMC technical support for more information on acquiring and installing alternative code versions.

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED “AS IS.” EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.