nexenta®
Global Leader in Software-Defined Storage.

NexentaStor 5.0.3 and NexentaFusion 1.0.2

Release Notes

Table of Contents

Revision History

Date	Description
April, 2017	NexentaStor 5.0.3 and NexentaFusion 1.0.2 GA versions.
June, 2017	Added a note in the release notes about disabling USB3 in the BIOS settings before installing NexentaStor 5.0.3

Part Number: 7000-nxs -5.0.3-nf-1.0.2-000006-B June 2017

Product Overview

This document provides the release notes for the GA versions of NexentaStor 5.0.3 and NexentaFusion 1.0.2, as well as known issues for the NexentaStor 5.0 VVOL plugin.

NexentaStor 5.0 is a software-defined storage (SDS) platform that can be deployed as a full storage operating system on standard x 86 servers providing standard file (NFS and SMB), as well as block (FC and iSCSI) protocol services. NexentaStor 5.0 can be run in single-node configurations on internal devices or in dual-node high-availability (HA) cluster configurations with SAS-connected shared backend devices. NexentaFusion 1.0 provides and intuitive graphical user interface (GUI) for managing NexentaStor appliances.

The NexentaFusion graphical user interface (GUI) enables you to intuitively manage NexentaStor appliances. You can create and configure pools, create and share file systems, as well as access appliance-level summaries of hardware, pools, NICs, file systems, shares, volumes, LUNs, and services. NexentaFusion uses drill-down menus, action cogs, and expand-contract arrows, to provide a full range of administrative functionality for provisioning, monitoring, and optimizing storage appliances. You access NexentaFusion online help through a Web browser. NexentaFusion 1.0.2 supports the latest version of Chrome, and Firefox v47 or later.

NexentaStor 5.0 and NexentaFusion 1.0 Feature Support

The following is a high-level list of supported features in NexentaStor 5.0 and NexentaFusion 1.0:

Protocols	File: NFSv3, NFSv4, SMB 1.0, SMB 2.1, SMB 3.0 Block: Fibre Channel, iSCSI
Configurations	Single node on bare metal or VMware virtual machine HA clustered nodes on bare metal or VMware virtual machines
Data Management	Striped mirrors; single, double and triple parity RAID and unprotected ZFS end-to-end data integrity Unlimited snapshots and clones Unlimited file system size Inline compression Inline deduplication Thin provisioning Scheduled replication Continuous replication
Management	Self-documenting REST API, CLI, NexentaFusion
Client OS Support	VMware, Microsoft, Linux, OpenStack, Docker
Ecosystem Integration	SMB 3 ODX for Microsoft Hyper-V VMware VAAI Block VMware Virtual Volume (VVOL) 2.0 VMware vCenter Plugin OpenStack Cinder & Manila Docker Volume Plugin

www.nexenta.com
Part Number: 7000-nxs -5.0.3-nf-1.0.2-000006-B June 2017

Reference Architectures

NexentaStor supports a wide selection of certified reference architectures (RAs), fully defined configurations that feature components from leading server vendors. A number of Nexenta server partners provide a seamless end-user experience by acting as a single point of contact for deployment and support of the end-to-end hardware and software solution.

License Editions

NexentaStor 5.0 is available in an Enterprise Edition or Community Edition. The scope of the license editions are as follows:

NexentaStor Enterprise Edition is sold as a perpetual software license based on raw capacity limits. Support and services are sold separately. Pricing is tiered on the amount of raw capacity required for a system, yielding a lower price per GB for larger configurations. The Enterprise Edition includes all core storage functionality such as snapshots, clones, inline data reduction, software RAID and scheduled replication. It also includes the right to use NexentaFusion as the Graphical User Interface (GUI) for the system running that license. Additional options are sold on a per node basis and include features such as High-Availability Cluster, continuous replication or Fibre Channel support.

NexentaStor Community Edition is a limited-functionality, limited-capacity, free version of the software that can be used for non-production, non-commercial deployments. The NexentaStor Community Edition has limited functionality, limited capacity, and outside of the online Nexenta Community forums, no support services are available. A NexentaFusion server can manage at most one NexentaStor Community Edition appliance. For more information, see the online Nexenta Community forums.

Part Number: 7000-nxs -5.0.3-nf-1.0.2-000006-B June 2017

What's New in NexentaStor 5.0.3 and NexentaFusion 1.0.2

This section provides an overview of the changes and feature enhancements in these updates.

QoS for All-Flash VMware NFS Datastores

Using the CLI, REST API or NexentaFusion, it is now possible to configure rate limits on NFS shares. The rate limit is expressed in bytes / second and applies to the overall throughput on the share.

Rate-limit monitoring capabilities include a Fusion analytics widget to display the shares utilizing the greatest percentage of their limit, simple filtering on datasets by rate limit, and alerts on high bandwidth utilization.

The target use case for this feature is all-flash NexentaStor appliances supporting multi-tenant VMware environments. In these configurations, where a given tenant is mapped to specific NFS Datastores, NexentaStor QoS allows the infrastructure provider to cap the maximum amount of throughput provided to specific tenants.

Resilver Performance Improvement

Nexenta has been leading the effort in the OpenZFS community around zfs resilver and zfs scrub performance improvements. The core changes are included in NexentaStor 5.0.3 and apply by default. The underlying design focus is maximizing sequential operations and minimizing random IO on the pool devices and the device being resilvered. The net result are improvements that range from 2x all the way to 5x faster scrub and resilver depending on the application workload on the pool.

Smart-Sparing and Auto-Replace

Smart-sparing and auto-replace are two new NexentaStor features that improve storage availability and simplify maintenance operations.

When a device in a pool fails, smart-sparing automatically selects the right spare device to activate by means of an ordered search using media type, size, and locality as criteria. Media types currently supported are HDD and SSD. The size attribute is used to ensure that the spare is at least the same size or bigger than the failed drive. Locality of the device refers to the storage enclosure. For example, for a pool configured with an SSD hot spare (for SLOG devices) and HDD hot spares (for data devices) in each storage enclosure:

- smart-sparing will ensure that the SSD spare is only activated in case of a SLOG SSD failure,
- in case of an HDD failure, smart-sparing will preferentially activate the HDD spare in the storage enclosure where the failure occurred.

With auto-replace, replacing a failed device no longer requires issuing system commands to control the operation. The user can simply remove the failed device and physically replace it with a new device. NexentaStor automatically detects the insertion of the new device and triggers re-silvering. If the failed device had been previously spared, the spare is then released back to the pool. Note that if a spare was activated following a device failure, the user should wait for the spare resilver to complete before physically swapping out the failed device.

Improved support for SNMPv2

Added support for additional MIBs as well as ability to alert/trap on FMA events. Contact support@nexenta.com to get the latest version of the NexentaStor MIB.

Part Number: 7000-nxs -5.0.3-nf-1.0.2-000006-B June 2017

Chassis Management Enhancements

NexentaStor 5.0.3 adds chassis management for the following storage enclosures:

- Ericsson HDS8000_SSU0101
- LENOVO D3284 84 Bay JBOD
- SMCI SC216BE2CJBOD
- HGST 1ES0034 60 Bay JBOD

SMB 3 Encryption

NexentaStor 5.0.3 adds support for encryption of in-flight data for SMB 3 shares. This feature is disabled by default and can be enabled on individual shares using the `smb set` command.

SMB 2 Changes

In NexentaStor 5.0.3, the default settings for exclusive oplocks have been set to disabled. This will help with some performance issues associated with Microsoft Office applications.

Refined Algorithm for Swap Space

In 5.0.3, rpool allocation for swap space has been tightened.

Swap Volume Size for ZFS File Systems

System Type	Swap Volume Size
System with about 4 GB of physical memory	1 GB
Mid-range server with about 4 to 16 GB of physical memory	2 GB
High-end server with about 16 to 128 GB of physical memory	4 GB
High-end server between 128 and 512 GB of physical memory	16 GB

Additional Enhancements

- Several improvements in the content, management and delivery of the support bundle.
- High-Availability improvements for block services, cluster robustness and node synchronization.
- Driver enhancements for the XL710 40GbE.
- Intel NIC, delivering line rate performance on 40GbE interfaces as well as on all 4x logical 10GbE interfaces. To get maximum performance, MTU must be set to 9000.
- HPR recover command now runs as “dry-run” by default. This provides the user with information on what a replication service recovery would need to do (specifically what snapshots will have to be deleted) to get each side to a common state and recover the service. The user can then make an informed decision on whether to proceed, or copy some of the snapshot data to a safe location before actually recovering the service.
- NexentaFusion Analytics widgets to monitor IP Link performance and FC Target port performance.
- Ability to initiate an inventory rescan from NexentaFusion.
- Ability to upgrade NexentaStor’s license using NexentaFusion.
- Improvements in NexentaFusion’s ability to authenticate Active Directory users as NexentaFusion users.
- Various security improvements, including requiring browsers to connect with TLS version 1.2 or greater, restricting the acceptable ciphers, and disabling ICMP timestamp responses.

Part Number: 7000-nxs -5.0.3-nf-1.0.2-000006-B June 2017

Resolved Issues

Table 1 lists the resolved issues as of NexentaStor 5.0.3. Table 2 lists resolved issues as of NexentaFusion 1.0.2.

Table 1: NexentaStor 5.0.3 Resolved Issues

Component	Key	Description
Commands + Daemons	NEX-6200	Corrected behavior such that hot spare drives are reactivated after being reinserted into an enclosure.
HA, NEF API	NEX-9117	Corrected the functionality of the CLI command 'hacluster create -H', which returned a syntax error if additional heartbeat nodes were added.
Installation	NEX-1881	Resolved issue where, under certain circumstances, NexentaStor clusters could have mismatched controller numbers between the nodes.
Kernel, Protocols	NEX-3485	Resolved issue where a cluster failover during deferred deletes could cause loss of service for NFS clients.
Kernel	NEX-2100	Resolved a panic with the signature "vmem_hash_delete(ffffff5b5dee0000, 0, 1): bad free", very rarely seen during kernel memory management activities.
Kernel	NEX-9301	Resolved a BAD Trap: Double Fault panic intermittently seen when destroying a snapshot.
Kernel	NEX-860	Resolved an issue where an offline vdev could return online after a reboot.
Libraries	NEX-7498	Resolved an issue where a user could not display a user quota larger than 2TB using quota(1M).
NEF	NEX-8031	Repaired the functionality for removing a network heartbeat using the NEF CLI.
NEF	NEX-8054	Resolved an issue where cluster nodes could fail to sync if a removed iSCSI target shared portals with another target.
NEF	NEX-8688	Resolved issue where the default gateway setting could be lost after multiple failovers or reboots.
NEF	NEX-8908	Restored transport functionality for uploading bundles via HTTP/HTTPS as well as FTP/SFTP.
NEF	NEX-9075	Resolved issue where drives with SCSI2 reservations could be listed as failed in NEF and Fusion.
NEF	NEX-9080	Resolved a panic where, under rare circumstances, a piece of memory could be overwritten leading to missing network configuration settings.
NEF, NEF API	NEX-9094	Resolved an issue where changing the settings of the static IP of an interface (established at time of installation) would not appropriately update the default route, leading to a network outage upon the next reboot.
NEF	NEX-9122	Resolved an issue where the 'haservice create' command could repeatedly fail and only return an IP address as an error message.
NEF	NEX-9217	Resolved an issue where a recursive replication service could fail to start if there was a non-recursive snapshot on the destination, displaying the message "Destination already exists."
NEF API	NEX-7959	Resolved issue when ALUA=true on both nodes of an HA cluster, the 'FC target list' command did not include FC targets from both nodes.

Part Number: 7000-nxs -5.0.3-nf-1.0.2-000006-B June 2017

NEF API	NEX-8533	Resolved an issue where renaming a dataset with scheduled replication would not rename the destination dataset, causing the replication to restart from the beginning.
Packaging	NEX-9493	Resolved a BAD TRAP: Null pointer dereference panic related to the mr_sas driver calling bzero with a zero address.
Plugin	NEX-9532	Resolved an issue causing NDMP errors that could appear when a file/directory had special characters.
Protocols	NEX-9098	Expanded the file handler count limit from 16k to 64k, and made the setting tunable. (default setting is now 32k)
Protocols	NEX-9106	Added SMB support for "Resource SID Compression".
Protocols	NEX-9190	Resolved an issue where files with owners not in /etc/passwd and not having inherited ACL's were being prevented from seeing ownership/permission settings via SMB.
Protocols	NEX-9731	Resolved an issue where users could see excessive delays when opening files while using SMB2.

Table 2: NexentaFusion 1.0.2 Resolved Issues

Component	Key	Description
Fusion	NEX-6934	Resolved situation where a LUN could still be shown on the LUNs view after confirming the dialog to destroy the LUN.
Fusion	NEX-7904	Fixed a UI issue where changes were not immediately visible after clicking SAVE to create a target and/or target group.
Fusion	NEX-9156	Added the ability to cancel a check for software upgrades, specifically due to an issue where upgrades become delayed due to an incorrectly configured proxy server.
Fusion	NEX-9231	Resolved an error received when attempting to promote a clone using the UI.
Fusion	NEX-9235	Resolved issue with the Fusion UI where users were unable to share a filesystem via NFS if the filesystem had been shared via SMB.
Fusion	NEX-9239	Resolved issue where a dataset, replication service, or snapshot name of the form "vn", where n is a numeric value, could be rejected.
Fusion	NEX-9242	Resolved issue where the Management/Data Protection or Dataset/Data Protection screen could sometimes fail to display, and instead show the error "Can't Connect to Appliance".

Part Number: 7000-nxs -5.0.3-nf-1.0.2-000006-B June 2017

Enhancements

Table 3 lists the enhancements of NexentaStor 5.0.3 and Table 4 lists the enhancements made in NexentaFusion 1.0.2.

Table 3: NexentaStor 5.0.3 Enhancements

Component	Key	Description
Commands + Daemons	NEX-5736	Automated the process for replacing a failed drive in a pool.
HA, NEF, NEF API	NEX-9574	Added an instant COMSTAR sync between two nodes, to be executed at the time of an HA cluster creation.
Kernel	NEX-8852	Added Quality-of-Service controls on a per NFS share basis.
Kernel	NEX-7822	Enhanced performance and support for 40Gb Intel XL710 NICs.
Kernel	NEX-6088	Dramatically enhanced the ZFS scrub/resilver algorithm to reduce long completion times seen especially on large files and with large amounts of IO.
NEF, Packaging	NEX-8788	Integrated SanDisk IFCLI with NexentaStor 5.0.x interfaces and packaging.
NEF	NEX-9081	Reduced the frequency of evbridge log entries to the NEF service log, increasing the time that the log will roll over.
NEF	NEX-9087	Added functionality to add/remove interfaces from an aggr.
NEF API	NEX-8217	Added NEF API and CLI ability to show "Metadata on Special Vdev" on a per pool basis.
Protocols	NEX-3758	Added support for remote stale lock detection.
Protocols	NEX-5273	Implemented SMB 3 encryption.

Part Number: 7000-nxs -5.0.3-nf-1.0.2-000006-B June 2017

Table 4: NexentaFusion 1.0.2 Enhancements

Component	Key	Description
Fusion	NEX-8706	Added functionality to the Fusion UI for updating NexentaStor licenses.
Fusion	NEX-9060	Fusion can be connected to a proxy server that requires authentication
Fusion	NEX-9345	As a 1.0.1 user, if you had configured AD and now upgraded to 1.0.2, you must redo the AD configuration.
Fusion	NEX-9434	Added x-xss-protection to Access-Control-Allow-Headers in order to allow Cross Origin Validation (CORS).

Known Issues

Table 5 lists the known issues as of NexentaStor 5.0.3. Table 6 lists known issues as of NexentaFusion 1.0.2.

Table 5: NexentaStor 5.0.3 Known Issues

Component	Key	Description	Workaround
Chassis Management	NEX-7773	Possible issues with the error reporting of MB-FAN4 or MB-FAN5. See workaround for determination of which node (primary or secondary), the MB-FAN4 or MB-FAN5 is failing.	If an MB-FAN4 or MB-FAN5 error message contains a hardware component with enclosure with the serial number ending in "7f", then the failing MB-FAN4 or MB-FAN5 is on the Primary node. If an MB-FAN4 or MB-FAN5 error message contains a hardware component with enclosure with the serial number ending in "ff", then the failing MB-FAN4 or MB-FAN5 is on the Secondary node.
Documentation	NEX-4523	Recovery from a failed ZFS Intent Log (ZIL) device without down time is currently impossible if the ZIL is not mirrored.	In all cases, a mirrored ZIL should be configured.
Installation	NEX-3488	Unable to boot NexentaStor from a drive with 4k native sector size.	Use 512 native or 512 emulated drives for NexentaStor installations.
Installation	NEX-8520	Changing the choice of Time Zone DURING an installation will lead to an incorrect time being reported on the system.	Avoid changing the choice of Time Zone during an installation, or manually update to current time of the recently selected time zone after the install.
Kernel	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.
Kernel	NEX-1760	In very isolated instances, system performance may momentarily degrade then recover during kernel memory reclamation (kmem_reap activity).	None.

Part Number: 7000-nxs -5.0.3-nf-1.0.2-000006-B June 2017

Kernel	NEX-3585	In rare circumstances, ZFS performance may degrade if kernel memory and the ZFS Adaptive Replacement Cache (ARC) contend for kernel memory.	None.
Kernel	NEX-7551	Current functionality allows a user to create a pool with drives consisting of mixed physical block sizes or to expand a pool by adding drives with different physical block sizes, resulting in the need to keep drives with multiple block sizes on hand as replacements.	When replacing drives, be certain to use drives with matching physical block sizes. If a problem is encountered, contact Nexenta customer support for assistance with resolution.
Kernel	NEX-8529	If the source dataset has been renamed and the user tires to disable a service on that dataset, the operation will hang until appliance is rebooted. Any other following operations like disable --force, destroy may also hang.	Reboot the node.
NEF	NEX-6285	There is currently no functionality via the Fusion UI or the NEF CLI for creating SNMPv3 accounts.	Contact Nexenta Support for assistance with creating SNMPv3 accounts.
NEF	NEX-6393	If the user renames a dataset which is child of a source of enabled continuous replication, related replication service goes to the faulted state with error: Session write stream error (UNIX_ERRNO_ENOENT)	Rename destination dataset respectively and re-enable replication service: filesystem rename test/dst/sub1 test/dst/sub2 hpr clear test hpr enable test
NEF	NEX-6394	HPR services can fail after a common source snapshot has been cloned and promoted.	Destroy or rename cloned dataset, then replace original dataset with promoted clone: filesystem rename test/src test/srcLegacy or filesystem destroy -r test/src filesystem rename test/clone test/src
NEF	NEX-7436	A misleading error is given when a user issues an NFS command while NFS is disabled.	Avoid using NFS commands if the NFS service is disabled.
NEF	NEX-7549	Recover/start with forceReceive cannot recover replication if renamed dataset has a clone on destination	1) Rename destination cloned dataset filesystem rename data/dst/sub data/dst/subLegacy 2) recover or clear and start service with forceReceive flag hpr recover test # or hpr clear test

Part Number: 7000-nxs -5.0.3-nf-1.0.2-000006-B June 2017

			hpr start -- properties=forceReceive=true test
NEF	NEX-7707	Recursive replication service fails after re-creating a child dataset	1) destroy destination dataset filesystem destroy test/dst/sub1 hpr clear test hpr enable test 2) or rename destination dataset filesystem rename test/dst/sub1Legacy hpr clear test hpr enable test 3) or start service with forceReceive to overwrite recreated dataset hpr clear test hpr start -- properties=forceReceive=true test hpr enable test 4) or recover service (the same as start with forceReceive): hpr recover test hpr enable test
NEF	NEX-7995	The current implementation limits a user to replicating filesystems and zvols and does not provide the option to replicate at the pool level.	None.
NEF API	NEX-6470	Neither NEF CLI nor REST API currently support LDAP directory bindings.	None.
NEF API	NEX-7162	Users are unable to destroy an HA cluster if one of the nodes is offline.	In order to destroy an HA cluster, both nodes must be online.
NEF API, RSF	NEX-7616	In situations where the date on two nodes differs by a matter of days or more, creating a cluster between the two can result in errors, such as the license not validating or one of the nodes not being recognized as being part of a cluster.	Confirm that the time/date are synchronized on two nodes before creating a cluster.
NEF API	NEX-8471	HPR does not currently provide a way to recreate services when source or destination pool is lost.	Destroy service with --force and create another one with the same options.
NEF API	NEX-8527	If a pool is imported with a new name, HPR services are not imported.	Export and import pool with old name or recreate any replication services.

Part Number: 7000-nxs -5.0.3-nf-1.0.2-000006-B June 2017

Kernel, Protocols	NEX-6776	Attempting to join a domain when the time/date on the system is not synced returns the misleading error of "Failed getting initial credentials. (Wrong password?)"	Ensure that the time/date on the system is synced before attempting to join a domain.
Protocols	NEX-9689	A failover of pool services on a HA cluster providing storage via SMB 3.0 to a Hyper-V server causes all VM's to time out and go offline.	Restart the VM's on the Hyper-V server after the failover completes to resume functionality.

Table 6: NexentaFusion 1.0 Known Issues

Component	Key	Description	Workaround
Fusion UI	NEX-6333	The maximum length (256 characters) of an SMB share description is not disclosed in the error received when it is surpassed.	Use SMB share descriptions 256 characters or less in length.
Fusion Installer	NEX-7214	The Fusion UI services do not start immediately after installation, and require a reboot.	Reboot after a Fusion installation.
Fusion UI	NEX-7434	Fusion continues to display the appliance as a cluster even after the cluster has been destroyed.	Unregister the cluster, and then re-register the individual nodes as separate appliances.
Fusion UI	NEX-7663	The Fusion UI allows users to attempt to import a pool even when it is unavailable for any reason. Until the import attempt is made, the user cannot tell the status of the pool.	If a pool import fails, resolve the condition making the pool unavailable and attempt again.
NEF API, Fusion UI	NEX-7731	The Fusion UI incorrectly allows the use of special characters when creating a network name, when the CLI does not.	Do not use special characters when creating a network name or address using the Fusion UI.
Fusion UI	NEX-7889	Dashboard and Analytics may not properly display metrics if appliance was initially registered while unlicensed.	Un-register and re-register the appliance after it is licensed, and clear the browser cache.
Fusion UI	NEX-7945	When connecting from Mac to Windows machine using built-in Mac remote desktop application and through vSphere client there accessing Fusion Console Wizard we see unexpected behavior. When clicking on VM console for the first time, it automatically starts checking for updates	Wait for the wizard to check for an upgrade and press cancel to return to main menu
Fusion UI	NEX-7998	Disabling HA service in Fusion is sometimes not reflected until the user clicks on refresh button.	Wait a few seconds, and click the refresh button.

Part Number: 7000-nxs -5.0.3-nf-1.0.2-000006-B June 2017

Fusion UI	NEX-8125	Creating a cluster between two nodes already registered in the Fusion UI will cause the Fusion UI to recognize the nodes as separate, unclustered nodes.	Either establish the cluster and then register, or un-register and re-register the cluster nodes.
Fusion UI	NEX-8417	When starting up Fusion using the Firefox browser, there may be some error messages the first time Fusion is started after install. (occurs only with self-signed certificate).	Acknowledge the errors and continue. Refresh the webpage if additional issues are encountered.
Fusion UI	NEX-8426	The Fusion UI does not allow a filesystem containing snapshots with clones to be destroyed. The error is: Failed to destroy snapshot: pool/filesystem@snapshot. Status code: EEXIST	Destroy filesystem from NEF CLI: filesystem destroy -R pool/filesystem
Fusion UI	NEX-8575	In situations where an appliance is heavily loaded, or the user is "fast clicking" between screens it is possible to see timeout errors displayed on the FUSION UI. Simply wait a few seconds and click refresh.	Simply wait a few seconds and click refresh
Fusion UI	NEX-9818	Default settings in the Fusion UI cause the FC Ports widget to show no data, due to the fcTargetStats probe not being enabled on upgrade.	On the Fusion Appliance/Administration/Data Settings page, check the box to enable the probe named "fcTargetStats" and click Save.
Fusion UI	NEX-9842	Fusion password reset URL does not work with some email clients.	Copy the link and add HTTPS to the URL.

Part Number: 7000-nxs -5.0.3-nf-1.0.2-000006-B June 2017

NexentaStor VVOL Known Issues

NexentaStor is designed with a multi-tenant VMware vCenter Plug-in and VMware Virtual Volume (VVOL) support. For more information, see the ***NexentaStor 5.0 VVOL Admin Guide***. The following table lists the NexentaStor 5.0.3 VVOL known issues.

Table 5: NexentaStor VVOL Known Issues

Component	Key	Description	Workaround
VVOL	NCC-62	When deploying OVF templates using the vSphere Web Client, a warning about an untrusted certificate appears.	Ignore the warning.
VVOL	NCC-301	Unable to upload a file directly to a VVOL datastore.	First create a folder on the VVOL datastore, and then upload the file to the folder.
VVOL	NCC-343	VMware Web Client does not properly validate certificate whereas vSphere Client validates properly. So when downloading certificate manually it displays proper information.	Download the certificate manually and validate it.
VVOL	NCC-349	A pool created on a NexentaStor appliance post registration with VASA, is not always visible for VVOL.	Unregister and then re-register the NexentaStor appliance.
VVOL	NCC-358	After taking snapshots and reverting, the VM is unable to boot.	Power off the VM and wait for 5 minutes, then power back on.

Part Number: 7000-nxs -5.0.3-nf-1.0.2-000006-B June 2017

Installation and Upgrade Procedures

Follow the instructions in the ***NexentaStor 5.0 and NexentaFusion 1.0 Installation QuickStart Guide*** to install and upgrade NexentaStor and NexentaFusion.

Recommendation

NexentaStor 5.0.3 does not support USB3. So USB3 in the BIOS settings must be disabled before installing NexentaStor, so that the installer does not break and go into maintenance mode.

Where to Find More Information

NexentaStor Product Guide
This document includes an overview of NexentaStor and its core components, describes key features, and provides relevant CLI commands. This manual is intended as a guide to NexentaStor concepts and not as a configuration guide.

NexentaStor 5.0 and NexentaFusion 1.0 Installation QuickStart Guide
This document includes the instructions to install and upgrade NexentaStor and NexentaFusion.

NexentaFusion 1.0 User Guide and Online Help
This documentation provides easy to follow step-by-step instructions for common configuration and monitoring tasks.

NexentaStor 5.0 CLI Configuration Guide
This guide demonstrates the basic steps and commands to configure and manage NexentaStor 5.0 appliances. Use this document in conjunction with the *NexentaStor 5.0 CLI Reference Guide,* and the *NexentaStor 5.0 HA CLI Admin Guide.*

NexentaStor 5.0 Command Line Interface Reference Guide
This reference guide provides a summary of the CLI commands. Use it in conjunction with the *NexentaStor 5.0 CLI Configuration Guide*.

NexentaStor 5.0 HA CLI Admin Guide
This guide demonstrates the basic steps and commands to configure and manage the NexentaStor 5.0 High Availability (HA) cluster using the NexentaStor 5.0 Command Line Interface (CLI).

NexentaStor 5.0 vCenter Plugin Admin Guide
This guide includes instructions to install NexentaStor 5.0 vCenter Web Client Plugin (vCenter Plugin), which enables VMware customers to configure and manage storage and virtualization through a single interface. You can use this plugin to access summary and detailed analytics and real time status monitoring of single and clustered NexentaStor appliances.

NexentaStor 5.0 VVOL Admin Guide
This guide describes the NexentaStor Virtual Volume (VVOL) solution. It provides instructions on how to deploy VVOL, integrate it with VMware vSphere, and enumerates storage operations it supports.

Part Number: 7000-nxs -5.0.3-nf-1.0.2-000006-B June 2017

NexentaStor 5.0 HPR User Guide

This document demonstrates how to configure High Performance Replication (HPR) to replicate datasets using the NexentaStor Command Line Interface (CLI) and using the NexentaFusion GUI.
For details on the list, see portal.nexenta.com.

Hardware Compatibility List for NexentaStor 5.0
This document provides a list of certified hardware for NexentaStor 5.0 and is intended for Nexenta Partners and Nexenta customer-facing organizations. The latest version of Nexenta Hardware Certification List (HCL) is posted on Partner Portal.

For information on the NexentaStor Openstack Cinder drivers (NFS/ iSCSI), see docs.openstack.org and search for 'NexentaStor 5.0'.

www.nexenta.com
Part Number: 7000-nxs -5.0.3-nf-1.0.2-000006-B June 2017