NexentaStor

Release Notes 4.0.3 FP4

Date: April 20, 2015

Subject: NexentaStor Release Notes

Software: NexentaStor

Software Version: 4.0.3 FP4

Part Number: 7000-nxs-4.0.3-FP4-000011-A

This page intentionally left blank

Contents

www.nexenta.com

What is New in this Release?

NexentaStor 4.0.3.FP4

Changes in 4.0.3 FP4:

- VAAI changes since 4.0.3 FP3, see VAAI Block Changes.

- Enhanced NDMP performance.

- Enhanced error handling, presentation, and logging for Active Directory domain join.

- NMS automatic recovery from report.db database corruption.

- Enhanced performance of license checks on systems with a large number of disks.

- Enhanced handling of deferred deletes to correct free space reporting and prevent failover delays.

- Enhanced performance of zvol management.

- Improved handling of disappearance of active cluster partner by ALUA proxy process on surviving node.

Enhancements to 4.0.3 FP4:

Chassis management has been added for:

• Dell MD1420 JBOD (NEX-2942)

• Dell MD1400 JBOD (NEX-2943)

• SGI Modular Infinite Storage MIS chassis (NEX-3220)

NexentaStor 4.0.3 FP4 fixes various product issues. See Resolved Issues, NexentaStor 4.0.3.FP4.

NexentaStor 4.0.3 FP3

NexentaStor 4.0.3 FP3 fixes several specific product issues. The key fixes in this release include:

- SMB bug fixes related to authentication, multi-user clients signing, using out-of-epoch date, connectivity to multi-homed AD servers.

- NFS bug fixes related to authentication cache and kernel panics

- Added chassis management support for the following:

• Fujitsu Storage ETERNUS JX40

• 90-bay Supermicro SuperChassis 847DE26-R2K02JBOD

• Besta U90

• 28-bay Supermicro SuperChassis 837E26-RJBOD1

- Security fixes for NTP

- VAAI is disabled by default except for UNMAP.

- Fixed issues related to upgrade from 3.1.x to 4.0.3 FP3.

VAAI Block Changes

To improve product stability, NexentaStor 4.0.3-FP3 and later changes the block stack defaults for the VAAI to disable support. No action is needed for new installs, but preparation must be made for upgrades, as removing Atomic Test and Set (ATS) disrupts VMFS locking mechanics for datastores that have it enabled. ATS is set by default on creation with VMFS5.

The procedures and background information provided here summarize information provided in VMware knowledge base articles. Customers are recommended to consult the original documents. The following KB articles were reviewed by Nexenta in consultation with VMware:

1033665

2037144

2006858

2030416

2094604

In case of any issues with these procedures, customers should first open support cases with VMware and then, as needed, with Nexenta as joint support.

Note: Consistent with the change in defaults, Nexenta does not provide an interface or documented procedure for re-enabling VAAI, and VAAI for block storage is not supported in this release.

Warning about upgrading without preparation

VMware and Nexenta both recommend against an upgrade (which changes defaults to disable ATS) without first disabling VMware VMFS ATS-only locking.

As per VMware KB 2037144, datastores configured to use ATS-only locking fail to mount after an upgrade and do not show up in the vSphere client datastore view. In this situation Nexenta recommends that customers revert to the previously running snapshot, thereby reverting the change in defaults, performing the preparatory steps outlined below, then returning to the upgrade checkpoint.

Customers running ESXi 6.0 with multi-extent datastores mounted by multiple hosts should consult KB 2094604 and open a support case with VMware as necessary, given the following notice in that KB:

> The combination of one host using ATS-only and another host using SCSI Reserve/Release might result in file system corruption.

This can result from other procedures to disable ATS documented by VMware but not recommended by Nexenta for this situation, including others from the listed KBs.

Planning for upgrade

Customers should schedule a maintenance window to prepare for upgrades on ESXi hosts and complete NexentaStor upgrades. VMware assesses the impact thus, as per KB 2006858 (italics added):

• Disabling ATS locking takes effect immediately and does not require a VMware host reboot. *But if there is a host that has the volume mounted successfully, you may need to restart all the hosts in order to clear the ATS-Only.* This is because the host accessing with ATS-Only is preventing a Non-ATS-Only host accessing it.

• Enabling or disabling ATS should not impact any virtual machines running, but it is highly recommended you make this change during a maintenance window. During this time it is expected that all guests will be powered off.

• This change must be implemented on each host individually. All hosts able to connect to this storage must be configured consistently in regards to ATS.

Also, as per KB 2030416, the datastore must be inactive (guests must either be migrated off the datastore or powered off) before disabling ATS:

• All virtual machines must be migrated off the affected datastore, or powered off, prior to running the below steps.

Preparing ESXi hosts for upgrade

Nexenta recommends disabling ATS on a per-device basis, consistent with VMware's recommendation in KB 2006858:

> Disabling VAAI entirely on the ESXi host may introduce issues in the environment. Instead of disabling VAAI for all devices, you can be disable it only for the affected LUN without impacting other LUNs.

VMFS datastores use one or more extents. ATS settings must be modified on the devices underlying these extents.

To enumerate mounted datastore and identify which extents they use, log into the ESXi console and type the following from the ESXi console (ssh into the ESXi host(s), using what is also termed "tech support mode"):

```
~ # esxcli storage vmfs extent list
Volume Name    VMFS UUID            Extent Number Device Name
Partition
--------------  ----------------------------------  -------------  ---------
-------------------------------------------------------------  ---------
ham01-zv01       546fcc0f-d40379dd-5ae5-002590daef96         0
naa.600144f0c140cf6e0000546fca5d0002                                    1
lrtsesx01-ds-01  53b43e1d-d4ab8871-1a8d-002590daef96         0
t10.ATA_____ST1000NM00332D9ZM173_____Z1W11CAL
3
```

To confirm that an extent is backed by a NexentaStor block device, use "`esxcli storage core device list -d <device>`", as in our example below:

```
~ # esxcli storage core device list -d
naa.600144f0c140cf6e0000546fca5d0002
naa.600144f0c140cf6e0000546fca5d0002
   Display Name: NEXENTA Fibre Channel Disk
(naa.600144f0c140cf6e0000546fca5d0002)
   Has Settable Display Name: true
   Size: 2097152
   Device Type: Direct-Access
   Multipath Plugin: NMP
   Devfs Path: /vmfs/devices/disks/
naa.600144f0c140cf6e0000546fca5d0002
   Vendor: NEXENTA
   Model: COMSTAR
   Revision: 1.0
   SCSI Level: 5
   Is Pseudo: false
   Status: on
   Is RDM Capable: true
   Is Local: false
   Is Removable: false
   Is SSD: false
   Is Offline: false
   Is Perennially Reserved: false
   Queue Full Sample Size: 0
   Queue Full Threshold: 0
   Thin Provisioning Status: yes
   Attached Filters:
   VAAI Status: unknown
   Other UIDs:
vml.0200010000600144f0c140cf6e0000546fca5d0002434f4d535441
   Is Local SAS Device: false
   Is USB: false
   Is Boot USB Device: false
   No of outstanding IOs with competing worlds: 32
```

Devices exported from NexentaStor are evident because the Vendor field is set to NEXENTA. For each mounted datastore using NextaStor-exported extents, use "`vmkfstools -Phv1 / vmfs/volumes/<datastore>`" to confirm that ATS is enabled, as in our example:

```
~ # vmkfstools -Phv1 /vmfs/volumes/ham01-zv01
VMFS-5.60 file system spanning 1 partitions.
File system label (if any): ham01-zv01
Mode: public ATS-only
Capacity 2 TB, 725.6 GB available, file block size 1 MB, max file size
62.9 TB
Volume Creation Time: Fri Nov 21 23:34:39 2014
Files (max/free): 130000/129619
Ptr Blocks (max/free): 64512/63162
Sub Blocks (max/free): 32000/31911
Secondary Ptr Blocks (max/free): 256/256
File Blocks (overcommit/used/overcommit %): 0/1353841/0
Ptr Blocks  (overcommit/used/overcommit %): 0/1350/0
Sub Blocks  (overcommit/used/overcommit %): 0/89/0
Volume Metadata size: 814383104
```

```
UUID: 546fcc0f-d40379dd-5ae5-002590daef96
Partitions spanned (on "lvm"):
        naa.600144f0c140cf6e0000546fca5d0002:1
Is Native Snapshot Capable: YES
OBJLIB-LIB: ObjLib cleanup done.
```

The "ATS-only" output in the mode line indicates that the datastore is configured to use ATS.

To disable ATS, use "`vmkfstools --configATSOnly 0 /vmfs/devices/disks/<extent>`", as in our example:

```
~ # vmkfstools --configATSOnly 0 /vmfs/devices/disks/
naa.600144f0c140cf6e0000546fca5d002:1
```

The command will produce the following output, including a prompt to confirm the change of settings:

```
VMware ESX Question:
VMFS on device naa.600144f0c140cf6e0000546fca5d0002:1 will be upgraded to or
downgraded from ATS capability. Please ensure that the VMFS-5 volume is not in
active use by any local or remote ESX 4.x servers.

Continue with configuration of ATS capability?

0) _Yes
1) _No

Select a number from 0-1: 0

Checking if remote hosts are using this device as a valid file system. This may
take a few seconds...
Downgrading VMFS-5 on 'naa.600144f0c140cf6e0000546fca5d0002:1' from ATS
capability...done
```

In case of any other output, customers are recommended to open a support case with VMware, requesting joint support from Nexenta as appropriate.

Once ATS-only mode has been disabled for the datastore, you may proceed with the upgrade, checking guest I/O afterwards. VMware KB 2006858 provides a list of symptoms to check in case resulting problems with storage availability are suspected or apparent.

Reverting to pre-FP3 checkpoints

Reverting checkpoints will revert defaults. As long as the above preparatory steps have been successfully completed, datastores with ATS-only locking disabled will continue to be accessible.

NexentaStor 4.0.3 FP2

NexentaStor 4.0.3 FP2 fixes several issues clustered around specific functional areas. These areas include:

- Seamless upgrades from 3.1.6 to 4.0.3
- SMB 2.1 Improvements

- NFS Improvements
- Ease of Use: Chassis Management

Changes in 4.0.3 FP2

NexentaStor 4.0.3 FP2 is a maintenance release that addresses some of the NexentaStor 4.0.3 and 4.0.3 FP1 issues. This release includes enhancements in the following areas:

- Seamless upgrade from NexentaStor 3.1.6 to 4.0.3

  NexentaStor supports seamless upgrades from 3.1.6 to 4.0.3 and beyond. For 4.0 users, upgrading from 4.0.x to 4.0.3 is straightforward without downtime, like any other maintenance upgrade. For 3.1.x users, it is required to upgrade to latest version of 3.1.6 before upgrading to 4.0.3.

- SMB

  - New Domain Controller Locator

  The new Domain Controller Locator uses a more efficient algorithm to determine the optimal Domain Controller. It is no longer necessary to use the `sharectl` option to specify a preferred Domain Controller.

  - AD-style join and IDMU support

  The AD-style join is the preferred method of joining the Active Directory Domain. This enables users to use the IDMU feature in the Identity Mapping Service.

Note:	In NexentaStor 3.1.x, RPC-style join was temporarily set as the default method. Therefore, upgrading from NexentaStor 3.1.x to 4.0.3 may require additional configuration steps.
	For more information, contact [Nexenta Support]().

  - Kerberos client authentication

  Added support for Kerberos authentication for Microsoft Windows clients.

- NDMP

  NexentaStor 4.0.3 FP3 NDMP support is certified by Commvault Simpana® 10 and Symantec NetBackup® 7.x for backup and recovery use cases.

- Block target provider

  Addressed several critical issues in iSCSI and FC target provider.

- I/O continuity and fault tolerance enhancements

- Security updates

- NexentaStor vCenter Web Client Plugin

  This is a new plugin that enables you to provision and manage NexentaStor iSCSI LUNs and NFS folders in VMware vCenter Web Client 5.1 or later. The plugin seamlessly integrates into the VMware Web Client User Interface, providing the capability to monitor, snapshot, and clone NexentaStor datasets.

Auto-Sync Changes

The ability to clone datasets from snapshots at destinations that were created by auto-services is disabled in NexentaStor 4.0.3 and later versions.

Note:	You may still manually create a snapshot either using NMV or in NMC, and you can clone datasets.

SMB Changes

Starting in NexentaStor 4.0.3 FP2, the file sharing protocol SMB1 is enabled by default. However, you can enable SMB 2.0 in bash.

❖*To enable SMB 2.0 in bash using NMC:*

1. Enter bash using NMC.

2. Type:

```
nmc:/$ option expert_mode=1
nmc:/$ !bash
```

3. Type:

```
# sharectl set -p smb2_enable=true smb
```

Note:	If you are using NexentaStor 4.0.x and performing a minor upgrade to 4.0.3 FP2, SMB 2.0 will be disabled and SMB1 will be enabled by default.
	If you were using SMB1 and want to switch to SMB2, you need to reboot to reflect the changes.

NexentaStor 4.0.3 FP1

NexentaStor 4.0.3-FP1 fixes the Shellshock Bash bug that affects all software that uses the Bash shell and parses values of environment variables.

Discontinued Functionality

Due to lack of customer demand, Nexenta discontinued the WebDAV sharing protocol and its support starting from NexentaStor 4.0.3. For further clarifications, contact support@nexenta.com.

Determining the Version of the Appliance

NexentaStor 4.0.3 FP4 is the current release of NexentaStor 4.0.3. You can determine the version of the appliance using NMC.

❖ *To determine the version of the appliance using NMC:*

◆ Type:

```
nmc:/$ show appliance version
```

System response:

```
NMS version:   40-0-47
NMC version:   40-0-39
NMV version:   40-0-45
Release Date: Mar 20 2015
Operating System: Nexenta/illumos (version 4.0.3-FP4)
```

System Requirements

For system requirements for each environment, refer to the "System Requirements" section in the *NexentaStor Installation Guide*.

List of SMB Supported Client Operating Systems

Network clients can access files on NexentaStor using the Server Message Block (SMB) protocol if NexentaStor can properly authenticate the domain users. When an SMB client connects to a Common Internet File System (CIFS) server, NexentaStor authenticates the user according to the permissions specified in the domain to which NexentaStor is joined and has an active machine account.

The following table describes the versions of Domain Controllers and client Operating Systems that have been successfully tested to work with NexentaStor.

Table 1: SMB Compatibility Matrix

	Windows Server R2 2012	Windows Server 2012	Windows Server R2 2008	Windows Server 2008	Windows Server R2 2003	Windows Server 2003	Workgroup Mode
Windows 2012 R2	X	X	X	X	X	X	X
Windows 8	X	X	X	X	X	X	X
Windows 2012	X	X	X	X	X	X	X
Windows 2008 R2	X	X	X	X	X	X	X
Windows 7	X	X	X	X	X	X	X
Windows 2008	X	X	X	X	X	X	X
Windows 2003 R2	X	X	X	X	X	X	X
Windows XP	X	X	X	X	X	X	X
Windows 2003	X	X	X	X	X	X	X
Red Hat/ CentOS 6.5	X	X	X	X	X	X	X
Ubuntu 12.04 TLS	X	X	X	X	X	X	X
Mac OS X 10.9.2	X	N/S	N/S	N/S	N/S	X	X

Upgrading

To upgrade between minor versions of NexentaStor 4.0.x, see: Upgrading Minor Versions of NexentaStor 4.0.x

To upgrade from NexentaStor from 3.1.x to 4.0.x, see Upgrading from Version 3.1.6 FP3 to 4.0.3 FP4 with No Internet Connection, Upgrading from Version 3.1.6 FP3 to 4.0.3 FP4 with an Internet Connection, Upgrading from Version 3.1.6 FP3 to 4.0.3 FP4 with No Internet Connection

Upgrading Minor Versions of NexentaStor 4.0.x

❖ *To upgrade NexentaStor 4.0.x to a minor version, type:*

```
nmc:/$ setup appliance upgrade
```

Upgrading from Version 3.1.x to 4.0.3 FP4

Seamless upgrade is a new method of upgrading a NexentaStor appliance version from 3.1.x to 4.0.3 FP4. Upgrading NexentaStor from version 3.1.x to 4.0.3 FP4 is a two-step process.

1. Upgrade to 3.1.6 FP3.
2. Then, upgrade to 4.0.3 FP4.

   See Upgrading from Version 3.1.6 FP3 to 4.0.3 FP4 with an Internet Connection.

During the upgrade, NexentaStor services and volumes remain available to network clients. The upgrade operation requires system restart. Therefore, it is recommended that the upgrade process be scheduled during a system maintenance window. All NexentaStor services and volumes are not available during the restart.

Upgrading from Version 3.1.6 FP3 to 4.0.3 FP4 with an Internet Connection

Before you upgrade the NexentaStor appliance from version 3.1.6 FP3 to version 4.0.3 FP4, obtain the license from http://nexenta.com/products/downloads/register-nexentastor and verify that your environment meets the following prerequisites:

• The network interface card is included in the hardware compatibility list for NexentaStor 4.0.x.

• No third-party applications or packages are present on your NexentaStor appliance. You may have third-party packages installed if you changed repository sources on your NexentaStor appliance. The upgrade will result in the loss of components that are not included with the NexentaStor build.

❖ *To upgrade from version 3.1.6.x to 4.0.3, using NMC:*

1. If you have not upgraded to NexentaStor 3.1.6 FP3, upgrade to it by typing:

    nmc:/$ `setup appliance upgrade`

    Now you may run the NMC command `setup nexentastor upgrade` to upgrade to 4.0.3 FP4. Running this command will automatically disable the multi-NMS and restart NMS.

2. Upgrade to NexentaStor 4.0.3 FP4 by typing:

    ```
    nmc:/$ setup nexentastor upgrade
    ```

    System response:

    ```
    Proceed to automatically disable multi-NMS and restart NMS?
    ```

3. Type y.

    Multi-NMS is disabled and NMS is restarted.

    System response:

    ```
    The upgrade process may take some time up to 30 seconds to complete.
    ```

    ```
    Do you know if your hardware has been certified for 4.0.x? (y/n)
    ```

4. Type y if your hardware is listed in the Hardware Certification List (HCL).

    ```
    Upgrade NexentaStor Appliance from version 3 to version 4.
    This process include upgrade kernel, drivers, base system and appliance.
    WARNING: We can't guarantee third-party software will continue to work properly
    after upgrade.
    WARNING: The system should be restarted at the end of the process.
    Proceed? (y/n)
    ```

5. Type y.

    System response:

    ```
    NexentaStor is upgrading.
    ```
    During the upgrade, do not switch off or restart the NexentaStor appliance.

6. NexentaStor notifies you about the upgrade process.

    ```
    The first phase of upgrade has completed successfully
    Reboot now to finish upgrade to 4.0?
    ```

7. Continue to use NexentaStor 3.1.6 or reboot to activate NexentaStor 4.0.

    Nexenta does not recommend continuing to work using NexentaStor 3.1.6 after the first stage of the upgrade is completed. You may postpone the restart if you have incomplete archiving tasks. Otherwise, proceed with the reboot. When rebooting, all NexentaStor services and datasets are unavailable for network clients.

8. Verify that syspool is mounted:

    1. In NMV, click **Settings > Appliance**.

    2. In the **Upgrade Checkpoints** pane, click **View**.

    You should see the list of upgrade checkpoints.

Warning:	After you upgrade the volume version, back up your system. Backups created for mirrored pools with earlier volume versions may not be available after the upgrade.

9. Optionally, upgrade NexentaStor volumes to version 28 by typing:

    ```
    nmc:/$ setup volume <volname> version-upgrade
    ```

10. Repeat Step 9 for all NexentaStor volumes.

Note:	To upgrade the HA Cluster plugin, see: *NexentaStor HA Cluster User Guide.*

Upgrading from Version 3.1.6 FP3 to 4.0.3 FP4 with No Internet Connection

Before you upgrade your appliance with no Internet connection, review Upgrading from Version 3.1.6 FP3 to 4.0.3 FP4 with an Internet Connection. Verify that your environment meets all prerequisites described in this section.

❖ *To upgrade from Version 3.1.6 FP3 to 4.0.3 FP4 with no Internet connection:*

1. If you are unable to connect to the Internet to upgrade your system, contact support@nexenta.com for the ISO image.

2. Mount or burn the ISO image.

    Complete Step 2 to Step 10 in Upgrading from Version 3.1.6 FP3 to 4.0.3 FP4 with an Internet Connection.

Upgrade to Version 4.0.3 FP4 After Rolling Back to 3.1.6 FP3

Generally, Nexenta does not recommend that you roll back a NexentaStor appliance to version 3.1.6 after the upgrade to 4.0.3 on a production system. If you upgrade the volume version during the upgrade to version 4.0.3, the data and system volumes will be unavailable in version 3.1.6, since volume version 28 is not supported in version 3.1.6.

Rollback and upgrade is somewhat acceptable on a testing system.

During the upgrade, NexentaStor creates a flag file `/volumes/.config/.3_to_4_upgrade`. If you try to run the upgrade after rolling back to version 3.1.6, the upgrade fails.

To re-run the upgrade to version 4.0.3, delete the `/volumes/.config/.3_to_4_upgrade` file and run the `setup nexentastor upgrade` command again.

❖ *To rerun the upgrade from version 3.1.6 to 4.0.3, using NMC:*

1. Log in to bash:

    ```
    nmc:/$ option expert_mode =1
    nmc:/$ !bash
    ```

2. Type:

```
# rm /.config/.3_to_4_upgrade
```

3. Exit bash by typing:

```
# exit
```

4. Run:

```
nmc:/$ setup nexentastor upgrade
```

Upgrading from Version 4.0.3 FPx, to 4.0.3 FP4 with an Internet Connection

You can upgrade from the Version 4.0.3 release or from earlier 4.0.3 FP releases with a single command.

❖ *To upgrade the appliance to 4.0.3 FP4 from 4.0.3 or 4.0.3 FPx releases:*

1. Type:

```
nmc:/$ setup appliance upgrade
```

Resolved Issues

NexentaStor 4.0.3 FP4

This section describes the issues fixed in NexentaStor 4.0.3 FP4.

Key	Description	Functional Area
SUP-960	Restored NMC cifs-server subcommand for editing DNS resolver configuration.	Appliance Management
NEX-1450	Enhanced NDMP performance when doing simultaneous file and tape restores.	Kernel
NEX-2058, NEX-979	Access Based Enumeration supported as SMB share option.	Appliance Management
NEX-2322	Resolved issue preventing editing SCSI Target host groups from NMV.	NMV
NEX-2419	Resolved ALUA-related panic after manual failover.	Kernel
NEX-2434	Resolved issue that resulted in fibre channel target groups being taken offline during manual failover.	Plugin
NEX-2451	NMV now correctly displays network interface information after an LACP aggregate link event.	Appliance
NEX-2476	Resolved issue preventing destruction of LACP aggregate links without IP address configured for link.	Appliance Management
NEX-2611	Resolved issue with RPC timeouts not being observed in some instances.	Autosync
NEX-2615	Resolved issue where auto-snap exclude property failed to exclude the intended auto-snap from the snapshot list.	NMS
NEX-2667, NEX-2774	Enhanced error handling, presentation, and logging for Active Directory domain join.	Protocols
NEX-2680, SUP-763	NMS can now automatically recover from report.db database corruption.	NMS
NEX-2827	Resolved issue where an enabled CIFS Server had a status incorrectly listed as disabled.	NMC
NEX-2859	Enhanced performance of license checks on systems with a large number of disks.	NMV

Key	Description	Functional Area
NEX-2877	Resolved issue causing the addition the local admin group to the ACL when editing CIFS properties.	NMV
NEX-2904	If Auto-tier 'from-snapshot' property is set up, it now correctly appears in the property editing list.	NMC
NEX-2944	Resolved FP2 regression in auto tier which would cause a sync error for directory path elements containing spaces.	Autosync
NEX-2965	Enhanced handling of deferred deletes to correct free space reporting and prevent failover delays.	Kernel
NEX-3008	OpenSSL upgraded to 0.9.8ze to address multiple CVEs.	Security
NEX-3050	Chassis management for the SMC 90-bay JBODs no longer logs potentially sensitive information on chassis IPMI access failure	Chassis Management
NEX-3080	Accessing SMB1 shares using FQDN host name with Kerberos authentication and signing enabled no longer fails to mount with client error code 58.	Protocols
NEX-3086	Upgrade to FP4 or later no longer resets QLogic HBAs from target to initiator mode.	Kernel
NEX-3106	Windows Server 2012 R2 ACL editor no longer crashes explorer during attempt to add an ACE.	Protocols
NEX-3155	Resolved issue with DNS lookups for AD domain discovery occasionally entering logging loops.	Protocols
NEX-3159	The Install script now correctly creates the necessary logging directories, allowing for successful backups.	Protocols
NEX-3162	Corrected Fujitsu ETERNUS JX40 chassis backside image.	Chassis Management
NEX-3268	Corrected handling of reservations when deleting a shared volume.	Plugin
NEX-3288	Resolved issue with fault management daemon failing after a seamless upgrade.	COMSTAR
NEX-3289	Enhanced performance of zvol management.	Kernel
NEX-3323/NEX-3200	Seamless upgrade to FP4 or later no longer disrupts logging for appliance services.	Logging
NEX-3334	Improved handling of disappearance of active cluster partner by ALUA proxy process on surviving node.	COMSTAR

NexentaStor 4.0.3 FP3

This section describes the issues fixed in NexentaStor 4.0.3 FP3.

Table 2-1: Resolved Issues in 4.0.3 FP3

Key	Description	Functional Area
NEX-2199	Fixed to display Enclosure Logical IDs	Chassis Management
NEX-2694	Updated Metis logic for SMC 90 bay JBOD to stop creating a pool with two disks from the same tray.	Chassis Management
NEX-2838	Possible to rename the JBOD.	Chassis Management
NEX-2888	Modified Metis logic to understand SMC 90.	Chassis Management
NEX-2895	Stopped JBODs with N/A unit serial number from collecting in any chassis.	Chassis Management
NEX-1555	Added chassis management support for the 90-bay Supermicro SuperChassis 847DE26-R2K02JBOD.	Chassis Management
NEX-2011	Added chassis management support for the 28-bay Supermicro SuperChassis 837E26-RJBOD1.	Chassis Management
NEX-2010	Added chassis management support for Besta U90.	Chassis Management
NEX-2800	Added chassis management support for Fujitsu Eternus JX40.	Chassis Management
NEX-2495	Fixed `sesctl` to display the unit serial number.	Chassis Management
NEX-2690	Successfully imports span media. Fixed NDMP4 to have record size persistent between mover connections and state transitions.	NDMP
NEX-2947	Fixed the directory entries to not truncate when it is too large.	NDMP
NEX-2911	Fixed NDMPD logging to use syslogd system. Added an option to turn off the debugging. By default it is turned on.	NDMP
NEX-2345	Fixed `nfsauth_cache_get()` to perform faster in NFS operation.	NFS
NEX-2949	Fixed system panic due to bad mutex, from `auth_cache` being previously freed.	NFS
NEX-2972	Fixed `nfsauth_access()` to always initialize both ngids and gids.	NFS

Table 2-1: Resolved Issues in 4.0.3 FP3

Key	Description	Functional Area
NEX-2982	Fixed multiple NTP security vulnerabilities.	NTP
NEX-2892	Fixed NexentaStor losing connectivity to multihomed Active Directory servers.	SMB
NEX-2842	Fixed SMB client authentication failing in `adt_set_user()` with IDMU enabled.	SMB
NEX-2869	Fixed SMB2 signing failing for multi-user clients like Citrix RDS.	SMB
NEX-2894	Allowing the use of date that is outside of the UNIX epoch fails on CIFS.	SMB
NEX-2975	Fixed SMB2 cancel request failing.	SMB
NEX-2976	Fixed SMB2 failing to connect when server requires signing.	SMB
NEX-3012	To eliminate Kernel panics, VAAI is disabled by default except for UNMAP.	VAAI
NEX-2848	Fixed memory leak in the `ZFS_release()` library call path.	ZFS

NexentaStor 4.0.3 FP2

This section describes the issues fixed in NexentaStor 4.0.3 FP2.

Table 2-2: Resolved Issues in 4.0.3 FP2

Key	Description	Functional Area
SUP-621	Fixed the AD issue when an appliance gets a service location error from smbadm that results in package capture showing STATUS_ACCESS_DENIED when trying to open `\lsarpc`.	AD
NEX-2825	SMB2 is disabled by default in this release. You may enable it if required.	CIFS
NEX-2798	Fixed the SMB 1 disconnect after large write attempt.	CIFS
NEX-2705	Revolved issue where in some conditions smbstats may not report correct statistics for reads.	CIFS
NEX-2666	Fixed the error while creating nested directory using smb share path in Windows commands line.	CIFS
NEX-2604	Fixed crash when security tab is accessed in Windows Explorer.	CIFS

Table 2-2: Resolved Issues in 4.0.3 FP2

Key	Description	Functional Area
NEX-2593	Fixed the inability to create a folder with a long file name in SMB2.	CIFS
NEX-2516	Added an option to disable exclusive oplocks.	CIFS
NEX-2107	Addressed issue where SMB2 Notify Change failed to return for directory time change.	CIFS
SUP-933	Fixed Auto-tier to create a snapshot to use as its source by default.	Auto Services
NEX-2634	Addressed issue where sources link for plug-ins could incorrectly point to community edition plug-in repository.	Installation, NMS, Packaging
SUP-898	Fixed nscd being slow when a local file is missing.	NFS
NEX-1687	Revolved issue in saving changes using the NMV for quotas on existing file systems.	NMV
NEX-1673	Fixed the numbering issues related to the diskslots for MD3060e to be in alignment with physical numbering.	Chassis Management
NEX-1974	Added support for more than 16 groups with AUTH_SYS for NFS.	NFS
SUP-755	Revolved a condition where a plugin may fail to install.	NMC/Appliance Management
NEX-2310	Added missing information to a predefined list of volume properties.	NMS
SUP-955	Fixed NMV to show JBOD Slotmap properly.	Chassis Management
NEX-2459	Added option to create IPMI support for chassis management in NexentaStor.	Chassis Management
NEX-2770	Fixed error when attempting to share folder using NFS and CIFS.	NMV
NEX-2750	Fixed the idmapd config parsing code for empty property values.	ID Map

NexentaStor 4.0.3 FP1

This section describes the issues fixed in NexentaStor FP1.

Table 2-3: Resolved Issues in 4.0.3 FP1

Key	Description	Functional Area
NEX-2658 NEX-2635	Security Update to address vulnerability CVE-2014-6271. This vulnerability CVE-2014-6271 could allow for arbitrary code execution.	Security
NEX-2657 NEX-2642	Security Update to address vulnerability CVE-2014-7169. This vulnerability CVE-CVE-2014-7169 involved bash allowing code execution via specially-crafted environment.	Security

Known Issues

This section lists all known issues as of NexentaStor 4.0.3 FP4.

Table 2-4: Known Issues in 4.0.3 FP4

Key	Description	Workaround
SUP-737	NMV may, over time, grow heap memory while failing to reclaim allocations.	Restart NMS if large amounts of memory are being used.
NEX-928	When using ZEUS IOPS drives in a JBOD, a mptsas deadlock may occur due to a poor connection with the backplane.	Ensure that required components are installed and properly configured when using ZEUS IOPS drives in a JBOD.
NEX-2529	The NFS service may enter maintenance mode after changing the hostname or during a volume import if the hostname had been previously changed.	Reboot the NexentaStor appliance after changing the hostname.
NEX-2782	On very large configurations, NMV "Create New Volume" may not show all profiles and available drives.	On systems exhibiting this behavior, manually create volumes without using metis.
NEX-2897	Joining a second cluster member to an existing AD can compromise the previously joined member's domain association.	Join the domain before clustering any nodes.
NEX-3084	Seamless upgrade to 4.0.3-FP2 and later inhibits local management of NTP.	Edit the configuration file as follows: To edit the ntp conf file, using NMC: 1. Type: nmc:/$ setup network service ntp-client edit-settings 2. Select the ntp.conf file. You can edit the conf file in editor. 3. Type restrict 127.0.0.1 on the last line of the conf file. 4. Save the changes 5. Type Y to reread the configuration file.

Global Headquarters
451 El Camino Real, Suite 201
Santa Clara, California 95050
USA

Nexenta EMEA Headquarters
Camerastraat 8
1322 BC Almere
Netherlands

APAC Headquarters
Room 806, Hanhai Culture Building,
Chaoyang District,
Beijing, China 100020

7000-nxs-4.0.3-FP4-000011-A

nexenta™