IBM System Storage N series

Data ONTAP 8.1 7-Mode Release Notes

GA32-1032-03

Contents

Data ONTAP 8.1 7-Mode Release Notes

These *Release Notes* describe new features, enhancements, and known issues for Data ONTAP® 8.1 7-Mode, as well as additional information related to running this release on specific storage systems.

Note: The terms *flexible volumes* and *FlexVol volumes* are used interchangeably in Data ONTAP documentation.

About the Data ONTAP 8.1 7-Mode release

Data ONTAP 8.1 7-Mode is a General Availability (GA) release in the Data ONTAP 8.1 7-Mode release family. For more information about Data ONTAP releases, refer to the following publication:

IBM System Storage N series Data ONTAP Release Model

For up to date information regarding the latest release of Data ONTAP, refer to the following publication:

NEWS: Recommended Release for IBM System Storage N series Data ONTAP

Data ONTAP 8.1 7-Mode is a feature release that includes all the functionality included in the Data ONTAP 7.x release family, as well as additional features. Major features that were available in Data ONTAP 7.3.x releases, such as SnapLock, support for IPv6, IBM N series Data Motion for vFiler, and support for SFTP and FPS, are also supported in Data ONTAP 8.1 7-Mode. For the Data ONTAP 8.0.x 7-Mode release family and the Data ONTAP 7.x release family, IBM strongly recommends the Data ONTAP 8.1 7-Mode release.

Attention: If you have a N6210 or N6040 storage system with Flash Cache modules installed, do not upgrade your system to Data ONTAP 8.1 7-Mode. Flash Cache modules are not supported in N6210 or N6040 storage systems with Data ONTAP 8.1.

The issue is under investigation and a long-term strategy will be communicated as soon as possible. See “N6210 series and N6040 series storage systems with Flash Cache modules are not supported” on page 81.

Attention: N series Storage Encryption (NSE) enabled Storage Controllers that are running Data ONTAP 8.1 RC2 or earlier that plan to upgrade to 8.1 RC3 or later must use a special upgrade procedure. This is due to a defect found on storage controllers with 10-character System IDs where one character is dropped from the NSE System ID. The effect is improper key fetching from the key manager.

This defect is fixed in 8.1 RC3 and later. After the upgrade is completed, a rekey must be performed to update the System IDs on each storage controller. See the following Flash (Alert) technote for procedure:

Data ONTAP upgrade from 8.0.x to 8.1 RC3 or later requires N series Storage Encryption (NSE) System ID updates

For a complete list of functionality changes introduced in this release, see "New and changed features in the Data ONTAP 8.1 7-Mode release family" on page 7. If you are upgrading from a Data ONTAP 7.3.x release, see also "New and changed features in the Data ONTAP 8.0 7-Mode release family" on page 29.

Some Data ONTAP features are not supported in this release. For more information, see "Unsupported features" on page 5.

About these release notes

All the information in this document applies to the Data ONTAP 8.1 7-Mode release and later for N series storage systems, also sometimes called filers or appliances and gateway systems, except where otherwise indicated.

It is a best practice for all Data ONTAP users to see the following sections:

- If Data ONTAP is already running on storage systems in your environment, you should familiarize yourself with relevant topics before upgrading to Data ONTAP 8.1 7-Mode.

  This information helps you identify and resolve issues that might affect the availability of your systems. Check the online version of the *Release Notes* periodically for new cautions or updates that might have been posted since you downloaded your software.
- "Changes to published documentation" on page 113 in these *Release Notes*. This release information became available after the set of guides provided with this release were published.

Websites

IBM maintains pages on the World Wide Web where you can get the latest technical information and download device drivers and updates. The following web pages provide N series information:

- A listing of currently available N series products and features can be found at the following web page:

  www.ibm.com/storage/nas
- The IBM System Storage N series support website requires users to register in order to obtain access to N series support content on the web. To understand how the N series support web content is organized and navigated, and to access the N series support website, refer to the following publicly accessible web page:

  www.ibm.com/storage/support/nseries/

  This web page also provides links to AutoSupport information as well as other important N series product resources.
- IBM System Storage N series products attach to a variety of servers and operating systems. To determine the latest supported attachments, go to the IBM N series interoperability matrix at the following web page:

  www.ibm.com/systems/storage/network/interophome.html
- For the latest N series hardware product documentation, including planning, installation and setup, and hardware monitoring, service and diagnostics, see the IBM N series Information Center at the following web page:

  http://publib.boulder.ibm.com/infocenter/nasinfo/nseries/index.jsp

Unsupported features

Some Data ONTAP features are not supported in the Data ONTAP 8.1 7-Mode release family.

Features not available in Data ONTAP 8.1 7-Mode

- FilerView

  FilerView is no longer available on systems running Data ONTAP 8.1 or later releases. You can use System Manager as a web-based graphical management interface to manage common storage system functions from a web browser.

  For more information about System Manager, see the IBM N series support web site, which is accessed and navigated as described in "Websites" on page 3.

- Netboot

  In the Data ONTAP 8.0 7-Mode and later release families, netboot is not a supported function, unless you are restoring the Data ONTAP image on the boot device, such as a PC CompactFlash card. If you need to boot the storage system from a Data ONTAP image stored on a remote server, contact technical support.

  For information about how to replace a PC CompactFlash card or restore the Data ONTAP image on the card, see the Replacing a CompactFlash Card flyer that is applicable to your version of Data ONTAP.

- SnapValidator for Oracle

  SnapValidator for Oracle is not supported in Data ONTAP 8.0 7-Mode and later 7-Mode releases. For more information, contact technical support.

- IPsec

  IPsec is not supported in Data ONTAP 8.0 7-Mode and later releases. If IPsec is enabled on your storage system, it will be automatically disabled during the upgrade.

- TOE

  TOE functionality is not supported in Data ONTAP 8.0 7-mode and later releases. There is no adverse effect on the performance of your storage system because TOE is disabled.

If you require these features in your business environment, contact your IBM N series support to evaluate the best upgrade path.

Features discontinued in the Data ONTAP 8.1 7-Mode release family

Beginning in Data ONTAP 8.1 7-Mode, the following features are discontinued:

- "Systems including EXN2000 storage expansion units with ESH2 modules" on page 8
- "2-Gb FC ports not supported as targets" on page 88

Beginning in Data ONTAP 8.0 7-Mode, the following features are discontinued:

- "Upgrade process changes with Data ONTAP 7-Mode software images" on page 79
- Hardware-based disk ownership
- SnapVault for NetBackup

Features discontinued in a future release of Data ONTAP

Support for NDMPv3 will be discontinued in a future release of Data ONTAP. When that occurs, only NDMPv4 will be supported.

New and changed features in the Data ONTAP 8.1 7-Mode release family

A number of features and enhancements have been added or changed in the Data ONTAP 8.1 7-Mode release family. Features that were present in the Data ONTAP 7.x release family are now supported in this release.

Note: Some new and changed features in this release might also be introduced in a maintenance release of an earlier Data ONTAP release family. Before upgrading, be sure to consult with your IBM representative about new Data ONTAP functionality to determine the best solution for your business needs.

Additional major changes made in Data ONTAP 8.1 7-Mode are described as follows:

New and changed platform and hardware support

The Data ONTAP 8.1 release family supports new and changed hardware as listed.

For information about supported systems, see “Supported systems” on page 73.

- “Support for the N3220 and N3240 system models”
- “Support for SAS tape drives”
- “Systems including EXN2000 storage expansion units with ESH2 modules”
- “Support for FC/SAS bridge (ATTO for IBM FibreBridge 6500N)” on page 9

Support for the N3220 and N3240 system models

This release of Data ONTAP introduces support for the N3220 and N3240 system models.

Both the models use the same controller module:

- The N3220 model is 2U high and supports 24 SAS small-form-factor drives.
- The N3240 model is 4U high and supports 24 SATA large-form-factor drives.

Both the models support the following features:

- One or two controllers in a chassis
- Four Gigabit Ethernet ports per controller
- Two 6-Gb SAS ports per controller
- Optional mezzanine card with two Fibre Channel or two 10-Gb Ethernet ports
- One private management (ACP) port per controller
- One remote management port per controller
- Service Processor
- 6-GB main memory per controller
- Support for up to 24 internal disks
- Support for EXN1000*, EXN3000, EXN3500, and EXN4000*

  (* - requires Fibre Channel mezzanine card)

Support for SAS tape drives

Starting with Data ONTAP 8.1, SAS tape drives are supported.

Systems including EXN2000 storage expansion units with ESH2 modules

Beginning with Data ONTAP 8.1, IBM N series EXN2000 Storage Expansion Unit with ESH2 storage I/O modules are no longer supported. If even one of these devices is attached to your storage system, do not upgrade to Data ONTAP 8.1 or later until after you replace the devices.

Upgrading a system with these devices attached to it results in an unsupported system configuration and shelf configuration errors.

If you want to upgrade to Data ONTAP 8.1 or a later release and your storage environment includes the obsolete EXN2000 units with ESH2 devices, you should contact your IBM representative to discuss upgrading to IBM N series EXN3000 Storage Expansion Unit or IBM N series EXN3500 Storage Expansion Unit.

Support for FC/SAS bridge (ATTO for IBM FibreBridge 6500N)

Starting with Data ONTAP 8.1, the FC/SAS bridge (ATTO for IBM FibreBridge 6500N Feature Code 2100), which is a Fibre Channel-to-SAS bridge that allows SAS disk shelves (with SAS or SATA disk drives) to be used in stretch and fabric MetroCluster configurations, is supported.

Manageability enhancements

This Data ONTAP release provides additional management capabilities using MultiStore and other tools. This section provides an overview of these management capabilities.

Cache rewarming for Flash Cache modules

Starting in Data ONTAP 8.1, the WAFL external cache preserves the cache in a Flash Cache module during a graceful shutdown.

When a storage system powers down, the WAFL external cache takes a snapshot of the data in a Flash Cache module. When the system powers up, it uses the snapshot to rebuild the cache. After the process completes, the system can read data from the cache. This process, called cache rewarming, helps to maintain system performance after a planned shutdown. For example, you might shut down a system to add hardware or upgrade software.

Cache rewarming is enabled by default if you have a Flash Cache module installed. Cache rewarming is available when both nodes in an HA pair are running Data ONTAP 8.1.

For more information about cache rewarming, see the *Data ONTAP 7-Mode System Administration Guide*.

Reallocation scans, read reallocation, and extents with deduplicated volumes

Starting in Data ONTAP 8.1, you can use reallocation scans, read reallocation, and extents to improve the performance of deduplicated volumes.

You use the following command options with deduplicated volumes:

Reallocation scans
To rearrange the blocks that are shared between files by deduplication, use the -p option when you run the `reallocate start` command. Reallocation scans skip deduplicated data if you do not specify the `-p` option.

Read reallocation
To improve file layout and sequential read performance of a deduplicated volume, set the `read_realloc` option to `space_optimized` when you run the `vol options` command. Read reallocation skips deduplicated data if you set the `read_realloc` option to `on`.

Extents
To enable extents in a deduplicated volume, set the `extent` option to `space_optimized` when you run the `vol options` command. Extents skip deduplicated data if you set the `extent` option to `on`.

For more information about these features, see the *Data ONTAP 7-Mode System Administration Guide*.

System health monitoring

You can proactively manage your system by monitoring a single, integrated health status.

If the status is degraded, you can view details about the problem, including the probable cause and recommended recovery actions. After you resolve the problem, the system health status automatically returns to OK.

The system health status reflects multiple separate health monitors. A degraded status in an individual health monitor causes a degraded status for the overall system health.

Currently, there are two health monitors: an overall System Health Monitor and a Node Connectivity health monitor for the Storage subsystem.

For information about monitoring your system's health, see the *Data ONTAP 7-Mode System Administration Guide* and the man pages for the `system health` commands.

AutoSupport enhancements

Starting in Data ONTAP 8.1, AutoSupport messages contain more targeted data, are easier to manage, and offer better protocol and privacy support.

The content of AutoSupport messages is more focused and compact because of the following changes:

- The data sent in event-triggered AutoSupport messages is now specific to the trigger event.
- Many log files that are sent in AutoSupport messages now contain only new lines added since the last AutoSupport message.
- The content of each message is all compressed into a single file attachment in 7z file format.

Managing AutoSupport is easier in the following ways:

- You have more visibility into past messages and their content, as well as the content that will be sent in future messages.
- You can add more data to future messages sent in response to specific triggers, and you can control whether your internal support organization receives messages for specific triggers.
- If an AutoSupport message is not successfully transmitted, you can manually resend it.
- By default, the system collects AutoSupport information and stores it locally even if AutoSupport is disabled.

  Local collection of AutoSupport files provides valuable historical information that technical support staff can use to quickly solve future problems.

Protocol support for AutoSupport has improved in the following ways:

- IPv6 is supported.
- HTTPS certificates are validated.
- HTTP(S) uses PUT requests, enabling failed messages to restart from where they left off.
- Message size limits are available for HTTP(S) and SMTP.

Privacy is improved when you use the `autosupport.content minimal` option. Instead of omitting all private data, some private data is now masked and encoded. Also, by default, the message subject line contains the server's system ID instead of its host name.

For more information, see the *Data ONTAP 7-Mode System Administration Guide*.

Default 64-bit root aggregate for new systems

Starting with Data ONTAP 8.1, newly created aggregates are 64-bit by default, and new systems are shipped with the root volume in a 64-bit aggregate.

UPS management is no longer supported

As of Data ONTAP 8.1, uninterruptible power supply (UPS) management (by using the `ups` command) is no longer supported.

Changes to default aggregate Snapshot reserve for newly created nonmirrored aggregates

Beginning with Data ONTAP 8.1, a newly created nonmirrored aggregate has the aggregate Snapshot reserve set to 0 percent by default. A newly created mirrored aggregate continues to have the aggregate Snapshot reserve set to 5 percent by default.

For information about managing aggregate Snapshot copies and considerations for increasing the aggregate Snapshot reserve, see the *Data ONTAP 7-Mode System Administration Guide*.

IPv6 support for SP and RLM

The Data ONTAP 8.1 release family supports IPv6 for SP and RLM.

To send SP traffic over IPv6, you must be running SP version 1.2 or later, SP must be configured for IPv6, and the storage system must also have IPv6 enabled.

To send RLM traffic over IPv6, you must be running RLM version 4.0 or later, RLM must be configured for IPv6, and the storage system must also have IPv6 enabled.

Note: BMC supports IPv4 only.

Support for Transport Layer Security protocol

The Data ONTAP 8.1 release family supports Transport Layer Security (TLS) version 1.0, which provides better security protections than previous SSL versions did.

If you enable TLS on a storage system, you can use it with HTTPS, LDAP, and FTPS traffic, provided that other required Data ONTAP options for HTTPS, LDAP, and FTPS are also enabled.

TLS is disabled by default, and setting up SSL does not automatically enable TLS. For information about how to enable TLS, see the *Data ONTAP 7-Mode System Administration Guide*.

Licensing changes

Starting with Data ONTAP 8.1, you no longer need to add license keys on your system for most features that are distributed free of cost.

In addition, some features are now grouped together so that only one license key is required to add a pack of features to a system. Also, some features and products are enabled when you add certain other license keys.

For information about Data ONTAP 8.1 licensing models and whether a license key must be added for a particular feature or pack, see the *Data ONTAP 7-Mode System Administration Guide* and the man pages for the `license` commands or the Technote FAQ at the following link:

Using License Keys with Data ONTAP 8.1 7-Mode

Storage resource management enhancements

This Data ONTAP release provides improved performance, resiliency, and management capabilities for storage resources.

- "Enhancements to aggregates"
- "N6210 now supports 500 FlexVol volumes"
- "Limit on number of subdirectories has been removed"
- "Enhancements to FlexClone files and FlexClone LUNs"

Enhancements to aggregates

Data ONTAP 8.1 and later releases support several enhancements for aggregates.

Starting in Data ONTAP 8.1, aggregates support the following enhancements:

- The ability to nondisruptively expand 32-bit aggregates to the 64-bit format, without requiring data to be copied or moved.
- 64-bit aggregates are now the default aggregate format.
- SnapMirror relationship support between 64-bit and 32-bit aggregates.
- Maximum aggregate size increase for some platforms.

  To determine the maximum aggregate size for your platform, see the *IBM System Storage N series Introduction and Planning Guide*.

N6210 now supports 500 FlexVol volumes

In Data ONTAP 8.0, the N6210 supported only 200 volumes. In Data ONTAP 8.1 and later releases, the N6210 supports 500 FlexVol volumes.

Limit on number of subdirectories has been removed

In earlier versions of Data ONTAP, you could not create more than 99,998 subdirectories in any directory. In Data ONTAP 8.1 and later versions, there is no limit on the number of subdirectories you can create.

Enhancements to FlexClone files and FlexClone LUNs

Starting with Data ONTAP 8.1, you can create instantaneous clones of files and LUNs present in a FlexVol volume. In addition, you can create FlexClone files from Snapshot copies of parent files present in the FlexVol volume.

You can create a maximum of 32,767 FlexClone files or FlexClone LUNs from a parent file or LUN without creating a physical copy of the parent entity. If you try to create more than 32,767 clones, Data ONTAP automatically creates a new physical copy of the parent file or LUN.

For more information, see the *Data ONTAP 7-Mode Storage Management Guide*.

High-availability pair (formerly active/active configuration) enhancements

This Data ONTAP release includes new features and enhancements for high-availability. This section provides an overview of these features and enhancements.

For more information about these features, see the *Data ONTAP 7-Mode High-Availability Configuration Guide*.

- "MetroCluster system support for shared-switches configuration"

MetroCluster system support for shared-switches configuration

Beginning with Data ONTAP 8.1, MetroCluster system supports shared-switches configuration. In a shared-switches configuration, two fabric-attached MetroClusters systems share the same four switches and the ISLs between them.

For more information about the cabling and setting the ports in shared-switches configuration, see the *Data ONTAP 7-Mode High-Availability Configuration Guide*.

Networking and security protocol enhancements

This Data ONTAP release includes a number of new features and enhancements for networking and security protocol enhancements. This section provides an overview of these features and enhancements.

Support for IPv6

Starting with Data ONTAP 8.1, IPv6 addressing is supported. You can enable IPv6 on your storage system or on an HA pair and perform various tasks such as configuring network interfaces, VLANs, and interface groups. IPv6 is supported over the CIFS, NFS, HTTP, FTP protocols.

You can enable IPv6 on your storage system during setup. For more information, see the *Data ONTAP 7-Mode Software Setup Guide*.

You can also enable IPv6 on your storage system during operation by setting the `options ip.v6.enable` option to `on`. For more information, see the *Data ONTAP 7-Mode Network Management Guide*.

IPv6 features in Data ONTAP 8.1

The following IPv6 features are supported in Data ONTAP 8.1:

- IPv6 dual stack mechanism to enable communication over IPv4 and IPv6
- Neighbor Discovery that includes Router Discovery and Duplicate Address Detection
- IPv6 stateless address autoconfiguration, requiring minimal manual configuration of hosts
- Internet Control Message Protocol version 6 (ICMPv6)
- Path MTU discovery for IPv6
- Transmission of IPv6 packets over Ethernet links
- IPv6 static routes and router alert option
- Network administration commands, such as the `traceroute6`, `ping6`, `netdiag`, and `pktt` commands
- Telnet server to accept IPv6 connection requests
- Syslog for the IPv6-related events
- Host name and address resolution with DNS, DDNS, and NIS over IPv6
- Configuration of VLANs with IPv6 addresses
- Configuration of base VLAN interfaces with IPv6 addresses

- Network Time Protocol (NTP)
- Configuration of single-mode, static multimode, and dynamic multimode (LACP) vifs with IPv6 across multiple NICs
- SNMPv1, SNMPv2c, and SNMPv3
- MIB for TCP, UDP, ICMPv6, and IPv6
- HA configuration, which includes takeover and giveback of IPv6 addresses and routes, mapping partner IPv6 interfaces, and executing commands with IPv6 addresses in the partner context.

  For more information, see the *Data ONTAP 7-Mode High-Availability Configuration Guide*.
- IPv6 addresses in the vFiler commands. For more information, see the *Data ONTAP 7-Mode MultiStore Management Guide*.
- iSCSI over IPv6

  For more information, see the *Data ONTAP 7-Mode Block Access Management Guide for iSCSI and FC*.
- File access protocols—CIFS, FTP, HTTP, NFSv2, NFSv3, and NFSv4—over IPv6

  For more information, see the *Data ONTAP 7-Mode File Access and Protocols Management Guide*.
- LDAP and Kerberos version 5 with IPv6
- HTTPS over IPv6 addresses

  HTTPS can be used for secure administrative access; however SecureAdmin SSL must be enabled before you can issue HTTPS requests to the storage system.
- SSH protocol version 2 over IPv6

  If IPv6 is enabled on your storage system, SecureAdmin SSH must be enabled before you can issue SSH requests to the storage system.
- SNMP traphosts with IPv6 addresses.

  You should specify only IPv6 addresses, and not host names, to identify IPv6 traphosts
- Fast path over IPv6

  For more information, see the *Data ONTAP 7-Mode Network Management Guide*.
- RLM over IPv6

  If IPv6 is enabled on your storage system, then you must ensure that the RLM firmware version is 4.0 or later. Disabling IPv6 on Data ONTAP also disables IPv6 on the RLM.

  Note: You cannot use IPv6 to connect to the BMC.

For information about installing and updating the RLM firmware, see the *Data ONTAP 7- Mode Upgrade and Revert/Downgrade Guide*.

For information about configuring the RLM, see the *Data ONTAP 7-Mode System Administration Guide*.

- Hardware-assisted takeover over IPv6

  The `cf.hw_assist.enable` option should be set to on and RLM must be enabled.

  For more information about the hardware-assisted takeover, see the *Data ONTAP 7-Mode High-Availability Configuration Guide*.
- MetroCluster configurations
- RSH protocol over IPv6

  To connect to the storage system over the RSH protocol, you must ensure that the `rsh.enable` option and the `ip.v6.enable` option are set to on.
- `Dump`, `restore`, and `ndmpcopy` commands.

  For more information about the commands, see the *Data ONTAP 7-Mode Data Protection Tape Backup and Recovery Guide*.
- SnapMirror, SnapVault, and volume copy.

  For more information, see the *Data ONTAP 7-Mode Data Protection Online Backup and Recovery Guide*.

Improving TCP network congestion with Appropriate Byte Counting

Appropriate byte counting (ABC) is an algorithm implemented in the TCP stack of Data ONTAP that enables you to improve TCP performance and security. Starting from Data ONTAP 8.1, ABC is enabled by default on all the storage controllers.

File access protocol enhancements

This Data ONTAP release includes a number of new features and enhancements for file access and protocols management. This section provides an overview of these features and enhancements.

For more information about these features, see the *Data ONTAP 7-Mode File Access and Protocols Management Guide*.

- "Support for SFTP"
- "Support for SMB 2.0"
- "Support for FTPS"

Support for SFTP

Beginning in Data ONTAP 8.1, clients can use the Secure File Transfer Protocol (SFTP) to access files on the storage system.

For more information, see the *Data ONTAP 7-Mode File Access and Protocols Management Guide*.

Support for SMB 2.0

Beginning in Data ONTAP 8.1, clients can use the SMB 2.0 protocol to access files on the storage system.

For more information, see the *Data ONTAP 7-Mode File Access and Protocols Management Guide*.

Support for FTPS

Beginning in Data ONTAP 8.1, clients can use the FTP over SSL (FTPS) protocol to access files on the storage system.

For more information, see the *Data ONTAP 7-Mode File Access and Protocols Management Guide*.

Data protection enhancements

This Data ONTAP release includes a number of new features and enhancements for data protection enhancements. This section provides an overview of these features and enhancements.

For more information about these features, see the *Data ONTAP 7-Mode Data Protection Online Backup and Recovery Guide* and the *Data ONTAP 7-Mode Data Protection Tape Backup and Recovery Guide*.

Support for volume SnapMirror replication between 32-bit and 64-bit volumes

Starting with Data ONTAP 8.1, you can replicate volumes by using SnapMirror between 32-bit and 64-bit volumes. For both synchronous and asynchronous volume replication, the SnapMirror source and destination volumes can be either 32-bit or 64-bit.

Changes to default FlexVol volume Snapshot reserve value

Starting with Data ONTAP 8.1, a newly created FlexVol volume has the Snapshot reserve set to 5 percent by default. However, the default Snapshot reserve for a traditional volume remains 20 percent.

Support for concurrent volume SnapMirror and SMTape backup operations

Starting with Data ONTAP 8.1, you can make an SMTape backup of a volume SnapMirror destination when SnapMirror transfers are in progress. You can run volume SnapMirror and SMTape backup operations concurrently by enabling the `vsm.smtape.concurrent.cascade.support` option on a volume SnapMirror destination system.

For more information, see the *Data ONTAP 7-Mode Data Protection Tape Backup and Recovery Guide*.

Protection of data at rest through Storage Encryption

Data ONTAP 8.1 7-Mode introduces the new Storage Encryption feature that allows you to protect your data at rest by automatically encrypting all data written to disk. The feature is available on certain supported storage controllers and disk shelves that contain disks with built-in encryption functionality.

For detailed information about feature requirements, configuration, and management, see the *Data ONTAP 7-Mode Software Setup Guide* and the Data *ONTAP 7-Mode Storage Management Guide*.

Support for SnapLock

Data ONTAP 8.1 7-Mode supports SnapLock feature. Several significant improvements are made to the SnapLock feature in this release.

Following are the key enhancements:

- System ComplianceClock
- Volume ComplianceClock
- Volume-level autocommit

For more information about these enhancements, see the *Data ONTAP 7-Mode Archive and Compliance Management Guide*.

Storage efficiency enhancements

This Data ONTAP release includes a number of new features and enhancements for storage efficiency enhancements. This section provides an overview of these features and enhancements.

- "Changes to deduplication"
- "Changes to data compression" on page 24

Changes to deduplication

Starting with Data ONTAP 8.1, you can enable the deduplication feature without adding a license. For deduplication, no limit is imposed on the supported maximum volume size. The maximum volume size limit is determined by the type of storage system regardless of whether deduplication is enabled.

For each FlexVol volume, two copies of the fingerprint database are maintained, where one copy of the database resides in the FlexVol volume and the other copy in the aggregate.

For more information about deduplication, see the *Data ONTAP 7-Mode Storage Management Guide*.

Changes to data compression

Starting with Data ONTAP 8.1, data compression is supported on SnapLock volumes and in stretch and fabric-attached MetroCluster configurations. For compression, no limit is imposed on the supported maximum volume size. The maximum volume size limit is determined by the type of storage system regardless of whether compression is enabled.

For more information about SnapLock, see the *Data ONTAP 7-Mode Archive and Compliance Management Guide* and for MetroCluster configurations, see the *Data ONTAP 7-Mode High-Availability Configuration Guide*.

MultiStore enhancements

This Data ONTAP release includes a number of new features and MultiStore enhancements.

- "Online migration support for vFiler units"
- "Interactive SSH support for vFiler units" on page 26
- "Data compression support on vFiler units" on page 27

Online migration support for vFiler units

Starting with Data ONTAP 8.1, you can perform online migration of vFiler units (also called Data Motion for vFiler) from one storage system to another without experiencing any disruption in data availability. You must be aware of the storage system models and disks that support online migration of vFiler units.

You must use the N series Management Console provisioning capability interface to perform online migration of vFiler units.

For more information about online migration, see the *OnCommand Provisioning and Data Protection Management Guide to Common Workflows for Administrators* and the *OnCommand Provisioning and Data Protection Management Printable Help*.

Supported storage systems

- High-end storage systems, such as N7000 series and N7x50T
- Mid-range storage systems, such as N5000 series, N6000, and N6200 series
- Low-end storage systems, such as N3220, N3240, and N3400

  Note: The gateway systems are not supported for online migration of vFiler units.

Table 1. Supported source and destination storage systems with number of volumes for migration

Source storage system	Destination storage system	Number of volumes for migration
• N7x50T • N7000 series	• N7x50T • N7000 series	20
Note: If the source or destination storage system is either N7600 or N7700, then you can migrate only 8 volumes.		
• N7x50T • N7000 series	• N6200 series • N6000 series • N5000 series	8

Table 1. Supported source and destination storage systems with number of volumes for migration (continued)

Source storage system	Destination storage system	Number of volumes for migration
• N6200 series • N6000 series • N5000 series	• N7x50T • N7000 series • N6200 series • N6000 series • N5000 series	8
• N3220 • N3240 • N3400	• N7x50T • N7000 series • N6200 series • N6000 series • N5000 series • N3220 • N3240 • N3400 series	4

Note: You cannot perform online migration of vFiler units when the source storage system is a high-end system or a mid-range system and the destination storage system is a low-end system.

Supported disk types

- FC
- SATA
- SAS
- BSAS

Interactive SSH support for vFiler units

Starting with Data ONTAP 8.1, you can establish interactive SSH sessions with vFiler units. A vFiler unit can have only one active interactive SSH session established at a time. You can also use IPv6 addresses to establish interactive SSH sessions.

Depending on the number of vFiler units allowed on that storage system, there are limits on the number of concurrent interactive SSH sessions that you can run on a storage system.

For more information about limits on the number of interactive SSH sessions, see the *Data ONTAP 7-Mode MultiStore Management Guide*.

Data compression support on vFiler units

Starting with Data ONTAP 8.1, data compression is supported on vFiler units. You can perform data compression operations from the CLI of all vFiler units, in addition to the CLI of vfiler0.

For more information, see the *Data ONTAP 7-Mode MultiStore Management Guide*.

New and changed features in the Data ONTAP 8.0 7-Mode release family

This section covers features that were added or changed in the Data ONTAP 8.0 7-Mode release family. If you are upgrading to Data ONTAP 8.1 or later from a 7.3.x release, these changes will apply to your system in addition to those introduced in the 8.1 release family.

Note: Some new and changed features in this release might also be introduced in a maintenance release of an earlier 7G release family. Before upgrading, be sure to consult with your IBM representative about new Data ONTAP functionality to determine the best solution for your business needs.

Data ONTAP 8.0 7-Mode and later Data ONTAP 8.0.x 7-Mode releases provide a new aggregate type, 64-bit aggregates, with a larger maximum aggregate and FlexVol sizes, as well as improved performance, resiliency, and management capabilities for storage resources.

For more information about 64-bit aggregates, see "Support for 64-bit aggregates" on page 37.

Data ONTAP 8.0 7-Mode and later Data ONTAP 8.0.x 7-Mode releases also provide new platform and hardware support as described in "New and changed platform and hardware support" on page 30, additional management capabilities such as SSL security improvements, additional capabilities using iSCSI and FC protocols for N series SAN environments, and enhanced data protection technologies such as SnapMirror and SnapVault.

Additional major changes made in the Data ONTAP 8.0 7-Mode release family are described as follows:

New and changed platform and hardware support

This Data ONTAP release supports new and changed hardware as listed and this section provides an overview of the new and changed hardware.

For information about supported systems, see "Supported systems" on page 73.

Support for N6200 series

Data ONTAP 8.0.1 and later Data ONTAP releases support the N6200 series.

The N6200 series supports the following features:

- One or two controllers in a chassis One-controller systems can be configured with a filler blank or an I/O expansion module, which provides four full-length PCIe slots.
- Two Gigabit Ethernet ports per controller
- Two HA ports per controller
- Two 3-Gb or 6-Gb SAS ports per controller
- Two 4-Gb Fibre Channel ports per controller
- One USB port per controller
- One private management (ACP) port per controller
- One remote management port per controller
- One full-length PCIe slot and one 3/4-length PCIe slot per controller
- Service Processor
- 4 GB, 8 GB, or 16 GB main memory per controller
- Support for EXN1000, EXN2000, EXN3000, EXN3500, and EXN4000 storage expansion units

- Maximum FlexVol volumes supported: N6210: 200; N6240 and N6270: 500
- Two on-board 10-GbE ports that are not available for configuration

Support for N7x50T

Data ONTAP 8.0.1 and later Data ONTAP releases support the N7x50T series.

The N7x50T has a large slot count and you can use as many Flash Cache cards, network adapters, and storage adapters as the solution requires with slots to spare.

Additionally, the N7x50T has faster DDR3 memory and a significant increase in the amount of memory. Available memory per controller is 96 GB.

It includes the following architectural features:

- PCIe v2.0 (Gen 2) x8 architecture
- Latest 64-bit processing architecture
- High-performance onboard 10-GbE and 8-Gb FC ports
  - 4 onboard 10-GbE ports with stateless offload per controller
  - 4 onboard 8/4/2-Gb FC ports configurable as targets or initiators per controller
- Reliability, availability, serviceability, and manageability (RASM) improvements
  - Persistent write log destages NVRAM to CompactFlash to safely protect write data not yet committed to disk during extended outages.
  - Service Processor (SP), the next-generation RLM technology, adds more RASM features and capabilities.
- I/O expansion module (IOXM)
  - Provides 10 additional slots to those in the controller
  - Provides configuration flexibility for HA solutions in 6U and 12U footprints

Support for 1-TB Flash Cache modules

Data ONTAP 8.0.2 and later releases support the 1-TB PCI-e-attached Flash Cache module that uses Flash technology.

The addition of Flash Cache optimizes the performance of random read-intensive workloads such as file services, messaging, virtual infrastructure, and OLTP databases without using more high performance disk drives.

For more information about Flash Cache modules supported with your storage system models, see the *IBM System Storage N series Introduction and Planning Guide*.

Support for 512-GB and 256-GB Performance Acceleration Module (PAM II)

Data ONTAP 8.0.1 7-Mode and later Data ONTAP 8.0.x 7-Mode releases support a PCIe-attached Performance Acceleration Module (PAM II also known as Flash Cache module) that uses Flash technology.

The addition of PAM II optimizes the performance of random read-intensive workloads such as file services, messaging, virtual infrastructure, and OLTP databases without using more high-performance disk drives.

For more information about PAM II modules supported with your storage system models, see *IBM System Storage N series Introduction and Planning Guide*.

Support for SSDs

Data ONTAP 8.0.1 7-Mode and later Data ONTAP 8.0.x releases support solid-state disks (SSDs). SSDs are flash memory-based storage devices that provide better overall performance than hard disk drives, or HDDs, which are mechanical devices using rotating media.

For more information about SSDs, see the *Data ONTAP 7-Mode Storage Management Guide*. For information about which storage system models support SSDs, see *IBM System Storage N series Introduction and Planning Guide*.

Supported tape drives

Data ONTAP 8.0.1 and later releases support Quantum LTO-4, Quantum LTO-5, Hewlett-Packard LTO-4, Hewlett-Packard LTO-5, and IBM LTO-5 tape drives.

Support for 3-TB SATA disks

In Data ONTAP 8.0.2 and later releases, 3-TB SATA disks are supported for the SAS disk connection type.

Support for 2-TB SATA disks

In Data ONTAP 8.0 and later releases, 2-TB SATA disks are supported for both the SAS and FC disk connection types. With these larger disks and 64-bit aggregates, you can create larger aggregates before being affected by spindle and aggregate size limits.

For more information about 64-bit aggregates, see "Support for 64-bit aggregates" on page 37.

Changes in storage expansion unit support

The Data ONTAP 8.0 7-Mode release includes a number of new features and enhancements for storage expansion unit support.

- "Support for EXN3500 storage expansion units"
- "Support for EXN3000 storage expansion units"

Support for EXN3500 storage expansion units

In Data ONTAP 8.0 7-Mode and later releases, Data ONTAP supports the EXN3500 storage expansion unit. The EXN3500 storage expansion unit contains external SAS disk drives and 6-Gb I/O modules.

EXN3500 storage expansion units are also supported on the following Data ONTAP 8.*x* and 7.*x* releases:

- Data ONTAP 8.*x* releases: Data ONTAP 8.0P1 or later, except N3400 storage systems, 8.0.1 or later.
- Data ONTAP 7.*x* releases: Data ONTAP 7.3.3P2 or later, except N3400 and N3600 storage systems, 7.3.4 or later.

For more information about which disk drives and storage system models are supported with the EXN3500 storage expansion unit, see the *IBM System Storage N series Introduction and Planning Guide*. For more information about the EXN3500 storage expansion unit, see the *EXN3500 Storage Expansion Unit Installation and Service Guide*.

Support for EXN3000 storage expansion units

Data ONTAP 8.0P1 and later releases support EXN3000 storage expansion units.

The EXN3000 storage expansion unit contains external SAS disk drives and 3-Gb I/O modules. The EXN3000 storage expansion unit is also supported on Data ONTAP 7.3.3P2 and later releases.

For more information about which disk drives and storage system models are supported with the EXN3000 storage expansion unit, see the *IBM System Storage N series Introduction and Planning Guide*. For more information about the EXN3000 storage expansion unit, see the *EXN3000 Storage Expansion Unit Installation and Service Guide*.

Manageability enhancements

You can find information about the new and changed manageability capabilities.

- "Reversion and downgrade support" on page 34
- "The default security settings" on page 34

Reversion and downgrade support

Beginning in Data ONTAP 8.0.2 7-Mode, you can revert to a Data ONTAP release in an earlier release family or downgrade to an earlier Data ONTAP release in the same family. You can perform these operations without assistance from technical support when transitioning new or test systems to earlier releases.

However, you must call technical support if you have problems during or after upgrading. If you need to transition to an earlier release, see the *Data ONTAP 8.0 7-Mode Upgrade and Revert/Downgrade Guide* to help determine the correct action in your environment.

The default security settings

On storage systems shipped with Data ONTAP 8.0 7-Mode or later, secure protocols are enabled and nonsecure protocols are disabled by default.

SecureAdmin is set up automatically on storage systems shipped with Data ONTAP 8.0 7-Mode or later. For these systems, the following are the default security settings:

- Secure protocols (including SSH, SSL, and HTTPS) are enabled by default.
- Nonsecure protocols (including RSH, Telnet, FTP, and HTTP) are disabled by default.

On storage systems shipped with Data ONTAP 8.0 7-Mode or later, the following are the default option settings for SSH and SSL:

- `options ssh.enable on`
- `options ssh2.enable on`
- `options ssh1.enable off`
- `options ssh.passwd_auth.enable on`
- `options ssh.pubkey_auth.enable on`
- `options httpd.admin.ssl.enable on`

Also on storage systems shipped with Data ONTAP 8.0 7-Mode or later, the following are the default option settings for the nonsecure protocols:

- `options ftpd.enable off`
- `options httpd.admin.enable off`
- `options httpd.enable off`

- `options rsh.enable off`
- `options telnet.distinct.enable on`
- `options telnet.enable off`

Note: These default settings apply only to storage systems shipped with Data ONTAP 8.0 7-Mode or later. For storage systems upgraded from an earlier version to Data ONTAP 8.0 release family, the above default settings do not apply. Instead, for those upgraded systems, the settings remain unchanged after the upgrade. Also, if you make security setting modifications after upgrading to Data ONTAP 8.0 release family or later, the modifications are preserved even if the system reverts back to the previous Data ONTAP version.

For more information about the default security settings, see the *Data ONTAP 8.0 7-Mode System Administration Guide*.

Setup for root account password

During the initial setup of a storage system shipped with Data ONTAP 8.0 7-Mode or later, you are prompted to set up a password for the root account.

The following are the default password rules for all accounts when `security.passwd.rules.enable` is set to `on` (the default):

- The password must be at least eight characters long.
- The password must contain at least one number.
- The password must contain at least two alphabetic characters.

Note: Subsequent invocations of the `setup` command do not prompt you to set up a password for the root account.

For more information about setting up the storage system, see the *Data ONTAP 8.0 7-Mode Software Setup Guide*.

Uses of the systemshell and the diagnostic account

A diagnostic account, named "diag," is provided with your storage system running Data ONTAP 8.0 or later. You can use the diagnostic account to perform troubleshooting tasks in the systemshell. The diagnostic account and the systemshell are intended only for low-level diagnostic purposes and should be used only with guidance from technical support.

The diagnostic account is the only account that can be used to access the systemshell, through the advanced command `systemshell`. The diagnostic account is disabled by default. You must enable the account and set up its password before using it. Neither the diagnostic account nor the systemshell is intended for general administrative purposes.

Boot menu enhancements and changes

Starting with Data ONTAP 8.0, the boot menu includes menu options that allow you to restore the configuration information from the root volume to the boot device, to install new software, or to reboot the storage system.

Data ONTAP 8.0 7-Mode and later releases allow you to create a new root FlexVol volume but not a new traditional root volume from the boot menu. However, preexisting traditional root volumes are still supported.

For information about the boot menu, see the na_floppyboot(1) man page and the *Data ONTAP 8.0 7-Mode System Administration Guide*.

Supported OpenSSH client versions

Data ONTAP 8.0.2 7-Mode and later releases support OpenSSH client version 4.4p1 only. To enhance security, OpenSSH client version 3.8p1 is no longer supported because it does not contain the latest security fix.

Root aggregate Snapshot reserve values reduced

The root aggregate and root volume Snapshot reserve values for new storage systems have been reduced starting with Data ONTAP 8.0.1.

To increase the amount of usable space on the storage system while still retaining all the benefits of volume Snapshot copies, IBM ships all new systems running Data ONTAP 8.0.1 or later with the following new Snapshot reserve values:

- Snapshot reserve for the root aggregate is set to 0%.

  The previous value was 5%.
- Snapshot reserve for the root volume is set to 5%.

  The previous value was 20%.

Existing systems, and systems configured at the factory to run MetroCluster, are not affected by this change.

Attention: If you later configure MetroCluster, or use RAID SyncMirror or the aggregate copy capability on the root aggregate, the root aggregate Snapshot reserve *must* be increased to 5% by using the `snap reserve` command.

For more information about using the `snap reserve` command, see the na_snap(1) man page.

Storage resource management enhancements

This Data ONTAP release provides improved performance, resiliency, and management capabilities for storage resources.

Support for 64-bit aggregates

In Data ONTAP 8.0 7-Mode and later releases, Data ONTAP supports a new type of aggregate, the 64-bit aggregate. 64-bit aggregates have a larger maximum size than aggregates created with earlier versions of Data ONTAP. In addition, volumes contained by 64-bit aggregates have a larger maximum size than volumes contained by aggregates created with earlier versions of Data ONTAP.

The maximum size of a 64-bit aggregate and the volumes it contains depends on the model of your storage system. To determine the maximum 64-bit aggregate size for your storage system model, see the *IBM System Storage N series Introduction and Planning Guide*. The maximum size of a volume contained by a 64-bit aggregate corresponds to the maximum size of its containing aggregate.

The maximum size for legacy aggregates, now called 32-bit aggregates, remains 16 TB.

For more information, see the *Data ONTAP 8.0 7-Mode Storage Management Guide* and the na_aggr(1) man page.

Data compression support

Starting with Data ONTAP 8.0.1, you can compress data within a FlexVol volume using the data compression technology. You can use data compression only on FlexVol volumes that are created on 64-bit aggregates on primary, secondary, and tertiary storage tiers.

After you enable data compression on a FlexVol volume, all subsequent writes to the volume are compressed inline. However, existing data remains uncompressed. You can use the data compression scanner to compress the existing data.

File space utilization report

The file space utilization report enables you to see the files and the amount of space that they occupy in a deduplicated volume. You can choose to either move or delete the files to reclaim the space.

This report provides a view of the total number of blocks in a file and the number of blocks that are shared by non-deduplicated or non-cloned files.

Note: Total blocks refer to the number of blocks in a file, including blocks that are required for storing the file metadata.

Upgrading to Data ONTAP 8.0.1 increases volume capacity after deduplication

After you upgrade to Data ONTAP 8.0.1 and later from an earlier release of Data ONTAP, you can increase the deduplicated volume size up to 16 TB for all platform models that support Data ONTAP 8.0.1.

Maximum simultaneous FlexClone file or FlexClone LUN operations per storage system

Starting in Data ONTAP 8.0 7-Mode and later, you can simultaneously run a maximum of 500 FlexClone file or FlexClone LUN operations on a storage system.

For more information about FlexClone files and FlexClone LUNs, see the *Data ONTAP 8.0 7-Mode Storage Management Guide*.

Support for FlexClone files and FlexClone LUNs on vFiler units

Starting in Data ONTAP 7.3.3 and later releases of the 7.0.*x* release family, and in Data ONTAP 8.0.1 and later, the FlexClone files and FlexClone LUNs commands are available in both the default and non-default vFiler contexts.

You can use the FlexClone files and FlexClone LUNs feature to create writable, space-efficient clones of parent files and parent LUNs within a vFiler unit. Storage owned by a vFiler unit cannot be accessed or discovered from other vFiler units by using the FlexClone file or FlexClone LUN commands.

For more information about FlexClone files and FlexClone LUNs, see the *Data ONTAP 8.0 7-Mode Storage Management Guide*.

Increased maximum RAID group size for SATA disks

Starting in Data ONTAP 8.0.1, the maximum RAID group size allowed for ATA, BSAS, and SATA disks has increased from 16 to 20 disks. The default size remains the same, at 14 disks.

Ability to decrease maxfiles

Starting in Data ONTAP 8.0, you can decrease the value of the maxfiles parameter for a volume, as long as you do not decrease it below the current number of files stored in the volume.

In previous versions of Data ONTAP, you could increase the value of the maxfiles parameter, but not decrease it.

High-availability pair (formerly active/active configuration) enhancements

You can find information about the new features and HA pair enhancements.

For more information about these features, see the *Data ONTAP 8.0 7-Mode High-Availability Configuration Guide*.

- "High-availability pair terminology changes"

High-availability pair terminology changes

The high-availability (HA) functionality referred to as an HA pair in Data ONTAP 8.0 was called an active/active configuration in the Data ONTAP 7.2 and 7.3 release families. In the Data ONTAP 7.1 release family and earlier releases, an HA pair was called a cluster. HA functionality is a distinct, separate feature from Data ONTAP 8.0 Cluster-Mode clustering. For more information about these features, see the *Data ONTAP 8.0 7-Mode High-Availability Configuration Guide*.

Networking and security protocols enhancements

This Data ONTAP release includes a number of new features and enhancements for networking and security protocol enhancements. This section provides an overview of these features and enhancements.

For more information about these features, see the *Data ONTAP 8.0 7-Mode Network Management Guide*.

- "Ability to block data traffic on the e0M interface" on page 40
- "Support for the SMB 2.0 protocol" on page 40
- "Support for CDP" on page 41
- "Port-based load-balancing option for multimode interface groups" on page 41
- "TSO in NICs" on page 41

Ability to block data traffic on the e0M interface

In Data ONTAP 8.0.2 and later releases, you can block certain types of traffic from the e0M interface, including SnapMirror transfers, SnapVault transfers, and data transfers using the CIFS, NFS, and NDMP protocols. This feature allows you to optimize system performance.

Data ONTAP 8.0.2 introduces a new option `interface.blocked.mgmt_data_traffic` to control the blocking of data transfer on the e0M interface. New systems that ship with Data ONTAP 8.0.2 and later releases have the default value of this option set to `on`, which prevents data transfer on the e0M interface. Systems upgraded to Data ONTAP 8.0.2 and later releases have the default value of the option set to `off`, which allows data transfer on the e0M interface.

Note: Data transfer using the iSCSI protocol is always blocked on systems upgraded to Data ONTAP 8.0 and later, and the data transfer is not affected by the option `interface.blocked.mgmt_data_traffic` setting.

The e0M port is a low-bandwidth interface that should be used only for management traffic using SSH and other management protocols. Configuring e0M to serve data traffic can cause performance degradation and routing problems. Therefore, e0M should be configured on a dedicated management LAN or it should be configured down. If an e0M interface is serving management traffic, it should be partnered with another e0M interface.

It is a best practice to set the option `interface.blocked.mgmt_data_traffic` to `on`, and to use the e0M interface only for management traffic. For more information about the e0M interface, see the *Data ONTAP 8.0 7-Mode System Administration Guide*.

Note: Blocking of data traffic on e0M is not supported over IPv6.

Support for the SMB 2.0 protocol

Data ONTAP 8.0.1 and later support the SMB 2.0 protocol, which is more suitable than the original SMB protocol in environments requiring an increased level of scalability and data integrity.

For more information, see the *Data ONTAP 8.0 7-Mode File Access and Protocols Management Guide*.

Support for CDP

Cisco Discovery Protocol (CDP) is supported in Data ONTAP 7.3.3 and later releases of the 7.x release family, and in Data ONTAP 8.0.1 and later. CDP enables you to automatically discover and view information about directly connected CDP-enabled devices in a network.

For more information about CDP, see the *Data ONTAP 8.0 7-Mode Network Management Guide*.

Port-based load-balancing option for multimode interface groups

Port-based load balancing is supported for multimode interface groups in Data ONTAP 7.3.2 and later releases of the 7.x release family, and in Data ONTAP 8.0.1 and later. On a multimode interface group, you can uniformly distribute outgoing traffic based on the transport layer (TCP or UDP) ports and network layer addresses (IPv4 or IPv6) by using the port-based load-balancing method.

The port-based load-balancing method uses a fast hashing algorithm on the source and destination IP addresses along with the transport layer (TCP or UDP) port number.

For more information about port-based load balancing, see the *Data ONTAP 8.0 7-Mode Network Management Guide*

TSO in NICs

TCP segmentation offload (TSO) is a hardware feature supported on NICs to increase the host CPU's efficiency.

Starting in Data ONTAP 8.0.1 and later, the network interface cards that support TSO are as follows:

- Dual 10G Ethernet Controller T320E-SFP+ and T320-XFP
- 10 Gigabit Ethernet Controller IX1-SFP+

Starting in Data ONTAP 8.0.2, the following network interface card also supports TSO:

- Dual 10G Ethernet Controller CNA-SFP+

For more information about TSO and the statistics displayed by the NICs, see the *Data ONTAP 8.0 7-Mode Network Management Guide*.

64-bit SNMP object identifiers (OIDs) are supported

In Data ONTAP 7.2 and 7.3 release families, some OIDs in the `netapp.mib` file have low and high 32-bit values. In Data ONTAP 8.0 7-Mode and later, these OIDs are replaced with 64-bit values. You should use SNMPv2 or SNMPv3 to query your storage system by using the 64-bit OIDs.

For example, the miscHighNfsOps and miscLowNfsOps OIDs have been replaced with the 64-bit OID misc64NfsOps. In the netapp.mib file, miscHighNfsOps and miscLowNfsOps are marked as deprecated.

Configuration for receiving untagged traffic on VLAN tagged interfaces

In Data ONTAP 8.0 7-Mode and later, you can configure an IP address for a network interface with VLANs. Any untagged traffic goes to the base interface, and the tagged traffic goes to the respective VLAN.

For more information about this feature, see the *Data ONTAP 8.0 7-Mode Network Management Guide*.

For information about reverting with a configuration for receiving tagged and untagged frames on the same network interface, see the *Data ONTAP 8.0 7-Mode Upgrade and Revert/Downgrade Guide*.

Vifs are now known as interface groups

Starting with Data ONTAP 8.0 7-Mode and later, vifs are known as interface groups. An interface group refers to a single virtual interface that is created by grouping together multiple physical interfaces. In the Data ONTAP 7.2 and 7.3 release families, this functionality is referred to as a vif.

You can use the ifgrp command to create and configure interface groups. For more information about interface groups and the ifgrp command, see the *Data ONTAP 8.0 7-Mode Network Management Guide*.

File access protocol enhancements

This Data ONTAP release includes a number of new features and enhancements for file access and protocols management. This section provides an overview of these features and enhancements.

For more detailed information about these features, see the *Data ONTAP 8.0 7-Mode File Access and Protocols Management Guide*.

- "Support for multiple open instances of the SMB named pipe on an FPolicy server"

Support for multiple open instances of the SMB named pipe on an FPolicy server

In Data ONTAP 8.0 7-Mode, you can enable multiple open instances of the SMB named pipe on an FPolicy server by using the fpolicy.multiple_pipes option.

For more information, see the *Data ONTAP 8.0 7-Mode File Access and Protocols Management Guide*.

Block protocols enhancements

This Data ONTAP release includes a number of new features and enhancements for block protocol enhancements. This section provides an overview of these features and enhancements.

For more information about these features, see the *IBM System Storage N series Data ONTAP 8.0 7-Mode Block Access Management Guide*.

10-GbE Unified Target Adapter protocol support

The current 10-GbE Unified Target Adapters (UTA) provide additional protocol options for SAN and NAS connectivity by extending support to IP storage.

With Data ONTAP 8.0.1, the UTAs add support for the iSCSI, NFS, and CIFS protocols and continue to support the FCoE protocol.

The 10-GbE UTAs are still offered in two versions:

- Optical - part number FC 1063
- Copper - part number FC 1064

iSCSI RADIUS support

Data ONTAP 8.0 7-Mode introduces support for iSCSI RADIUS, which allows you to centrally manage iSCSI initiator authentication.

RADIUS still uses CHAP to authenticate iSCSI initiators, but it allows you to manage the authentication process from a central RADIUS server, rather than manage them manually on each storage system. In larger SAN environments, this can greatly simplify iSCSI initiator management and provide added security.

In addition to simplifying CHAP password management, RADIUS also reduces the load on your storage system. The RADIUS client service runs on the storage system and communicates with the RADIUS server and initiators, but most of the authentication processing is handled by the RADIUS server.

For more information, see to the *Data ONTAP 8.0 7-Mode Block Access Management Guide for iSCSI and FC*.

Support for Data Motion for Volumes

Data ONTAP 8.0.1 7-Mode or later supports Data Motion for Volumes, which enables you to nondisruptively move a volume from one aggregate to another within the same controller to satisfy service-level agreements and capacity utilization and improved performance. In a SAN environment, FlexVol volumes and the LUNs in the volumes are moved nondisruptively from one aggregate to another.

The volume move occurs in three phases: setup phase, data copy phase, and cutover phase.

For more information about the volume move, see *Data ONTAP 8.0 7-Mode Block Access Management Guide for iSCSI and FC*.

VMware VAAI features for ESX hosts support

Data ONTAP 8.0.1 and later supports certain VMware vStorage APIs for Array Integration (VAAI) features when the ESX host is running ESX 4.1 or later. These features help offload operations from the ESX host to the storage system and increase the network throughput.

The ESX host enables the features automatically in the correct environment. You can determine the extent to which your system is using the VAAI features by checking the statistics contained in the VAAI counters.

For more information about the VMware VAAI features for ESX hosts, see *Data ONTAP 8.0 7-Mode Block Access Management Guide for iSCSI and FC*.

igroup scalability limits

Data ONTAP 8.0.1 introduces support to expand the host side scalability by expanding the number of igroups supported on N6000 series and N7000 series systems from 512 per controller to 1024 per controller.

Data protection enhancements

This Data ONTAP release includes a number of new features and enhancements for data protection enhancements. This section provides an overview of these features and enhancements.

For more information about these features, see the *Data ONTAP 8.0 7-Mode Data Protection Online Backup and Recovery Guide* and the *Data ONTAP 8.0 7-Mode Data Protection Tape Backup and Recovery Guide*.

- "SnapVault update schedules for volume SnapMirror destination backups" on page 45
- "Support for 840 disk drives on fabric-attached MetroCluster configuration" on page 45

SnapVault update schedules for volume SnapMirror destination backups

When backing up a volume SnapMirror destination using SnapVault in Data ONTAP 8.0.2, the `snapvault.snapshot_for_dr_backup` option allows you to choose the SnapVault behavior for updating the destination system.

You can set the following values for the `snapvault.snapshot_for_dr_backup` option:

- `named_snapshot_only`: Schedules the SnapVault updates from the most recent Snapshot copy with the scheduled base name for scheduled backup.
- `named_snapshot_preferred`: Schedules the SnapVault updates from the most recent Snapshot copy created by volume SnapMirror if the scheduled Snapshot copy is not available.
- `vsm_base_only`: Schedules the SnapVault updates from the most recent Snapshot copy created by volume SnapMirror. This is the default value.

In Data ONTAP 8.0 and Data ONTAP 8.0.1 7-Mode, SnapVault uses a named Snapshot copy and not the Snapshot copy created by volume SnapMirror to update the destination system.

Support for 840 disk drives on fabric-attached MetroCluster configuration

In Data ONTAP 7.3.5 and later releases of 7.x release family, and Data ONTAP 8.0.1 7-Mode and later releases of 8.x release family, fabric-attached MetroCluster configurations can support up to 840 disk drives.

For more information, see the *Data ONTAP 8.0 7-Mode High-Availability Configuration Guide*.

Support for out-of-order frame delivery for SnapMirror over Fibre Channel

Data ONTAP 8.0.1 and later support out-of-order frame delivery for SnapMirror over Fibre Channel.

When enabled, out-of-order frame delivery for SnapMirror over Fibre Channel eliminates the requirement to deliver all the frames in the same sequence in which the frames were transmitted. This feature ensures the uninterrupted SnapMirror transfers regardless of the order in which the frames are delivered.

For more information about out-of-order frame delivery, see *Data ONTAP 8.0 7-Mode Data Protection Online Backup and Recovery Guide*.

Support for SnapMirror relationship between two FlexClone volumes

Data ONTAP 8.0.1 and later support SnapMirror relationship between two FlexClone volumes.

The SnapMirror relationship between two FlexClone volumes that have a common base Snapshot copy can be established without transferring the common Snapshot data again to the destination system.

For more information about SnapMirror relationship between two FlexClone volumes, see *Data ONTAP 8.0 7-Mode Data Protection Online Backup and Recovery Guide*.

Support for SnapMirror network compression

Data ONTAP 7.3.2 and later releases of the 7.*x* release family, and Data ONTAP 8.0.1 and later releases of the 8.x release family support SnapMirror network compression. This feature is supported only for asynchronous volume SnapMirror.

Note: The SnapMirror destination system should be using a Data ONTAP release that supports SnapMirror network compression.

The SnapMirror network compression feature compresses the data stream on the source system, transfers the compressed data stream over the network, and uncompresses the data stream on the destination system before writing it to disk. It helps in optimizing network bandwidth utilization between SnapMirror source and destination systems. This feature can be especially useful for connections that have relatively low bandwidth, such as WAN connections.

For more information about SnapMirror network compression, see the *Data ONTAP 8.0 7-Mode Data Protection Online Backup and Recovery Guide*.

Support for designated range of ports for NDMP data connections

Data ONTAP 8.0.1 and later releases support designated range of ports that can be used for NDMP data connections in response to NDMP_DATA_LISTEN and NDMP_MOVER_LISTEN operations. Therefore, you can perform data migration by using the `ndmpcopy` command and three-way tape backups even in environments where the source and destination networks are separated by a firewall.

If volumes with deduplication exceed the maximum supported size

Volumes continue to be online when they exceed the maximum supported size. For more information about the maximum volume size allowed for different storage systems, with and without deduplication, see the *Data ONTAP 8.0 7-Mode Data Protection Online Backup and Recovery Guide*.

Nearline license is not required for deduplication

Starting with Data ONTAP 8.0.1 7-Mode, you do not have to enable the Nearline personality license to use deduplication.

Maximum concurrent deduplication operations supported

You can run a maximum of eight concurrent deduplication operations on all storage systems.

Prerequisite for backing up data to tape using NDMP services

Starting from Data ONTAP 8.0 7-Mode, NDMP users must have the login-ndmp capability for successfully authenticating NDMP sessions.

A predefined role named backup, by default, has the login-ndmp capability. To provide a user with the login-ndmp capability, the backup role can be assigned to the group to which the user belongs. However, when a group is assigned the backup role, all users within the group get the login-ndmp capability. Therefore, it is best to group all NDMP users in a single group that has the backup role.

Snapshot copy schedules

Scheduled Snapshot copy creation might fail for various reasons, such as a volume being offline. When the volume becomes online again, Data ONTAP detects the scheduled Snapshot copy creation that has failed and automatically creates a Snapshot copy for that schedule. This feature is available in Data ONTAP 8.0 7-Mode and later releases in the Data ONTAP 8.0 7-Mode release family.

For more information about this feature, see the *Data ONTAP 8.0 7-Mode Data Protection Online Backup and Recovery Guide*.

SnapMirror support for 64-bit volumes

Data ONTAP 8.0 and later releases support 64-bit volumes in addition to 32-bit volumes. SnapMirror supports replication between 64-bit volumes and

also between 32-bit volumes. However, there are certain considerations when replicating volumes and qtrees using SnapMirror.

When replicating volumes by using SnapMirror, synchronously or asynchronously, the source and destination volumes must be of the same type. Both the source and destination volumes must be 64-bit volumes or they both must be 32-bit volumes.

When replicating qtrees by using SnapMirror, the source and destination volumes can be of different types. Either the source and or destination volume can be 64-bit or 32-bit.

For more information about SnapMirror support for 64-bit volumes and see the *Data ONTAP 8.0 7-Mode Data Protection Online Backup and Recovery Guide*.

SnapVault support for 64-bit volumes

Data ONTAP 8.0 and later releases support 64-bit volumes. SnapVault supports replication between 64-bit volumes, in addition to supporting replication between 32-bit volumes. When replicating qtrees by using SnapVault, the source and destination volumes can be of different types. The source and destination volumes can be either 64-bit or 32-bit.

For more information about SnapVault replication, see the *Data ONTAP 8.0 7-Mode Data Protection Online Backup and Recovery Guide*.

Changes to the Data ONTAP and gateway libraries

The *Data ONTAP 8.0 7-Mode Software Setup Guide* now provides information for basic setup of all systems that run Data ONTAP, including gateway systems. Data ONTAP guides and gateway guides are now available on the same web page.

Starting in Data ONTAP 7.3.2, much of the information about using Data ONTAP features with gateway systems was integrated into the general Data ONTAP guides. This effort continued in Data ONTAP with the integration of gateway system setup instructions into the *Data ONTAP 8.0 7-Mode Software Setup Guide*. As of Data ONTAP 8.0 7-Mode, there is no longer a separate setup guide for the gateway.

The gateway documents now focus primarily on information about implementation with the back-end storage arrays.

New and changed commands and options in the Data ONTAP 8.1 7-Mode release

This section provides information about the commands, options, and configuration files that have been changed or added to the Data ONTAP 8.1 7-Mode release family. These changes are described in the following topics:

New commands in Data ONTAP 8.1 7-Mode

Many new commands have been added in the Data ONTAP 8.1 7-Mode release family.

For each command family and each command, the following table gives this information:

- The purpose of the command
- The location of documentation about the feature
- The Data ONTAP 8.1 7-Mode release in which the command was introduced

Command	Purpose	Documentation	Release added
`autosupport destinations show`	View a summary of all addresses and URLs that receive AutoSupport messages	*Data ONTAP 7-Mode System Administration Guide* `autosupport destinations show` man page	8.1
`autosupport history retransmit`	Retransmit a locally stored AutoSupport message, identified by its AutoSupport sequence number	*Data ONTAP 7-Mode System Administration Guide* `autosupport history retransmit` man page	8.1

Command	Purpose	Documentation	Release added
`autosupport history show`	Display information about one or more of the 50 most recent AutoSupport messages	*Data ONTAP 7-Mode System Administration Guide* `autosupport history show` man page	8.1
`autosupport manifest show`	View the information in the AutoSupport messages including the name and size of each file collected for the message along with any errors	*Data ONTAP 7-Mode System Administration Guide* `autosupport manifest show` man page	8.1
`autosupport trigger modify`	Enable and disable AutoSupport messages to your internal support organization for individual trigger events, and specify additional subsystem reports to include in messages sent in response to individual trigger events	*Data ONTAP 7-Mode System Administration Guide* `autosupport trigger modify` man page	8.1
`autosupport trigger show`	Display the system events that can trigger AutoSupport messages	*Data ONTAP 7-Mode System Administration Guide* `autosupport trigger show` man page	8.1
`disk encrypt destroy`	Cryptographically destroy self-encrypting disks on a Storage Encryption enabled system	*Data ONTAP 7-Mode Storage Management Guide*	8.1
`disk encrypt lock`	Lock self-encrypting disks on a Storage Encryption enabled system	Man page	8.1
`disk encrypt rekey`	Rekey self-encrypting disks on a Storage Encryption enabled system.	*Data ONTAP 7-Mode Storage Management Guide*	8.1
`disk encrypt sanitize`	Cryptographically erase self-encrypting disks on a Storage Encryption enabled system	*Data ONTAP 7-Mode Storage Management Guide*	8.1
`disk encrypt show`	Display self-encrypting disks on a Storage Encryption enabled system	*Data ONTAP 7-Mode Storage Management Guide*	8.1
`key_manager add`	Add key management servers to the storage system	*Data ONTAP 7-Mode Storage Management Guide*	8.1
`key_manager query`	Display key IDs stored on the key management servers	*Data ONTAP 7-Mode Storage Management Guide*	8.1

Command	Purpose	Documentation	Release added
`key_manager rekey`	Change the authentication key of self-encrypting disks	*Data ONTAP 7-Mode Storage Management Guide*	8.1
`key_manager remove`	Remove key management servers from the storage system	*Data ONTAP 7-Mode Storage Management Guide*	8.1
`key_manager restore`	Restore authentication keys stored on key management servers to the storage system	*Data ONTAP 7-Mode Storage Management Guide*	8.1
`key_manager setup`	Run the Storage Encryption setup wizard	*Data ONTAP 7-Mode Software Setup Guide*	8.1
`key_manager show`	Display key management servers registered with the storage system	*Data ONTAP 7-Mode Storage Management Guide*	8.1
`key_manager status`	Display the communication status of key management servers registered with the storage system	*Data ONTAP 7-Mode Storage Management Guide*	8.1
`nfs nsdb flush`	Removes entries from the name server database cache.	*Data ONTAP 7-Mode File Access and Protocols Management Guide* `nfs` man page	8.1
`sftp stat`	Displays SFTP statistics.	*Data ONTAP 7-Mode File Access and Protocols Management Guide* `sftp` man page	8.1
`storage show bridge`	Displays information about FC-to-SAS bridges.	*Data ONTAP 7-Mode Storage Management Guide*	8.1
`system health alert definition show`	Displays information about the alerts that a health monitor can potentially generate.	*Data ONTAP 7-Mode System Administration Guide* `system health alert definition show` man page	8.1
`system health alert delete`	Deletes an alert that was not automatically cleared	*Data ONTAP 7-Mode System Administration Guide* `system health alert delete` man page	8.1
`system health alert modify`	Suppresses or acknowledges an alert.	*Data ONTAP 7-Mode System Administration Guide* `system health alert modify` man page	8.1

Command	Purpose	Documentation	Release added
`system health alert show`	Displays information about generated alerts, such as the resource and node where the alert was triggered, and the alert's severity and probable cause.	*Data ONTAP 7-Mode System Administration Guide* `system health alert show` man page	8.1
`system health autosupport trigger history show`	Displays information about the AutoSupport messages that alerts triggered within the last week—for example, to determine if an alert triggered an AutoSupport message.	*Data ONTAP 7-Mode System Administration Guide* `system health autosupport trigger history show` man page	8.1
`system health config show`	Displays information about health monitors, such as their nodes, names, subsystems, and status.	*Data ONTAP 7-Mode System Administration Guide* `system health config show` man page	8.1
`system health node-connectivity adapter show`	Displays the status of adapters, along with other information, such as the owner node, whether they are used and enabled, and the number of shelves attached.	*Data ONTAP 7-Mode System Administration Guide* `system health node-connectivity adapter show` man page	8.1
`system health node-connectivity disk show`	Displays the status of disks, along with other information, such as the owner node, disk name and bay number, and the number of paths to the disk.	*Data ONTAP 7-Mode System Administration Guide* `system health node-connectivity disk show` man page	8.1
`system health node-connectivity shelf show`	Displays the status of shelves from the node-level view, along with other information, such as the owner node, shelf name, and how many disks and paths the shelf has.	*Data ONTAP 7-Mode System Administration Guide* `system health node-connectivity shelf show` man page	8.1
`system health policy definition modify`	Enables or disables the policy that controls whether a specific resource state raises a specific alert.	*Data ONTAP 7-Mode System Administration Guide* `system health policy definition modify` man page	8.1

Command	Purpose	Documentation	Release added
`system health policy definition show`	Displays information about health monitor policies, which determine when alerts are raised.	*Data ONTAP 7-Mode System Administration Guide* `system health policy definition show` man page	8.1
`system health status show`	Displays the status of the entire system.	*Data ONTAP 7-Mode System Administration Guide* `system health status show` man page	8.1
`snaplock clock initialize`	Initializes the system ComplianceClock	*Data ONTAP 7-Mode Archive and Compliance Management Guide*	8.1
`snaplock clock status`	Displays the system ComplianceClock and volume ComplianceClock time	*Data ONTAP 7-Mode Archive and Compliance Management Guide*	8.1

Changed commands in Data ONTAP 8.1 7-Mode release family

A number of commands have been changed in the Data ONTAP 8.1 7-Mode release family.

For each command family and each command, the table provides the following information:

- The change in the command
- The location of documentation about the command
- The Data ONTAP 8.1 7-Mode release in which the change was introduced

Command	Change	Documentation	Release command changed in
`aggr add`	The `64bit-upgrade` option has been added. This option enables the administrator to upgrade an aggregate from 32-bit to 64-bit format by adding enough storage to exceed the 16-TB maximum 32-bit aggregate size.	`na_aggr(1)` man page and *Data ONTAP 7-Mode Storage Management Guide*	8.1

Command	Change	Documentation	Release command changed in
`aggr create`	The `-c` option has been added. This option enables the administrator to select disks or array LUNs with a specific checksum type when creating an aggregate.	`na_aggr(1)` man page	8.1
`aggr status`	The `-R` option has been added. This option displays the serial number and other information used by technical support for the disks in an aggregate.	`na_aggr(1)` man page	8.1
`aggr status`	For the `r` option, the number of blocks for failed disks is now displayed as "-".		8.1
`disk assign`	The `-shelf` option has been added. This option enables the administrator to assign all unassigned disks on a specific shelf to the specified controller.	`na_disk(1)` man page	8.1
`flexcache eject`	The `-i` option has been added. This option enables you to specify the inode rather than the file name (for example, `flexcache eject -i /vol/foo/inode:24529`). The `-i` option can be useful if the file name is unknown or the path to the file name cannot be resolved.		8.1
`flexcache fstat`	The `-i` option has been added. This option enables you to specify the inode rather than the file name (for example, `flexcache fstat -i /vol/foo/inode:24529`). The `-i` option can be useful if the file name is unknown or the path to the file name cannot be resolved.		8.1

Command	Change	Documentation	Release command changed in
`sis config`	The **manual** value for the `-s` option has been added. This option can be used only on SnapVault destination volumes that have qtrees. This option ensures that the deduplication operation is not triggered automatically after every update to the destination volumes.	`na_sis(1)` man page and *Data ONTAP 7-Mode Storage Management Guide*	8.1
`sis config`	The `-I` option has been added. This option allows the administrator to enable or disable in-line compression.	`na_sis(1)` man page	8.1
`sis config`	The `-C` option has been added. This option enables the administrator to enable or disable post-process compression.	`na_sis(1)` man page	8.1
`sis start`	The `-p` option has been added. This option enables the deduplication operation to use the previous check point.	`na_sis(1)` man page and *Data ONTAP 7-Mode Storage Management Guide*	8.1
`sis start`	The `-q` option has been added. This option enables the administrator to queue the deduplication operations.	`na_sis(1)` man page	8.1
`sis status`	The `-l` option has been modified. The output of the `sis status -l` command now includes the status of inline-compression and post-process compression for a volume.	`na_sis(1)` man page and *Data ONTAP 7-Mode Storage Management Guide*	8.1
`snap autodelete`	The **file_clone** value for the `destroy_list` option has been added. This value is used to delete Snapshot copies that are locked by file clones.	`na_snap(1)` man page and *Data ONTAP 7-Mode Data Protection Online Backup and Recovery Guide*	8.1

Command	Change	Documentation	Release command changed in
`snapmirror resync`	The `-c` has been added. This option creates a Snapshot copy (with the name, snapshot_name) on the destination after the resynchronization transfer is complete. This is done to ensure that the transfer does not coincide with any ongoing updates. **Note:** This option is valid only for a qtree.	`na_snapmirror(1)` man page and *Data ONTAP 7-Mode Data Protection Online Backup and Recovery Guide*	8.1
`sysconfig`	The `-a` option now includes information about any FC-to-SAS bridges present.		8.1
`vol modify`	The `space-mgmt-try-first` option has been added. This option enables the administrator to choose between the `autogrow` functionality and `autodelete` snapshot as the first choice for providing more free space for a volume.	`na_vol(1)` man page and *Data ONTAP 7-Mode Storage Management Guide*	8.1
`vol status`	The output of this command now includes the format (32-bit or 64-bit) of the volume.	`na_vol(1)` man page and *Data ONTAP 7-Mode Storage Management Guide*	8.1
`vol options`	The `snaplock_autocommitt_period` option is added to set the autocommit period.	*Data ONTAP 7-Mode Archive and Compliance Management Guide*	8.1

Replaced or removed commands in Data ONTAP 8.1 7-Mode release family

The following information lists replaced or removed commands in Data ONTAP 8.1 7-Mode.

Support for the following commands will be discontinued in a future version of Data ONTAP. To perform the equivalent operation, use the `aggr` command.

- `vol add`
- `vol media_scrub`

- `vol migrate`
- `vol mirror`
- `vol scrub`
- `vol split`
- `vol verify`
- `vol wafliron`

These commands are removed in Data ONTAP 8.1 7-Mode:

- `vol compress`
- `date -c`
- `date -c initialize`
- `filestats`

New options in Data ONTAP 8.1 7-Mode release family

This release includes new options that you can use with the `options` command, the following table gives this information:

- Purpose of the option
- The default value for the option
- The Data ONTAP release in which the option was introduced

For more information about the `options` command and individual options, see the `na_options(1)` man page.

Option	Purpose	Default value	Release added
`autosupport.max_http_size`	Specifies the maximum file size for HTTP and HTTPS transfers of AutoSupport messages.	10 MB	8.1
`autosupport.max_smtp_size`	Specifies the maximum email message size for SMTP (email) transfers of AutoSupport messages.	5 MB	8.1
`autosupport.payload_format`	Specifies the file format of the compressed file that contains AutoSupport data.	`7z`	8.1
`autosupport.support.put_url`	Indicates where AutoSupport messages for IBM technical support are sent if `autosupport.support.transport` is `http` or `https` and the server receiving the message supports HTTP PUT requests. Read only.	eccgw01.boulder.ibm.com/support/electronic/nas	8.1
`autosupport.validate_digital_certificate`	Determines whether the storage system validates the remote digital certificates that it receives. Applies only when `autosupport.support.transport` is set to HTTPS.	on	8.1

Option	Purpose	Default value	Release added
cifs.smb2.client.enable	Enables or disables the storage system's SMB 2.0 client capability.	off	8.1
cifs.smb2.durable_handle.enable	Enables or disables SMB 2.0 durable handles.	on	8.1
cifs.smb2.durable_handle.timeout	Specifies the maximum lifetime of SMB 2.0 durable handles before they expire.	960 seconds	8.1
cifs.smb2.enable	Enables or disables the SMB 2.0 protocol.	on	8.1
cifs.smb2.signing.required	Enforces the requirement for clients to sign SMB 2.0 messages.	off	8.1
flexscale.rewarm	Determines whether the WAFL external cache preserves the cache in a Flash Cache module during a graceful shutdown.	on	8.1
ftpd.explicit.allow_secure_data_conn	Allows or prevents the opening of explicit FTPS data connections in secure mode.	on	8.1
ftpd.explicit.enable	Enables or disables explicit FTPS.	off	8.1
ftpd.implicit.enable	Enables or disables implicit FTPS.	off	
ip.tcp.abc.enable	Enables or disables the use of Appropriate Byte Counting (ABC) in TCP congestion control.	on	8.1
ip.tcp.abc.l_limit	Specifies the value of the L limit used to increase the congestion window during the slow start phase in TCP.	22	8.1
ip.tcp.rfc3390.enable	Enables or disables the use of RFC 3390 to increase the initial window used by TCP connections.	on	8.1
licensed_feature.disk_sanitization.enable	Enables or disables the disk sanitization feature on all systems. Note that after you enable disk sanitization on your system, it cannot be disabled.	off	8.1
licensed_feature.fcp.enable	Enables or disables the use of iSCSI on N3400, N5000 series, N6000series, and N7000 series systems. For all other systems, you must purchase a license to use this protocol and administer it by using the `license` commands.	off	8.1
licensed_feature.flexcache_nfs.enable	Enables or disables the use of FlexCache with NFS clients on all systems.	off	8.1
licensed_feature.iscsi.enable	Enables or disables the use of the iSCSI protocol on N3400, N5000, N6000, and N7000 series systems. For all other systems, you must purchase a license to use this protocol and administer it by using the `license` commands.	off	8.1
licensed_feature.multistore.enabl e	Enables or disables MultiStore on N3220, N3240, N3400, N6200 series, and N7x50T systems. For all other systems, you must purchase a license to use this feature and administer it by using the `license` commands.	off	8.1

Option	Purpose	Default value	Release added
licensed_feature.nearstore_option.enable	Enables or disables the Nearline feature on all systems.	off	8.1
licensed_feature.vld.enable	Enables or disables VLD on all systems.	off	8.1
nfs.always.deny.truncate	Controls whether NFSv2 and NFSv3 clients can truncate files in UNIX qtrees that are also opened from a CIFS client with DENY write permissions.	on	8.1
nfs.v3.snapshot.active.fsid.enable	Specifies the file system ID handling behavior for NFSv3.	on	8.1
nfs.v4.snapshot.active.fsid.enable	Specifies the file system ID handling behavior for NFSv4.	off	8.1
sftp.auth_style	Specifies the SFTP authentication style.	mixed	8.1
sftp.bypass_traverse_checking	Enables or disables SFTP bypass traverse checking.	off	8.1
sftp.dir_override	Specifies the SFTP override path for user home directories.	"" (null)	8.1
sftp.dir_restriction	Enables or disables SFTP user home directory restrictions.	off	8.1
sftp.enable	Enables or disables SFTP.	off	8.1
sftp.idle_timeout	Specifies the maximum SFTP connection idle time before termination in seconds.	900	8.1
sftp.locking	Enables or disables SFTP file locking.	none	8.1
sftp.log_enable	Enables or disables SFTP event logging.	on	8.1
sftp.log_filesize	Specifies the maximum size of the SFTP log files.	512K	8.1
sftp.log_nfiles	Specifies the maximum number of SFTP log files.	6	8.1
sftp.max_connections	Specifies the maximum number of SFTP connections.	15	8.1
sftp.max_connections_threshold	Specifies when to generate a maximum SFTP connection warning in percent.	75	8.1
sftp.override_client_permissions	Enables or disables UNIX permissions specified by SFTP clients.	off	8.1
snapmirror.volume.local_nwk_bypass.enable	Determines whether local SnapMirror transfer optimization is enabled.	on	8.1
tftpd.enable	Enables or disables the TFTP server.	off	8.1
tftpd.max_connections	Specifies the maximum number of TFTP connections.	8	8.1
vsm.smtape.concurrent.cascade.support	Enables or disables concurrent volume SnapMirror and SMTape backup operations	off	8.1

Changed options in Data ONTAP 8.1 7-Mode release family

This table lists options that have changed or become obsolete.

For each option, the following table gives this information:

- The name of the changed option
- The nature of the change
- The Data ONTAP 8.1 7-Mode release in which the change was introduced

For more information about the `options` command and individual options, see the `na_options(1)` man page.

Option	Change	Release changed
`autosupport.content`	The minimal setting encodes and masks certain private data, instead of omitting it.	8.1
`autosupport.local.nht_data.enable`	Removed	8.1
`autosupport.local.performance_data.enable`	Removed	8.1
`autosupport.mailhost`, `autosupport.proxy`, and `autosupport.support.url`	Support IPv6 addresses, as well as IPv4 addresses.	8.1
`autosupport.support.url`	Applies only to HTTP POST requests, not to HTTP PUT requests, which are configured using `autosupport.support.put_url`	8.1
`cifs.max_mpx`	The default for this option has been changed to 253.	8.1
`options snaplock.autocommit_period`	This system-level option can be used only for viewing the autocommit time period of the SnapLock volumes that were upgraded. This option is now in read-only state.	8.1

Removed gateways environment variable requirement for Data ONTAP 8.1

Starting in Data ONTAP 8.1, the `fc-non-array-adapter-list` environment variable is no longer required for gateway systems with native disk shelves that use MultiPath Storage.

If you revert from Data ONTAP 8.1 to an earlier release, Data ONTAP automatically configures this environment variable for you. It is required in releases prior to 8.1.

New and changed commands and options in the Data ONTAP 8.0 7-Mode release

This section provides information about the commands, options, and configuration files that have been changed or added to the Data ONTAP 8.0 7-Mode release family. If you are upgrading to Data ONTAP 8.1 or later from a 7.3.x release, these changes will apply to your system in addition to those introduced in the 8.1 release family.

New commands in Data ONTAP 8.0 7-Mode

Many new commands have been added in the Data ONTAP 8.0 7-Mode release family.

For each command family and each command, the following table gives this information:

- The purpose of the command
- The location of documentation about the feature
- The Data ONTAP 8.0 7-Mode release in which the command was introduced

Command	Purpose	Documentation	Release introduced
`acpadmin configure`	Configures the ACP subsystem.	*Data ONTAP 8.0 7-Mode Storage Management Guide* na_acpadmin(1) man page	8.0
`acpadmin list_all`	Displays information about the ACP (Alternate Control Path) storage subsystem.	*Data ONTAP 8.0 7-Mode Storage Management Guide* na_acpadmin(1) man page	8.0

Command	Purpose	Documentation	Release introduced
`cdpd`	Displays information about devices that advertise themselves by using the CDPv1 protocol.	*Data ONTAP 8.0 7-Mode Network Management Guide*	8.0.1
`du`	Displays the files and amount of space that they occupy in a deduplicated volume.	*Data ONTAP 8.0 7-Mode Storage Management Guide*	8.0.1
`ifgrp`	Manages interface groups on your storage system. This command replaces the `vif` command. However, the options remain the same.	*Data ONTAP 8.0 7-Mode Network Management Guide*	8.0
`revert_to`	Transitions Data ONTAP to a release in an earlier release family	*Data ONTAP 8.0 7-Mode Upgrade and Revert/Downgrade Guide* revert_to(1) man page	8.0
`smtape abort`	Aborts a backup or restore job initiated by the SMTape engine.	*Data ONTAP 8.0 7-Mode Data Protection Tape Backup and Recovery Guide* na_smtape man page	8.0
`smtape backup`	Backs up blocks of data to tape.	*Data ONTAP 8.0 7-Mode Data Protection Tape Backup and Recovery Guide* na_smtape man page	8.0
`smtape continue`	Continues an SMTape-initiated backup or restore operation after it has reached the end of current tape and is in the wait state to write output to or accept input from a new tape.	*Data ONTAP 8.0 7-Mode Data Protection Tape Backup and Recovery Guide* na_smtape man page	8.0

Command	Purpose	Documentation	Release introduced
`smtape restore`	Restores blocks of data from tape.	*Data ONTAP 8.0 7-Mode Data Protection Tape Backup and Recovery Guide* na_smtape man page	8.0
`smtape status`	Display the status of SMTape-initiated backup and restore operations	*Data ONTAP 8.0 7-Mode Data Protection Tape Backup and Recovery Guide* na_smtape man page	8.0
`sp help`	Displays the Data ONTAP `sp` commands that you can enter at the storage system prompt.	*Data ONTAP 8.0 7-Mode System Administration Guide* na_sp(1) man page	8.0.1
`sp reboot`	Reboots the SP and causes the SP to perform a self-test.	*Data ONTAP 8.0 7-Mode System Administration Guide* na_sp(1) man page	8.0.1
`sp setup`	Initiates the interactive SP setup script.	*Data ONTAP 8.0 7-Mode System Administration Guide* na_sp(1) man page	8.0.1
`sp status`	Displays the current status and the network configuration of the SP.	*Data ONTAP 8.0 7-Mode System Administration Guide* na_sp(1) man page	8.0.1
`sp test autosupport`	Sends a test email to all recipients specified with the `autosupport.to` option.	*Data ONTAP 8.0 7-Mode System Administration Guide* na_sp(1) man page	8.0.1
`sp test snmp`	Performs SNMP test on the SP, forcing the SP to send a test SNMP trap to all trap hosts specified in the `snmp traphost` command.	*Data ONTAP 8.0 7-Mode System Administration Guide* na_sp(1) man page	8.0.1

Command	Purpose	Documentation	Release introduced
`sp update`	Updates the SP firmware.	*Data ONTAP 8.0 7-Mode Upgrade and Revert/Downgrade Guide* na_sp(1) man page	8.0.1
`storage array modify`	Modifies attributes of array profile records.	na_storage(1) man page	8.0
`storage array purge-database`	Removes all records from the controller's array profile database.	na_storage(1) man page	8.0
`storage array remove`	Removes records for the specified array from the controller's array profile database.	na_storage(1) man page	8.0
`storage array remove-port`	Removes ports associated with an array profile.	na_storage(1) man page	8.0
`storage array show`	Lists all array profile records known to the controller.	na_storage(1) man page	8.0
`storage array show-config`	Provides a summary of the connectivity to SAN-attached arrays connected to the gateway system's FC initiator ports.	*Gateway Installation Requirements and Reference Guide* na_storage(1) man page	8.0
`storage array show-luns array-name`	Lists all array LUNs exported from a named storage array.	na_storage(1) man page	8.0
`storage array show-ports`	Lists all target ports for all storage arrays known to the gateway system.	na_storage(1) man page	8.0
`storage show acp`	Displays information about the ACP (Alternate Control Path) storage subsystem.	*Data ONTAP 8.0 7-Mode Storage Management Guide* na_acpadmin(1) man page	8.0

Changed commands in Data ONTAP 8.0 7-Mode

This table lists the commands that have been changed in the Data ONTAP 8.0 7-Mode release family.

For each command family and each command, the following table gives this information:

- The change in the command
- The location of documentation about the feature
- The Data ONTAP 8.0 7-Mode release in which the change was introduced

Command	Change	Documentation	Release command changed in
`aggr create`	The `-B` option has been added. This option is used to create a 64-bit aggregate.	na_aggr(1) man page *Data ONTAP 8.0 7-Mode Storage Management Guide*	8.0
`df`	The `-x` option has been added. This option suppresses the display of the .snapshot lines.	na_df(1) man page	8.0
`disk assign`	You can no longer use this command to change the ownership of a disk or array LUN that is already owned unless you are running the command on the system that owns the disk already.	na_disk(1) man page and	8.0
`environment shelf`	The Complex Programmable Logic Device (CPLD) version has been added to the output.	na_environ(1) man page	8.0
`flexcache fstat`	The `-inode-file` option has been added. This option displays the number of blocks used by the FlexCache volume's inode file.	na_flexcache(1) man page	8.0.3
`ifgrp create multi`	The `port` value (port-based load-balancing) for the `-b` option has been added.	*Data ONTAP 8.0 7-Mode Network Management Guide*	8.0.1
`software update`	The `-r` option, which suppresses automatic reboot, is now the default. To request an automatic reboot, you now must specify the `-R` option.	na_software(1) man page *Data ONTAP 8.0 7-Mode Upgrade and Revert/Downgrade Guide*	8.0.1

Command	Change	Documentation	Release command changed in
`storage show acp`	A column for "Module type" has been added to the output. This shows the type of the I/O module.	na_storage(1) man page	8.0.1
`storage show expander`	The system interconnect link (SIL) ports (the last four rows of output) are now shown as [SIL0] through [SIL3]. Previously they were shown as [DIS0] through [DIS3].	na_storage(1) man page	8.0
`storage show expander`	The EXN3000 and EXN3500 storage expansion unit ports are now listed as [SQR0]-[SQR3] for the square ports and [CIR4]-[CIR7] for the circle ports. Previously these ports were listed as [IO 0]-[IO7].	na_storage(1) man page	8.0
`storage show fault`	You can now specify a storage expansion unit name for this command to see information about a specific storage expansion unit.		8.0.1
`sysconfig`	When the `-r` option is used to display disk information for SAS-connected disks, the CHAN (channel) column now displays the port as "A" or "B", just as it does for FC-connected disks. Previously, "1" and "2" were used.	na_sysconfig(1) man page	8.0
`sysconfig`	When the `-a` option is used, the output includes status and power information for any IOXM modules present.	na_sysconfig(1) man page	8.0.1
`sysconfig`	When the `-v` option is used, any disabled ports show "N/A" for the data link rate.	na_sysconfig(1) man page	8.0.2

Command	Change	Documentation	Release command changed in
`vif`	This command has been replaced by the `ifgrp` command.	*Data ONTAP 8.0 7-Mode Network Management Guide*	8.0
`vol options`	The `extent` option enables extents but can only be used on FlexVol volumes.	na_vol(1) man page and the *Data ONTAP 8.0 7-Mode System Administration Guide*	8.0
`vol options`	The `read_realloc` option enables read reallocation but can only be used on FlexVol volumes.	na_vol(1) man page	8.0
`vol status`	When the `-r` option is used to display disk information for SAS-connected disks, the CHAN (channel) column now displays the port as "A" or "B", just as it does for FC-connected disks. Previously, "1" and "2" were used.	na_vol(1) man page	8.0

Replaced or removed commands in Data ONTAP 8.0 7-Mode release family

The following information lists replaced or removed commands in Data ONTAP 8.0 7-Mode.

Support for the following commands will be discontinued in a future version of Data ONTAP. To perform the equivalent operation, use the `aggr` command.

- `vol add`
- `vol media_scrub`
- `vol migrate`
- `vol mirror`
- `vol scrub`
- `vol split`
- `vol verify`
- `vol wafliron`

These commands are removed in Data ONTAP 8.0 7-Mode.

- `snapmirror store`

- `snapmirror use`
- `snapmirror retrieve`

In Data ONTAP 8.0 7-Mode release, the `vif` command has been replaced by the `ifgrp` command. For more information, see the *Data ONTAP 8.0 7-Mode Network Management Guide*.

New options in Data ONTAP 8.0 7-Mode release family

For each new option that can be used with the `options` command, the following table gives this information:

- A description of the option's purpose
- The default value for the option
- The Data ONTAP 8.0 7-Mode release in which the option was introduced

For more information about the `options` command and individual options, see the na_options(1) man page.

Option	Purpose	Default value or example	Release introduced
`autosupport.performance_ data.doit` *`any_string`*	Triggers a performance snapshot AutoSupport message when any string is added.	N/A	8.0
`autosupport.periodic.tx_ window` *`time`*	Specifies the randomized delay window for periodic AutoSupport messages.	60 minutes	8.0.1
`cf.takeover.on_panic`	Triggers a takeover if the partner mode panics.	`On`	8.0
`cf.takeover.on_reboot`	Triggers a takeover if the partner node reboots.	The default is `on`, unless FCP or iSCSI is licensed, in which case the default is off.	8.0
`cf.givegack. auto.delay.seconds`	Adjusts the giveback delay time for automatic giveback.	`300 seconds`	8.0
`lun_ic_alua_changed`	Disables ALUA State Change Unit Attention on interconnect up or down events.	`off`	8.0.1 and 8.0.3 **Note:** This option is not available in Data ONTAP 8.0.2.

Option	Purpose	Default value or example	Release introduced
interface.blocked.mgmt_data_traffic	Blocks or allows data traffic on the management interface, e0M	off for systems upgraded from an earlier release; on for new systems	8.0.2
ndmpd.data_port_range	Specifies a port range on which the NDMP server can listen for data connections.	all	8.0.1
nfs.always.deny.truncate	Controls whether NFSv2 and NFSv3 clients can truncate files in UNIX qtrees that are also opened from a CIFS client with DENY write permissions.	on	8.0.2
nfs.max_num_aux_ groups	Specifies the maximum number of auxiliary UNIX groups that a user can be a member of.	32	8.0
nfs.v3.snapshot.active.fsid.enable	Determines whether the FSID of objects in a Snapshot copy matches the FSID of the active file system for NFSv3.	on	8.0.1
nfs.v4.snapshot.active.fsid.enable	Determines whether the FSID of objects in a Snapshot copy matches the FSID of the active file system for NFSv4.	off	8.0.1
fpolicy.multiple_ pipes	Enables multiple open instances of the SMB named pipe on an FPolicy server.	on	8.0
snapvault.snapshot_for_dr_backup	Enables you to specify the Snapshot copy to use for updating the destination system when backing up a volume SnapMirror destination using SnapVault.	vsm_base_only	8.0.2
sp.setup	Displays whether the SP has been configured.	(N/A)	8.0.1
ssl.v2.enable	Enables or disables SSLv2.	on	8.0.1
ssl.v3.enable	Enables or disables SSLv3.	on	8.0.1

New option for the `vfiler dr configure` command

Data ONTAP 8.0.3 and later provide a new option `-u` for the `vfiler dr configure` command. This option enables you to set up a disaster recovery vFiler unit without reinitializing the existing SnapMirror relationship between the source and the destination storage systems.

You can use the -u option when the SnapMirror relationship between the volumes of the source vFiler unit and the respective volumes on the destination storage system is already initialized.

For more information about using this option, see the na_vfiler(1) man page.

Changed options in Data ONTAP 8.0 7-Mode

This table lists options that have changed or become obsolete.

For each option, the following table gives this information:

- The name of the changed option
- The nature of the change
- The Data ONTAP 8.0 7-Mode release in which the change was introduced

For more information about the options command and individual options, see the na_options(1) man page.

Option	Change	Release changed
autosupport.minimal.subject.id	The default for this option has been changed to *systemid* for systems shipped with Data ONTAP 8.0.2 7-Mode or later.	8.0.2
cifs.max_mpx	The default for this option has been changed to 253.	8.0.2
flexscale.max_io_qdepth	This option has become obsolete.	8.0
httpd.admin.enable	The default for this option has been changed to off for systems shipped with Data ONTAP 8.0 7-Mode or later.	8.0
httpd.admin.ssl.enable	The default for this option has been changed to on for systems shipped with Data ONTAP 8.0 7-Mode or later.	8.0
rsh.enable	The default for this option has been changed to off for systems shipped with Data ONTAP 8.0 7-Mode or later.	8.0
ssh.enable	The default for this option has been changed to on for systems shipped with Data ONTAP 8.0 7-Mode or later.	8.0

Option	Change	Release changed
ssh2.enable	The default for this option has been changed to on for systems shipped with Data ONTAP 8.0 7-Mode or later.	8.0
security.passwd.rules.everyone	The default for this option has been changed to on for systems shipped with Data ONTAP 8.0 7-Mode or later.	8.0
security.passwd.rules.history	The default for this option has been changed to 6 for systems shipped with Data ONTAP 8.0 7-Mode or later.	8.0
telnet.distinct.enable	The default for this option has been changed to on for systems shipped with Data ONTAP 8.0 7-Mode or later.	8.0
telnet.enable	The default for this option has been changed to off for systems shipped with Data ONTAP 8.0 7-Mode or later.	8.0
timed.max_skew	This option has become obsolete.	8.0
timed.proto	This option has become obsolete. The default option is ntp.	8.0
timed.sched	This option has become obsolete.	8.0
timed.window	This option has become obsolete.	8.0

Requirements for running Data ONTAP 8.1 7-Mode

You can use the information in this section to verify that you have the storage systems and firmware needed to run software in the Data ONTAP 8.1 7-Mode release family.

To find out your storage system model's capacity and maximum volume size, see the *IBM System Storage N series Introduction and Planning Guide*.

Supported systems

You need one of the supported storage systems listed in this section to run Data ONTAP 8.1 7-Mode family.

The following models of storage systems are supported:

- N5300 and N5600 storage systems
- N3220 and N3240 storage systems
- N3400 storage systems
- N6000 series systems
- N6200 series systems
- N7000 series systems
- N7x50T

All systems supported by Data ONTAP 8.1 7-Mode release family can be configured in high-availability configuration.

For additional information about supported storage systems in the Data ONTAP 8.1 7-Mode release family, see the *IBM System Storage N series Introduction and Planning Guide*.

Unsupported systems

The following N series storage systems models are not supported in Data ONTAP 8.1 7-Mode release family:

- N3300 and N3600 storage systems
- N5200 and N5500 storage systems
- N3700 storage systems

Storage system firmware

You need to confirm that you have the latest firmware for your storage system, disks, and storage expansion units.

The following storage system components have firmware that sometimes requires upgrading:

- Motherboard (also known as system or storage system firmware)
- Disk drives
- Disk storage expansion unit

Storage system firmware

It is best to upgrade to the latest version of system firmware for your storage system. For the latest firmware, you can go to the IBM N series support website, which is accessed and navigated as described in "Websites" on page 3.

Note: The latest system firmware is included with Data ONTAP upgrade packages. For more information, see the *Data ONTAP 8.1 7-Mode Upgrade and Revert/Downgrade Guide*.

Disk firmware

For information about the latest disk firmware, see the IBM N series support website, which is accessed and navigated as described in "Websites" on page 3.

Note: New disk firmware is sometimes included with Data ONTAP upgrade packages. For more information, see the *Data ONTAP 8.1 7-Mode Upgrade and Revert/Downgrade Guide*.

Disk storage expansion unit and ESH firmware

For information about the latest disk storage expansion unit and ESH (Embedded Switched Hub) firmware, see the IBM N series support website, which is accessed and navigated as described in "Websites" on page 3.

Gateway requirements and support information

Not all Data ONTAP releases support the same features, configurations, storage system models, and storage array models for gateway systems. The Gateway Support Matrix is the final authority on supported configurations, storage array firmware and microcode versions, switches, and so on.

See the Gateway Support Matrix, located on the IBM N series support website, which is accessed and navigated as described in "Websites" on page 3, for complete information about supported gateway models and storage arrays, as well as supported microcode, license code, and storage array firmware versions. The Gateway Support Matrix also identifies switch connectivity and topology that can be used with gateway systems.

Important cautions

Before upgrading to this release of Data ONTAP, make sure that you read the following items to identify and resolve issues that might affect the operation of your storage systems.

Upgrade and revert cautions

If you are upgrading to this Data ONTAP release or reverting from this release to an earlier release, you should review these issues, and if any apply in your environment, take appropriate action.

For more information about procedures and planning, see the *Data ONTAP 8.1 7-Mode Upgrade and Revert/Downgrade Guide*.

Change in nondisruptive upgrade procedure

When you upgrade to this Data ONTAP release, you should be aware of changes in the `software update` command syntax and the requirement for boot environment access.

Beginning with 7.3.5 and 8.0.1, system firmware is updated automatically. It is no longer necessary to access the boot environment for upgrades from a Data ONTAP 8.0.x release to a later release.

Note: This change only refers to minor nondisruptive upgrades (within a release family). When upgrading to a Data ONTAP 8.0.x release from an earlier release family, you must enter the boot environment during the takeover phase to ensure that the Data ONTAP 8.0.x release is running the correct firmware release.

Beginning with 7.3.5 and 8.0.1, the `-r` option (no automatic reboot) is the default for the software update command.

Note: However, when you first upgrade to Data ONTAP 7.3.5 or 8.0.1 or a later release in the 8.0 family, you must specify the `-r` option for nondisruptive upgrades. In subsequent major and minor nondisruptive upgrades, it will no longer be required to specify the option.

Upgrade process changes with Data ONTAP 7-Mode software images

When you upgrade to Data ONTAP 8.0 and later releases, you must obtain Data ONTAP software images from the IBM N series support website, which is accessed and navigated as described in "Websites" on page 3 and copy them to your storage system. Media kits, including CD-ROMs with Data ONTAP software images, are no longer available, and the process of installing upgrade images from UNIX or Windows clients is no longer supported.

Beginning with Data ONTAP 8.0, media kits including CD-ROMs are no longer available. You must obtain software images from the IBM N series support website, which is accessed and navigated as described in "Websites" on page 3 and copy them to your storage system or to an HTTP server in your environment.

Beginning with Data ONTAP 8.0, the following processes are no longer supported for extracting and installing Data ONTAP upgrade images:

- Using the `tar` command from UNIX clients
- Using the setup.exe file and WinZip from Windows clients

For the upgrade to Data ONTAP 8.0 and later releases, .exe images are no longer available. You must use one of the following image types depending on the upgrade you are performing:

- .zip images, for upgrades from an earlier release family to Data ONTAP 8.0
- .tgz images, for upgrades from any Data ONTAP 8.0 release to a later release

After you have upgraded to Data ONTAP 8.0 or later, you can only use .tgz images for further upgrades.

After you have copied the .zip or .tgz image to your storage system, you can install it with the `software update` command. Alternatively, you can make the .zip or .tgz image available from an HTTP server in your environment, then use the `software update` command to copy the upgrade image from the HTTP server, extract and install the system files, and download the files to the boot device with one command.

For more information about upgrade images, see the *Data ONTAP 7-Mode Upgrade and Revert/Downgrade Guide*.

EXN2000 storage expansion units with ESH2 modules no longer supported

Beginning with Data ONTAP 8.1, EXN2000 storage expansion units with ESH2 storage I/O modules are no longer supported. If even one of these devices is attached to your storage system, do not upgrade to Data ONTAP 8.1 or later until after you replace the devices. For more information, see "Systems including EXN2000 storage expansion units with ESH2 modules" on page 8.

License updates required before upgrading

If you are upgrading the N3400, N6200 series, or N7x50T storage systems from a Data ONTAP 8.0.x release to a 8.1.x release, you must relicense certain features. This requirement does not apply to the N6000 and N7000 series storage systems.

Beginning in the Data ONTAP 8.1 release family, features are packaged together so that only one license key is required to add a group of features to N3220, N3240, N3400, N6200, or N7x50T.

If you were using a feature in a Data ONTAP 8.0.x release and you upgrade to Data ONTAP 8.1.x, the action you take depends on how your features were licensed in the Data ONTAP 8.0.x release.

- You purchased a license pack, but you added individual feature keys only. You must add the license key for the packs that include any individual feature key you were using previously.
- You acquired your individual feature keys before license packs were available and have not yet purchased a license pack.

  You must contact your IBM representative to purchase and install license packs that include the features you were using.

To ensure continued access to a feature that requires a license, you should add the pack license key before you upgrade to Data ONTAP 8.1.x. If you do not add the pack license key before upgrading, the features are not available when you boot into the new Data ONTAP release, and you must add the key after upgrading.

For information about Data ONTAP 8.1 licensing models and whether a license key must be added for a particular feature or pack, see the *Data ONTAP 7-Mode System Administration Guide* and the man pages for the `license` commands or the Technote FAQ at the following link:

Using License Keys with Data ONTAP 8.1 7-Mode

N6210 series and N6040 series storage systems with Flash Cache modules are not supported

If you have a N6210 series and N6040 series storage system with Flash Cache modules installed, do not upgrade your system to Data ONTAP 8.1 7-Mode. Flash Cache modules are not supported on N6210 series and N6040 storage systems with Data ONTAP 8.1 7-Mode.

This issue is under investigation and a long-term strategy will be communicated as soon as possible.

NDU not available for SAN systems with some versions of Linux hosts running high-speed interconnects

For some versions of Linux, you cannot upgrade to Data ONTAP 8.1 or earlier using the nondisruptive upgrade (NDU) method with SAN hosts that have ALUA enabled and have high-speed interconnects (8 Gb or faster).

The following versions of Linux running on hosts can encounter host hangs or long delays in I/O operations during the failover phase of the Data ONTAP (NDU), which causes disruption of services to the hosts:

- Red Hat Enterprise Linux 6.x or 5.x prior to 5.8
- SUSE Linux Enterprise Server 10.x and 11.x
- Oracle Linux 5.x and 6.x

To perform a NDU with Red Hat Enterprise Linux, you must ensure you are using Red Hat Enterprise Linux 5.8. Otherwise, you need to plan for a disruptive Data ONTAP upgrade.

For more information, see I/O delays sometimes seen after controller failover on Linux hosts with ALUA.

IPv6 address entries in /etc/exports file missing brackets after upgrading

If you are upgrading from the Data ONTAP 7.3.x release family to Data ONTAP 8.1 7-Mode and you have IPv6 enabled, you must manually update the `/etc/exports` file and add the missing square brackets around each IPv6 address.

After finishing the upgrade, check each entry in the `/etc/exports` file that contains an IPv6 address. In the following example, the IPv6 addresses are missing the required square brackets ([ ]):

```
/vol/vol3 -
sec=sys,rw=FD20:81BE:B255:4136:10.72.58.30,root=FD20:81BE:B255:4136:10.72.5
8.30
```

If your IPv6 address entries are missing these brackets, you must manually update the file and add the square brackets around each IPv6 address so that the entry looks similar to the following example:

```
/vol/vol3 -
sec=sys,rw=[FD20:81BE:B255:4136:10.72.58.30],root=[FD20:81BE:B255:4136:10.7
2.58.30]
```

You can update the `/etc/exports` file either by using a text editor or the `exportfs` command. For more information, see the *Data ONTAP 7-Mode File Access and Protocols Management Guide*.

Erroneous reboot message during Data ONTAP reversion

When reverting from Data ONTAP 8.1 to an 8.0.x release, you might see a screen message directing you to enter the `reboot` command. That direction is incorrect, you should enter the `revert_to` command instead.

Here is an example of the incorrect message:

```
software: installation of image.tgz completed.
Please type "reboot" for the changes to take effect.
```

The correct message will be displayed when the problem is fixed in a future Data ONTAP release.

Reverting to an earlier release on a N6210 with more than 200 volumes can cause a system panic

Data ONTAP 8.1 and later releases support 500 volumes on the N6210. For previous Data ONTAP release families, only 200 volumes are supported. If you attempt to revert a N6210 with more than 200 volumes to an earlier release of Data ONTAP, not all of your volumes will come online.

To avoid this issue, ensure that you have 200 or fewer volumes before reverting to an earlier release family on a N6210.

Validation of LUNs fails when reverting from Data ONTAP 8.1 to some earlier releases

Validation of LUNs created in Data ONTAP 8.1 might fail when you revert from Data ONTAP 8.1 to some earlier releases. In Data ONTAP 8.1 and later

releases, LUN serial numbers can contain characters, such as number sign (#) and ampersand (&), which are not supported in some earlier releases.

Data ONTAP 8.1 supports the following characters in LUN serial numbers: number sign (#), ampersand (&), dollar sign ($), percent (%), asterisk (*), plus sign (+), less than sign (<), equal sign (=), greater than sign (>), question mark (?), at sign (@), open bracket ([), exclamation point (!), close bracket (]), caret (^), and tilde (~).

If your LUN serial numbers contain these characters in Data ONTAP 8.1 or later, you cannot revert to Data ONTAP releases earlier than version 8.0.3 in the 8.0.x release family or version 7.3.7 in the 7.3.x release family.

Manageability cautions

If you are a storage system administrator, you should familiarize yourself with these manageability issues.

- "Certificates signed with MD5 could cause loss of connectivity to secure clients"
- "If your root FlexVol volume does not meet the new size requirements"

Certificates signed with MD5 could cause loss of connectivity to secure clients

To enhance security, starting with Data ONTAP 8.0.2, Data ONTAP uses the SHA256 message-digest algorithm to sign the contents of digital certificates (including certificate signing requests (CSRs) and root certificates) on the storage system. Use of the MD5 message-digest algorithm, which was used to sign CSRs and root certificates, is no longer officially supported.

Depending on the certificate depth verification, clients might need to use SHA256 to verify digital certificates presented by Data ONTAP 8.0.2 and later.

Data ONTAP 8.0 and 8.0.1 use the MD5 message-digest algorithm to sign digital certificates. Due to the CVE-2004-2761-IETF X.509 certificate MD5 signature collision vulnerability, and to minimize security risks when using a certificate signed with MD5, you should have the CSRs further signed by a certificate authority (CA) using SHA256 or SHA1.

If your root FlexVol volume does not meet the new size requirements

The minimum required size for root FlexVol volumes has been increased for every system running the Data ONTAP 8.0 release family or later. If your root FlexVol volume does not meet the new requirements, you should increase its size as soon as you complete the upgrade procedure.

The root volume must have enough space to contain system files, log files, and core files. If a system problem occurs, these files are needed to provide technical support.

For more information about root volumes and the root FlexVol volume requirements for your platform, see the *Data ONTAP 7-Mode System Administration Guide*.

Storage management cautions

Review the following section for important information regarding storage management cautions.

For more information about these issues, see the *Data ONTAP 8.1 7-Mode Storage Management Guide*.

- "Write operations might fail or LUNs might go offline if deduplication metadata increases"

Write operations might fail or LUNs might go offline if deduplication metadata increases

In volumes with deduplication enabled, the deduplication metadata increases if the deduplication schedule is turned off or if the data is overwritten at a very high rate before deduplication is run. The increase in metadata might cause write operations to fail or LUNs to go offline.

To avoid this issue, you must schedule deduplication to be run periodically by using the `sis config -s` command.

If the metadata in the volume has increased, then you must disable deduplication by using the sis off command and delete the metadata by using the `sis reset` command.

For more information about deduplication, see the *Data ONTAP 7-Mode Storage Management Guide*.

Network protocol cautions

This information addresses network protocols cautions. Review the following section for important information regarding network management.

For more information about these issues, see the *Data ONTAP 7-Mode Network Management Guide*.

- "System might panic if the network configuration entries in the /etc/rc file are not in the recommended order"
- "Do not reconfigure the losk interface"

System might panic if the network configuration entries in the `/etc/rc` file are not in the recommended order

You should ensure that the entries in the `/etc/rc` file are in the recommended order. The incorrect order can cause prolonged giveback or system reboot time, which might result in a system panic.

For more information about the ordering of entries in the `/etc/rc` file, see the *Data ONTAP 7-Mode System Administration Guide*.

Do not reconfigure the losk interface

If you modify the default configuration of the losk interface, it can result in a system outage. If any IP address or routing configurations related to the losk interface exists in the `/etc/rc` file, you must remove these configurations to avoid any undesirable behavior on the storage system.

File access and protocols cautions

If your storage system is deployed in a NAS environment, you should review the important cautions regarding file access and protocols management and take appropriate action before upgrading or reinstalling.

For more information about these cautions, see the *Data ONTAP 8.0 7-Mode File Access and Protocols Management Guide*.

- "Storage system might panic when not specifying an export path"
- "Oplock breaks might cause panic when using durable handles"

Storage system might panic when not specifying an export path

If you enter the CLI command `exportfs -uf` to remove all entries from the access cache and unexport file system paths, the storage system might panic if you do not specify an export path. It is valid to use the `-f` option without specifying an export path, but not the `-u` option.

To avoid this issue, do not use the `-u` and `-f` options at the same time. Use the `exportfs -f` command to remove all entries from the access cache. Use the `exportfs -ua` command to unexport all file system paths. Use the `exportfs -u` path command to unexport a specific file system path.

Oplock breaks might cause panic when using durable handles

When SMB 2.0 durable handles are enabled, the storage system might panic when sending an oplock break.

To avoid this issue, disable SMB 2.0 durable handles by entering the following command:

```
options cifs.smb2.durable_handle.enable off
```

In a MultiStore environment, you should enter the command for each vFiler unit.

Block access protocol cautions

If your storage system is deployed in a SAN environment, you should review these issues and take appropriate action before upgrading or reinstalling.

For more information about these issues, see the *Data ONTAP 8.1 7-Mode Block Access Management Guide for iSCSI and FC*.

- "2-Gb FC ports not supported as targets"
- "Non-ASCII characters in the comment string of the lun setup command result in system panic"

2-Gb FC ports not supported as targets

Data ONTAP 8.1 does not support the onboard 2-Gb Fibre Channel ports in N7600 or N7800 systems as targets.

The 2-Gb FC ports cannot be initialized if they are configured as targets. If you are upgrading a N7600 or N7800 system from an earlier release, be sure you have moved any FC target traffic to other ports before installing Data ONTAP 8.1.

The onboard 2-Gb Fibre Channel ports can still be used as initiators.

Non-ASCII characters in the comment string of the lun setup command result in system panic

If you enter non-ASCII characters in the comment string while running the `lun setup` command, the system panics. To avoid system panic, you must enter only ASCII characters in the comment string of the `lun setup` command.

Data protection cautions

If your storage system is configured with licenses for data protection technologies, you should review these issues and take appropriate action before upgrading or reinstalling.

For more information about these issues, see the *Data ONTAP 8.0 7-Mode Data Protection Online Backup and Recovery Guide*.

Reversion requirements with volume ComplianceClock and autocommit period of SnapLock volumes

If you are reverting to a previous release of Data ONTAP that supports SnapLock, you must consider the status of the volume ComplianceClock time and autocommit period of the SnapLock volumes.

- Before reverting to a previous release, you must ensure that the volume ComplianceClock value of the SnapLock volumes does not exceed the date, 19 January 2038.

  If it exceeds this date, the revert fails. You can check the volume ComplianceClock time by using the `snaplock clock status` command.
- When reverting to a previous release, if the SnapLock volumes have different autocommit periods, you have to accept the prompt to set the system-wide autocommit period option to `none`.

  You can check the autocommit period of the SnapLock volumes by using the `vol status –v` command.

SnapLock API not supported

Starting with Data ONTAP 8.1, the API `snaplock-get-compliance-clock` and the input parameter is-compliance-clock for the API `clock-get-clock` is no longer supported for SnapLock.

For more information, see the *Data ONTAP 7-Mode Archive and Compliance Management Guide*.

Storage Encryption pre-configuration requirements

In Data ONTAP 8.1 7-Mode, you must perform a number of required steps before you can configure the Storage Encryption feature. If you do not perform these steps before running the Storage Encryption setup wizard, setup fails and you cannot use Storage Encryption.

Configuring `bootarg` variables for Storage Encryption

You must manually configure four bootarg variables before you configure Storage Encryption. You must also perform these steps to update the bootarg variables if the network interface configuration of your storage system changes.

Steps

1. Halt the storage system.
2. At the LOADER prompt, enter the following commands:

   ```
   setenv kmip.init.interface interface_name
   setenv kmip.init.ipaddr interface_ip_address
   setenv kmip.init.netmask netmask
   setenv kmip.init.gateway gateway_ip_address
   ```

Variable	Description
`interface_name`	Specifies the Data ONTAP network interface you want to use. This interface must be dedicated for Storage Encryption use and cannot participate in network trunking or VIF configuration.
`interface_ip_address`	Specifies the IP address of the network interface you specified for `kmip.init.interface`. This is the same IP address you assigned during Data ONTAP setup.
`netmask`	Specifies the netmask for the network interface. This is the same netmask you assigned in Data ONTAP setup.
`gateway_ip_address`	Specifies the gateway for the network interface. This is the same gateway you assigned in Data ONTAP setup.

3. Save the new values by entering the following command:

   ```
   saveenv
   ```

4. Boot Data ONTAP by entering the following command:

   ```
   boot_ontap
   ```

Result

After you complete these steps, you can configure Storage Encryption. For setup instructions for Storage Encryption, see the *Data ONTAP 7-Mode Software Setup Guide*.

Storage system panic due to non-responsive key management server

If one or more of the key management servers configured with Storage Encryption are not available and you use the `key_manager query` command without the `-key_server` option, the storage system might panic.

To avoid this issue, enter the `key_manager status` command before entering the `key_manager query` command. If all key management servers are responding, you can then use the `key_manager query` command as desired. If one or more key management servers are not responding, either first remove them from the configuration using the `key_manager remove` command or query available key management servers individually by using the `key_manager query` command with the `- key_server` option.

Retrieving authentication keys might cause storage system panic

When retrieving authentication keys from all specified key management servers simultaneously, you should avoid a certain scenario to prevent a storage system panic.

When your storage system is configured to use Storage Encryption, you might want to use the `key_manager restore` command to retrieve authentication keys from key management servers. If you run the `key_manager restore` command with the `-all` option to retrieve authentication keys from all specified key management servers simultaneously, but one of the specified key management servers is not available, the storage system might panic.

To avoid this scenario, either verify that all specified key management servers are available before using the `key_manager restore -all` command, or retrieve authentication keys from each key management server individually by entering the following command for each one:

```
key_manager restore -key_server key_server_ip_address [-key_tag key_tag]
```

Known problems and limitations

Some unexpected and potentially undesired behaviors, and in some cases, workarounds to avoid these behaviors, have been identified after upgrading to this release.

Manageability issues

This section describes known issues and limitations with the management interface that affect your ability to manage the storage system. These issues might include problems with command behavior, command output, or error messages presented in the Data ONTAP CLI or web interface and problems with UNIX or operating system commands used to interface with your storage system.

The wrfile command might fail to capture all input during a cut-and-paste operation performed through the RLM or SP

If you access the system console from the RLM or SP and you perform a cut-and-paste operation on graphic input that involves using the `wrfile` command, the command might fail to capture all input.

This behavior is a result of the unusually high sustained data rate in the cut-and-paste operation. You can avoid this issue by using an SSH console session instead of accessing the system console through the RLM or SP.

vFiler DR configuration with the `snapmirror.checkip.enable` option on fails, if SnapMirror fails to authenticate destination IPv6 address

When you configure vFiler units for disaster recovery, if the `snapmirror.checkip.enable` option is set to `on` on the source storage system and the IPv6 address of the source storage system is used for communication, SnapMirror requires the IPv6 address of the destination storage system to set up a SnapMirror relationship.

You must specify the destination storage system's IPv6 address in the list of allowed addresses for SnapMirror relationship on the source storage system. You can add the destination storage system's IPv6 address either to the `snapmirror.access` option, or to the `/etc/snapmirror.allow` file if the `snapmirror.access` option is set to `legacy`.

For more information about the `snapmirror.checkip.enable` option, see the *Data ONTAP 7- Mode Data Protection Online Backup and Recovery Guide*.

NTP version used to communicate with a newly configured NTP server defaults to v3

Starting with Data ONTAP 8.0.2, the Network Time Protocol (NTP) version to be used for communicating with a newly configured NTP server defaults to v3 instead of v4. This change is to address situations where certain time servers support only NTP v3.

Releases prior to Data ONTAP 8.0 use Simple NTP v3 (SNTPv3) by default, while Data ONTAP 8.0 and 8.0.1 use NTP v4 by default. For Data ONTAP 8.0.2 and later releases, the NTP daemon continues to use the highest supported version (v4 in this case) to communicate with the time servers that were configured prior to Data ONTAP 8.0.2.

To reset the time servers to use NTP v3, you can use the `options timed.servers` command to reconfigure the list of servers.

If your system uses `rtc` or `rdate` as the protocol for time synchronization

Starting with Data ONTAP 8.0, the Network Time Protocol (NTP) protocol is the only supported protocol for time synchronization. The `rtc` and the `rdate` protocols of the `timed.proto` option are obsolete and no longer take effect after you upgrade to Data ONTAP 8.0 or later.

If your system does not use NTP as the time-synchronization protocol, it will not keep accurate time after you upgrade it to Data ONTAP 8.0 or later. Problems can occur when the storage system clock is inaccurate.

If your system does not already use NTP as the protocol for time synchronization, immediately after upgrading to Data ONTAP 8.0 or later you must set `timed.proto` to `ntp`, set `timed.servers` to use time servers that support NTP, and ensure that `timed.enable` is set to `on`.

Note: After you set `timed.proto` to `ntp`, the setting remains in effect even if you revert back to a release prior to Data ONTAP 8.0.

For information about how to synchronize the system time, see the *Data ONTAP 7-Mode System Administration Guide*.

If you modify the timed options and then revert to a release prior to the Data ONTAP 8.0 release family

Starting with Data ONTAP 8.0, several `timed` options are obsolete although they remain visible in the CLI and can be modified.

The following `timed` options have no effect in Data ONTAP 8.0 or later:

- The `timed.max_skew` option
- The `timed.sched` option
- The `timed.window` option
- The `rtc` and the `rdate` protocols of the `timed.proto` option

If you attempt to set the above options when the system is running Data ONTAP 8.0 or later, they will have no effect. However, these settings will take effect if the system is reverted back to a release prior to the Data ONTAP 8.0 release family.

Issues regarding the timed log

Starting with Data ONTAP 8.0, the NTP daemon automatically adjusts the storage system time to keep the system clock synchronized with the specified NTP server. However, time adjustments made by the NTP daemon are not logged even when the `timed.log` option is set to `on`.

Issues with `exportfs` commands in non-interactive SSH sessions

Executing `exportfs` commands in non-interactive SSH sessions might fail intermittently.

Running `exportfs` commands by using non-interactive SSH fails when the commands are executed in the following order:

1. `exportfs -p -v` *`options path`*
2. `exportfs -z` *`path`*
3. `exportfs -p -v` *`options path`*

The first two commands execute successfully. However, the third command fails to export the file system path specified as an argument, resulting in the failure of adding an export entry into the `/etc/exports` file.

As a workaround, you can execute `exportfs` before executing the `exportfs -p -v` command, in the following sequence:

1. `exportfs`
2. `exportfs -p -v` *`options path`*
3. `exportfs -z` *`path`*
4. `exportfs`
5. `exportfs -p -v` *`options path`*

Features with the ENABLED keyword in the license command output might require setting the options

Output of the `license` command displays the ENABLED keyword instead of the license key for some features. Before using the features, you might need to use the `options` command to enable them.

For features that were not used with previous versions of Data ONTAP but are now provided free of cost or as part of a software pack for which you have installed a license key, the output of the `license` command displays ENABLED in Data ONTAP 8.1 or later releases. You can enable the following features by using the `options` command:

- Disk sanitization (`licensed_feature.disk_sanitization.enable`)
- Fibre Channel (`licensed_feature.fcp.enable`)
- FlexCache (`licensed_feature.flexcache_nfs.enable`)
- iSCSi (`licensed_feature.iscsi.enable`)
- Multistore (`licensed_feature.multistore.enable`)
- NearStore (`licensed_feature.nearstore_option.enable`)
- VLD (`licensed_feature.vld.enable`)

For more information, see the na_options(1) man page and the Technote FAQ at the following link:

Using License Keys with Data ONTAP 8.1 7-Mode

Storage resource management issues

You should familiarize yourself with these storage resource management issues in this release.

- "Aggregate expansion or the deduplication of a FlexCache origin volume running Data ONTAP 8.1 can cause a system panic"
- "After changing the port assigned to ACP, a reboot is required to regain use of the original port"
- "Configuring ACP to use a different port on N3220 and N3240 storage systems disables ACP for the local SAS expander" on page 99
- "SSD Spare blocks consumed limit reported as "N/A"" on page 99
- "Entering dummy network addresses during ACP setup can cause a system panic" on page 99

Aggregate expansion or the deduplication of a FlexCache origin volume running Data ONTAP 8.1 can cause a system panic

A storage system containing a FlexCache can panic if a Data ONTAP 8.1 origin volume or its containing aggregate undergo aggregate expansion or deduplication.

This problem can occur on FlexCache volumes running a release earlier than Data ONTAP 7.3.6 in the 7.3 release family or Data ONTAP 8.0.2 in the 8.0 release family, with an origin volume running Data ONTAP 8.1. The problem is fixed in Data ONTAP 7.3.6, 8.0.2, 8.1, and later. However, both the FlexCache system and the origin system must have the fix to prevent the problem.

To avoid this problem, take the FlexCache volume offline by using the `vol offline` command before the deduplication of the origin volume or aggregate expansion. When the deduplication or expansion is complete, place the FlexCache volume back online by using the `vol online` command.

After changing the port assigned to ACP, a reboot is required to regain use of the original port

If you reconfigure ACP to use a new port, the port that was configured for ACP before becomes available for use by another subsystem only after you reboot the storage system.

Configuring ACP to use a different port on N3220 and N3240 storage systems disables ACP for the local SAS expander

If you configure ACP to use a different port than e0P (the default) on N3220 and N3240 storage systems, the internal ACPP module IOM6E becomes unresponsive, disabling ACP for the local SAS expander. Unless you are experiencing hardware issues on port e0P, always use the default port for ACP for the N3220 and N3240 storage systems.

SSD Spare blocks consumed limit reported as "N/A"

When Data ONTAP reports status information for SSDs, the Spare blocks consumed limit value is displayed as "N/A." The limit for currently shipping SSDs is 90%.

Entering dummy network addresses during ACP setup can cause a system panic

If you enter dummy network addresses for the networking parameters for ACP, with the intention of filling in real values later, the system could panic.

To avoid this issue, always use correct IP addresses when setting up ACP. See the guidelines published by the Internet Engineering Task Force (www.ietf.org) in RFC1918, Internet Subnets and RFC-1918, Address Allocation for Private Internets.

Network protocol issues

You should familiarize yourself with these network protocol issues in this release.

For more information about these issues, see the *Data ONTAP 8.1 7-Mode Network Management Guide*.

- "SnapMirror transfer cannot be blocked using the interface.blocked.mgmt_data_traffic option"

SnapMirror transfer cannot be blocked using the `interface.blocked.mgmt_data_traffic` option

In a single path SnapMirror transfer, you cannot use the `interface.blocked.mgmt_data_traffic` option to block SnapMirror traffic from e0M on the destination storage system. You can use this option to block SnapMirror transfer only on the source storage system.

To block the SnapMirror traffic on the destination, you must ensure that the IP addresses used in the SnapMirror relationship are not configured on e0M, and

the static, subnet, or default routes configured on the destination do not use e0M to reach the source storage system.

File access protocol issues

If your storage systems provide CIFS, NFS, or FTP client services, you might need to familiarize yourself with file access protocol issues.

For more information about these issues, see the *Data ONTAP 7-Mode File Access and Protocols Management Guide*.

CIFS shares with comment ending with backslash disappear

If you create a CIFS share with a comment that ends with a backslash (\ ), the CIFS share might disappear after rebooting the storage system or restarting CIFS.

To prevent this issue from occurring, do not end comments for CIFS shares with a backslash.

To recover CIFS shares that disappeared due to this issue, follow these steps:

1. Open the file `/etc/cifsconfig_share.cfg`.
2. Locate the command that originally created the CIFS shares that disappeared.
3. Execute the command again but either remove the trailing backslash or add a character such as a space after the backslash.

Error NFS4_BADOWNER when NFSv4 client passes UID as string

NFSv4 specifies users and groups as strings instead of the 32-bit numeric values used by NFSv2 and v3. However, when an NFSv4 client passes the UID as a string instead of the format user_name@domain_name, the NFSv4 server returns the error `NFSV4_BADOWNER` when setting file attributes and user nobody (65534) when obtaining file attributes.

CIFS clients must reopen files after you break locks

If you issue a `lock break` command on files that CIFS clients have currently opened, the CIFS clients must close and reopen the files to be able to further modify them. This is required because breaking locks invalidates the file handles. CIFS clients receive a new valid file handle after reopening the files.

File screening requests fail due to FPolicy server connection timeout

The storage system uses synchronous RPC to ensure reliable communication with FPolicy servers. If the RPC request is not acknowledged, the storage system retransmits the request. If this fails, the request times out after 30 seconds and the storage system breaks the connection with the FPolicy server.

During the 30-second timeout period, the storage system does not handle any further file screening requests.

The storage system attempts to connect to alternative FPolicy servers in the environment if available. If no alternatives are available or the available alternatives also do not respond, FPolicy fails until the storage system can reconnect successfully to an FPolicy server.

Large number of locks might cause temporary performance degradation

If there is a large number of locks (100K+), especially Network Lock Manager (NLM) locks, entering commands that affect locks can cause temporary high CPU utilization and performance degradation. The commands also might take a few minutes to run.

The following commands are affected:

- `lock break`
- `nfs off` followed by `nfs on`
- `cf giveback`

Domain user unable to execute CLI commands

If you log in to the storage system CLI as a domain user and enter the command `cifs gpupdate`, all subsequently entered CLI commands fail with the following error message:

```
[useradmin.unauthorized.user:warning] User domain_name\user_name denied
access - missing required capability: 'cli-options'.
```

If you encounter this issue, log out, then log back in to the CLI.

Storage system requests to Windows Server 2008 might fail

The storage system might encounter Vscan or FPolicy failures when sending scan requests to Vscan or FPolicy servers hosted on Windows Server 2008. This issue is caused by an authentication expiration timer introduced in SMB 2.0 that times out SMB 2.0 connections.

As a workaround, disable SMB 2.0 on the Windows server hosting the Vscan or FPolicy server, or disable the storage system's SMB 2.0 client capability by entering the following command:

```
options cifs.smb2.client.enable off
```

User mapping fails for users in a trusted domain

If a user is a member of a trusted Windows Server 2008 domain, user mapping fails. This is because the storage system tries to communicate with the trusted domain controller using the realm of the domain controller that it is connected to. As a result, Kerberos authentication fails, which then causes user mapping to fail.

The following are possible workarounds for this issue:

- Use domain controllers other than Windows Server 2008 and Windows Server 2003.
- Use Windows Server 2003 domain controllers that do not have Microsoft hotfixes MS11-005 or MS11-014 applied.
- If the domain controller is running Windows Server 2003 and has Microsoft hotfix MS11-014 applied, also apply the patch for hotfix MS11-014.

Reboot required after updating the krb5.conf file

After updating the Kerberos v5 configuration file `/etc/krb5.conf`, you normally have to restart NFS for the change to take effect and Data ONTAP to read the updated file. However, this step currently does not work as expected. Data ONTAP fails to read the updated file after restarting NFS.

To avoid this issue and force Data ONTAP to read the updated file, you must reboot the storage system.

Specification of the default keytab file

When you edit the `/etc/krb5.conf` file to specify a default keytab file, you must use the proper syntax to prevent Kerberos authentication failure.

When using Kerberos v5 for NFS with a UNIX-based KDC, you can optionally edit the principal file `/etc/krb5.conf` to point to a default keytab file. You specify the default keytab file by adding the following line in the `[libdefaults]` section of the principal file `/etc/krb5.conf`:

```
default_keytab_name = FILE:/etc/UNIX_krb5.keytab
```

It is important that you add FILE: to the path to the keytab file. If the Kerberos realm for NFS is an Active Directory-based KDC, Data ONTAP reads the keytab file from memory. However, if the Kerberos realm for NFS is a UNIX-based KDC, Data ONTAP must read the keytab file during authentication. Omitting the FILE: parameter or specifying MEMORY: can lead to Kerberos authentication failure.

Client notification messages in Windows domains require NetBIOS

The Windows client notification feature used for client messaging, shutdown notices, and vscan alerts requires NetBIOS over TCP to be enabled in Data ONTAP.

Similarly, NetBIOS over TCP must be enabled on Windows clients and the Windows Messenger service must be running.

By default, the Windows Messenger service is disabled on Windows 2003 and Windows XP SP2 clients.

Configuration issue for clients that mount NFS shares using a non-reserved port

The `nfs.mount_rootonly` option should be set to `off` on a storage system that must support clients that mount NFS shares using a non-reserved port even when the user is logged in as root. Such clients include Hummingbird clients and Solaris NFS/IPv6 clients.

If the `nfs.mount_rootonly` option is set to on, Data ONTAP allows only clients that use reserved ports (that is, ports with numbers lower than 1024) to mount the NFS shares.

Certain special characters are case sensitive

Some special characters do not have a one-to-one mapping between uppercase and lowercase. Such characters are case sensitive.

For example, if the Unicode character U+03C2 (Greek Small Letter Final Sigma) is present in a file name in the file system, a search for the file fails when using the uppercase Sigma (U+03A3).

This happens because the file system forces characters to lowercase before performing a case-insensitive comparison. The uppercase Sigma is transformed to a lowercase non-final Sigma, which does not match.

To avoid this issue, use the same characters without changing the case when accessing the file. Alternatively, avoid using such characters in file names altogether.

Widelinks are not accessible from Mac clients

When a user attempts to connect to a share using widelinks from a Mac OS X client, the attempt fails. Widelinks are not accessible from Mac OS X clients.

Block access protocol issues

If your storage systems are part of a SAN environment, you might need to familiarize yourself with block access protocol issues in this release.

For more information about these issues, see the *Data ONTAP 7-Mode Block Access Management Guide for iSCSI and FC*.

- "I/O delays sometimes seen after controller failover on Linux hosts with ALUA"
- "If you use the automatic sizing feature on thinly provisioned LUNs when snap reserve is set to a non-zero value"

I/O delays sometimes seen after controller failover on Linux hosts with ALUA

During a controller failover (CFO), hosts running versions of Red Hat Enterprise Linux 6.x or 5.x prior to 5.8; SUSE Linux Enterprise Server 10.x and 11.x; or Oracle Linux 5.x and 6.x with ALUA enabled sometimes encounter either host hangs or long delays in I/O operations. This issue can also cause problems with nondisruptive upgrades (NDU).

The problem occurs when the recovery from the CFO is delayed. The delay causes the ALUA transition period on the controller, which is running Data ONTAP, to take longer. The controller responds to the requests with the message:

```
NOT READY: Asymmetric Access State Transition
```

At that point, the Linux host starts continually retrying its requests. The increased number of retries overwhelms the target and eventually leads to degraded performance, such as long and sometimes stalled I/O operations or situations where the host hangs.

This issue is usually seen in environments that use high-speed interconnects (8 Gb or faster).

This issue is resolved in Red Hat Enterprise Linux 5.8. For more information, see NDU not available for SAN systems with some versions of Linux hosts running high-speed interconnects.

If you use the automatic sizing feature on thinly provisioned LUNs when snap reserve is set to a non-zero value

Generally, before you thinly provision LUNs, you should set `snap reserve` to zero. However, there are rare exceptions that require you to set `snap reserve`

to a value other than zero. In these instances, you must use the automatic sizing feature for thinly provisioned LUNs in FlexVol volumes to work properly.

Using the automatic sizing feature is required because the space from deleted Snapshot copies can only be used to fulfill Snapshot space requests. Furthermore, the automatic deletion process will not begin until the snap reserve value is exceeded.

1. Enter the following command:

   ```
   vol autosize vol_name [-m size] [-I size] on
   ```

   `-m size` is the maximum size to which the volume will grow. Specify a size in `k` (KB), `m` (MB), `g` (GB), or `t` (TB).

   `-I size` is the increment by which the volume's size increases. Specify a size in `k` (KB), `m` (MB), `g` (GB) or `t` (TB).

If the specified FlexVol volume is about to run out of free space and is smaller than its maximum size, and if there is space available in its containing aggregate, the FlexVol volume's size will increase by the specified increment.

Data protection issues

If you use data protection products that include Snapshot technology (such as SnapRestore, SnapVault, SnapMirror, and SnapManager), you might have to familiarize yourself with relevant data protection issues.

For more information about these issues, see the *Data ONTAP 7-Mode Data Protection Online Backup and Recovery Guide* and the *Data ONTAP 7-Mode Data Protection Tape Backup and Recovery Guide*.

Aggregate Snapshot copy creation and `aggr copy` commands fail with an aggregate Snapshot reserve of 0 percent

Starting with Data ONTAP 8.1, a newly created nonmirrored aggregate has the aggregate Snapshot reserve set to `0` percent by default. This default prevents you from creating an aggregate Snapshot copy or running the `aggr copy` commands.

For aggregate Snapshot copy creation and the `aggr copy` commands to succeed, you must increase the aggregate Snapshot reserve to a non-zero percentage.

SMTape restore to an offline volume overwrites the data on that volume

If you perform an SMTape restore to an offline volume, the data on tape overwrites the data on that offline volume.

Restore engine does not honor any mandatory or advisory locks on files

The destination volume for a restore operation might have files with mandatory or advisory locks. When you initiate a restore operation to such a volume, the restore engine does not honor these locks. It ignores these locks and overwrites the files.

Tape devices behind Decru DataFort are not detected unless a known SCSI device is mapped to LUN 0

If a known SCSI device is not mapped to LUN 0 when using a Decru DataFort appliance, the tape drives and media changers behind the Decru DataFort appliance are not detected.

To avoid this issue, you must ensure that the following actions have been performed:

- When configuring a tape library, you must assign LUN 0 to SCSI devices such as, tape drives, media changers, and SCC devices for them to be detected and accessed by the storage system.
- When connecting a tape library through a Decru DataFort appliance, the tape drive, media changer, or SCC device assigned to LUN 0 must also be mapped to a DataFort Cryptainer.

  This enables the storage system to detect LUN 0 and also the SCSI devices attached to it.

Third-party storage issues (Gateway systems only)

There are certain issues and restrictions you should be aware of when Data ONTAP uses third-party storage.

- "Restrictions for gateway system upgrade to Data ONTAP 8.1"
- "Exceeding the maximum number of assigned devices results in a panic"

Restrictions for gateway system upgrade to Data ONTAP 8.1

Do not upgrade your gateway system to run Data ONTAP 8.1 unless the Gateway Support Matrix lists your storage array as supported in Data ONTAP 8.1.

Before starting an upgrade of your gateway system to run Data ONTAP 8.1, check the Gateway Support Matrix to ensure that your storage array is supported in Data ONTAP 8.1.

See the Gateway Support Matrix, located on the IBM N series support website, which is accessed and navigated as described in "Websites" on page 3

If your storage array is not supported in Data ONTAP 8.1, and you attempt to upgrade to 8.1, Data ONTAP generates an error message such as the following:

```
[sundance1:mlm.array.unsupported:warning]: Array LUN [S/N
'60050768019181C8B00000000000004E' vendor 'xxx ' product 'yyy '] is not
supported in this version of Data ONTAP.
```

If you upgrade your gateway system to run Data ONTAP 8.1 and the storage array is not supported in 8.1, you must revert Data ONTAP to an earlier release. See the *Upgrade Downgrade/Revert Guide* for information about how to revert your system to an earlier release.

Exceeding the maximum number of assigned devices results in a panic

If more than 256 LUNs from the same storage array port to the same gateway FC initiator port are assigned to the gateway system, the gateway system panics if you try to boot it and issues a message similar to the following:

```
PANIC: ../common/raidv2/pool_sort.c:2359: Assertion failure. in SK process
config_thread on release Data ONTAP Release 7.3.2
```

Platform maintenance issues

You need to be familiar with the known issues and limitations that affect your ability to perform hardware maintenance on the storage system.

- "Possible giveback failure during controller or NVRAM8 replacement on N7x50T or N6200 series"

Possible giveback failure during controller or NVRAM8 replacement on N7x50T or N6200 series

Due to a known issue, when doing a nondisruptive replacement of the NVRAM8 adapter on a N7x50T or a controller module on a N6200 series, the `cf giveback` or `storage failover giveback` command might fail after the hardware replacement is complete.

Changes to published documentation

Some information about this release has become available after the set of guides provided with this release were published. The information should be used in conjunction with the guides provided with this release of Data ONTAP.

Changes to the System Administration Guide

Additional information has become available since the last revision of the *Data ONTAP 7-Mode System Administration Guide*.

- "UPS management information is no longer applicable"
- "Corrections for the location of the secureadmin.pem file"
- "Corrections to AutoSupport options"

UPS management information is no longer applicable

You can disregard the uninterruptible power supply (UPS) information in the *Data ONTAP 7-Mode System Administration Guide*. As of Data ONTAP 8.1, the `ups` command is no longer supported. However, the UPS device continues to function.

Corrections for the location of the secureadmin.pem file

The 'Installing a certificate-authority-signed certificate' section of the *Data ONTAP 7-Mode System Administration Guide* contains incorrect information for the location of the `secureadmin.pem` file. The correct directory for the file is `/etc/keymgr/csr`.

Corrections to AutoSupport options

The section titled AutoSupport options in the *Data ONTAP 7-Mode System Administration Guide* includes incorrect and missing information.

The following information is incorrect or missing in the AutoSupport options section:

- The name of the `autosupport.validate_http_certificate` option is incorrect. The correct name is `autosupport.validate_digital_certificate`.
- The following AutoSupport options are missing:

  autosupport.cifs.verbose
  Enables and disables inclusion of CIFS session and share information in AutoSupport messages. The default is `off`.

  autosupport.local_collection
  Enables and disables local storage of AutoSupport files when sending of AutoSupport messages is disabled. The default setting is `on`, which causes the node to store AutoSupport files locally even if AutoSupport is disabled.

  autosupport.payload.format
  Specifies the file format of the compressed file that contains AutoSupport data. Use `7z` to specify 7-Zip archive format. Use `tgz` to specify GNU zipped tar file. The default is `7z`.

Changes to the High-Availability Configuration Guide

There are some changes to the existing content of the Data ONTAP 7-Mode High-Availability Configuration Guide.

- "Incorrectly specified default value of the cf.giveback.auto.terminate.bigjobs option"
- "Mention of ESH2 disk shelf modules"
- "Preferred primary port information in the shared-switches section"

Incorrectly specified default value of the cf.giveback.auto.terminate.bigjobs option

The section Setting giveback to terminate long-running processes in the Data ONTAP 7-Mode High-Availability Configuration Guide states that the default value of the `cf.giveback.auto.terminate.bigjobs` option is `on`. However, the default value is actually `off`.

Mention of ESH2 disk shelf modules

Note that although the *Data ONTAP 7-Mode High-Availability Configuration Guide* mentions the ESH2 module, the ESH2 module is not supported in this release of Data ONTAP.

Preferred primary port information in the shared-switches section

Although the information about setting the preferred primary port is provided in the shared-switches section, it is also applicable to the dedicated switches in a MetroCluster configuration.

For more information about setting the preferred primary port, *see the Data ONTAP 7-Mode High-Availability Configuration Guide*.

Changes to the Commands Manual Page Reference

New information has become available since the previous revision of the *Data ONTAP Commands: Manual Page Reference*.

- "Commands not supported in Data ONTAP 8.1 7-Mode release"

Commands not supported in Data ONTAP 8.1 7-Mode release

The `ups` and `filestats` commands are included in the latest version of the *Data ONTAP 7-Mode Commands: Manual Page Reference, Volume 1*, but these commands are not supported in the Data ONTAP 8.1 7-Mode release.

Changes to the File Access and Protocols Management Guide

New information has become available since the previous revision of the *Data ONTAP 7-Mode File Access and Protocols Management Guide*.

- "Corrections to the FPolicy commands to monitor directory operations"
- "Correction of SFTP options"

Corrections to the FPolicy commands to monitor directory operations

The *Data ONTAP 7-Mode File Access and Protocols Management Guide* includes incorrect FPolicy commands for monitoring directory operations.

The correct FPolicy commands to monitor directory operations are as follows:

If you want to monitor directory operations for...	Enter the command...
Creating	`fpolicy monitor add policy_name create_dir`
Renaming	`fpolicy monitor add policy_name rename_dir`
Deleting	`fpolicy monitor add policy_name delete_dir`

Correction of SFTP options

The *Data ONTAP 7-Mode File Access and Protocols Management Guide* mentions three options with an incorrect name in the section *Managing the Secure File Transfer Protocol*.

The options and their correct names are as follows:

Option name as mentioned	Correct option name
`sftp.log.enable`	`sftp.log_enable`
`sftp.log.filesize`	`sftp.log_filesize`
`sftp.log.nfiles`	`sftp.log_nfiles`

Changes to the Block Access Management Guide for iSCSI and FC

New information has become available since the previous revision of the *Data ONTAP Block Access Management Guide for iSCSI and FC*.

Correction to the DCB setting example

The result in the topic *Displaying DCB settings* has an incorrect example. The *Applications* column incorrectly lists *IP* instead of *unassigned* .

The corrected example is as follows:

```
system1> dcb priority show e2b
  Interface  Priority  Applications  Flow Control  PGID
  ---------  --------  ------------  ------------  ----
  e2b
             0         unassigned    enabled          0
             1         unassigned    disabled         1
             2         unassigned    disabled         1
             3         FCoE          enabled          2
             4         unassigned    disabled         1
             5         unassigned    disabled         1
             6         unassigned    disabled         1
             7         unassigned    disabled         1
```

Enabling the FC license

You must enable FC license to use the FCP target service.

About this task

Depending on the hardware platforms, you can enable the FC license by either adding the license key or turning the `fcp` option `on`.

You must enable the `fcp` option for the N3400 hardware platform.

Step

1. Depending on your hardware platform, enter the appropriate command to enable FC:

If you want to...	Enter the following command...
Enable the fcp option	licensed_feature.fcp.enable on
Enable the FC license	license add *fcp_license_code*

The following output example shows that the FC license is enabled:

```
A fcp site license has been installed.
Run 'fcp start' to start the FCP service.
Also run 'lun setup' if necessary to configure LUNs.
        FCP enabled.
Mon Mar 26 12:18:31 UTC [system1: rc:notice]: fcp licensed
```

Disabling the FC license

If you do not want to use the FCP target service on the system, you can disable the FC license.

About this task

Depending on the hardware platforms, you can disable the FC license by either deleting the license key or turning the fcp option off.

You must disable the fcp option for the N3400 hardware platform.

Note: If you delete the license, you cannot access the FCP service and the FCP target connectivity is lost. Therefore, any LUNs being served to the initiators are terminated.

Step

1. Depending on your hardware platform, enter the appropriate command to disable FC:

If you want to...	Enter the following command...
Disable the fcp option	licensed_feature.fcp.enable off
Disable the FC license	license delete fcp

The following output example shows that the FC license is disabled:

```
Mon Mar 26 12:17:15 UTC [system1: rc:notice]: fcp unlicensed
Mon Mar 26 12:17:14 UTC [system1:fcp.service.shutdown:info]: FCP service shutdown
```

Enabling the iSCSI license

You must enable the iSCSI license to use the iSCSI target service.

About this task

Depending on the hardware platforms, you can enable the iSCSI license by either adding the license key or turning the `iscsi` option `on`.

You must enable the `iscsi` option for the N3400, N5000, N6000, and N7000 hardware platforms.

Step

1. Depending on your hardware platform, enter the appropriate command to enable iSCSI:

If you want to...	Enter the following command...
Enable the `iscsi` option	`licensed_feature.iscsi.enable on`
Enable the iSCSI license	`license add` *`iscsi_license_code`*

The following output example shows that the iSCSI license is enabled:

```
system1>license add IKVAREM
A iscsi site license has been installed.
system1> Successfully wrote license db update for volume aggr0
Run 'iscsi start' to start the iSCSI service.
Also run 'lun setup' if necessary to configure LUNs.
Mon Mar 26 15:58:53 GMT [system1: rc:notice]: iscsi licensed
```

Disabling the iSCSI license

If you do not want to use the iSCSI service on the system, you can disable the iSCSI license.

About this task

Depending on the hardware platforms, you can disable the iSCSI license by either deleting the license key or turning the `iscsi` option `off`.

You must disable the `iscsi` option for the N3400, N5000, N6000, and N7000 hardware platforms.

Note: If you delete the iSCSI license, all the iSCSI sessions close and iSCSI connectivity is lost.

Step

1. Depending on your hardware platform, enter the appropriate command to disable iSCSI:

If you want to...	Enter the following command...
Disable the `iscsi` option	`licensed_feature.iscsi.enable off`
Disable the iSCSI license	`license delete iscsi`

The following output example shows that the iSCSI license is disabled:

```
system1> license delete iscsi
Mon Mar 26 16:00:55 GMT [system1:iscsi.service.shutdown:info]: iSCSI service shutdown
unlicensed iscsi.
        iSCSI disabled.
Mon Mar 26 16:00:56 GMT [system1: rc:notice]: iscsi unlicensed
```

Changes to the Requirements for performing a volume move topic

The "Requirements for performing a volume move" topic has an update and some incorrect information.

- You cannot move a volume from a 32-bit aggregate to a 64-bit aggregate, or from a 64-bit aggregate to a 32-bit aggregate.

  This is the update.
- A compressed 64-bit volume to a 32-bit volume is an incorrect statement and should be removed.
- The existing note about fingerprint database and change logs is incorrect.

  The correct information is that the fingerprint database and change logs are moved along with the source volume.

iSCSI does not support ALUA

The "Configuring iSCSI target portal groups" topic in the "iSCSI network management" chapter includes information about enabling ALUA. This topic has to be removed because you cannot enable ALUA on iSCSI groups.

Changes to the Upgrade and Revert/Downgrade Guide

New information about upgrade procedures has become available since the previous revision of the *Data ONTAP 7-Mode Upgrade and Revert/Downgrade Guide*.

- “Incorrect examples for software image installation” on page 121

Incorrect examples for software image installation

The topic Installing software images from the `/etc/software` directory includes examples describing installation from an HTTP server. The HTTP examples are not relevant to this topic and can be safely ignored.

Changes to the Storage Management Guide

Additional information has become available since the last revision of the *Data ONTAP 7-Mode Storage Management Guide*.

- "SnapMirror semi-synchronous mode is not supported with deduplication"
- "SnapMirror semi-synchronous mode is not supported with data compression"
- "Correction to the total logical size of FlexClone files and FlexClone LUNs in a FlexVol volume"

SnapMirror semi-synchronous mode is not supported with deduplication

The topic titled Deduplication interoperability with Data ONTAP features does not indicate that deduplicated volumes cannot be replicated using semi-synchronous SnapMirror.

SnapMirror semi-synchronous mode is not supported with data compression

The topic titled Features not supported with data compression does not indicate that data compression is not supported with semi-synchronous SnapMirror operations.

Correction to the total logical size of FlexClone files and FlexClone LUNs in a FlexVol volume

The section titled How FlexClone files and FlexClone LUNs work incorrectly mentions the total logical size of FlexClone files and FlexClone LUNs in a FlexVol volume as 16TB.

The total logical size of FlexClone files and FlexClone LUNs in a FlexVol volume is 640 TB, and is independent of the maximum size limit for the volume.

Changes to Gateway documentation

Additional information has become available since the last revision of the gateway documentation

- "Format change to the Gateway Implementation Guides"

Format change to the Gateway Implementation Guides

Details about deploying all storage arrays with gateway systems are now provided in a single implementation guide.

Previously, details about deploying gateway systems with storage arrays were provided in separate vendor-specific Implementation Guides (for example, the *Gateway Implementation Guide* for IBM Storage). Details about all vendors' storage arrays are now covered in a single implementation guide called the *Gateway Implementation Guide for Third-party Storage*. The guide contains a separate section for the information specific to each vendor.

Copyright and trademark information

This section includes copyright and trademark information, and important notices.

Copyright information

The product described in this manual may be protected by one or more U.S.A. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark information

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. A complete and current list of other IBM trademarks is available on the Web at http://www.ibm.com/legal/copytrade.shtml

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

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

UNIX is a registered trademark of The Open Group in the United States and other countries.

NetApp, the NetApp logo, Network Appliance, the Network Appliance logo, Akorri, ApplianceWatch, ASUP, AutoSupport, BalancePoint, BalancePoint Predictor, Bycast, Campaign Express, ComplianceClock, Cryptainer, CryptoShred, Data ONTAP, DataFabric, DataFort, Decru, Decru DataFort, DenseStak, Engenio, Engenio logo, E-Stack, FAServer, FastStak, FilerView, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexSuite, FlexVol, FPolicy, GetSuccessful, gFiler, Go further, faster, Imagine Virtually Anything, Lifetime Key Management, LockVault, Manage ONTAP, MetroCluster, MultiStore, NearStore, NetCache, NOW (NetApp on the Web), Onaro, OnCommand, ONTAPI, OpenKey, PerformanceStak, RAID-DP, ReplicatorX, SANscreen, SANshare, SANtricity, SecureAdmin, SecureShare, Select, Service Builder, Shadow Tape, Simplicity, Simulate ONTAP, SnapCopy, SnapDirector, SnapDrive, SnapFilter, SnapLock, SnapManager, SnapMigrator, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapSuite, SnapValidator, SnapVault, StorageGRID, StoreVault, the StoreVault logo, SyncMirror, Tech OnTap, The evolution of storage, Topio, vFiler, VFM, Virtual File Manager, VPolicy, WAFL, Web Filer, and XBB are trademarks or registered trademarks of NetApp, Inc. in the United States, other countries, or both.

All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such.

NetApp is a licensee of the CompactFlash and CF Logo trademarks.

NetApp NetCache is certified RealSystem compatible.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe on any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, N.Y. 10504-1785
U.S.A.

For additional information, visit the web at:
http://www.ibm.com/ibm/licensing/contact/

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make

improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM web sites are provided for convenience only and do not in any manner serve as an endorsement of those web sites. The materials at those web sites are not part of the materials for this IBM product and use of those web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

If you are viewing this information in softcopy, the photographs and color illustrations may not appear.

NA 210-05602_A0, Printed in USA

GA32-1032-03