## Contents

### Data ONTAP 7.3.6 Release Notes
- About the Data ONTAP 7.3.6 release ..................................................... 1
- About these release notes ................................................................. 1
- Upgrade information ............................................................................ 2
- Websites ................................................................................................. 2

### Changes introduced since Data ONTAP 7.3
- Changes in the 7.3.6 release ................................................................. 3
- Changes in the 7.3.5.1 release ............................................................... 6
- Changes in the 7.3.5 release ................................................................. 8
- Changes in the 7.3.4 release ................................................................. 11
- Changes in the 7.3.3 release ................................................................. 14
- Changes in the 7.3.2 release ................................................................. 17
- Changes in the 7.3.1.1L1 release ........................................................... 21
- Changes in the 7.3.1.1 release ............................................................... 22
- Changes in the 7.3.1 release ................................................................. 24

### New and changed features
- Changes to supported hardware and features.......................................... 31
  - TOE automatically disabled ................................................................. 32
  - Flow control may be reported randomly by FC 1031 10-Gb NIC with certain switches ......................................................... 32
  - Considerations .................................................................................... 32
  - Support for SnapVault integration options for use with NetBackup ........ 33
- New platform and hardware support ....................................................... 34
  - Support for the N6200 series storage systems .................................... 34
  - Support for 2 TB SATA disks ............................................................... 35
  - Unrestricted increased aggregate capacity for N3300 systems ............. 35
  - New disk drive AutoSupport message sent weekly ............................ 35
  - Support for N3400 ........................................................................... 35
  - Support for EXN3500 storage expansion units .................................. 35
  - Support for EXN3000 storage expansion units .................................. 36
  - Support for N6000 series systems ..................................................... 36
  - Nondisruptive Upgrade Supported for SATA disk drives ................. 36
  - UPS support .................................................................................... 37
  - Support for 512-GB and 256-GB Flash Cache modules ...................... 37
  - Supported tape drives ................................................................... 37
- Manageability enhancements ................................................................. 38
  - Supported OpenSSH client versions .................................................. 38
  - The Service Processor for the N6200 series storage systems ............. 38
  - Enhancements that allow you to specify SSL versions ...................... 40
  - SSL security improvements ............................................................... 40
  - Nondisruptive upgrades for storage expansion units controlled by AT-FCX modules .......................................................... 40
  - Changes to the upgrade preparation process ..................................... 40
  - Improved support for nondisruptive upgrades in SAN environments ... 41
  - Read reallocation of data ................................................................ 41
<table>
<thead>
<tr>
<th>Feature</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extents for FlexVol volumes</td>
<td>41</td>
</tr>
<tr>
<td>Option to disable root access to the storage system</td>
<td>42</td>
</tr>
<tr>
<td>Audit log enhancement</td>
<td>42</td>
</tr>
<tr>
<td>Read-only access to FilerView</td>
<td>43</td>
</tr>
<tr>
<td>Physical reallocation of data</td>
<td>43</td>
</tr>
<tr>
<td>Performance Acceleration Module (PAM), Flash Cache module, and WAFL external cache</td>
<td>43</td>
</tr>
<tr>
<td>FilerView enhancements</td>
<td>44</td>
</tr>
<tr>
<td>The e0M interface</td>
<td>44</td>
</tr>
<tr>
<td>Data ONTAP supports up to 24 SSH sessions</td>
<td>45</td>
</tr>
<tr>
<td>Only critical AutoSupport notifications are sent to the autosupport.to recipients</td>
<td>45</td>
</tr>
<tr>
<td>Partner recipients for AutoSupport email notifications</td>
<td>45</td>
</tr>
<tr>
<td>File access protocol enhancements</td>
<td>46</td>
</tr>
<tr>
<td>Support for multiple open instances of the SMB named pipe on an FPolicy server</td>
<td>46</td>
</tr>
<tr>
<td>Support for the SMB 2.0 protocol</td>
<td>46</td>
</tr>
<tr>
<td>Kerberos Multi Realm support</td>
<td>46</td>
</tr>
<tr>
<td>NFSv4 enhancements</td>
<td>47</td>
</tr>
<tr>
<td>Enhancements to NFS access cache management</td>
<td>47</td>
</tr>
<tr>
<td>Improved security for Perfmon connections</td>
<td>48</td>
</tr>
<tr>
<td>New commands for debugging CIFS access control problems</td>
<td>48</td>
</tr>
<tr>
<td>New option for setting the minimum authentication level and session security level that clients must use</td>
<td>48</td>
</tr>
<tr>
<td>FPolicy enhancements</td>
<td>48</td>
</tr>
<tr>
<td>Maximum number of auxiliary UNIX groups supported for a user</td>
<td>49</td>
</tr>
<tr>
<td>Compatibility with Windows Vista and Windows Server 2008</td>
<td>49</td>
</tr>
<tr>
<td>Block protocols enhancements</td>
<td>50</td>
</tr>
<tr>
<td>10-GbE Unified Target Adapter protocol support</td>
<td>50</td>
</tr>
<tr>
<td>Takeover and giveback performance enhancements in a SAN environment</td>
<td>50</td>
</tr>
<tr>
<td>Ability to delete backing Snapshot copies of deleted LUN clones</td>
<td>50</td>
</tr>
<tr>
<td>New default value for the maximum number of iSCSI connections per session</td>
<td>51</td>
</tr>
<tr>
<td>WWPN aliases</td>
<td>51</td>
</tr>
<tr>
<td>New windows_2008 LUN Multiprotocol Type (ostype)</td>
<td>51</td>
</tr>
<tr>
<td>New solaris_Efi, xen, and hyper_v LUN Multiprotocol Types (ostypes)</td>
<td>52</td>
</tr>
<tr>
<td>Networking and Security protocols enhancements</td>
<td>53</td>
</tr>
<tr>
<td>Ability to block data traffic on the e0M interface</td>
<td>53</td>
</tr>
<tr>
<td>Support for IPv6</td>
<td>54</td>
</tr>
<tr>
<td>IPv6 RFCs supported</td>
<td>54</td>
</tr>
<tr>
<td>Support for CDP</td>
<td>56</td>
</tr>
<tr>
<td>Transport Layer Security protocol</td>
<td>57</td>
</tr>
<tr>
<td>TLS support in FilerView</td>
<td>57</td>
</tr>
<tr>
<td>Port-based load-balancing option for multimode vifs</td>
<td>58</td>
</tr>
<tr>
<td>WAFL External cache group added to netapp.mib</td>
<td>58</td>
</tr>
<tr>
<td>Round-robin load balancing is supported</td>
<td>58</td>
</tr>
<tr>
<td>SNMPv3 supported</td>
<td>59</td>
</tr>
<tr>
<td>New maximum number of network interfaces</td>
<td>59</td>
</tr>
<tr>
<td>RLM supports IPv6</td>
<td>60</td>
</tr>
<tr>
<td>Data protection enhancements</td>
<td>61</td>
</tr>
<tr>
<td>Use of SnapVault to protect a volume SnapMirror destination</td>
<td>62</td>
</tr>
<tr>
<td>TCP window size for a SnapMirror relationship</td>
<td>62</td>
</tr>
<tr>
<td>Retention of older SnapVault Snapshot copies on SnapVault secondary volumes</td>
<td>62</td>
</tr>
<tr>
<td>Support for SnapMirror network compression</td>
<td>63</td>
</tr>
</tbody>
</table>
If volumes with deduplication exceed the maximum supported size.

Snapshot copies and log files of SnapLock for SnapVault use system clock for naming.

Changes to the SnapLock autocommit feature.

Backing up LUN clones to tape.

SnapLock supported in Data ONTAP 7.3.1 and later.

LockVault now known as the SnapLock for SnapVault feature.

More concurrent transfers for qtree SnapMirror, volume SnapMirror, and SnapVault.

Maximum number of concurrent replication operations with ATA disks.

Reservation of storage system resources for volume SnapMirror, qtree SnapMirror, and SnapVault replication operations.

Synchronous SnapMirror modes.

Space guarantee for a volume SnapMirror destination.

Support for SnapMirror over Fibre Channel on N3600 storage systems.

SnapVault integration with SnapManager.

SnapVault primary and secondary on the same storage system.

Enhancements to SnapVault for NetBackup.

Bandwidth optimization for Open Systems SnapVault.

SnapVault for NetBackup supports basic block mode backups.

SnapVault with deduplication.

Deduplication metadata relocated.

Deduplication configuration data relocated.

Deduplication support on SnapLock volumes.

Deduplication checkpoint feature.

SnapLock support for vFiler units.

Qtree SnapMirror with deduplication.

Volume SnapMirror with deduplication.

Limit on entries in the snapmirror.conf file for each storage system.

Automatic schedule for deduplication.

Support for 840 disk drives on fabric-attached MetroClusters.

Storage resource management enhancements.

FlexClone files and FlexClone LUNs.

Aggregate size calculation changes.

Maximum number of data disks per 16-TB aggregate.

SnapMirror destination space guarantee not disabled.

Autogrow capability for FlexCache volumes.

Support for changing to software-based disk ownership nondisruptively.

Disconnected operation for FlexCache volumes.

FlexClone files and FlexClone LUNs support on vFiler units.

Active/active configuration enhancements.

Hardware-assisted takeover feature support for IPv6 addresses.

MetroCluster support for IPv6 addresses.

Support for 672 disk drives on fabric-attached MetroClusters.

MetroCluster nodes on separate subnets.

Hardware-assisted takeover.

Deduplication support on stretch and fabric-attached MetroClusters.

Major nondisruptive upgrades for fabric-attached MetroClusters.

MultiStore enhancements.

New option for the vfiler dr configure command.

Online migration support on vFiler units.

Commands supported by the ONTAPI interface library.
Secure communication for setup of disaster recovery and data migration .................................. 79
SnapMover license is not required ................................................................................................. 79
Deduplication support on vFiler units ......................................................................................... 79
New AutoSupport message for transparent vfiler migration ....................................................... 79

New and changed commands and options. ................................................................................ 81
New commands in Data ONTAP 7.3. ............................................................................................ 82
Changed commands in Data ONTAP 7.3 . .................................................................................... 87
New options in Data ONTAP 7.3 . ............................................................................................... 96
Changed options in Data ONTAP 7.3 . ....................................................................................... 102
Replaced or removed commands in Data ONTAP 7.3. ................................................................. 104
SnapMirror commands that become obsolete in Data ONTAP 8.0. ........................................... 105

Requirements for running Data ONTAP 7.3.6 .................................................................... 107
Storage system firmware .................................................................................................. 108
Storage systems that support Multipath Storage .................................................................. 109
Gateway requirements and support information .................................................................... 110

Important cautions. .................................................................................................................. 111
Manageability cautions ............................................................................................................ 112
Issues in certificate MD5 signature collision vulnerability ....................................................... 112
Upgrade and revert cautions .................................................................................................... 113
New FlexVol volume space requirements when upgrading from a release earlier than Data ONTAP 7.3 . .......................................................................................................................... 113
Determining system capacity and space guarantees ................................................................. 114
If you are upgrading an N6000 or N6200 series storage system in an iSCSI environment .... 114
New RLM firmware and its upgrade requirements .................................................................. 115
If you are performing a nondisruptive upgrade on a system with VMware ESX Server hosts .. 115
If you are upgrading a system that includes FlexCache volumes ............................................. 116
If you are upgrading an N5500 storage system ...................................................................... 116
If you have been using the flex_cache license ....................................................................... 117
If you are using SharedStorage ............................................................................................... 117
If you are upgrading an N3300 system running Data ONTAP 7.2.2L1 .................................... 117
BMC firmware upgrades for N3300, N3400 or N3600 storage systems .............................. 117
If you are upgrading to a 4 Gb HBA in a SAN environment .................................................... 118
If you are upgrading from a 2 Gb onboard port to a 4 Gb adapter in a SAN environment ....... 118
Requirements for reverting to a Data ONTAP release with a lower maximum capacity ...... 118
If you are reverting to a previous release and you use large ACLs under NFSv4 ................. 119
If you revert a system that has an FC 1062 or FC 1065 Ethernet card installed .................... 120

Network protocol cautions ........................................................................................................ 121
If you use a vif that is named "vip" ......................................................................................... 121
Renaming a vif ....................................................................................................................... 121
If your system uses ATM for network connectivity ................................................................. 121
Block access protocol cautions ............................................................................................... 122
Identical WWPNs can occur on both nodes in a cluster ......................................................... 122
If you deploy ALUA on storage systems with FCP or iSCSI ............................................... 122
If jumpers J3 and J4 on 2 Gbps Fibre Channel target expansion are in positions 2 and 3 ....... 122
If you use Solaris 10 and the Emulex Fibre Channel Adapter driver ........................................ 123
If an iSCSI target HBA fails .................................................................................................. 123
If you use the automatic sizing feature on thinly provisioned LUNs when snap reserve is set to a non-zero value

Considerations ............................. 123
Example. .................................... 123

Data protection cautions ............................. 124
SnapLock Compliance volume upgrade requirement ........................................... 124
Issues in SnapLock interaction with active/active configuration .............................. 125
Issues in moving SnapLock disks ...................................................................... 125
Issues in booting a system running Data ONTAP 7.3.1 with the first release of Data ONTAP 7.3 126
Issues in upgrading to Data ONTAP 7.3 if you have SnapLock volumes ....................... 126
If you upgrade systems running FPolicy .................................................................. 127
Issues in reverting to Data ONTAP 7.3 if you have SnapLock volumes ....................... 127
If you are reverting to a previous release that does not support deduplication with SnapLock volumes ................................................................. 127
If you use SnapLock Compliance and FlexClone copies ........................................ 128
Limitation of SnapLock for SnapVault relationship ............................................... 128
If you use DataFabric Manager to manage SnapMirror or SnapVault relationships between vFiler units ................................................................. 128
If you revert to a prior release, for a SnapMirror destination with volumes using deduplication or clone operations ........................................................... 129
Storage management cautions ............................................................................ 130
If you are reverting to a previous release and you use deduplication ......................... 130

Known problems and limitations ................................................................. 133
Manageability issues .................................................................................... 134
Issues with exportfs commands in non-interactive SSH sessions ......................... 134
vFiler DR configuration with the snapmirror.checkip.enable option on fails, if SnapMirror fails to authenticate destination IPv6 address ........................................... 134
No IPv6 support for AutoSupport e-mail notifications ........................................ 135
AutoSupport option settings ............................................................................ 135
Change in systat -x command output ............................................................... 135
RLM configuration is not saved if the RLM's Ethernet cable is not connected .......... 135
File access protocol issues ............................................................................ 136
Order of steps when enabling SSL for LDAP traffic ........................................... 136
FPolicy quota and user reports show incorrect file size ........................................ 137
Failed CIFS connections due to signature mismatch ........................................ 137
Configuring user mapping for a default user quota with CIFS not enabled could severely degrade performance ............................................................... 137
Excessive pending CIFS authentication requests can cause service disruption ......... 138
Empty CIFS/SMB2.x change notifications ....................................................... 138
Correction to required FPolicy screening requests ............................................ 139
FPolicy file extension issue on revert ............................................................... 139
FPolicy compatibility issue in NFSv4 environments .......................................... 139
Limitations in the naming of FPolicy policies ................................................... 140
Some Group Policy Objects (GPOs) are applied differently on storage systems than on Windows systems ................................................................. 140
Client notification messages in Windows domains require NetBIOS ...................... 140
Unsupported Windows features in the file serving environment ........................... 140
Configuration issue for clients that mount NFS shares using a non-reserved port .................................................. 141
NFSv4 client compatibility .................................................... 141
Unicode character 0x0080 is not supported .................................. 141
The FTP server does not support Unicode characters .................... 141
No IPv6 support in FPolicy .................................................. 142
Network protocol issues .................................................... 143
FC 1062 interface on an N3600 storage system fails if the configuration settings are changed .................. 143
Authentication failure when IPsec is used with Kerberos ............ 143
The ping6 usage message is incorrect ..................................... 143
Single-mode vif does not fail over correctly ................................ 144
TOE is disabled ............................................................. 144
No IPv6 support for RIP and IPsec ......................................... 145
Do not use vlan delete -q with ipsec ..................................... 145
Enable caching with NIS lookup ........................................... 145
Potentially reduced performance for IPsec traffic ....................... 145
Block access protocol issues .............................................. 146
Disks offline in Windows 2008 after a standard upgrade ............. 146
“option lun.partner_unreachable.default-partner.behavior: Value must be ‘drop’, ‘error’, or ‘start’” error message periodically displays ................................................. 146
FCoE adapters may fail to come online if the FCP service is stopped and started too quickly .......... 147
Brocade 200E switch speed must be set manually ....................... 147
Setting Brocade 200E switch speed manually .......................... 147
Ongoing cfmode support ................................................... 148
cfmode restrictions for 8-Gb target expansion adapters ................ 148
Data protection issues ..................................................... 149
Data transfer speed reduces when LSI Logic 1030 Ultra320 SCSI HBA is used with tape drives (FC 1024) ................................................................. 149
Data recovery using SnapVault or SnapMirror for a qtree with LUN clones .................................................. 150
SnapVault ................................................................. 150
Qtree SnapMirror ........................................................ 150
Using SnapVault for NetBackup to protect applications ................ 150
SnapVault for NetBackup is not supported with Symantec Veritas NetBackup 6.5 ........................ 151
Changes to deduplication usage with SnapVault for NetBackup ...... 151
NetBackup managed SnapVault is unavailable ......................... 151
Limitations when using SnapVault with vfiler units .................. 151
SnapVault cannot be enabled on vfiler units when SnapLock for SnapVault relationships are present in vfiler0 ................................................................. 153
Compatibility with SnapDrive and SnapManager ...................... 153
Synchronous SnapMirror not supported for volumes with deduplication .................................................. 153
Creating more than 64 mirrored aggregates might impair disaster recovery .................................................. 153
The N series Management Console data protection capability 3.7 does not perform optimally with deduplication ................................................................. 153
Improved sequential read performance for deduplicated FlexVol volumes .................................................. 153
Volumes with deduplication are disabled after a nondisruptive upgrade .................................................. 154
SnapVault issues in cascaded configurations .......................... 154
Suboptimal space savings with deduplication when 16 GB Performance Acceleration Module is installed .................. 155
Storage resource management issues ................................ 156
Configuring user mapping for a default user quota with CIFS not enabled could severely degrade performance ................................................................. 156
After changing the port assigned to ACP, a reboot is required to regain use of the original port.
The `df -S` command is not supported in Data ONTAP 7.3.3.
DataFabric Manager requires a patch to view the 2 TB disks.
The `all` keyword for the `aggr add` command is not yet implemented.
Moving disks to a system running an earlier version of Data ONTAP could cause disk identification issues.
Data ONTAP can silently select varying disk sizes when enlarging or creating an aggregate.
Adding disks when varying sized disks are in use.
Discovering what disks Data ONTAP will automatically select.
Qtree quotas might prevent explicit quotas from overriding the default.
Overriding default qtree quotas.
Adding a FlexCache origin volume to a vFiler unit might cause caching system to panic.

Third-party storage issues.
Exceeding the maximum number of assigned devices results in a panic.
No support for REP with zone checksum type array LUNs.
Limitation on EMC CX storage array LUN numbering.

Active/active configuration issues.
Re-creating mirrored aggregates when the base Snapshot copy is deleted.
If takeover is enabled for network interface failure, automatic giveback should be disabled.

**Changes to published documentation.**
Changes to the Archive and Compliance Management Guide.
Changes to the Data Protection Online Backup and Recovery Guide.
Changes to the Data ONTAP Data Protection Tape Backup and Recovery Guide.
Changes to the File Access and Protocols Management Guide.
Corrections to various SFTP topics.
Correction for disabling virus scanning.
Enhancements to NFS access cache management.
Changes to the MultiStore Management Guide.
Changes to the Storage Management Guide.
Changes to the System Administration Guide.
Changes to the Upgrade Guide.
Change to the Gateway Implementation Guide for native storage expansion units.
Array LUN sizing with 2 TB disks is not documented in all Gateway Implementation Guides.

**Copyright and trademark information.**
Trademark information.

**Notices.**
Data ONTAP 7.3.6 Release Notes

The Data ONTAP® 7.3.6 release is a maintenance release in the Data ONTAP 7.3 release family. Maintenance releases are primarily a collection of minor enhancements and important problem fixes to improve the overall robustness and stability of the release family.

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

About the Data ONTAP 7.3.6 release

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

Attention:

Upgrading to Data ONTAP 7.3 or later from an earlier release will cause existing FlexVol volumes to require more free space from their containing aggregate. You should therefore ensure that all systems upgrading to Data ONTAP 7.3 have sufficient free space in their aggregates before upgrading. For more information, see "New FlexVol volume space requirements when upgrading from a release earlier than Data ONTAP 7.3" on page 113.

About these release notes

All the information in this document applies to the Data ONTAP 7.3.6 release for N series storage systems, also sometimes called filers or appliances. Most of the information in this document also applies to gateway systems running Data ONTAP 7.3 except where otherwise indicated.

Note: There are no longer separate release notes for gateway systems.
Upgrade information

If you are upgrading to this release, make sure that you also read both of the following:

• "Important cautions" on page 111 in these Release Notes. You must read these before downloading Data ONTAP.

  This information helps you identify and resolve issues that might affect the availability of your systems. Check this online version of the Release Notes periodically for new cautions or updates that might have been posted since you downloaded your software.

• The Data ONTAP 7.3 Upgrade Guide.

  This guide describes how to upgrade to the Data ONTAP 7.3 release family and provides information you need before upgrading your software or reverting it to an earlier version.

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:

• 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
Changes introduced since Data ONTAP 7.3

If you are already familiar with an earlier release in the Data ONTAP 7.3 family and you want to see what is new since that release, you can see exactly what changes are introduced with each release in the Data ONTAP 7.3 family—and therefore pinpoint what has changed since the Data ONTAP 7.3.x release you are familiar with.

Note: If you are new to the Data ONTAP 7.3 family, it is not necessary to read this section; you can go directly to “Changes in the 7.3.6 release” on page 31.

- “Changes in the 7.3.5.1 release” on page 6
- “Changes in the 7.3.5 release” on page 8
- “Changes in the 7.3.4 release” on page 11
- “Changes in the 7.3.3 release” on page 14
- “Changes in the 7.3.2 release” on page 17
- “Changes in the 7.3.1.1L1 release” on page 21
- “Changes in the 7.3.1.1 release” on page 22
- “Changes in the 7.3.1 release” on page 24

Changes in the 7.3.6 release

The Data ONTAP 7.3.6 release includes support for new hardware, software enhancements, and problem fixes.

New and changed features in Data ONTAP 7.3.6

Data ONTAP 7.3.6 includes the following new and changed features:
- “Supported OpenSSH client versions” on page 38
- “Ability to block data traffic on the e0M interface” on page 53

New or changed commands in Data ONTAP 7.3.6

There were no new or changed commands added to Data ONTAP 7.3.6.

For more information about commands in the Data ONTAP 7.3 release family, see “New commands in Data ONTAP 7.3” on page 82.
New options in Data ONTAP 7.3.6

Data ONTAP 7.3.6 includes the following new options:

- `interface.blocked.mgmt_data_traffic`
- `nfs.always.deny.truncate`

For more information about options in the Data ONTAP 7.3 release family, see "New options in Data ONTAP 7.3" on page 96

Changed options in Data ONTAP 7.3.6

Data ONTAP 7.3.6 includes the following changed option:

- `cifs.max_mpx`

For more information about options in the Data ONTAP 7.3 release family, see "Changed options in Data ONTAP 7.3" on page 102

Cautions in Data ONTAP 7.3.6

There were no new caution in Data ONTAP 7.3.6.

New known limitations in Data ONTAP 7.3.6

Data ONTAP 7.3.6 includes the following new known limitations:

- "Configuring user mapping for a default user quota with CIFS not enabled could severely degrade performance" on page 137
- "After changing the port assigned to ACP, a reboot is required to regain use of the original port" on page 157
- "Authentication failure when IPsec is used with Kerberos" on page 143
- "Order of steps when enabling SSL for LDAP traffic" on page 136
- "FPolicy quota and user reports show incorrect file size" on page 137
- "Failed CIFS connections due to signature mismatch" on page 137
- "Excessive pending CIFS authentication requests can cause service disruption" on page 138
- "Data transfer speed reduces when LSI Logic 1030 Ultra320 SCSI HBA is used with tape drives (FC 1024)" on page 149

For more information about known limitations in the Data ONTAP 7.3 release family, see "Known problems and limitations" on page 133
Limitations removed in Data ONTAP 7.3.6

The following limitation that was included in the Data ONTAP 7.3.1 Release Notes is been removed from Data ONTAP 7.3.6

- SMB 2.0 not supported for SnapLock

Documentation changes for Data ONTAP 7.3.6

The following new or changed information supplements the documentation you received for the Data ONTAP 7.3.6 release:

- “Changes to the System Administration Guide” on page 177
- “Changes to the Data Protection Online Backup and Recovery Guide” on page 168
- “Changes to the File Access and Protocols Management Guide” on page 171
- “Changes to the Upgrade Guide” on page 180

For more information about documentation changes in the Data ONTAP 7.3 release family, see “Changes to published documentation” on page 165.
Changes in the 7.3.5.1 release

A caution that was added in Data ONTAP 7.3.5 is removed in Data ONTAP 7.3.5.1 release.

New and changed features in Data ONTAP 7.3.5.1

There were no new features introduced in Data ONTAP 7.3.5.1.

New platform and hardware support in Data ONTAP 7.3.5.1

There were no new platform and hardware support in Data ONTAP 7.3.5.1.

New or changed commands in Data ONTAP 7.3.5.1

There were no new or changed commands added to Data ONTAP 7.3.5.1.

For more information about commands in the Data ONTAP 7.3 release family, see "New commands in Data ONTAP 7.3" on page 82.

New or changed options in Data ONTAP 7.3.5.1

There were no new or changed options in Data ONTAP 7.3.5.1.

For more information about options in the Data ONTAP 7.3 release family, see "New options in Data ONTAP 7.3" on page 96.

Cautions in Data ONTAP 7.3.5.1

There were no new caution in Data ONTAP 7.3.5.1.

Cautions removed in Data ONTAP 7.3.5.1

The following caution that was included in the Data ONTAP 7.3.5 Release Notes has been removed in Data ONTAP 7.3.5.1:

• If your system is in an HA pair and hosting block-based services over FCP

Storage controllers in an HA pair that are hosting block-based services (LUNs) over FCP (FC/FCoE SAN) may experience an unexpected storage controller panic. The panic could result in a controller failover and disruption in service.

Customers in this configuration are strongly advised not to upgrade to Data ONTAP 7.3.5. Data ONTAP 7.3.5P1 addresses this issue and customers are advised to upgrade to Data ONTAP 7.3.5P1 instead.
This issue does not impact systems in an HA pair that are not hosting block-based services via FCP, and those systems that are in a single node configuration (even if they are using LUNs over FCP).

**New known limitations in Data ONTAP 7.3.5.1**

There were no new known limitations in Data ONTAP 7.3.5.1.

For more information about known limitations in the Data ONTAP 7.3 release family, see "Known problems and limitations" on page 133.

**Documentation changes for Data ONTAP 7.3.5.1**

The following new or changed information supplements the documentation you received for the Data ONTAP 7.3.5.1 release:

- "Changes to the Upgrade Guide" on page 180
- "Changes to the MultiStore Management Guide" on page 173

For more information about documentation changes in the Data ONTAP 7.3 release family, see "Changes to published documentation" on page 165.
Changes in the 7.3.5 release

The Data ONTAP 7.3.5 release includes support for the N6200 series storage systems in addition to improvements and problem fixes.

New and changed features in Data ONTAP 7.3.5

Data ONTAP 7.3.5 includes the following new features:

- "New option for the vfiler dr configure command" on page 78
- "The Service Processor for the N6200 series storage systems" on page 38
- "Support for 840 disk drives on fabric-attached MetroClusters" on page 71

For more information about new and changed features, see "New and changed features" on page 31.

New platform and hardware support in Data ONTAP 7.3.5

Data ONTAP 7.3.5 supports new hardware and platforms as described in this section.

- "Support for the N6200 series storage systems" on page 34
- "Support for EXN3500 storage expansion units" on page 35
- "Supported tape drives" on page 37

For more information about all new platform and hardware support, see "New platform and hardware support" on page 34.

New commands in Data ONTAP 7.3.5

Data ONTAP 7.3.5 includes the following new commands:

- `options snapvault.snapshot_for_dr_backup named_snapshot_only`
- `options snapvault.snapshot_for_dr_backup named_snapshot_preferred`
- `options snapvault.snapshot_for_dr_backup vsm_base_only`
- `sp help`
- `sp reboot`
- `sp setup`
- `sp status`
- `sp test autosupport`
- `sp test snmp`
- `sp update`

For more information, see "New commands in Data ONTAP 7.3" on page 82.
Changed commands in Data ONTAP 7.3.5

Data ONTAP 7.3.5 includes the following changed command:

- `storage show acp`

For more information, see “Changed commands in Data ONTAP 7.3” on page 87.

New options in Data ONTAP 7.3.5

There are no new options in Data ONTAP 7.3.5.

For more information, see “New options in Data ONTAP 7.3” on page 96.

Changed options in Data ONTAP 7.3.5

There are no changed options in Data ONTAP 7.3.5.

For more information, see “Changed options in Data ONTAP 7.3” on page 102.

Cautions in Data ONTAP 7.3.5

Data ONTAP 7.3.5 includes the following new cautions:

- “If you are upgrading an N6000 or N6200 series storage system in an iSCSI environment” on page 114
- “Issues in certificate MD5 signature collision vulnerability” on page 112
- “SnapLock Compliance volume upgrade requirement” on page 125

For more information, see “Important cautions” on page 111.

New known limitations in Data ONTAP 7.3.5

Data ONTAP 7.3.5 includes the following new known limitations:

- “Empty CIFS/SMB2.x change notifications” on page 138
- “The df -S command is not supported in Data ONTAP 7.3.3” on page 157
- “Re-creating mirrored aggregates when the base Snapshot copy is deleted” on page 161

For more information, see “Known problems and limitations” on page 133.
Limitations removed in Data ONTAP 7.3.5

The following limitation was removed from the Known problems and limitations, Data protection issues section in the Data ONTAP 7.3.5 Release Notes:

- Limitations of incremental dump backup

For more information, see “Known problems and limitations” on page 133.

Documentation changes for Data ONTAP 7.3.5

The following new or changed information supplements the documentation you received for the Data ONTAP 7.3.5 release:

- “Changes to the System Administration Guide” on page 177
- “Changes to the MultiStore Management Guide” on page 173.
- “Changes to the Storage Management Guide” on page 175
- The topic titled Corrections to the “Deduplication requires additional free space in aggregates after upgrading section” was removed from “Changes to the Upgrade Guide” on page 180.

For more information, see “Changes to published documentation” on page 165.
Changes in the 7.3.4 release

The Data ONTAP 7.3.4 release contains enhancements and known issues for Data ONTAP 7.3.4 including enhancements that allow you to specify SSL versions and support for aggregates larger than 8 TB for N3300 storage systems without restrictions.

New and changed features in Data ONTAP 7.3.4

The Data ONTAP 7.3.4 release introduces the following new and changed features:

- “Maximum number of data disks per 16-TB aggregate” on page 73
- “Enhancements that allow you to specify SSL versions” on page 40

For more information about new and changed features in Data ONTAP 7.3.4, see “New and changed features” on page 31.

New platform and hardware support in Data ONTAP 7.3.4

Data ONTAP 7.3.3 and later supports aggregates larger than 8 TB for N3300 storage systems without restrictions.

For more information about new platform and hardware support in the Data ONTAP 7.3 release family, see “Unrestricted increased aggregate capacity for N3300 systems” on page 35.

Data ONTAP 7.3.2 and later releases support 2 TB SATA disks. For information, see “Support for 2 TB SATA disks” on page 35.

For more information about all new platform and hardware support in the Data ONTAP 7.3 release family, see “New platform and hardware support” on page 34.

New commands in Data ONTAP 7.3.4

Data ONTAP 7.3.4 does not include any new commands.

For more information, see “New commands in Data ONTAP 7.3” on page 82.

Changed commands in Data ONTAP 7.3.4

Data ONTAP 7.3.4 does not include any changed commands.

For more information, see “Changed commands in Data ONTAP 7.3” on page 87.
New options in Data ONTAP 7.3.4

Data ONTAP 7.3.4 includes the following options:

- nfs.v3.snapshot.active.fsid.enable
- nfs.v4.snapshot.active.fsid.enable
- ssl.v2.enable
- ssl.v3.enable

For more information, see “New options in Data ONTAP 7.3” on page 96.

Changed options in Data ONTAP 7.3.4

Data ONTAP 7.3.4 includes the following changed option:

- cifs.max_mpx

For more information, see “New options in Data ONTAP 7.3” on page 96.

New cautions in Data ONTAP 7.3.4

There were no new cautions introduced in Data ONTAP 7.3.4.

For more information, see “Important cautions” on page 111.

Changed cautions in Data ONTAP 7.3.4

The following cautions were changed in Data ONTAP 7.3.4:

- “Determining system capacity and space guarantees” on page 114
- “If you are upgrading an N3300 system running Data ONTAP 7.2.2L1” on page 117

For more information about cautions in the Data ONTAP 7.3 release family, see “Important cautions” on page 111.

Cautions removed in Data ONTAP 7.3.4

The following cautions that was included in the Data ONTAP 7.3.3 Release Notes has been removed from Data ONTAP 7.3.4 Release Notes:

- Using ACP can cause system panic
  (ACP can now be enabled by setting the acp.enabled option to on)

For more information, see “Important cautions” on page 111.
New known limitations in Data ONTAP 7.3.4

Data ONTAP 7.3.4 includes the following new limitations:
- "vFiler DR configuration with the snapmirror.checkip.enable option on fails, if SnapMirror fails to authenticate destination IPv6 address" on page 134
- "Re-creating mirrored aggregates when the base Snapshot copy is deleted" on page 161.

For more information, see “Known problems and limitations” on page 133.

Limitations removed in Data ONTAP 7.3.4

The following limitations were removed from Data ONTAP 7.3.4:
- Guidelines for creating a clone of a SnapVault destination volume
- Guidelines for creating a clone of a qtree SnapMirror destination volume

For more information, see “Known problems and limitations” on page 133.

Documentation changes in Data ONTAP 7.3.4

Data ONTAP 7.3.4 has the following new and modified documentation:
- “Changes to the Data ONTAP Commands Manual Page Reference” on page 167
- “Changes to the File Access and Protocols Management Guide” on page 171
- “Changes to the Storage Management Guide” on page 175
- “Changes to the System Administration Guide” on page 177
- “Changes to the MultiStore Management Guide” on page 173

For more information, see “Changes to published documentation” on page 165.
Changes in the 7.3.3 release

The Data ONTAP 7.3.3 release contains online migration support on vFiler units, additional IPv6 support, and other new features and enhancements.

New and changed features in Data ONTAP 7.3.3

The Data ONTAP 7.3.3 release introduces the following new and changed features:

- “Online migration support on vFiler units” on page 78
- “Support for IPv6” on page 54
- “Support for CDP” on page 57
- “Enhancements to NFS access cache management” on page 47
- “Improved security for Perfmon connections” on page 48
- “New RLM firmware and its upgrade requirements” on page 115

For more information about new and changed features in Data ONTAP 7.3.3, see “New and changed features” on page 31.

New commands in Data ONTAP 7.3.3

Data ONTAP 7.3.3 includes the following new command:

- cdpd
- nfs nsdb flush

For more information about new commands in Data ONTAP 7.3.3, see “New commands in Data ONTAP 7.3” on page 82.

Changed commands in Data ONTAP 7.3.3

Data ONTAP 7.3.3 includes the following changed commands:

- exportfs -c
- exportfs -f
- fcp portname set
- fcp portname swap
- storage show fault

For more information about changed commands in Data ONTAP 7.3.3, see “Changed commands in Data ONTAP 7.3” on page 87.
New options in Data ONTAP 7.3.3

Data ONTAP 7.3.6 includes the following new options:
- cdpd.holdtime
- cdpd.interval
- cifs.perfmon.allowed_users
- tftpd.max_connections

For more information about new options in Data ONTAP 7.3.3, see "New options in Data ONTAP 7.3" on page 96.

New cautions in Data ONTAP 7.3.3

The following new caution was introduced in Data ONTAP 7.3.3:
- "New RLM firmware and its upgrade requirements" on page 115

For more information, see "Important cautions" on page 111.

Cautions removed in Data ONTAP 7.3.3

The following cautions that were included in the Data ONTAP 7.3.2 Release Notes were removed from the Data ONTAP 7.3.3 Release Notes:
- If you are upgrading a system that includes FlexVol volumes
- SnapMirror commands that become obsolete in Data ONTAP 8.0
- Routes for a vFiler unit not added in the partner node during takeover
- If you are upgrading a system with AT-FCX disk shelves attached

New known limitations in Data ONTAP 7.3.3

Data ONTAP 7.3.3 includes the following new known limitations:
- "SnapVault issues in cascaded configurations" on page 154
- "Single-mode vif does not fail over correctly" on page 144
- "Disks offline in Windows 2008 after a standard upgrade" on page 146
- "The ping6 usage message is incorrect" on page 143
- "RLM configuration is not saved if the RLM’s Ethernet cable is not connected" on page 135

For more information, see "Known problems and limitations" on page 133.
Limitations removed in Data ONTAP 7.3.3

The following limitations that were included in the Data ONTAP 7.3.2 Release Notes have been removed from Data ONTAP 7.3.3 Release Notes:

- Metadata not backed up during dump of qtree SnapMirror destinations
- Limitation when destroying a vFiler unit that is part of an IP space
- Delayed I/O seen on the host during controller forced takeover or giveback and reboots

The descriptions for the following limitations that were included in the Data ONTAP 7.3.2 Release Notes have been moved to the Data ONTAP MultiStore Management Guide:

- Limitation when migrating a vFiler unit between the nodes of an active/active configuration
- Limitation when you create a vFiler unit in a nondefault IP space
- Default limit on the number of vFiler units
- Syntax correction of the `vfiler migrate start` command
- Maximum vFiler units allowed in N3400 systems

Documentation changes for Data ONTAP 7.3.3

The following new or changed information supplements the documentation you received for the Data ONTAP 7.3.3 release:

- “Changes to the Archive and Compliance Management Guide” on page 166
- “Changes to the Data ONTAP Data Protection Tape Backup and Recovery Guide” on page 170
- “Changes to the Data Protection Online Backup and Recovery Guide” on page 168
- “Changes to the File Access and Protocols Management Guide” on page 171
- “Change to the Gateway Implementation Guide for native storage expansion units” on page 182
- “Array LUN sizing with 2 TB disks is not documented in all Gateway implementation Guides” on page 183

For more information about these and other important documentation changes, see “Changes to published documentation” on page 165.
Changes in the 7.3.2 release

The Data ONTAP 7.3.2 release supports FlexClone technology for files and LUNS and adds support for Transport Layer Security (TLS) version 1.0. Data ONTAP 7.3.2 also supports port-based load balancing for multimode vifs. Data ONTAP 7.3.2 introduces the ability to upgrade fabric-attached MetroClusters from one release family to another nondisruptively (major nondisruptive upgrades) and also includes changes to the SnapLock autocommit feature. FilerView in Data ONTAP 7.3.2 supports the TLS protocol.

New and changed features in Data ONTAP 7.3.2

The Data ONTAP 7.3.2 release introduces the following new and changed features:

- “TOE automatically disabled” on page 32
- “New disk drive AutoSupport message sent weekly” on page 35
- “Support for EXN3000 storage expansion units” on page 36
- “Support for N3400” on page 35
- “Major nondisruptive upgrades for fabric-attached MetroClusters” on page 77
- “TLS support in FilerView” on page 58
- “Transport Layer Security protocol” on page 57
- “WAFL External cache group added to netapp.mib” on page 58
- “Support for multiple open instances of the SMB named pipe on an FP inside server” on page 46
- “10-GbE Unified Target Adapter protocol support” on page 50
- “If volumes with deduplication exceed the maximum supported size” on page 63
- “Retention of older SnapVault Snapshot copies on SnapVault secondary volumes” on page 62
- “Support for SnapMirror network compression” on page 63
- “Changes to the SnapLock autocommit feature” on page 63
- “Snapshot copies and log files of SnapLock for SnapVault use system clock for naming” on page 63
- “Port-based load-balancing option for multimode vifs” on page 58
- “FlexClone files and FlexClone LUNs” on page 72
- “Support for 672 disk drives on fabric-attached MetroClusters” on page 76
- “SnapMover license is not required” on page 79
For more information about changes to supported hardware and features in Data ONTAP 7.3.2, see "Changes to supported hardware and features" on page 32.

**New commands in Data ONTAP 7.3.2**

For a description of the five new commands in Data ONTAP 7.3.2, see:

- "New commands in Data ONTAP 7.3" on page 82

**Changed commands in Data ONTAP 7.3.2**

For a description of the nine changed commands in Data ONTAP 7.3.2, see:

- "Changed commands in Data ONTAP 7.3" on page 87

**New options in Data ONTAP 7.3.2**

For a description of the nine new options in Data ONTAP 7.3.2, see:

- "New options in Data ONTAP 7.3" on page 96

**Changed options in Data ONTAP 7.3.2**

For a description of the four changed options in Data ONTAP 7.3.2, see:

- "Changed options in Data ONTAP 7.3" on page 102

**New cautions in Data ONTAP 7.3.2**

The following new cautions were introduced in Data ONTAP 7.3.2:

- "If you are upgrading a system that includes FlexCache volumes" on page 116
- "Identical WWPNs can occur on both nodes in a cluster" on page 122
- If you are upgrading a system that includes deduplicated volumes

**Cautions removed in Data ONTAP 7.3.2**

The following cautions that were included in the *Data ONTAP 7.3.1.1 Release Notes* have been removed from Data ONTAP 7.3.2:

- If the storage system panics during upgrade from the Data ONTAP 7.1 release family
- If you upgrade systems running SnapMirror
- If you upgrade storage systems with iSCSI targets
- If you want to change a storage system's hostname
- If you are using SnapLock in a MetroCluster configuration
- Aggregate reallocation is not supported on aggregates created before Data ONTAP 7.2
- Volume reallocation is not supported
- The wafliron tool requires free space in the root volume to run successfully
- When restoring a Snapshot copy, no deletion of the backing Snapshot copy until the LUN clone split is complete
- iSCSI Target HBA support
- The ostype parameter now required when creating LUNs and igroups
- Enabling iSNS server v.3.0
- Partition alignment problems cause an iSCSI LUN performance problem
- Brocade switch support for fabric-attached MetroCluster configurations
- Failed disks can cause giveback to fail
- CFO partner node's SSL certificate is used after takeover and giveback

**New known limitations in Data ONTAP 7.3.2**

Data ONTAP 7.3.2 includes the following new limitations:

- "AutoSupport option settings" on page 135
- "TOE is disabled" on page 144
- "FCoE adapters may fail to come online if the FCP service is stopped and started too quickly" on page 147
- "No support for REP with zone checksum type array LUNs" on page 160
- ""option lun.partner_unreachable.default-partner.behavior: Value must be 'drop', 'error', or 'start'" error message periodically displays" on page 146

For more information, see "Known problems and limitations" on page 133.

**Limitations removed in Data ONTAP 7.3.2**

The following limitations that were included in the *Data ONTAP 7.3.1.1 Release Notes* have been removed from Data ONTAP 7.3.2:

- TOE acceleration is not available for vifs
- MAC address hard limits for TOE cards
- IPv6 not supported with FlexCache
- Operations involving vFiler units can disable quotas
- Aggregate reallocation is not supported on aggregates created before Data ONTAP 7.2
- Volume reallocation is not supported
- The wafliron tool requires free space in the root volume to run successfully
• When restoring a Snapshot copy, no deletion of the backing Snapshot copy until the LUN clone split is complete
• iSCSI Target HBA support
• The ostype parameter now required when creating LUNs and igroups
• Enabling iSNS server v.3.0
• Partition alignment problems cause an iSCSI LUN performance problem
• Brocade switch support for fabric-attached MetroCluster configurations
• Failed disks can cause giveback to fail
• CFO partner node's SSL certificate is used after takeover and giveback
• Limitation of incremental backup

Documentation changes for Data ONTAP 7.3.2

The following new or changed information supplements the documentation you received for the Data ONTAP 7.3.2 release:
• Default limit on the number of vFiler units (Describes the limits on the number of vFiler units in storage systems that have the MultiStore license enabled.)
• “Change to the Gateway Implementation Guide for native storage expansion units” on page 182 (Describes changes to the Gateway Implementation Guide for Native Disk Shelves.)
• Syntax correction of the vfiler migrate start command (Describes the syntax correction of the vfiler migrate start command.)

For more information about these and other important documentation changes, see “Changes to published documentation” on page 165.
Changes in the 7.3.1.1L1 release

Data ONTAP 7.3.1.1L1 provides critical fixes for storage controllers with the FC 1031 10-GbE network adapter card running any Data ONTAP 7.3.x release.

Changes to supported hardware and features

The Data ONTAP 7.3.1.1L1 release introduces the following changes to supported hardware and features:

- "Flow control may be reported randomly by FC 1031 10-Gb NIC with certain switches" on page 32

For more information about changes to supported hardware and features in Data ONTAP 7.3.1.1L1, see "Changes to supported hardware and features" on page 32.
Changes in the 7.3.1.1 release

Data ONTAP 7.3.1.1 now supports the round-robin load balancing option for multimode vifs and includes additional considerations when planning to rejoin split aggregates. Data ONTAP 7.3.1.1 also includes many problem fixes.

New and changed features in Data ONTAP 7.3.1.1

The Data ONTAP 7.3.1.1 release introduces the following new and changed features:

- Round-robin load balancing is supported

For more information about new and changed features in Data ONTAP 7.3.1.1, see "New and changed features" on page 31.

New or changed commands in Data ONTAP 7.3.1.1

Data ONTAP 7.3.1.1 includes the following changed command.

- vif create

For more information about changed commands in Data ONTAP 7.3.1.1, see "Changed commands in Data ONTAP 7.3" on page 87.

New or changed options in Data ONTAP 7.3.1.1

There were no new or changed options introduced in Data ONTAP 7.3.1.1.

Cautions removed in Data ONTAP 7.3.1.1

The following cautions that were included in the Data ONTAP 7.3.1 Release Notes have been removed from Data ONTAP 7.3.1.1:

- If you are upgrading a system that has vifs configured with the round-robin option
- Modifying the persistent configuration to remove round-robin load balancing

New known limitations in Data ONTAP 7.3.1.1

Data ONTAP 7.3.1.1 includes the following new limitations:

- Data recovery using SnapVault or SnapMirror for a qtree with LUN clones

For more information, see "Known problems and limitations" on page 133.
Documentation changes for Data ONTAP 7.3.1.1

The following new or changed information supplements the documentation you received for the Data ONTAP 7.3.1.1 release:

- **Changes to the Archive and Compliance Management Guide** (contains updated information about cross-references to SnapLock information.)
- **Changes to the Data Protection Online Backup and Recovery Guide** (contains updated information when planning to rejoin split aggregates that previously used MetroCluster to mirror SnapLock volumes.)
- **Changes to the Files Access and Protocols Management Guide** (contains updated information regarding changes to creating a SnapLock Compliance SnapMirror relationship section, changes to limitations of FPolicy, hyphen supported as a special character in Policy Name, caution before destroying a file policy, changes to configuring native file blocking section, and steps for configuring native file blocking.)
- **Changes to the Archive and Compliance Management Guide** (contains updated information about creating a SnapLock Compliance SnapMirror, restricting the destination volume before initializing the SnapMirror relationship cross-references to SnapLock information.)

For more information about these and other important documentation changes, see “Changes to published documentation” on page 165.
Changes in the 7.3.1 release

Data ONTAP 7.3.1 includes support for IPv6 and new features related to deduplication, FlexCache, and WAFL. Data ONTAP 7.3.1 also includes problem fixes, such as features related to the ability to use Telnet or Remote Shell (RSH) sessions to update RLM firmware.

New and changed features in Data ONTAP 7.3.1

The Data ONTAP 7.3.1 release introduces the following new and changed features:

- “Support for N6000 series systems” on page 36
- “Nondisruptive upgrades for storage expansion units controlled by AT-FCX modules” on page 40
- “Changes to the upgrade preparation process” on page 40
- “Read reallocation of data” on page 41
- “Extents for FlexVol volumes” on page 41
- “Support for IPv6” on page 54
- “IPv6 RFCs supported” on page 56
- “Kerberos Multi Realm support” on page 47
- “Support for the SMB 2.0 protocol” on page 46
- “FPolicy enhancements” on page 48
- “Maximum number of auxiliary UNIX groups supported for a user” on page 49
- “New solaris_efi, xen, and hyper_v LUN Multiprotocol Types (ostypes)” on page 52
- “SnapLock supported in Data ONTAP 7.3.1 and later” on page 64
- “Support for SnapMirror over Fibre Channel on N3600 storage systems” on page 67
- “Deduplication support on SnapLock volumes” on page 69
- “SnapLock support for vFiler units” on page 70
- “Support for changing to software-based disk ownership nondisruptively” on page 74
- “Disconnected operation for FlexCache volumes” on page 75
- “Commands supported by the ONTAPI interface library” on page 78
- “Using SnapVault for NetBackup to protect applications” on page 150
- “Changes to deduplication usage with SnapVault for NetBackup” on page 151

For more information about new and changed features in Data ONTAP 7.3.1, see “New and changed features” on page 31.
New commands in Data ONTAP 7.3.1

Data ONTAP 7.3.1 introduces the following new commands:

- ndp
- ping6
- snaplock log archive
- snaplock log status
- snaplock log volume
- snaplock options
- snaplock privdel
- traceroute6

For more information, see "New commands in Data ONTAP 7.3" on page 82.

Changed commands in Data ONTAP 7.3.1

Data ONTAP 7.3.1 introduces the following changed commands:

- cifs setup
- environ shelf
- lock break
- nfs setup
- snap autodelete
- snapvault start
- storage show hub
- vfiler dr configure
- vfiler dr delete
- vfiler migrate
- vfiler migrate start
- vfiler migrate cancel
- vfiler migrate complete
- vfiler dr resynch
- vol clone create
- vol options
- vol options extent
- vol options read_realloc
- vol status -v
- vol status -w
For more information, see “Changed commands in Data ONTAP 7.3” on page 87.

**Commands removed in Data ONTAP 7.3.1**

The following command was removed in Data ONTAP 7.3.1:

- software install

For more information, see “Replaced or removed commands in Data ONTAP 7.3” on page 104.

**New options in Data ONTAP 7.3.1**

Data ONTAP includes the following options:

- autosupport.partner.to
- cifs.audit.liveview.allowed_users
- cifs.ipv6.enable
- cifs.smb2.client.enable
- cifs.smb2.enable
- cifs.smb2.durable_handle.enable
- cifs.smb2.durable_handle.timeout
- cifs.smb2.signing.required
- flexcache.deleg.high_water
- flexcache.deleg.low_water
- ftpd.ipv6.enable
- httpd.ipv6.enable
- ip.v6.enable
- ip.v6.ra_enable
- nfs.ifc.rcv.high
- nfs.ifc.rcv.low
- nfs.ipv6.enable
- nfs.max_num_aux_groups
- nfs.thin_prov.ejuke
- nfs.v4.setattr_acl_preserve
- raid.disktype.enable
- shelf.atfcx.auto.reset.enable
- shelf.esh4.auto.reset.enable
- snaplock.autocommit_period
- snaplock.compliance.write_verify
• snaplock.log.default_retention
• snaplock.log.maximum_size
• snapvault.nbu.archival_snap_default
• snapvault.ossv.compression
• vif.failover.link_degraded

For more information, see “New options in Data ONTAP 7.3” on page 96.

**Changed options in Data ONTAP 7.3.1**

The following options were changed in Data ONTAP 7.3.1:
• nlm.cleanup.timeout

For more information, see “Changed options in Data ONTAP 7.3” on page 102.

**New cautions in Data ONTAP 7.3.1**

The following new cautions were introduced in Data ONTAP 7.3.1:
• “If you revert to a prior release, for a SnapMirror destination with volumes using deduplication or clone operations” on page 129
• “If you are reverting to a previous release that does not support deduplication with SnapLock volumes” on page 127
• “If you are reverting to a previous release and you use large ACLs under NFSv4” on page 119

For more information, see “Important cautions” on page 111.

**Cautions removed in Data ONTAP 7.3.1**

The following cautions that were included in the *Data ONTAP 7.3 Release Notes* have been removed from Data ONTAP 7.3.1:
• If you are upgrading an N3300 system that includes aggregates larger than 8 TB.
• SnapLock not supported
  SnapLock is not supported in the first release of Data ONTAP 7.3. However, Data ONTAP 7.3.1 supports SnapLock with new features.
• If you are upgrading a system to this release and you use deduplication
• Lasers do not shut off on 2 Gbps Fibre Channel target expansion adapters.
The workaround for this problem is to change the position of jumpers J3 and J4 on the adapter from positions 2 and 3 to positions 1 and 2, respectively.
New known limitations in Data ONTAP 7.3.1

Data ONTAP 7.3.1 includes the following new limitations:

- "No IPv6 support in FPolicy" on page 142
- "cfmode restrictions for 8-Gb target expansion adapters" on page 148
- "SnapVault cannot be enabled on vFiler units when SnapLock for SnapVault relationships are present in vfiler0" on page 153
- SMB 2.0 not supported for SnapLock (removed in 7.3.6)
- Limitation of incremental backup (removed limitation in 7.3.2)
- IPv6 not supported with FlexCache (removed limitation in 7.3.2)

For more information, see "Known problems and limitations" on page 133.

Limitations removed in Data ONTAP 7.3.1

The following limitations were removed from Data ONTAP 7.3.1:

- Certain timeout options for FlexCache attribute cache not always correctly displayed
- Creation of FlexClone volumes with space guarantee of none and fractional reserve of zero is not prevented
- Restriction on maximum volume size
  If a volume has ever been larger than the maximum supported deduplication volume size on a storage system, then deduplication cannot be enabled on the volume, even if the volume has been shrunk to a size supported by the storage system.
- Solaris hosts using a 2-Gb Fibre Channel HBA require FCP Solaris Host Utilities 4.3
  Solaris hosts using a 2-Gb Fibre Channel HBA must use FCP Solaris Host Utilities 4.3 in order for the sanlun command to function properly.

Documentation changes in Data ONTAP 7.3.1

Data ONTAP 7.3.1 has the following new and modified documentation:

- The Data ONTAP Active/Active Configuration Guide contains new information about active/active configurations.
- The Data ONTAP Archive and Compliance Management Guide is a new guide in the Data ONTAP 7.3.1 release and describes how to archive and protect data for compliance purposes.
- The Data ONTAP Data Protection Online Backup and Recovery Guide contains new information about SnapVault for NetBackup and configuring SnapMirror over Fibre Channel.
• The Data ONTAP File Access and Protocols Management Guide contains new information related to Kerberos Multi Realm support, including changes to the procedures for configuring Kerberos authentication for CIFS and NFS.

• The Data ONTAP Network Management Guide contains information about the link local address for VLANs created on a network interface and also contains examples of the options interface command.

• The Data ONTAP Storage Management Guide contains new information about support for 450-GB SAS and FC disks.

• The Data ONTAP System Administration Guide contains new information about SSH requests and IPv6 support.

For more information, see “Changes to published documentation” on page 165.
New and changed features

This section covers features that were added or changed in the Data ONTAP 7.3 release family.

The major changes made in Data ONTAP 7.3 family releases are described here. For other important information in these release notes about changes to the product during these releases, see “New and changed commands and options” on page 81.

- “Changes to supported hardware and features” on page 32
- “New platform and hardware support” on page 34
- “Manageability enhancements” on page 38
- “File access protocol enhancements” on page 46
- “Block protocols enhancements” on page 50
- “Networking and Security protocols enhancements” on page 53
- “Data protection enhancements” on page 61
- “Storage resource management enhancements” on page 72
- “Active/active configuration enhancements” on page 76
- “MultiStore enhancements” on page 78
Changes to supported hardware and features

Data ONTAP 7.3 and later releases provide additional changes to supported hardware and features.

- "TOE automatically disabled"
- "Flow control may be reported randomly by FC 1031 10-Gb NIC with certain switches"
- "Support for SnapVault integration options for use with NetBackup" on page 33

TOE automatically disabled

If you upgrade to Data ONTAP 7.3.2, TCP offload engine (TOE) functionality is automatically disabled.

Flow control may be reported randomly by FC 1031 10-Gb NIC with certain switches

Unpredictable status results may occur when trying to enable flow control on an FC 1031 10-Gb NIC attached to a Cisco Nexus family switch.

Even when all options are correctly enabled, reboots or other methods of forcing flow control renegotiation such as resetting ports, might result in the storage system port negotiating flow control correctly but reporting incorrect results.

For example, the storage system port may report random values of flow control as read from the ifstat commands Send, Receive, Full or None, with no immediate pattern recognizable.

On the Cisco Nexus 5000 Series switch, Ethernet interfaces do not automatically detect the link-level flow control capability because link-level flow control capability is disabled. You should set flow control explicitly on both the switch and storage system port to your desired settings (on or off) and ignore the erroneous reports.

Considerations

Even when all options are correctly enabled, reboots or other methods of forcing flow control renegotiation such as resetting ports, may result in the filer port negotiating flow control correctly but reporting incorrect results.

For example, the filer port may report random values of flow control as read from the ifstat commands Send, Receive, Full or None, with no immediate pattern recognizable.

On the Cisco Nexus 5000 Series switch, Ethernet interfaces do not automatically detect the link-level flow control capability because link-level
flow control capability is disabled. You should set flow control explicitly on both the switch and filer to your desired settings (on or off) and ignore the erroneous reports.

**Support for SnapVault integration options for use with NetBackup**
SnapVault for NetBackup continues to be supported in the 7.3 release family. However, Data ONTAP 8.0 and later releases of Data ONTAP will not support SnapVault integration options for use with NetBackup.
New platform and hardware support

Data ONTAP 7.3 supports new hardware.

- “Support for the N6200 series storage systems”
- “Support for N6000 series systems” on page 36
- “Unrestricted increased aggregate capacity for N3300 systems” on page 35
- “Support for EXN3500 storage expansion units” on page 35
- “Support for EXN3000 storage expansion units” on page 36
- “Support for 2 TB SATA disks” on page 35
- “Nondisruptive Upgrade Supported for SATA disk drives” on page 36
- “New disk drive AutoSupport message sent weekly” on page 35
- “Supported tape drives” on page 37
- “UPS support” on page 37
- “Support for 512-GB and 256-GB Flash Cache modules” on page 37

Support for the N6200 series storage systems

Data ONTAP 7.3.5 and later releases support the N6200 series storage systems.

The N6200 series storage systems support 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 or 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 2 TB SATA disks

In Data ONTAP 7.3.2 and later releases, 2 TB SATA disks are supported for both the SAS and FC disk connection types.

Unrestricted increased aggregate capacity for N3300 systems

Beginning with Data ONTAP 7.3.3, N3300 support aggregate capacities of up to 16 TB with no restrictions.

For more information about N3300 systems' storage capacity, see the IBM System Storage N series Introduction and Planning Guide.

New disk drive AutoSupport message sent weekly

Beginning with Data ONTAP 7.3.2, a weekly health trigger AutoSupport message provides information about any failed disk drives.

The message is sent each Sunday between 12:00 a.m. and 1 a.m. local time. If no drives failed during the past week, no weekly drive health test message is sent.

By default, the health test message is sent only to technical support.

Support for N3400

Data ONTAP 7.3.2 and later releases support the N3400 platform which supports the following features:

• One or two controllers
• Up to 12 internal SAS or SATA disks
• Four Gigabit Ethernet ports per controller
• One SAS port per controller
• One ACP (Alternate Control Path) port per controller
• Two 4-Gb Fibre Channel ports per controller
• Baseboard management controller (BMC) remote management device
• 4 GB memory per controller

Support for EXN3500 storage expansion units

The EXN3500 storage expansion unit contains external SAS disk drives and 6-Gb I/O modules.

The EXN3500 storage expansion unit is supported on the following Data ONTAP 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 disks and storage expansion unit are supported with your storage system model, 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 Hardware and Service Guide*.

**Support for EXN3000 storage expansion units**

Starting with Data ONTAP 7.3.2, the EXN3000 storage expansion unit is supported. The EXN3000 storage expansion unit contains external SAS or SAS-connected SATA disk drives.

For more information about which storage expansion units are supported with your storage system model, 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*.

**Support for N6000 series systems**

Data ONTAP 7.3 and later releases support the N6000 series systems. The N6040 and N6070 storage systems were introduced in Data ONTAP 7.3, and the N6060 is part of the Data ONTAP 7.3.1 release.

- The N6040 storage system has 4 GB memory and one processor. The N6040 storage system also includes four available PCI-Express slots, two Gigabit Ethernet ports, one Management port, and four 4-Gb Fibre Channel ports.
- The N6070 storage system has 16 GB memory and two processors. The N6070 storage system also includes four available PCI-Express slots, two Gigabit Ethernet ports, one Management port, and four 4-Gb Fibre Channel ports.
- The N6060 storage system has 8 GB memory and two processors. The N6060 storage system also includes four available PCI-Express slots, two Gigabit Ethernet ports, one Management port, and four 4-Gb Fibre Channel ports. These are all per-controller. Typically, a chassis contains two controllers.

For information about each storage system model’s capacity and maximum volume size, see the *IBM System Storage N series Introduction and Planning Guide*.

**Nondisruptive Upgrade Supported for SATA disk drives**

Nondisruptive upgrades (NDU) Data ONTAP 7.3 releases are now fully supported for NFS and SAN storage environments employing SATA disk drives.
UPS support

Data ONTAP 7.2.4 and later releases support Uninterruptible Power Supply (UPS) devices from American Power Conversion Corporation (APC). All models of APC SmartUPS and SymmetraUPS are currently supported.

Support for 512-GB and 256-GB Flash Cache modules

Note: Flash Cache modules were formerly referred to as Performance Acceleration Modules (PAM) II.

Data ONTAP 7.3.5 and later releases support a PCIe-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.

Supported tape drives

Data ONTAP 7.3.5 and later releases support Quantum LTO-4, Quantum LTO-5, Hewlett-Packard LTO-4, Hewlett-Packard LTO-5, and IBM LTO-5 tape drives.
Manageability enhancements

Data ONTAP 7.3 and later releases provide additional management capabilities using MultiStore, FilerView, and other tools.

- "Supported OpenSSH client versions"
- "The Service Processor for the N6200 series storage systems"
- "Enhancements that allow you to specify SSL versions" on page 40
- "SSL security improvements" on page 40
- "Nondisruptive upgrades for storage expansion units controlled by AT-FCX modules" on page 40
- "Changes to the upgrade preparation process" on page 40
- "Improved support for nondisruptive upgrades in SAN environments" on page 41
- "Read reallocation of data" on page 41
- "Extents for FlexVol volumes" on page 41
- "Option to disable root access to the storage system" on page 42
- "Audit log enhancement" on page 42
- "Read-only access to FilerView" on page 43
- "Physical reallocation of data" on page 43
- "Performance Acceleration Module (PAM), Flash Cache module, and WAFL external cache" on page 43
- "FilerView enhancements" on page 44
- "The e0M interface" on page 44
- "Data ONTAP supports up to 24 SSH sessions" on page 45
- "Only critical AutoSupport notifications are sent to the autosupport.to recipients" on page 45
- "Partner recipients for AutoSupport email notifications" on page 45

Supported OpenSSH client versions

Starting with Data ONTAP 7.3.6, Data ONTAP supports OpenSSH client versions 4.0p1 and 4.4p1 on UNIX platforms. To enhance security, OpenSSH client version 3.8p1 is no longer supported because it does not contain the latest security fix.

The Service Processor for the N6200 series storage systems

The Service Processor (SP) is a remote management device that is included in the N6200 series storage systems. The SP enables you to access, monitor, and troubleshoot the storage system remotely.

The SP provides the following capabilities:
The SP enables you to access the storage system remotely to diagnose, shut down, power-cycle, or reboot the system, regardless of the state of the storage controller.

The SP is powered by a standby voltage, which is available as long as the system has input power to at least one of the system’s power supplies.

The SP is connected to the system through the serial console. You can log in to the SP by using a Secure Shell client application from an administration host. You can then use the SP CLI to monitor and troubleshoot the system remotely. In addition, you can use the SP to access the system console and run Data ONTAP commands remotely.

You can access the SP from the system console or access the system console from the SP. The SP allows you to open both an SP CLI session and a separate system console session simultaneously.

The SP monitors environmental sensors and logs system events to help you take timely and effective service actions in the event that a system problem occurs.

The SP monitors the system temperatures, voltages, currents, and fan speeds. When the SP detects that an environmental sensor has reached an abnormal condition, it logs the abnormal readings, notifies Data ONTAP of the issue, and takes proactive actions as necessary to send alerts and “down system” notifications through an AutoSupport message.

If SNMP is enabled for the SP, the SP generates SNMP traps to configured trap hosts for all “down system” events.

The SP also logs system events such as boot progress, Field Replaceable Unit (FRU) changes, Data ONTAP-generated events, and SP command history.

Hardware-assisted takeover is available on systems that support the SP and have the SP configured.

For more information about the SP, see the Data ONTAP System Administration Guide.

For more information about hardware-assisted takeover, see the Data ONTAP Active/Active Configuration Guide.

You must ensure that your system has the latest SP firmware version. You can use the sp status command to display the SP firmware version on your system, and, if necessary, update the SP to the latest version. For instructions on how to download and update the SP firmware, see the Data ONTAP Upgrade Guide.
Enhancements that allow you to specify SSL versions
If your storage system has the SSL protocol enabled, you can further specify the SSL version(s) to use by using the `ssl.v2.enable` and the `ssl.v3.enable` options.

SSL security improvements
As a precautionary measure due to security vulnerability CVE-2009-3555, the SSL renegotiation feature is disabled in Data ONTAP.

Nondisruptive upgrades for storage expansion units controlled by AT-FCX modules
Data ONTAP 7.3.1 introduces the ability to update the firmware for EXN1000 storage expansion units with AT-FCX modules without needing to schedule system downtime for maintenance.

Your system must meet the following requirements to upgrade AT-FCX firmware nondisruptively:
- Data ONTAP 7.3.1 is installed.
- Multipath HA Storage is configured.
- Firmware version 37 or later is running on all storage expansion units with AT-FCX modules.

Attention: It is strongly recommended that AT modules run firmware version 37 or later.

Upgrading storage expansion unit firmware to version 37 or later from any version earlier than 36 requires downtime.

For more information about nondisruptive AT-FCX firmware upgrades, see the Data ONTAP Upgrade Guide.

Changes to the upgrade preparation process
Beginning in Data ONTAP 7.3.1, there are new recommendations for obtaining and installing Data ONTAP upgrade images.

In previous releases, there were several methods available for obtaining Data ONTAP upgrade images and installing system files on your system. Beginning with Data ONTAP 7.3.1, the following method is recommended:
- Copy Data ONTAP .exe upgrade images to your storage system or an HTTP server on your network.
- Install and manage upgrade images with the `software` command family.
  - Use the `software update` command to upgrade from Data ONTAP 7.2 and later releases.
  - Use the `software install` command to upgrade from Data ONTAP 7.1.x.
The software commands include checks and validations to help ensure an efficient upgrade.

The following processes and commands are deprecated beginning in Data ONTAP 7.3.1. They will not be supported in later release families.

- The use of client-based extraction and installation tools
  Instead of using the tar command on UNIX hosts or setup.exe files on Windows hosts, copy the upgrade .exe file to the storage system and install it with the software command.

- The use of the software install command on systems running Data ONTAP 7.2 and later
  You must use the software install command to update a system running Data ONTAP 7.1 family. However, to upgrade from Data ONTAP 7.2 or later releases, you must use the software update command.

For more information, see the *Data ONTAP Upgrade Guide*.

**Improved support for nondisruptive upgrades in SAN environments**

Beginning with the release of Data ONTAP 7.3, major version or cross-family NDU is supported in SAN configurations (FCP and iSCSI). Although end users can perform an NDU process, careful qualification and preparation are essential, particularly in SAN environments.

*Note:* Before performing a nondisruptive upgrade in a SAN environment, be sure to prepare carefully using recommendations in the *Data ONTAP Upgrade Guide*.

**Read reallocation of data**

For workloads that perform a mixture of random writes and large and multiple sequential reads, the read reallocation function improves the file’s layout and sequential read performance.

When you enable read reallocation, by using the `vol options read_realloc` command, Data ONTAP analyzes the parts of the file that are read sequentially. If the associated blocks are not already largely contiguous, Data ONTAP updates the file's layout by rewriting those blocks to another location on disk. The rewrite improves the file’s layout, thus improving the sequential read performance the next time that section of the file is read.

For more information about the `vol options read_realloc` command, see the `na_vol(1)` man page.

**Extents for FlexVol volumes**

Enabling extents, by setting the `vol options extent` command to `on`, might improve performance of Exchange database validation. However, to enable
extents when storage space is a concern, you should set the vol options extent command to space_optimized instead of on.

The space_optimized option conserves space. However, it results in degraded read performance through the Snapshot copies. Therefore, if fast read performance through Snapshot copies is a higher priority to you than storage space, do not use the space_optimized option.

For more information about the vol options extent command, see the na_vol(1) man page.

**Option to disable root access to the storage system**

By default, the root account’s access to the storage system is enabled. You have the option to disable the root account’s access to the storage system, preventing the root account from logging in to the system or executing any commands.

To prevent the root account from logging in to the system or executing any commands, a non-root user with the security-complete-user-control security capability can disable the root account’s access by setting the new option security.passwd.rootaccess.enable to off.

To reset the security.passwd.rootaccess.enable option to on (the default) to enable root access, a user must first change the root account’s password.

The option to enable or disable root access is supported if you access the storage system through Telnet, RSH, SSH, HTTP Admin, NDMP, or the serial console.

The option to enable or disable root access is not supported if you access the storage system through the Remote Lan Module (RLM).

For more information about how to disable the root account’s access to the storage system, see the *Data ONTAP System Administration Guide*.

**Audit log enhancement**

Changes made to configuration and registry files are now audited. Read-only APIs by default are not audited but you can enable auditing of read-only APIs with the auditlog.readonly_api.enable option.

When a configuration changes, the audit log shows the following information:

- What configuration files were accessed
- When the configuration files were accessed
- What has been changed in the configuration files

For more information see the *Data ONTAP System Administration Guide*.
Read-only access to FilerView

Users with the new filerview-readonly capability have read-only access to FilerView and can view objects on a storage system that FilerView manages. These users are not able to add or modify objects through FilerView.

For more information, see the Data ONTAP System Administration Guide.

Physical reallocation of data

A physical reallocation (using the -p option of the reallocate start command) reallocates user data on the physical blocks in the aggregate, while preserving the logical block locations within a flexible volume. You can perform physical reallocation with flexible volumes or with files and LUNs within flexible volumes.

Physical reallocation might reduce the extra storage requirements in a flexible volume when reallocation is run on a volume with Snapshot copies. It might also reduce the amount of data that needs to be transmitted by SnapMirror on its next update after reallocation is performed on a SnapMirror source volume.

Physical reallocation is not supported on flexible volumes or on files and LUNs within flexible volumes that are in an aggregate created by a version of Data ONTAP earlier than version 7.2.

Note: LUNs in this context refer to the LUNs that Data ONTAP serves to clients, not to the array LUNs used for storage on a storage array.

Note: A file reallocation scan using reallocate start or reallocate start -p does not rearrange blocks that are shared between files by deduplication on deduplicated volumes. Since a file reallocation scan does not predictably improve read performance when used on deduplicated volumes, performing file reallocation on deduplicated volumes is not recommended. Instead, for files to benefit from the reallocation scan, they should be stored on volumes that are not enabled for deduplication.

For more information, see the Data ONTAP System Administration Guide.

Performance Acceleration Module (PAM), Flash Cache module, and WAFL external cache

Note: Flash Cache modules were formerly referred to as Performance Acceleration Modules (PAM) II.

You can increase Write Anywhere File Layout (WAFL) cache memory in storage systems running Data ONTAP 7.3 and later by using WAFL external
cache and PAMs or Flash Cache modules. WAFL external cache is a software component of Data ONTAP and requires a license.

WAFL external cache provides extra WAFL cache memory to improve the performance of the storage system by reducing the number of the system’s disk reads. The options flexscale commands enable you to control how user data blocks are cached.

With WAFL external cache and PAMs or Flash Cache modules, your storage system’s cache memory can hold up to 31 aggregates (which would mean 31 traditional volumes, if your system uses only traditional volumes). As long as your storage system has fewer than 31 aggregates total, there is no limit to the number of flexible volumes that can be cached by the WAFL external cache.

For more information, see the Data ONTAP System Administration Guide.

**FilerView enhancements**

FilerView in Data ONTAP 7.3 and later releases provides enhanced management capabilities.

FilerView now supports NFS version 4.

In addition, you can perform the following tasks using FilerView:

- Enable viewing objects
- Create FlexCache volumes
- View reclaimable size of Snapshot copies
- Create aggregates with mutually compatible disks

For more information about these features, see the FilerView online Help.

**The e0M interface**

Available on N6000 series storage systems, the e0M interface is dedicated to Data ONTAP management activities. The e0M interface enables you to access the storage system remotely to perform administrative tasks. By using the e0M interface, you can separate management traffic from data traffic on the storage system for security and throughput benefits.

On N6000 series storage systems, the Ethernet port that is indicated by a wrench icon on the rear of the chassis connects to an internal Ethernet switch. The internal Ethernet switch then provides connectivity to the e0M interface and the Remote LAN Module (RLM). Because the e0M interface and the RLM each have unique IP and MAC addresses, the Ethernet switch is able to direct traffic to either the e0M interface or the RLM.
You can use the e0M interface to access the storage system with these protocols: Telnet, RSH, SNMP, HTTP, and—if SecureAdmin is enabled—SSH.

For information on how to set up the e0M interface, see the *Data ONTAP Software Setup Guide*. For more information about the e0M interface, see the *Data ONTAP System Administration Guide* and the *Data ONTAP Network Management Guide*.

**Data ONTAP supports up to 24 SSH sessions**
Starting with Data ONTAP 7.3, the maximum number of SSH administrative sessions you can run concurrently is increased to 24.

**Only critical AutoSupport notifications are sent to the autosupport.to recipients**
Starting with Data ONTAP 7.3, only critical AutoSupport email notifications are sent to the recipients defined in the autosupport.to option. Non-critical notifications are suppressed.

All AutoSupport notifications, regardless of their level of severity, continue to be sent to technical support as displayed by the read-only option autosupport.support.to.

For more information about the AutoSupport options, see the na_options(1) man page.

**Partner recipients for AutoSupport email notifications**
The new option autosupport.partner.to allows you to define the list of partner recipients for AutoSupport email notifications.

Whereas the autosupport.support.to option is read-only and displays where email-based AutoSupport notifications are sent to technical support when the autosupport.support.enable option is set to on (the default), the autosupport.partner.to option allows you to define a list of partner recipients who will receive all AutoSupport notifications regardless of the severity level or the setting of the autosupport.support.enable option.

Using the autosupport.partner.to option, you can specify up to five email addresses for partner recipients to receive AutoSupport notifications. The email addresses should be entered as a comma-separated list with no spaces in between. By default, the autosupport.partner.to option is not defined and has an empty list.

To receive any email-based AutoSupport notifications, you must also define a mail host by using the autosupport.mailhost option.
File access protocol enhancements

Data ONTAP 7.3 and later releases provide new features of NFSv4 and FPolicy, new commands for debugging CIFS file access control problems, a new option for specifying the minimum levels of authentication and session security that clients must use, and compatibility with Windows Vista and Windows Server 2008.

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

- "Support for multiple open instances of the SMB named pipe on an FPolicy server"
- "Support for the SMB 2.0 protocol"
- "Kerberos Multi Realm support" on page 47
- "NFSv4 enhancements" on page 47
- "Enhancements to NFS access cache management" on page 47
- "Improved security for Perfmon connections" on page 48
- "Compatibility with Windows Vista and Windows Server 2008" on page 49
- "New commands for debugging CIFS access control problems" on page 48
- "New option for setting the minimum authentication level and session security level that clients must use" on page 48
- "FPolicy enhancements" on page 48
- "Maximum number of auxiliary UNIX groups supported for a user" on page 49

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

Starting with Data ONTAP 7.3.2, 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 File Access and Protocols Management Guide.

Support for the SMB 2.0 protocol

Data ONTAP 7.3.1 supports 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.

To support the SMB 2.0 protocol, Data ONTAP 7.3.1 includes several new options. For more information, see "New options in Data ONTAP 7.3" on page 96.
Kerberos Multi Realm support
In Data ONTAP 7.3.1 and later releases, you can configure Data ONTAP to use a UNIX-based KDC for NFS and an Active Directory-based KDC for CIFS. This configuration is called a Kerberos Multi Realm configuration.

For more information, see the Data ONTAP File Access and Protocols Management Guide.

NFSv4 enhancements
Data ONTAP 7.3 and later releases provide new NFSv4 features and enhancements.

These are the new NFSv4 features:
• Support for nested export rules
• Support for Unicode
• Support for Kerberized callbacks
• Support for the `fsecurity show` command (displays ACLs on files and directories)
• Support for SKT_TRACE modules

These are the NFSv4 enhancements:
• Access to .snapshot entries from Solaris clients
• Support for the "nosuid" export rule
• Increase of the maximum size of ACLs from 192 to 400 ACEs
• More read and write parallelism in WAFL through Waffinity changes
• Delegation callback enhancements:
  – A new thread-pool is added for delegation callback.
  – Callbacks now use non-reserved ports.
• A rewritten reply cache that is now multi-processor (MP) enabled
• Resolution of issues with UID/GID name mapping, especially in regard to cluster failover (CFO) configurations
• Handling of Incoming UTF-8 strings as sym-link data

Enhancements to NFS access cache management
Beginning in Data ONTAP 7.3.6, the `exportfs` command includes updated options for managing entries in the NFS access cache.

The `-c` option of the `exportfs` command has been updated to take multiple IP addresses as arguments. This enables verification of current export rights for multiple clients in one operation.
The `-f` option of the `exportfs` command now includes a `-n` parameter, which allows you to flush access cache entries that correspond to a specific host.

For more information, see the `exportfs(1)` man page and the Data ONTAP File Access and Protocols Management Guide.

**Improved security for Perfmon connections**

Beginning in Data ONTAP 7.3.6, only administrative users are granted Perfmon connections to Data ONTAP by default. Access for other users or groups must be defined explicitly.

In earlier releases, Data ONTAP did not check access permissions for connections from the Microsoft Perfmon tool. As a result, any user could use Perfmon to access a storage system, view performance data, and set counters, which could lead to security and performance problems.

Data ONTAP 7.3.6 and later releases include the `cifs.perfmon.allowed_users` option, which takes arguments that grant access only to specified users or groups. By default, no argument is set, which restricts access to Administrators only.

For more information about the `cifs.perfmon.allowed_users` option, see the `options(1)` man page.

**New commands for debugging CIFS access control problems**

Data ONTAP 7.3 and later releases provide new commands for debugging CIFS access control problems.

Commands for debugging CIFS access control problems include the `sectrace add`, `sectrace remove`, `sectrace show`, and `sectrace print-status` commands. For more information about these commands, see the Data ONTAP File Access and Protocols Management Guide and the `na_sectrace(1)` man page.

**New option for setting the minimum authentication level and session security level that clients must use**

Data ONTAP 7.3 and later releases provide a new option, `cifs.LMCompatibilityLevel`, for setting the minimum authentication level and session security level that clients must use to access files on the storage system.

For more information about this option, see the Data ONTAP File Access and Protocols Management Guide and the `na_options(1)` man page.

**FPolicy enhancements**

FPolicy for Data ONTAP 7.3.1 introduces a number of new features.

Following are the new features of FPolicy:
- Support for screening of certain CIFS operations on alternate data streams
- Support for registration of multiple FPolicy servers from a single IP address
- Support for screening of CIFS operations from SMB 2.0 clients
- Enhancements are made to the internal implementation of the FPolicy subsystem that improve the way multiple requests are handled in parallel. This is expected to improve the request processing throughput of the FPolicy subsystem. The actual increase in throughput varies depending on the third party FPolicy application server being used and on the load on the storage subsystem.

Maximum number of auxiliary UNIX groups supported for a user

If you use Kerberos V5 authentication, the maximum number of auxiliary UNIX groups that a user can be a member of is 32 by default. You can increase the maximum to 256 groups by setting the \texttt{nfs.max_num_aux_groups} option to 256. However, in FlexCache setups, Data ONTAP supports a maximum of 32 auxiliary UNIX groups for FlexCache volumes, regardless of the value set for this option.

If you do not use Kerberos V5 authentication, the maximum number of auxiliary UNIX groups that a user can be a member of is 16.

For more information about the \texttt{nfs.max_num_aux_groups} option, see the \texttt{na_options(1)} man page.

Compatibility with Windows Vista and Windows Server 2008

Data ONTAP 7.2.5.1 and later releases are compatible with Windows Vista clients, Windows Server 2008 clients, and Windows Server 2008 domain controllers.

For more information, see the Windows File Services (CIFS) Compatibility Matrix, available on the IBM N series support website, which is accessed and navigated as described in "Websites" on page 2.
Block protocols enhancements

Data ONTAP 7.3 and later releases provide additional capabilities using iSCSI and FC protocols for N series SAN environments.

For more information about these features, see the Data ONTAP Block Access Management Guide.

- “10-GbE Unified Target Adapter protocol support”
- “Takeover and giveback performance enhancements in a SAN environment”
- “Ability to delete backing Snapshot copies of deleted LUN clones”
- “New default value for the maximum number of iSCSI connections per session” on page 51
- “WWPN aliases” on page 51
- “New windows_2008 LUN Multiprotocol Type (ostype)” on page 51
- “New solaris_efi, xen, and hyper_v LUN Multiprotocol Types (ostypes)” on page 52

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 - FC 1063
- Copper - FC 1064

Takeover and giveback performance enhancements in a SAN environment

Takeover and giveback times are significantly improved on systems with a large number of LUNs between 500 and 2000 and systems under heavy I/O load in a SAN environment.

Note: LUNs in this context refer to Data ONTAP served LUNs, not LUNs on third-party storage.

Ability to delete backing Snapshot copies of deleted LUN clones

Starting with Data ONTAP 7.3, you can enable a system to lock backing Snapshot copies of the active LUN clone only. If you enable the locking of the active LUN clone only and then want to delete the active LUN clone, you can delete the base Snapshot copy without having to first delete the more recent backing Snapshot copies.
Before Data ONTAP 7.3, the system automatically locked all backing Snapshot copies when Snapshot copies of LUN clones were taken.

To enable a system to lock backing Snapshot copies for the active LUN clone only, enter the following command: `vol options volume_name snapshot_clone_dependency on`.

**Note:** The `snapshot_clone_dependency` option is set to `off` by default.

For more information, see the *Data ONTAP Block Access Management Guide for iSCSI and FCP*.

**New default value for the maximum number of iSCSI connections per session**

Starting with Data ONTAP 7.3, the default value for the maximum number of iSCSI connections per session is 32. You can change the default value by setting the `iscsi.max_connections_per_second` option to a value from 1 to 32. To change the option back to the default, set the `iscsi.max_connections_per_second` option to `use_system_default`.

**WWPN aliases**

World Wide Port Names (WWPNs) are identified by a unique, 64-bit identifier displayed as a 16-character hexadecimal value in Data ONTAP. However, SAN administrators might find it easier to identify Fibre Channel ports using an alias instead, especially in larger SANs.

Starting with Data ONTAP 7.3, you can use the `wwpn-alias` sub-command to create, remove, and display WWPN aliases.

**New windows_2008 LUN Multiprotocol Type (ostype)**

In Data ONTAP 7.3 and later, you can use the new `windows_2008` Multiprotocol Type for Windows Server 2008. You specify this LUN Multiprotocol Type by using `windows_2008` as the value for `ostype`.

If you are using Windows Server 2008 in conjunction with Data ONTAP, you must specify the `windows_2008` LUN Multiprotocol Type as the value of `ostype` to avoid performance problems. However, note that if you are using SnapDrive to create your LUNs, SnapDrive uses the `windows_gpt` LUN Multiprotocol Type, but partitions the LUNs in a way that avoids performance problems.

Data ONTAP actually implements the `windows_2008` LUN Multiprotocol Type to achieve the best performance with the standard partitioning.

**Note:** Future versions of SnapDrive will use the `windows_2008` LUN Multiprotocol Type.
New `solaris_efi`, `xen`, and `hyper_v` LUN Multiprotocol Types (ostypes)

Beginning in Data ONTAP 7.3.1, you can use the following new LUN Multiprotocol Types: `solaris_efi`, `xen`, and `hyper_v`. You specify the LUN Multiprotocol Type by using `solaris_efi`, `xen`, or `hyper_v` as the value for `ostype`.

Follow these guidelines when using the new LUN Multiprotocol Types:

<table>
<thead>
<tr>
<th>LUN Multiprotocol Type</th>
<th>When to use</th>
</tr>
</thead>
</table>
| `solaris_efi`          | If you are using Solaris EFI labels.  
  **Note:** Using any other LUN Multiprotocol Type with Solaris EFI labels might result in LUN misalignment problems. Refer to your Solaris Host Utilities documentation and release notes for more information. |
| `xen`                  | If you are using Xen and your LUNs will be configured with Linux LVM with Dom0.  
  **Note:** For raw LUNs, use the type of guest operating system as the LUN Multiprotocol Type. |
| `hyper_v`              | If you are using Windows Server 2008 Hyper-V and your LUNs contain virtual hard disks (VHDs).  
  **Note:** For raw LUNs, use the type of child operating system as the LUN Multiprotocol Type. |
Networking and Security protocols enhancements

Data ONTAP 7.3 and later releases provide enhanced network performance and security features.

For more information about these features, see the Data ONTAP Network Management Guide.

- "Ability to block data traffic on the e0M interface"
- "Support for IPv6" on page 54
- "Support for CDP" on page 57
- "Transport Layer Security protocol" on page 57
- "TLS support in FilerView" on page 58
- "Port-based load-balancing option for multimode vifs" on page 58
- "WAFL External cache group added to netapp.mib" on page 58
- "Round-robin load balancing is supported" on page 58
- "SNMPv3 supported" on page 59
- "New maximum number of network interfaces" on page 59
- "RLM supports IPv6" on page 60

Ability to block data traffic on the e0M interface

In Data ONTAP 7.3.6 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 7.3.6 introduces a new option interface.blocked.mgmt_data_traffic to control the blocking of data transfer on the e0M interface. New systems that are shipped with Data ONTAP 7.3.6 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 7.3.6 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 7.3.5 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 System Administration Guide*.

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

**Support for IPv6**

Starting with Data ONTAP 7.3.1, IPv6 addressing is supported. You can enable IPv6 on your storage systems, and use most features of IPv6.

You can enable IPv6 on your storage system during setup. For more information, see the *Data ONTAP 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 Network Management Guide*.

**IPv6 features in Data ONTAP 7.3.1**

The following IPv6 features are supported starting with Data ONTAP 7.3.1:

- 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
- Support for IPv6 in network administration commands, such as the `traceroute6`, `ping6`, `netdiag`, and `pkt6` commands
- Support for a 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
- Configuring VLANs with IPv6 addresses
- Configuring single-mode, static multimode, and dynamic multimode (LACP) vifs with IPv6 across multiple NICs
- Support for SNMP v1, SNMP v2c, and SNMP v3 over IPv6
- Management Information Base (MIB) for TCP, UDP, ICMPv6, and IPv6
• Active/active configuration support for IPv6, 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 Active/Active Configuration Guide*.

• MultiStore support for IPv6 addresses as network resources that can be assigned to the *vFiler* units. IPv6 addresses are supported in the *vfiler* commands. For more information, see the *Data ONTAP MultiStore Management Guide*.

• Support for iSCSI over IPv6
  For more information, see the *Data ONTAP Block Access Management Guide for iSCSI and FCP*.

• Support for file access protocols—CIFS, FTP, HTTP, NFSv2, NFSv3, and NFSv4—over IPv6
  For more information, see the *Data ONTAP File Access and Protocols Management Guide*.

• Support for LDAP and Kerberos v5 with IPv6

• IPv6 addresses can be used to connect to the storage system over HTTPS for secure administrative access
  SecureAdmin SSL must be enabled before you can issue HTTPS requests to the storage system.

• To connect to the storage system for SSH protocol version 2 if IPv6 is enabled
  SecureAdmin SSH must be enabled before you can issue SSH requests to the storage system.

**IPv6 features in Data ONTAP 7.3.2**

Starting with Data ONTAP 7.3.2, you can add SNMP traphosts with IPv6 addresses. You should specify only IPv6 addresses, and not host names, to identify IPv6 traphosts.

**IPv6 features in Data ONTAP 7.3.3**

Starting with Data ONTAP 7.3.3, you can use IPv6 addresses for the following functions:

• Fast path over IPv6
  For more information, see the *Data ONTAP Network Management Guide*.

• To connect to the RLM if you have set up and enabled IPv6 for Data ONTAP, your RLM firmware version is 4.0 or later, and you have configured the RLM for IPv6
  Disabling IPv6 on Data ONTAP also disables IPv6 on the RLM.
Note: Using IPv6 to connect to the BMC is currently not supported.
For information about installing and updating the RLM firmware, see the
Data ONTAP Upgrade Guide.
For information about configuring the RLM, see the Data ONTAP System
Administration Guide.
• In the hwassist options if IPv6 is set up and enabled in Data ONTAP and
IPv6 is enabled on the RLM.
• In MetroCluster configurations if IPv6 is set up and enabled in Data
ONTAP
• To connect to the storage system over the RSH protocol if both the
rsh.enable option and the ip.v6.enable option are set to on
• To access FilerView for managing the storage system if both the
ip.v6.enable option and the httpd.ipv6.enable option are set to on.

Note: Internet Explorer 6.0 does not support IPv6. To access FilerView
using IPv6, you must use Internet Explorer 7.
• For the dump, restore, and ndmpcopy commands over IPv6
For more information, see the Data ONTAP Data Protection Tape Backup and
Recovery Guide.
• IPv6 is supported with SnapMirror, SnapVault, and volume copy over IPv6
For more information, see the Data ONTAP Data Protection Online Backup
and Recovery Guide.

IPv6 RFCs supported
Support for Internet Protocol version 6 (IPv6) in Data ONTAP is extended
based on certain RFCs. The following table lists the RFCs supported for this
release.

<table>
<thead>
<tr>
<th>RFC</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 1094</td>
<td>NFSv2</td>
</tr>
<tr>
<td>RFC 1813</td>
<td>NFSv3</td>
</tr>
<tr>
<td>RFC 3530</td>
<td>NFSv4</td>
</tr>
<tr>
<td>RFC 1886</td>
<td>DNS extensions to support IPv6</td>
</tr>
<tr>
<td>RFC 1981</td>
<td>Path MTU Discovery for IPv6</td>
</tr>
<tr>
<td>RFC 2136</td>
<td>DNS and DDNS for IPv6</td>
</tr>
<tr>
<td>RFC 2292</td>
<td>Advanced Sockets API for IPv6</td>
</tr>
<tr>
<td>RFC 2460</td>
<td>IPv6 specification</td>
</tr>
<tr>
<td>RFC 2461</td>
<td>Neighbor Discovery for IPv6</td>
</tr>
<tr>
<td>RFC 2462</td>
<td>IPv6 Stateless Address Autoconfiguration</td>
</tr>
<tr>
<td>RFC</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>------------------------------------------------------------------</td>
</tr>
<tr>
<td>RFC 2464</td>
<td>Transmission of IPv6 Packets over Ethernet Networks</td>
</tr>
<tr>
<td>RFC 2465</td>
<td>Management Information Base for IP Version 6: Textual Conventions and General Group</td>
</tr>
<tr>
<td>RFC 2466</td>
<td>Management Information Base for IP Version 6: ICMPv6</td>
</tr>
<tr>
<td>RFC 2553</td>
<td>Basic Socket Interface Extensions for IPv6</td>
</tr>
<tr>
<td>RFC 2711</td>
<td>IPv6 Router Alert Option</td>
</tr>
<tr>
<td>RFC 2893</td>
<td>Transition Mechanisms for IPv6 Hosts and Routers (Dual Stack Mode)</td>
</tr>
<tr>
<td>RFC 3164</td>
<td>BSD Syslog Protocol (Syslog capabilities for IPv6-related events)</td>
</tr>
<tr>
<td>RFC 4007</td>
<td>IPv6 Scoped Address Architecture</td>
</tr>
<tr>
<td>RFC 4022</td>
<td>Management Information Base for the Transmission Control Protocol</td>
</tr>
<tr>
<td>RFC 4113</td>
<td>Management Information Base for the User Datagram Protocol</td>
</tr>
<tr>
<td>RFC 4120</td>
<td>Kerberos v5</td>
</tr>
<tr>
<td>RFC 4193</td>
<td>Unique Local IPv6 Unicast Addresses</td>
</tr>
<tr>
<td>RFC 4254</td>
<td>Secure Shell (SSHv2)</td>
</tr>
<tr>
<td>RFC 4291</td>
<td>IPv6 Addressing Architecture</td>
</tr>
<tr>
<td>RFC 4443</td>
<td>ICMPv6 for IPv6</td>
</tr>
<tr>
<td>RFC 4512</td>
<td>LDAP</td>
</tr>
</tbody>
</table>

### Support for CDP

Starting with Data ONTAP 7.3.3, Cisco Discovery Protocol (CDP) is supported. 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 Network Management Guide*.

### Transport Layer Security protocol

Data ONTAP 7.3.2 and later versions in the Data ONTAP 7.3 release family add support for 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 FTP over SSL (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 System Administration Guide*.

**TLS support in FilerView**

FilerView in Data ONTAP 7.3.2 and later supports the Transport Layer Security (TLS) protocol.

To enable the TLS protocol on a storage system, you have to enable the TLS feature by setting `tls.enable` to `on`. The default value is `off`.

**Note:** Before setting the TLS feature, you have to enable Secure Sockets Layer (SSL). For more information, see the *Data ONTAP System Administration Guide*.

**Port-based load-balancing option for multimode vifs**

Port-based load balancing is supported for multimode vifs 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 vif, 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 Network Management Guide*.

**WAFL External cache group added to netapp.mib**

In Data ONTAP 7.3.2, a new group, `extcache`, is added to the `netapp.mib` file. A management utility can use this group to query the storage system for the status and statistics of the Flash Cache module or the Performance Acceleration Module (PAM) card by using SNMP.

The object identifier (OID) of the `extcache` group is 1.3.6.1.4.1.789.1.26.X.0, where X is a field under the `extcache` group.

**Round-robin load balancing is supported**

Data ONTAP 7.3.1.1 supports the round-robin load balancing option for multimode vifs. Load balancing ensures that all the interfaces of a multimode vif are equally utilized for outgoing traffic.
You should use the round-robin option for load balancing a single connection's traffic across multiple links to increase single connection throughput. However, this method might cause out-of-order packet delivery. If the remote TCP endpoints do not handle TCP reassembly correctly or lack sufficient memory to store out of order packets, they may be forced to drop packets, and this can lead to unnecessary retransmissions from the storage controller.

For more information about the other load balancing options available for multimode vifs, see the Data ONTAP Network Management Guide.

SNMPv3 supported

Data ONTAP 7.3 and later releases support SNMPv3, giving users security enhancements not available in earlier versions of SNMP. Data ONTAP has also changed its netapp.mib file to conform to SNMPv2 and SNMPv3 MIB guidelines. SNMPv3 supports a new "authentication, no privacy" privilege, counter64-based MIBs, and new client-side commands.

SNMPv3 includes these new features that work with Data ONTAP:

- An authentication, no privacy privilege using MD5
- Counter64-based MIBs, which reduce errors caused by having two entries that denote high and low values for 64-bit variables
- These new client-side commands, are supported by SNMPv3:
  - snmpbulkwalk displays all the leaves on an SNMP tree as a result of a single query
  - snmpbulkget collects all the leaves on an SNMP tree as a result of a single query

For additional information about these features see the Data ONTAP Network Management Guide.

New maximum number of network interfaces

Beginning with Data ONTAP 7.3, N series storage systems, except for the smallest models, are no longer limited to 128 interfaces per storage system. Larger storage systems can accommodate from 256 to 1024 network interfaces per system depending on the system’s memory and whether they are in a clustered or active/active configuration.

Run the sysconfig command and refer to the Memory size field displayed for your storage system’s slot 0 system board to determine your storage system memory.

The new maximum number of network interfaces allowed for each system are shown in the following table. The total number of interfaces can include physical, vif, VLAN, vh, and loopback interfaces.
Storage system memory | Maximum number of network interfaces
--- | ---
2 GB or less | 128
2 GB or less in an active/active configuration | 256
6 GB or less | 256
6 GB or less in an active/active configuration | 512
More than 6 GB | 512
More than 6 GB in an active/active configuration | 1024

The number of physical interfaces depends on the storage system model. Each storage system can support up to 16 vifs. The maximum number of VLANs that can be supported equals the maximum number of network interfaces shown in the following table minus the total number of physical interfaces, vifs, vh, and loopback interfaces supported by the storage system.

The number of physical interfaces depends on the storage system model. See your storage system documentation for the number of supported physical interfaces.

**RLM supports IPv6**

Beginning with Data ONTAP 7.3.3, the RLM supports IPv6. To send RLM traffic over IPv6, you must be running RLM version 4.0 and IPv6 must be enabled on the storage system.

For more information see “New RLM firmware and its upgrade requirements” on page 115
Data protection enhancements

Data ONTAP 7.3 and later releases provide enhanced Snapshot data protection technologies (such as SnapMirror), tape backup support, and security administration.

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

- "Use of SnapVault to protect a volume SnapMirror destination" on page 62
- "TCP window size for a SnapMirror relationship" on page 62
- "Retention of older SnapVault Snapshot copies on SnapVault secondary volumes" on page 62
- "Support for SnapMirror network compression" on page 63
- "If volumes with deduplication exceed the maximum supported size" on page 63
- "Snapshot copies and log files of SnapLock for SnapVault use system clock for naming" on page 63
- "Changes to the SnapLock autocommit feature" on page 63
- "Backing up LUN clones to tape" on page 64
- "SnapLock supported in Data ONTAP 7.3.1 and later" on page 64
- "LockVault now known as the SnapLock for SnapVault feature" on page 64
- "More concurrent transfers for qtree SnapMirror, volume SnapMirror, and SnapVault" on page 64
- "Maximum number of concurrent replication operations with ATA disks" on page 65
- "Reservation of storage system resources for volume SnapMirror, qtree SnapMirror, and SnapVault replication operations" on page 65
- "Synchronous SnapMirror modes" on page 65
- "Space guarantee for a volume SnapMirror destination" on page 66
- "Support for SnapMirror over Fibre Channel on N3600 storage systems" on page 67
- "SnapVault integration with SnapManager" on page 68
- "SnapVault primary and secondary on the same storage system" on page 68
- "Enhancements to SnapVault for NetBackup" on page 68
- "Bandwidth optimization for Open Systems SnapVault" on page 68
- "SnapVault for NetBackup supports basic block mode backups" on page 69
- "SnapVault with deduplication" on page 69
- "Deduplication metadata relocated" on page 69
- "Deduplication configuration data relocated" on page 69
Use of SnapVault to protect a volume SnapMirror destination

In Data ONTAP 7.3.2 and later releases in the Data ONTAP 7.3 release family, SnapVault supports the use of a user-specified Snapshot copy for backing up a volume SnapMirror destination.

**Note:** To be able to specify a Snapshot copy for the SnapVault backup of a SnapMirror destination, you need to preserve the Snapshot copy.

For more information about the use of SnapVault for backing up a volume SnapMirror destination, see the *Data ONTAP Data Protection Online Backup and Recovery Guide*.

TCP window size for a SnapMirror relationship

Data ONTAP 7.3.2 and later releases in the Data ONTAP 7.3 release family support TCP window sizes up to 14 MB for a multipath SnapMirror relationship. This option is applicable only for asynchronous SnapMirror relationships.

**Note:** You should only adjust the TCP window size for a SnapMirror relationship, if there are throughput issues related to bandwidth utilization.

For more information about adjusting the TCP window size for a SnapMirror relationship, see the *Data ONTAP Data Protection Online Backup and Recovery Guide*.

Retention of older SnapVault Snapshot copies on SnapVault secondary volumes

In Data ONTAP 7.3.2 and later, you can retain SnapVault Snapshot copies on SnapVault secondary volumes.

You enable the *preservesnap* or *preserve* option to retain SnapVault Snapshot copies on SnapVault secondary volumes. When you enable this option, SnapVault does not delete an older Snapshot copy to create a new Snapshot copy when the maximum retention limit is reached. In such a case, you can manually delete some Snapshot copies to make space available for new
Snapshot copies. You can also clone the volume to create new Snapshot copies on this new volume while preserving the older Snapshot copies intact on the old base volume.

For more information about retaining older SnapVault Snapshot copies on SnapVault secondary volumes, see the Data ONTAP 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 support SnapMirror network compression. This feature is supported only for asynchronous volume SnapMirror.

**Note:** The SnapMirror destination system should be using Data ONTAP 7.3.2 or a later release that supports SnapMirror network compression.

SnapMirror network compression 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 the compression feature for volume SnapMirror, see the Data ONTAP Data Protection Online Backup and Recovery Guide.

**If volumes with deduplication exceed the maximum supported size**

In Data ONTAP 7.3.2, volumes continue to be online when they exceed the maximum supported size. However, deduplication is disabled on such volumes. For more information about the maximum volume size allowed for different storage systems, with and without deduplication, see the Data ONTAP Data Protection Online Backup and Recovery Guide.

**Snapshot copies and log files of SnapLock for SnapVault use system clock for naming**

Starting with Data ONTAP 7.3.2, the time value specified in the names of the Snapshot copies and the log files that are created by the SnapLock for SnapVault feature uses the system clock instead of complianceclock.

For more information, see the Data ONTAP Archive and Compliance Management Guide.

**Changes to the SnapLock autocommit feature**

Starting with Data ONTAP 7.3.2, the SnapLock autocommit operation uses the system clock to commit a file to the WORM state.
For more information about this feature, see the *Data ONTAP Archive and Compliance Management Guide*.

**Backing up LUN clones to tape**

When you back up data to tape, the *dump* command will not back up the LUN clones that are inconsistent.

For all other LUN clones, the *dump* command will lock their backing snapshot copies to ensure that they do not become inconsistent during the back up.

*Note:* LUNs in this context refer to Data ONTAP served LUNs, not LUNs on third-party storage.

**SnapLock supported in Data ONTAP 7.3.1 and later**

Data ONTAP 7.3.1 supports SnapLock, with new features.

Beginning with Data ONTAP 7.3.1, you can create SnapLock Enterprise and SnapLock Compliance volumes on a storage system.

SnapLock includes the following new features in Data ONTAP 7.3.1:

- Privileged delete
- SnapLock logging
- Fingerprinting

SnapLock supports the following Data ONTAP features:

- Deduplication
- vFiler unit compatibility

For more information about these features, see the *Data ONTAP Archive and Compliance Management Guide* and the *Data ONTAP Upgrade Guide*.

**LockVault now known as the SnapLock for SnapVault feature**

Starting with Data ONTAP 7.3.1, the LockVault feature is known as the SnapLock for SnapVault feature.

**More concurrent transfers for qtree SnapMirror, volume SnapMirror, and SnapVault**

In Data ONTAP 7.3 and later, qtree SnapMirror, asynchronous volume SnapMirror, and SnapVault each support a higher number of concurrent transfers. However, Open Systems SnapVault does not have a higher limit of concurrent transfers.

For more details, see the *Data ONTAP Data Protection Online Backup and Recovery Guide*. 
Maximum number of concurrent replication operations with ATA disks

In Data ONTAP 7.3 and later, the use of ATA disks does not affect the maximum number of concurrent replication operations a storage system can perform.

For more information, about the 'Data protection using SnapMirror' in the Data ONTAP Data Protection Online Backup and Recovery Guide.

Reservation of storage system resources for volume SnapMirror, qtree SnapMirror, and SnapVault replication operations

In Data ONTAP 7.3 and later, you can reserve resources for a specific number of volume SnapMirror, qtree SnapMirror, or SnapVault replication operations on a storage system. The reserved resources would not be available for other types of replication.

For example, if you reserve a specified number of volume SnapMirror replication operations, the resources required for the operations are reserved on the storage system. This means that a volume SnapMirror replication operation for the storage system, acting as a source or a destination, is guaranteed to start until the specified limit of reserved operations is met. It also means that the maximum number of operations for other types of replication, such as qtree SnapMirror or SnapVault, would be reduced in order to keep the resources free for volume SnapMirror replication operations.

**Note:** If the total number of concurrent replication operations is below the maximum limit, the storage system would run more of the replication operations, above the limit reserved for a specific type of replication.

You can specify the number of reserved transfers using one of the following commands:

For volume SnapMirror:

```bash
options replication.volume.reserved_transfers n
```

For qtree SnapMirror and SnapVault:

```bash
options replication.logical.reserved_transfers n
```

$n$ is the number of reserved transfers. The default value of $n$ is 0.

Synchronous SnapMirror modes

In Data ONTAP 7.3 and later, the outstanding parameter is not used for semi-synchronous SnapMirror configurations.

- This change affects the `snapmirror.conf` file syntax.
- This change does not affect synchronous SnapMirror configurations.
• This change does not disrupt the operation of storage systems.

A new option called semi-sync replaces the outstanding parameter. This new option provides a recovery point objective of approximately 10 seconds. This means that you might lose the data updated in the last 10 seconds or less. This change is intended to optimize performance.

Therefore, starting with Data ONTAP 7.3 and later, synchronous SnapMirror is available in two modes:
• SnapMirror Sync: The source storage system acknowledges a client write operation only after both the source and destination storage systems have completed the write operation.
• SnapMirror Semi-Sync: The source storage system acknowledges the client write operation immediately after the source receives the data. The destination storage system is synchronized with the source at intervals of approximately 10 seconds.

To avoid disrupting the existing configuration, SnapMirror interprets the old outstanding options as follows:
• If the outstanding parameter is set as less than 10 seconds or less than 500 operations, the relationship is converted to SnapMirror Sync (equivalent to sync in the /etc/snapmirror.conf file).
  For example, these might be two entries in the /etc/snapmirror.conf file.
  systemA:vol-1 systemB:vol-2 outstanding=1s sync
  systemA:vol-1 systemB:vol-2 outstanding=200ops sync
  Either of the two preceding entries, would be interpreted as this command:
  systemA:vol-1 systemB:vol-2 - sync
• If the outstanding parameter is set as more than or equal to 10 seconds, or more than or equal to 500 ops, the relationship is converted to SnapMirror Semi-Sync (equivalent to sync in the /etc/snapmirror.conf file).
  For example, these are two entries in the /etc/snapmirror.conf file.
  systemA:vol-1 systemB:vol-2 outstanding=10s sync
  systemA:vol-1 systemB:vol-2 outstanding=500ops sync
  Either of the two preceding entries, would be interpreted as:
  systemA:vol-1 systemB:vol-2 - semi-sync

Note: SnapMirror does not modify the content of the snapmirror.conf file.

**Space guarantee for a volume SnapMirror destination**

Starting with Data ONTAP 7.3, you can enable space guarantee for a SnapMirror destination FlexVol volume. This feature enables you to reserve space in an aggregate for a SnapMirror destination volume.
Data ONTAP 7.1 and later releases support space guarantees for FlexVol volumes. Data ONTAP 7.3 extends this feature to SnapMirror destination volumes.

When you upgrade a volume SnapMirror destination to Data ONTAP 7.3, the volume guarantees are not set for the SnapMirror destination volumes. This is indicated by `upgraded_replica`, listed as one of the options displayed for the volume, when you use the `vol status` command.

```
176 system-b> vol status sm-dst-vol
151 Volume State  Status  Options
137 sm-dst-vol    online  raid_dp, flex snapmirrored=on, snapmirrored=on,
121  read-only  upgraded_replica, upgraded_replica,
113  fs_size_fixed=on, fs_size_fixed=on,
111  guarantee=volume, guarantee=volume(disabled)
176 Containing aggregate: 'aggr2'
```

You can change the space guarantee for the volume by using the following command.

```
vol options vol_name guarantee {none | file | volume}
```

```
120 system-b> vol options sm-dst-vol guarantee volume
```

If you use the `vol status` command for the volume after setting the space guarantee, the `upgraded_replica` option will not be displayed.

```
176 system-b> vol status sm-dst-vol
151 Volume State  Status  Options
137 sm-dst-vol    online  raid_dp, flex snapmirrored=on, snapmirrored=on,
121  read-only  fs_size_fixed=on, fs_size_fixed=on,
113  guarantee=volume, guarantee=volume
176 Containing aggregate: 'aggr2'
```

For more information about volume space guarantees, see the *Data ONTAP Storage Management Guide*.

**Note:** In a volume SnapMirror relationship, you can enable volume guarantees for both the source and the destination volumes.

As releases earlier than Data ONTAP 7.3 do not support space guarantees for a volume SnapMirror destination, reverting to an earlier release would make the guarantees ineffective.

**Support for SnapMirror over Fibre Channel on N3600 storage systems**

In Data ONTAP 7.3.1 and later releases, SnapMirror over Fibre Channel is supported for N3600 storage systems. You need to add a Fibre Channel NIC adapter (FC 1033) to use this feature.
For more information about hardware support, see *IBM System Storage N series Introduction and Planning Guide.*

**SnapVault integration with SnapManager**

Data ONTAP 7.3 and later provides disk-to-disk backup and restore functionalities for SnapManager by integrating SnapVault functionality with SnapManager 5.0 and later and with SnapDrive 6.0 for Windows and later. You need Protection Manager to make this solution work. SnapManager uses SnapDrive as a conduit to support Protection Manager retention policies and schedules. Starting with Data ONTAP 7.3, the SnapVault restore functionality provides nondisruptive baseline and incremental restores. This new functionality is exported to SnapManager using Data ONTAP APIs.

**SnapVault primary and secondary on the same storage system**

Beginning in Data ONTAP 7.3, the SnapVault primary and secondary feature can be on the same storage system. This capability allows customers to license both the SnapVault primary license and the SnapVault secondary license on the same storage system.

A storage system licensed for both the SnapVault primary license and the SnapVault secondary license can send and receive SnapVault backups from other storage systems or locally within itself (for example, between FC and ATA aggregates).

*Note:* The primary and secondary qtrees cannot be within the same volume of the storage system.

**Enhancements to SnapVault for NetBackup**

SnapVault for NetBackup is available and supported beginning with Data ONTAP 7.3.

Several significant improvements have been made to SnapVault for NetBackup. The following are the key enhancements:

- **Performance**
  - Write throughput rates, for both unstructured (file) data, significantly improved over earlier versions
- **Improvements in metadata storage efficiency**
- **Support for active-active storage controller configurations**

**Bandwidth optimization for Open Systems SnapVault**

Beginning with Data ONTAP 7.3, the SnapVault secondary storage systems support bandwidth optimization for Open Systems SnapVault. However, qtree SnapMirror, volume SnapMirror, and SnapVault do not support bandwidth optimization.
SnapVault for NetBackup supports basic block mode backups
Starting with Data ONTAP 7.3.1, SnapVault for NetBackup supports basic block mode backups.

Basic block mode backups provide speed and inline deduplication capabilities of regular File System Export (FSE) mode backups without exposing the file system for export.

For more information about this feature, see the Data ONTAP Data Protection Online Backup and Recovery Guide.

SnapVault with deduplication
In Data ONTAP 7.3 and later, the deduplication feature is integrated with SnapVault. Every baseline or incremental SnapVault transfer initiates a deduplication operation after the archival Snapshot copy is taken on the destination system.

Deduplication metadata relocated
In Data ONTAP 7.3 and later, the fingerprint database and the change logs used by the deduplication process are located outside the volume, in the aggregate. The fingerprint database and the change logs form the deduplication metadata. Because the metadata resides in the aggregate outside the volume, it is not included in the FlexVol volume Snapshot copies. This change enables deduplication to achieve higher space savings.

For information about the use of SnapMirror for replicating volumes that use deduplication, see the Data ONTAP Data Protection Online Backup and Recovery Guide.

Deduplication configuration data relocated
In Data ONTAP 7.3 and later, the deduplication configuration data for a given volume is located in a metafile within the volume. (Previously, it was located in the registry in the root volume.) This change helps volume-level operations such as volume SnapMirror, snap restore, vol copy, and vol clone to keep the deduplication configuration data about the volume on the destination consistent with the source.

Deduplication support on SnapLock volumes
Beginning with Data ONTAP 7.3.1, deduplication is supported on SnapLock volumes.

However, if deduplication is enabled on a SnapLock volume and you attempt to revert to a Data ONTAP release that does not support deduplication on SnapLock volumes, you will see an error message. To avoid or recover from this situation, contact technical support.
**Deduplication checkpoint feature**

The checkpoint feature is used to log the execution process of a deduplication operation periodically.

When a deduplication operation is stopped for any reason and a checkpoint data exists, the same deduplication process can resume from the latest checkpoint file.

**SnapLock support for vFiler units**

Starting with Data ONTAP 7.3.1, SnapLock is compatible with vFiler units. However, SnapLock disallows vFiler unit creation if the root of the vFiler unit is on a SnapLock volume. The privileged delete feature is also not supported on the vFiler units.

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

**Qtree SnapMirror with deduplication**

In Data ONTAP 7.3 and later, the deduplication feature supports qtree SnapMirror. Qtree SnapMirror does not automatically initiate a deduplication operation at the completion of every individual qtree SnapMirror transfer. However, you can set up a deduplication schedule independent of your qtree SnapMirror transfer schedule.

When using qtree SnapMirror with deduplication, remember the following:

- To use deduplication with qtree SnapMirror, you should enable both deduplication and SnapMirror licenses.
- Deduplication can be enabled on the source system, the destination system, or both systems.
- The source system sends duplicate blocks to the destination system even if deduplication is enabled on the source system. Therefore, there are no network bandwidth savings.
- The deduplication schedule is not tied to a qtree SnapMirror update and can be configured just like the deduplication schedule for any volume.

**Volume SnapMirror with deduplication**

In Data ONTAP 7.3 and later, the fingerprint database and the change logs that the deduplication process uses are located outside a volume, in its aggregate. Therefore, volume SnapMirror does not transfer them to a destination. This change provides additional network bandwidth savings.

**Limit on entries in the snapmirror.conf file for each storage system**

The limit on the number of valid entries for each storage system in the `/etc/snapmirror.conf` file is increased to 1,024.
**Note:** This limitation is different from the maximum number of concurrent replications you can have on a storage system.

For more information, see the SnapMirror chapter in the *Data ONTAP Data Protection Online Backup and Recovery Guide*.

**Automatic schedule for deduplication**

Deduplication runs automatically when the number of blocks added or changed since the last deduplication operation exceeds a specified percentage (20 percent by default) of the total number of blocks that the deduplication operation has already processed. Starting with Data ONTAP 7.3.2, you can configure this percentage value by using the `sis config -s auto@num /vol/volname` command. Here, `num` is a two-digit number to specify the percentage.

**Support for 840 disk drives on fabric-attached MetroClusters**

In Data ONTAP 7.3.5 and Data ONTAP 8.0.1 7-Mode, fabric-attached MetroCluster configurations can support up to 840 disk drives.

For more information, see the *Data ONTAP Active/Active Configuration Guide*. 
Storage resource management enhancements

Data ONTAP 7.3 and later releases provide improved performance, resiliency, and management capabilities for storage resources.

- “FlexClone files and FlexClone LUNs support on vFiler units” on page 75
- “Aggregate size calculation changes”
- “FlexClone files and FlexClone LUNs”
- “SnapMirror destination space guarantee not disabled” on page 73
- “Autogrow capability for FlexCache volumes” on page 74
- “Support for changing to software-based disk ownership nondisruptively” on page 74
- “Disconnected operation for FlexCache volumes” on page 75

FlexClone files and FlexClone LUNs

Starting with Data ONTAP 7.3.2, you can clone files and LUNs inside a FlexVol volume using the FlexClone technology. You can clone a LUN without the need of a backing Snapshot copy. A cloned file is called a FlexClone file and a cloned LUN is called a FlexClone LUN.

In Data ONTAP 7.3.1, the FlexClone files and FlexClone LUNs feature commands are available in the priv set advanced mode. Starting with Data ONTAP 7.3.2, the feature commands are available in the admin mode.

For more information about FlexClone files and FlexClone LUNs, see the Data ONTAP Storage Management Guide.

Aggregate size calculation changes

In Data ONTAP 7.3 and later releases, the total size of an aggregate is computed using the usable size of its data disks rather than the raw size of all of its disks.

In previous releases of Data ONTAP, the total size of an aggregate was computed by adding together the raw size of all disks in the aggregate, including parity disks, and regardless of the amount of disk space available to be used in each data disk. This method of computing the aggregate size could result in an aggregate exceeding the maximum allowable size even though the amount of usable space in that aggregate was much smaller than the maximum allowable aggregate size.

In Data ONTAP 7.3 and later releases, only the “used size” (as reported by the sysconfig -r command) of data disks is used to calculate the total aggregate size. If you were prevented from adding disks to an aggregate due to aggregate size constraints in an earlier version of Data ONTAP, you might be able to add more disks to that aggregate after upgrading to Data ONTAP 7.3.
**Maximum number of data disks per 16-TB aggregate**

With the aggregate size calculation changes present in Data ONTAP 7.3, you can include more data disks in an aggregate without exceeding the aggregate size limit.

The following table shows the maximum number of data disks that can be included in a 16-TB aggregate for Data ONTAP 7.3 and for previous releases.

<table>
<thead>
<tr>
<th>Data disk size</th>
<th>Data disk type</th>
<th>Maximum with Data ONTAP 7.2 and earlier</th>
<th>Maximum with Data ONTAP 7.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>36 GB</td>
<td>FC</td>
<td>421</td>
<td>493</td>
</tr>
<tr>
<td>72 GB</td>
<td>FC</td>
<td>212</td>
<td>246</td>
</tr>
<tr>
<td>144 GB</td>
<td>FC/SAS</td>
<td>106</td>
<td>123</td>
</tr>
<tr>
<td>300 GB</td>
<td>FC/SAS</td>
<td>51</td>
<td>61</td>
</tr>
<tr>
<td>450 GB</td>
<td>FC/SAS</td>
<td>33</td>
<td>40</td>
</tr>
<tr>
<td>250 GB</td>
<td>SATA</td>
<td>68</td>
<td>79</td>
</tr>
<tr>
<td>320 GB</td>
<td>SATA</td>
<td>53</td>
<td>61</td>
</tr>
<tr>
<td>500 GB</td>
<td>SATA</td>
<td>33</td>
<td>39</td>
</tr>
<tr>
<td>750 GB</td>
<td>SATA</td>
<td>22</td>
<td>26</td>
</tr>
<tr>
<td>1 TB</td>
<td>SATA</td>
<td>15</td>
<td>19</td>
</tr>
<tr>
<td>2 TB</td>
<td>SATA</td>
<td>N/A</td>
<td>9</td>
</tr>
</tbody>
</table>

**SnapMirror destination space guarantee not disabled**

In Data ONTAP 7.3 and later releases, the space guarantee on SnapMirror destination FlexVol volumes is no longer automatically disabled. If you are upgrading the storage system to Data ONTAP 7.3, and you have existing SnapMirror destination volumes, you need to enable the guarantee on these volumes.

Starting in Data ONTAP 7.3, when you designate a FlexVol volume as a SnapMirror destination volume, its space guarantee remains enabled.

When you upgrade a system to Data ONTAP 7.3 with an existing FlexVol volume that is a SnapMirror destination with a disabled space guarantee that was originally of type volume, the `vol status` command displays the new volume option `upgraded_replica`. This option indicates that the space guarantee on this volume, originally of type volume, was disabled because the volume was used as a SnapMirror destination in a Data ONTAP version earlier than 7.3.
If you have sufficient space in the volume's containing aggregate, you can use the `vol` option command to change the space guarantee to either `volume` or `none`. When you make that change, the `upgraded_replica` volume option disappears.

**Autogrow capability for FlexCache volumes**

In Data ONTAP 7.3 and later releases, FlexCache volumes can be configured to increase their size automatically as the size of the cached data increases.

In earlier releases, the best way to size a FlexCache volume to avoid performance issues due to incorrect sizing was to size all FlexCache volumes to be the same size as their containing aggregate. With Data ONTAP 7.3, however, you should size new FlexCache volumes to use the automatic resizing capability.

With this new capability enabled, Data ONTAP automatically increases the size of the FlexCache volume when the size of the working set becomes too large for the current size of the FlexCache volume.

Data ONTAP never decreases the size of the FlexCache volume. However, as for previous releases of Data ONTAP, if there is contention between FlexCache volumes for free space, the FlexCache volumes with the most data accesses are allocated more space, while FlexCache volumes that are accessed less frequently are truncated. When a FlexCache volume is truncated, no data is lost.

New FlexCache volumes created in Data ONTAP 7.3 and later releases have the Autogrow capability enabled by default. If necessary, you can use the `vol` options command to disable the `flexcache_autogrow` option.

FlexCache volumes created using an earlier version of Data ONTAP, and then upgraded to Data ONTAP 7.3, have the Auotgrow capability disabled by default. If you want to enable it, you can use the `vol` options command to enable the `flexcache_autogrow` option.

**Note:** If you have sized your FlexCache volumes to be the same size as their containing aggregate in a previous release and you are satisfied with the configuration, you do not need to reconfigure these FlexCache volumes to use the new automatic resizing capability.

For more information about the FlexCache Autogrow capability, see the *Data ONTAP Storage Management Guide*.

**Support for changing to software-based disk ownership nondisruptively**

Starting with Data ONTAP 7.3.1, you can change an active/active configuration from hardware-based disk ownership to software-based disk ownership.
ownership without having to take both nodes of an active/active
configuration offline at the same time. Future versions of Data ONTAP will
not support hardware-based disk ownership.

Disconnected operation for FlexCache volumes
In Data ONTAP 7.3.1 and later releases, a FlexCache volume can be
configured to return cached data even when it has lost its connection to its
origin volume. You can configure how long the disconnected FlexCache
volume serves potentially stale data. Connection to the origin volume should
be reestablished as quickly as possible.

For more information, see the information about the flex_cache volume
options on the na_vol(1) man page.

FlexClone files and FlexClone LUNs support on vFiler units
In Data ONTAP 7.3.3 and later releases of the 7.x release family, and in Data
ONTAP 8.0.1 and later, the FlexClone files and FlexClone LUNs commands
are available in the default and nondefault vfiler contexts.

You can use FlexClone files and 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 unit by using the FlexClone file or LUN commands.

For more information about FlexClone files and FlexClone LUNs, see the Data
ONTAP Storage Management Guide.
**Active/active configuration enhancements**

Data ONTAP 7.3 and later releases include the new Multipath Storage feature and additional MetroCluster support.

For more information about these features, see the Data ONTAP Active/Active Configuration Guide.

- “Hardware-assisted takeover feature support for IPv6 addresses”
- “MetroCluster support for IPv6 addresses”
- “Support for 672 disk drives on fabric-attached MetroClusters”
- “MetroCluster nodes on separate subnets”
- “Hardware-assisted takeover”
- “Deduplication support on stretch and fabric-attached MetroClusters” on page 77
- “Major nondisruptive upgrades for fabric-attached MetroClusters” on page 77

**Hardware-assisted takeover feature support for IPv6 addresses**

Starting with the Data ONTAP 7.3.3 release, IPv6 addresses can be used in the hwassist options if IPv6 is enabled and set up in Data ONTAP and IPv6 is enabled on the RLM.

**MetroCluster support for IPv6 addresses**

Starting with the Data ONTAP 7.3.3, IPv6 addresses can be used in MetroCluster configurations if IPv6 is enabled and set up in Data ONTAP.

**Support for 672 disk drives on fabric-attached MetroClusters**

Starting with the Data ONTAP 7.3.2 release, fabric-attached MetroCluster configurations can support up to 672 disk drives (if that is within the maximum storage capacity of the system).

For more information, see the Data ONTAP Active/Active Configuration Guide.

**MetroCluster nodes on separate subnets**

Starting with the Data ONTAP 7.3.2, nodes in a MetroCluster configuration can be configured on separate subnets.

To do this, you must create an /etc/mcrc file and enable the cf.takeover.use_mcrc_file option on both nodes.

For more information, see the Data ONTAP Active/Active Configuration Guide.

**Hardware-assisted takeover**

In the Data ONTAP 7.3 release family, active/active configurations support hardware-assisted takeover. Hardware-assisted takeover allows systems with
Remote LAN Modules (RLMs) to improve the speed with which takeover events are detected, thereby speeding up the takeover time.

**Note:** The hardware-assisted takeover feature is available only on systems that support Remote LAN Modules (RLMs) and have the RLM installed and set up. It is not supported on the N3300 and N3600 storage systems, which use the Baseboard Management Controller (BMC) as a remote management card.

When enabled, hardware-assisted takeover takes advantage of the remote management card’s capabilities to detect failures on the local machine that could require a takeover. If a failure is detected, the card sends an alert to the partner node and the partner, if the failure is of a certain type, performs a takeover. These alerts can speed takeover, because if an alert is received, the Data ONTAP takeover process on the partner does not have to take the time to verify that the failing system is no longer giving a heartbeat and confirm that a takeover is actually required.

The hardware-assisted takeover option (cf.hw_assist) is enabled by default. The cf hw_assist status and cf hw_assist stats commands display information about the hardware-assisted takeover functionality, and the cf hw_assist test command tests the functionality.

For more information, see the Data ONTAP Active/Active Configuration Guide.

**Deduplication support on stretch and fabric-attached MetroClusters**

Data ONTAP 7.3.1 and later releases support deduplication on stretch and fabric-attached MetroClusters. This support applies to N series and gateway systems.

For more information about deduplication support on active/active configurations and MetroClusters, see the Data ONTAP Data Protection Online Backup and Recovery Guide and Implementing IBM Storage Data Deduplication Solutions (IBM Redbook SG247888).

**Major nondisruptive upgrades for fabric-attached MetroClusters**

Data ONTAP 7.3 introduces the ability to upgrade fabric-attached MetroClusters from one release family to another nondis disruptively (major nondisruptive upgrades).

For more information about fabric-attached MetroClusters, see the Data ONTAP Active/Active Configuration Guide.

For more information about nondisruptive upgrades, see the Data ONTAP Upgrade Guide.
MultiStore enhancements

Data ONTAP 7.3 and later releases provide additional MultiStore capabilities.

- "New option for the vfiler dr configure command"
- "Online migration support on vFiler units"
- "Commands supported by the ONTAPI interface library"
- "Secure communication for setup of disaster recovery and data migration” on page 79
- "SnapMover license is not required” on page 79
- "Deduplication support on vFiler units” on page 79
- "New AutoSupport message for transparent vfiler migration” on page 79

New option for the vfiler dr configure command

Data ONTAP 7.3 and later releases provide a new option -u for the vfiler dr configure command. You can use this 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.

When you use the -u option with the vfiler dr configure command to set up a disaster recovery vFiler unit, the existing SnapMirror relationship between the source and the destination storage system is not re-initialized.

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

Online migration support on vFiler units

Starting with Data ONTAP 7.3.3, MultiStore supports online migration of vFiler units. By using online migration, users can migrate vFiler units without experiencing any disruption in data availability. You must use Provisioning Manager to perform online migration of vFiler units.

For more information about online migration of vFiler units, see the Provisioning Manager and Protection Manager Guide to Common Workflows for Administrators and the Provisioning Manager and Protection Manager Printable Help for use with DataFabric Manager® Server 4.0.

Commands supported by the ONTAPI interface library

The ONTAPI interface library, which is part of the Manage Data ONTAP solutions, supports some new functions.

The following new functions are supported:

- Retrieve vFiler unit network settings such as the following:
  - DNS domain name and DNS server IP addresses
  - NIS domain name and NIS server IP address
  - Netmask in IP address binding information
- Migrate the vFiler unit and view the status
- Set the snapshot reserve percentage values
- Get or set the optional descriptive comment for a LUN

**Secure communication for setup of disaster recovery and data migration**

MultiStore supports disaster recovery and data migration implemented over SSL. When setting up or controlling disaster recovery or data migration, SSL is used only for the setup and control communication between storage systems running Data ONTAP. The data being migrated or copied is not encrypted using SSL.

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

**SnapMover license is not required**

Starting with Data ONTAP 7.3.2, the SnapMover license is not required to use the `vfiler migrate -m nocopy` command.

**Deduplication support on vFiler units**

Data ONTAP 7.3.1 and later releases provide enhanced deduplication support on vFiler units. You can perform deduplication operations from the CLI of all vFiler units, in addition to the CLI of vfiler0.

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

**New AutoSupport message for transparent vfiler migration**

In Data ONTAP 7.3.3, an AutoSupport message is sent when transparent vfiler migration from one controller to another controller fails. Failure is defined by cutover exceeding 120 seconds.

The message will be triggered from both the source and destination controllers whenever transparent vfiler migration fails.

In addition, information about all the migrations that occurred during the past week are included in the weekly AutoSupport message. If a migration failed, the weekly message also contains information about the failure.
New and changed commands and options

This section provides information about the commands, options, and configuration files that have been changed or added to the Data ONTAP 7.3 release family. These changes are described in the following topics:

- “New commands in Data ONTAP 7.3” on page 82
- “Changed commands in Data ONTAP 7.3” on page 87
- “New options in Data ONTAP 7.3” on page 96
- “Changed options in Data ONTAP 7.3” on page 102
- “Replaced or removed commands in Data ONTAP 7.3” on page 104
- “SnapMirror commands that become obsolete in Data ONTAP 8.0” on page 105
## New commands in Data ONTAP 7.3

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 7.3 release in which the command was introduced

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
<th>Documentation</th>
<th>Release introduced</th>
</tr>
</thead>
<tbody>
<tr>
<td>acpadmin list_all</td>
<td>Displays information about the ACP (Alternate Control Path) storage subsystem.</td>
<td>Data ONTAP Storage Management Guide</td>
<td>7.3.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>na_acpadmin(1) man page</td>
<td></td>
</tr>
<tr>
<td>cdpd</td>
<td>Displays information about devices that advertise themselves by using the CDPv1 (Cisco Discovery Protocol) protocol.</td>
<td>Data ONTAP Network Management Guide</td>
<td>7.3.3</td>
</tr>
<tr>
<td>cf hw_assist stats</td>
<td>Displays statistics about hardware-assisted takeovers.</td>
<td>Data ONTAP Configuration Guide</td>
<td>7.3</td>
</tr>
<tr>
<td>cf hw_assist status</td>
<td>Displays the status of the hardware-assisted takeover feature.</td>
<td>Data ONTAP Active/Active Configuration Guide</td>
<td>7.3</td>
</tr>
<tr>
<td>cf hw_assist test</td>
<td>Sends a test alert to the partner to verify operation of the hardware-assisted takeover feature.</td>
<td>Data ONTAP Active/Active Configuration Guide</td>
<td>7.3</td>
</tr>
<tr>
<td>clone clear</td>
<td>Clears the status of a failed FlexClone file or FlexClone LUN operation.</td>
<td>Data ONTAP Storage Management Guide</td>
<td>7.3.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>na_clone(1) man page</td>
<td></td>
</tr>
<tr>
<td>clone start</td>
<td>Creates a FlexClone file or FlexClone LUN of a parent file or LUN inside a FlexVol volume.</td>
<td>Data ONTAP Storage Management Guide</td>
<td>7.3.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>na_clone(1) man page</td>
<td></td>
</tr>
<tr>
<td>clone status</td>
<td>Views the status of all FlexClone files or FlexClone LUNs operations currently running, FlexClone operations that failed, and the reason for the failure.</td>
<td>Data ONTAP Storage Management Guide</td>
<td>7.3.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>na_clone(1) man page</td>
<td></td>
</tr>
<tr>
<td>Command</td>
<td>Purpose</td>
<td>Documentation</td>
<td>Release introduced</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>--------------------</td>
</tr>
</tbody>
</table>
| clone stop            | Stops a FlexClone file or FlexClone LUN operation.                      | Data ONTAP Storage Management Guide  
an_clone(1) man page                                                           | 7.3.2              |
| file fingerprint      | Calculates the fingerprint of the file using md5 or sha-256 digest algorithm. | Data ONTAP Archive and Compliance Management Guide                               | 7.3.1              |
| fpolicy servers show  | Displays the status of all the FPolicy servers that are registered to a file policy | na_fpolicy(1) man page                                                          | 7.3                |
| ndp                   | Controls or diagnoses IPv6 neighbor discovery protocol.                  | na_ndp(1) man page                                                             | 7.3.1              |
| nfs nsdb flush        | Flushes specified entries from the name server database cache (NSDB).    | na_nfs(1) man page                                                             | 7.3.3              |
| options               | Schedules the SnapVault transfer updates from a specific Snapshot copy when backing up a volume SnapMirror destination using SnapVault | Data ONTAP Data Protection Online Backup and Recovery Guide  
na_snapvault(1) man page | 7.3.5              |
| snapvault.snapshot_for_dr_backup named_snapshot_only | Schedules the SnapVault transfer updates from a specific Snapshot copy when backing up a volume SnapMirror destination using SnapVault | Data ONTAP Data Protection Online Backup and Recovery Guide  
na_snapvault(1) man page | 7.3.5              |
| snapvault.snapshot_for_dr_backup named_snapshot_preferred | Schedules the SnapVault transfer updates from a specific Snapshot copy when backing up a volume SnapMirror destination using SnapVault | Data ONTAP Data Protection Online Backup and Recovery Guide  
na_snapvault(1) man page | 7.3.5              |
| snapvault.snapshot_for_dr_backup vsm_base_only | Schedules the SnapVault transfer updates from a specific Snapshot copy when backing up a volume SnapMirror destination using SnapVault | Data ONTAP Data Protection Online Backup and Recovery Guide  
na_snapvault(1) man page | 7.3.5              |
| ping6                 | Sends ICMPv6 ECHO_REQUEST packets to network hosts.                      | Data ONTAP Network Management Guide  
n_a_ping6(1) man page                                                         | 7.3.1              |
<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
<th>Documentation</th>
<th>Release introduced</th>
</tr>
</thead>
<tbody>
<tr>
<td>rdfile</td>
<td>Reads the specified file and writes the contents to standard output.</td>
<td>Data ONTAP System Administration Guide</td>
<td>7.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>na_rdfile(1) man page</td>
<td></td>
</tr>
<tr>
<td>rlm test snmp</td>
<td>Performs an SNMP test on the RLM.</td>
<td>Data ONTAP System Administration Guide</td>
<td>7.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>na_rlm(1) man page</td>
<td></td>
</tr>
<tr>
<td>rshstat</td>
<td>Displays information about active RSH sessions.</td>
<td>Data ONTAP System Administration Guide</td>
<td>7.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>na_rshstat(1) man page</td>
<td></td>
</tr>
<tr>
<td></td>
<td>You can add up to 10 permission tracing filters.</td>
<td>na_sectrace(1) man page</td>
<td></td>
</tr>
<tr>
<td>sectrace print-status</td>
<td>Displays information about why Data ONTAP allowed or denied access to a particular client or user.</td>
<td>Data ONTAP File Access and Protocols Management Guide</td>
<td>7.3</td>
</tr>
<tr>
<td></td>
<td>Data ONTAP provides this extra information in addition to the information it logs to the console when the criteria of a permission tracing filter are met.</td>
<td>na_sectrace(1) man page</td>
<td></td>
</tr>
<tr>
<td>sectrace remove</td>
<td>Removes a permission tracing filter. Because permission tracing filters have a minor effect on performance, you should use them for debugging purposes only, removing them when you are finished.</td>
<td>Data ONTAP File Access and Protocols Management Guide</td>
<td>7.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>na_sectrace(1) man page</td>
<td></td>
</tr>
<tr>
<td>sectrace show</td>
<td>Displays one or all permission tracing filters on a storage system.</td>
<td>Data ONTAP File Access and Protocols Management Guide</td>
<td>7.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>na_sectrace(1) man page</td>
<td></td>
</tr>
<tr>
<td>Command</td>
<td>Purpose</td>
<td>Documentation</td>
<td>Release introduced</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------------------------------------------------------------------</td>
<td>--------------------------------------------</td>
<td>--------------------</td>
</tr>
</tbody>
</table>
| snaplock log archive | Archives active SnapLock log file.                                      | Data ONTAP Archive and Compliance Management Guide  
na_snaplock(1) man page                             | 7.3.1              |
| snaplock log status     | Displays the status of active SnapLock log files on a volume.          | Data ONTAP Archive and Compliance Management Guide  
na_snaplock(1) man page                             | 7.3.1              |
| snaplock log volume     | Sets the active SnapLock log volume to the volume name specified. If the volume name is not specified, displays the current active log volume name. | Data ONTAP Archive and Compliance Management Guide  
na_snaplock(1) man page                             | 7.3.1              |
| snaplock options      | The privdel option shows state of the privileged delete option on the SnapLock Enterprise volume. | Data ONTAP Archive and Compliance Management Guide  
na_snaplock(1) man page                             | 7.3.1              |
| snaplock privdel       | Deletes unexpired files on a SnapLock Enterprise volume.                | Data ONTAP Archive and Compliance Management Guide  
na_snaplock(1) man page                             | 7.3.1              |
| sp help               | Displays the Data ONTAP sp commands that you can enter at the storage system prompt. | Data ONTAP System Administration Guide  
na_sp(1) man page                                     | 7.3.5              |
| sp reboot             | Reboots the SP and causes the SP to perform a self-test.               | Data ONTAP System Administration Guide  
na_sp(1) man page                                     | 7.3.5              |
| sp setup              | Initiates the interactive SP setup script.                             | Data ONTAP System Administration Guide  
na_sp(1) man page                                     | 7.3.5              |
| sp status             | Displays the current status and the network configuration of the SP.   | Data ONTAP System Administration Guide  
na_sp(1) man page                                     | 7.3.5              |
<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
<th>Documentation</th>
<th>Release introduced</th>
</tr>
</thead>
<tbody>
<tr>
<td>sp test autosupport</td>
<td>Sends a test e-mail to all recipients specified with the autosupport.to option.</td>
<td>Data ONTAP System Administration Guide</td>
<td>7.3.5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>na_sp(1) man page</td>
<td></td>
</tr>
<tr>
<td>sp test snmp</td>
<td>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.</td>
<td>Data ONTAP System Administration Guide</td>
<td>7.3.5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>na_sp(1) man page</td>
<td></td>
</tr>
<tr>
<td>sp update</td>
<td>Updates the SP firmware.</td>
<td>Data ONTAP System Administration Guide</td>
<td>7.3.5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>na_sp(1) man page</td>
<td></td>
</tr>
<tr>
<td>stats list presets</td>
<td>Displays the list of defined presets in a system.</td>
<td>Data ONTAP System Administration Guide</td>
<td>7.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>na_stats(1) man page</td>
<td></td>
</tr>
<tr>
<td>storage show acp</td>
<td>Displays information about the ACP (Alternate Control Path) storage subsystem.</td>
<td>Data ONTAP Storage Management Guide</td>
<td>7.3.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>na_acpadmin(1) man page</td>
<td></td>
</tr>
<tr>
<td>storage show fault</td>
<td>Provides information about storage expansion unit faults.</td>
<td>na_storage(1) man page</td>
<td>7.3.2</td>
</tr>
<tr>
<td>traceroute6</td>
<td>Prints the route IPv6 packets take to reach the destination.</td>
<td>na_traceroute6(1) man page</td>
<td>7.3.1</td>
</tr>
<tr>
<td>wrfile</td>
<td>Reads data from standard input, which is input from the console or a file, and writes or appends the input into the specified file.</td>
<td>Data ONTAP System Administration Guide</td>
<td>7.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>na_wrfile(1) man page</td>
<td></td>
</tr>
</tbody>
</table>
## Changed commands in Data ONTAP 7.3

Commands have been modified to improve storage expansion unit support and enhance network and storage resources management. Additionally, changes have been made to the `snap autodelete`, `vfiler`, `vol options`, and `vol status` commands.

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 7.3 release in which the change was introduced

<table>
<thead>
<tr>
<th>Command</th>
<th>Change</th>
<th>Documentation</th>
<th>Release command changed in</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>aggr create</code></td>
<td>For native storage, the default RAID type for traditional volumes is now RAID-DP.</td>
<td><code>na_aggr(1) man page Data ONTAP Storage Management Guide</code></td>
<td>7.3</td>
</tr>
<tr>
<td><code>cifs setup</code></td>
<td>Includes new and modified prompts related to Kerberos Multi Realm support.</td>
<td><code>na_cifs_setup(1) man page and Data ONTAP File Access and Protocols Management Guide</code></td>
<td>7.3.1</td>
</tr>
<tr>
<td><code>disk assign</code></td>
<td>The <code>-T</code> option has been added. This option enables you to specify the disk type when you assign disks or array LUNs.</td>
<td><code>na_disk(1) man page and Data ONTAP Storage Management Guide</code></td>
<td>7.3</td>
</tr>
<tr>
<td><code>disk assign</code></td>
<td>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.</td>
<td><code>na_disk(1) man page and Data ONTAP Storage Management Guide</code></td>
<td>7.3.2</td>
</tr>
<tr>
<td><code>environment shelf</code></td>
<td>Output changed to include whether a storage expansion unit supports automatic powercycling.</td>
<td><code>na_environ(1) man page</code></td>
<td>7.3.1</td>
</tr>
<tr>
<td><code>environment shelf</code></td>
<td>Output changed to include SES information.</td>
<td><code>na_environ(1) man page</code></td>
<td>7.3.2</td>
</tr>
<tr>
<td>Command</td>
<td>Change</td>
<td>Documentation</td>
<td>Release command changed in</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------------------------------------------------------------------</td>
<td>------------------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>exportfs -c</td>
<td>The -c option has been updated to take multiple IP addresses as arguments. This enables verification of current export rights for multiple clients in one operation.</td>
<td>na_exportfs(1) man 7.3.3 page</td>
<td>7.3.3</td>
</tr>
<tr>
<td>exportfs -f</td>
<td>The -f option now includes a -n parameter, which allows you to flush access cache entries that correspond to a specific host.</td>
<td>na_exportfs(1) man 7.3.3 page</td>
<td>7.3.3</td>
</tr>
<tr>
<td>fcp portname set</td>
<td>The -f option has been added. If you use the -f, it overrides the warning message you receive when changing the WWPNs.</td>
<td>na_portname(1) man page</td>
<td>7.3.3</td>
</tr>
<tr>
<td>fcp portname swap</td>
<td>The -f option has been added. If you use the -f, it overrides the warning message you receive when changing the WWPNs.</td>
<td>na_portname(1) man page</td>
<td>7.3.3</td>
</tr>
<tr>
<td>flexcache fstat</td>
<td>The -inode-file option has been added. This option displays the number of blocks used by the FlexCache volume's inode file.</td>
<td>na_flexcache(1) man page</td>
<td>7.3.5</td>
</tr>
<tr>
<td>fpolicy options</td>
<td>The cifs_disconnect_check option is added. When the cifs_disconnect_check option is enabled (set to on), specifies that CIFS requests associated with disconnected sessions will not be sent to FPolicy servers for screening.</td>
<td>na_fpolicy(1) man page</td>
<td>7.3</td>
</tr>
<tr>
<td>fpolicy options</td>
<td>Displays the current setting for the cifs_setattr option. If set to on, then the CIFS requests to change the file security descriptor will be screened by the policy.</td>
<td>na_fpolicy(1) man page</td>
<td>7.3</td>
</tr>
<tr>
<td>Command</td>
<td>Change</td>
<td>Documentation</td>
<td>Release command changed in</td>
</tr>
<tr>
<td>--------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>------------------------------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>fpolicy option</td>
<td>Sets or displays the value of serverprogress_timeout for the policy. This is the maximum time an FPolicy server can remain unresponsive while processing the maximum allowed number of screen requests.</td>
<td>na_fpolicy(1) man page</td>
<td>7.3</td>
</tr>
<tr>
<td>fpolicy options</td>
<td>Sets or displays the value of reqcancel_timeout for the policy. This is the maximum time allowed to an FPolicy server to screen a request.</td>
<td>na.fpolicy(1) man page</td>
<td>7.3</td>
</tr>
<tr>
<td>fpolicy options</td>
<td>The monitor_ads option is added. This option enables or disables notification for CIFS operations performed on alternate data streams.</td>
<td>na_fpolicy(1) man page</td>
<td>7.3.1</td>
</tr>
<tr>
<td>fpolicy servers show</td>
<td>The -I option is added. This option displays a list of FPolicy servers connected to the storage system from the given IP address.</td>
<td>FPolicy for Data ONTAP User’s Guide</td>
<td>7.3.1</td>
</tr>
<tr>
<td>ifconfig</td>
<td>The dad_attempts option has been added. This option is used to specify the number of consecutive Neighbor Solicitation messages to be sent while performing Duplicate Address Detection on a tentative address.</td>
<td>Data ONTAP Network Management Guide</td>
<td>7.3.2</td>
</tr>
<tr>
<td>lock break</td>
<td>The -net option is added. This option breaks locks of the specified network family. This command affects NLM protocols only.</td>
<td>na_lock(1) man page</td>
<td>7.3.1</td>
</tr>
<tr>
<td>lun show</td>
<td>When the new LUN class of staging is specified, information about the temporary LUNs preserved in the staging area is reported.</td>
<td>na_lun(1) man page</td>
<td>7.3</td>
</tr>
<tr>
<td>Command</td>
<td>Change</td>
<td>Documentation</td>
<td>Release command changed in</td>
</tr>
<tr>
<td>---------------</td>
<td>------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>nfs setup</td>
<td>Includes new and modified prompts related to Kerberos Multi Realm support.</td>
<td>na_nfs(1) man page and Data ONTAP File Access and Protocols Management Guide</td>
<td>7.3.1</td>
</tr>
<tr>
<td>ping</td>
<td>IPv6 address can be used as an argument. <strong>Note:</strong> It is no longer necessary to use the ping6 command to reach IPv6 hosts.</td>
<td>Data ONTAP Network Management Guide</td>
<td>7.3.3</td>
</tr>
<tr>
<td>reallocate start</td>
<td>The -p option has been added. The option reallocates user data on the physical blocks in the aggregate, while preserving the logical block locations within a flexible volume.</td>
<td>Data ONTAP System Administration Guide na_reallocate(1) man page</td>
<td>7.3</td>
</tr>
<tr>
<td>snap autodelete</td>
<td>The destroy value for the commitment option destroys only Snapshot copies locked because of data backing and data protection mechanisms.</td>
<td>na_snap(1) man page and Data ONTAP Data Protection Online Backup and Recovery Guide</td>
<td>7.3.1</td>
</tr>
<tr>
<td>snap autodelete</td>
<td>The destroy_list option controls what type of locked Snapshot copies, if any, can be deleted.</td>
<td>na_snap(1) man page and Data ONTAP Data Protection Online Backup and Recovery Guide</td>
<td>7.3.1</td>
</tr>
<tr>
<td>snapvault status</td>
<td>The -t option has been added. This option displays the relationships that are active.</td>
<td>na_snapvault(1) man page and Data ONTAP Data Protection Online Backup and Recovery Guide</td>
<td>7.3</td>
</tr>
<tr>
<td>Command</td>
<td>Change</td>
<td>Documentation</td>
<td>Release command changed in</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>snapvault start</td>
<td>The <code>-o</code> option has been added. <code>-o compression=on</code> enables the compression feature for bandwidth optimization for a new Open Systems SnapVault relationship.</td>
<td><code>na_snapvault(1)</code> man page and <code>Data ONTAP Data Protection Online Backup and Recovery Guide</code></td>
<td>7.3.1</td>
</tr>
<tr>
<td>stats show</td>
<td>The <code>-p flexscale</code> option has been added and displays information about a system's WAFL extended cache configuration.</td>
<td><code>Data ONTAP System Administration Guide</code> and <code>na_stats(1)</code> man page</td>
<td>7.3</td>
</tr>
<tr>
<td>stats show</td>
<td>The <code>-p flexscale-access</code> option has been added and displays usage and access information related to WAFL extended cache.</td>
<td><code>Data ONTAP System Administration Guide</code> and <code>na_stats(1)</code> man page</td>
<td>7.3</td>
</tr>
<tr>
<td>stats show</td>
<td>The output of the <code>-p flexscale-access</code> option now includes information about replaced disk IOs and metadata hits and misses.</td>
<td><code>Data ONTAP System Administration Guide</code> and <code>na_stats(1)</code> man page</td>
<td>7.3.2</td>
</tr>
<tr>
<td>storage disable</td>
<td>The <code>-f</code> option is no longer required to disable a tape device if the device is not in use.</td>
<td><code>na_storage(1)</code> man page</td>
<td>7.3</td>
</tr>
<tr>
<td>storage show acp</td>
<td>Displays an addition column, Module type, which shows the type of the IOM.</td>
<td><code>na_storage(1)</code> man page</td>
<td>7.3.5</td>
</tr>
<tr>
<td>storage show expander</td>
<td>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].</td>
<td><code>na_storage(1)</code> man page</td>
<td>7.3.2</td>
</tr>
<tr>
<td>Command</td>
<td>Change</td>
<td>Documentation</td>
<td>Release command changed in</td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>storage show expander</td>
<td>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 [IO0]-[IO7].</td>
<td>na_storage(1) man page</td>
<td>7.3.2</td>
</tr>
<tr>
<td>storage show fault</td>
<td>You can now specify a storage expansion unit name for this command.</td>
<td>na_storage(1) man page</td>
<td>7.3.3</td>
</tr>
<tr>
<td>storage show hub</td>
<td>The output now includes more counters when ESH4 storage expansion unit firmware version 13 or later is present.</td>
<td>na_storage(1) man page</td>
<td>7.3.1</td>
</tr>
<tr>
<td>sysconfig</td>
<td>The <code>-h</code> option has been added. This option displays the same detailed information as the <code>-a</code> option, except that an appropriate unit is used (KB, GB, or TB) and these units are calculated based on the powers of two. For example, for disks, a GB is equal to ((1024 \times 1024 \times 1024)), or 1,073,741,824 bytes.</td>
<td>na_sysconfig(1) man page</td>
<td>7.3</td>
</tr>
<tr>
<td>sysconfig</td>
<td>When the <code>-r</code> option is used to display disk information for SAS-connected disks, the CHAN (channel) column now displays the port as &quot;A&quot; or &quot;B&quot;, just as it does for FC-connected disks. Previously, &quot;1&quot; and &quot;2&quot; were used.</td>
<td>na_sysconfig(1) man page</td>
<td>7.3.2</td>
</tr>
<tr>
<td>useradmin user list</td>
<td>The new <code>-x</code> option displays the extended information for all administrators.</td>
<td>Data ONTAP System Administration Guide</td>
<td>7.3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command</th>
<th>Change</th>
<th>Documentation</th>
<th>Release command changed in</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Data ONTAP System Administration Guide</td>
<td>7.3</td>
</tr>
<tr>
<td>Command</td>
<td>Change</td>
<td>Documentation</td>
<td>Release command changed in</td>
</tr>
<tr>
<td>------------------</td>
<td>------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>useradmin whoami</td>
<td>Displays the username of the user running this command.</td>
<td><em>Data ONTAP System Administration Guide</em></td>
<td>7.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>na_useradmin(1) man page</td>
<td></td>
</tr>
<tr>
<td>vfiler dr configure</td>
<td>The <code>-c secure</code> option has been added. The <code>-c secure</code> option can be used when you want to use the SSL command channel for disaster recovery.</td>
<td>na_vfiler(1) man page and <em>Data ONTAP MultiStore Management Guide</em></td>
<td>7.3.1</td>
</tr>
<tr>
<td>vfiler dr delete</td>
<td>The <code>-c secure</code> option has been added. The <code>-c secure</code> option can be used when you want to use the SSL command channel for disaster recovery.</td>
<td>na_vfiler(1) man page and <em>Data ONTAP MultiStore Management Guide</em></td>
<td>7.3.1</td>
</tr>
<tr>
<td>vfiler migrate</td>
<td>The <code>-c secure</code> option has been added. The <code>-c secure</code> option can be used when you want to use the SSL command channel for disaster recovery.</td>
<td>na_vfiler(1) man page and <em>Data ONTAP MultiStore Management Guide</em></td>
<td>7.3.1</td>
</tr>
<tr>
<td>vfiler migrate start</td>
<td>The <code>-c secure</code> option has been added. The <code>-c secure</code> option can be used when you want to use the SSL command channel for disaster recovery.</td>
<td>na_vfiler(1) man page and <em>Data ONTAP MultiStore Management Guide</em></td>
<td>7.3.1</td>
</tr>
<tr>
<td>vfiler migrate cancel</td>
<td>The <code>-c secure</code> option has been added. The <code>-c secure</code> option can be used when you want to use the SSL command channel for disaster recovery.</td>
<td>na_vfiler(1) man page and <em>Data ONTAP MultiStore Management Guide</em></td>
<td>7.3.1</td>
</tr>
<tr>
<td>vfiler migrate complete</td>
<td>The <code>-c secure</code> option has been added. The <code>-c secure</code> option can be used when you want to use the SSL command channel for disaster recovery.</td>
<td>na_vfiler(1) man page and <em>Data ONTAP MultiStore Management Guide</em></td>
<td>7.3.1</td>
</tr>
<tr>
<td>Command</td>
<td>Change</td>
<td>Documentation</td>
<td>Release command changed in</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>vfiler dr resync</td>
<td>The -c secure option has been added. The -c secure option can be used when you want to use the SSL command channel for disaster recovery.</td>
<td>na_vfiler(1) man page and Data ONTAP MultiStore Management Guide</td>
<td>7.3.1</td>
</tr>
<tr>
<td>vif create</td>
<td>The rr value (round robin load balancing) for the -b option has been added.</td>
<td>na_vif(1) man page and Data ONTAP Network Management Guide</td>
<td>7.3.1</td>
</tr>
<tr>
<td>vif create</td>
<td>The port value (port-based load-balancing) for the -b option has been added.</td>
<td>Data ONTAP Network Management Guide</td>
<td>7.3.2</td>
</tr>
<tr>
<td>vol clone create</td>
<td>The -f option is added. It is used to force the creation of clone on SnapLock volumes.</td>
<td>Data ONTAP Archive and Compliance Management Guide</td>
<td>7.3.1</td>
</tr>
<tr>
<td>vol create</td>
<td>For native storage, the default RAID type for traditional volumes is now RAID-DP.</td>
<td>na_aggr(1) man page and Data ONTAP Storage Management Guide</td>
<td>7.3</td>
</tr>
<tr>
<td>vol offline</td>
<td>If you attempt to take a volume offline while any files contained by that volume are open, Data ONTAP now returns the names of the open files and the process that opened them along with the failure message.</td>
<td>Data ONTAP Storage Management Guide</td>
<td>7.3</td>
</tr>
<tr>
<td>vol options</td>
<td>The new flexcache_autogrow volume option enables or disables the Autogrow capability for FlexCache volumes.</td>
<td>Data ONTAP Storage Management Guide</td>
<td>7.3</td>
</tr>
<tr>
<td>vol options</td>
<td>The nbu_archival_snap option has been added. Setting this option to on for a volume enables archival Snapshot copies for SnapVault for NetBackup.</td>
<td>na_vol(1) man page and Data ONTAP Data Protection Online Backup and Recovery Guide</td>
<td>7.3.1</td>
</tr>
<tr>
<td>Command</td>
<td>Change</td>
<td>Documentation</td>
<td>Release command changed in</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>vol option</td>
<td>The snapshot_clone_dependency option has been added. Setting this option to on enables a system to lock backing Snapshot copies for the active LUN clone only.</td>
<td>na_vol(1) man page and Data ONTAP Block Access Management Guide</td>
<td>7.3</td>
</tr>
<tr>
<td>vol options</td>
<td>The extent option enables extents like on but can only be used on FlexVol volumes.</td>
<td>na_vol(1) man page</td>
<td>7.3.1</td>
</tr>
<tr>
<td>vol options</td>
<td>The read_realloc option enables read reallocation like on but can only be used on FlexVol volumes.</td>
<td>na_vol(1) man page</td>
<td>7.3.1</td>
</tr>
<tr>
<td>vol status</td>
<td>Returns upgraded_replica option when a SnapMirror destination volume's space guarantee has been disabled after an upgrade.</td>
<td>na_vol(1) man page</td>
<td>7.3</td>
</tr>
<tr>
<td>vol status -v</td>
<td>The -v option now returns autodelete and autosize settings.</td>
<td>na_vol(1) man page</td>
<td>7.3.1</td>
</tr>
<tr>
<td>vol status -w</td>
<td>The -w is added. This option prints the expiration time for the SnapLock volume.</td>
<td>na_vol(1) man page and Data ONTAP Archive and Compliance Management Guide</td>
<td>7.3.1</td>
</tr>
<tr>
<td>vol status</td>
<td>When the -r option is used to display disk information for SAS-connected disks, the CHAN (channel) column now displays the port as &quot;A&quot; or &quot;B&quot;, just as it does for FC-connected disks. Previously, &quot;1&quot; and &quot;2&quot; were used.</td>
<td>na_vol(1) man page</td>
<td>7.3.2</td>
</tr>
</tbody>
</table>
### New options in Data ONTAP 7.3

Options that can be used with the option command have been added to enable new storage system features and to improve network, file access, block access, data protection, IPv6, disk types, and storage resources management.

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 or an example value used with the option
- The Data ONTAP 7.3 release in which the option was introduced

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Purpose</th>
<th>Default value or example</th>
<th>Release introduced</th>
</tr>
</thead>
<tbody>
<tr>
<td>auditlog.readonly_api.enable</td>
<td>Controls auditing of APIs based on their roles.</td>
<td>off</td>
<td>7.3</td>
</tr>
<tr>
<td>autosupport.local.nht_data.enable</td>
<td>Sends a copy of health disk data to the customer &quot;to&quot; list.</td>
<td>off</td>
<td>7.3.2</td>
</tr>
<tr>
<td>autosupport.nht_data.enable</td>
<td>Sends a copy of health disk drive data to home.</td>
<td>on</td>
<td>7.3.2</td>
</tr>
<tr>
<td>autosupport.partner.to</td>
<td>Defines the list of recipients who will receive all AutoSupport email notifications regardless of the severity level.</td>
<td>not configured</td>
<td>7.3.1</td>
</tr>
<tr>
<td>cdpd.enable</td>
<td>Enables or disables Cisco Discovery Protocol (CDP) on the storage system.</td>
<td>on</td>
<td>7.3.3</td>
</tr>
<tr>
<td>cdpd.holdtime</td>
<td>Configures the hold time for CDP advertisements.</td>
<td>180 seconds</td>
<td>7.3.3</td>
</tr>
<tr>
<td>cdpd.interval</td>
<td>Configures the time interval for CDP advertisements.</td>
<td>60 seconds</td>
<td>7.3.3</td>
</tr>
<tr>
<td>cf.hw_assist.enable</td>
<td>Enables or disables hardware-assisted takeover. Hardware-assisted takeover is enabled by default on systems that use Remote LAN Module (RLM).</td>
<td>on</td>
<td>7.3</td>
</tr>
<tr>
<td>cf.hw_assist.partner.address</td>
<td>Sets the partner address used by the hardware-assisted takeover process on the remote management card.</td>
<td>IP address on the e0a port of the partner</td>
<td>7.3</td>
</tr>
<tr>
<td>Option</td>
<td>Purpose</td>
<td>Default value or example</td>
<td>Release introduced</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>cf.hw_assist.partner.port</td>
<td>Sets the partner port used by the hardware-assisted takeover process on the remote management card.</td>
<td>4004</td>
<td>7.3</td>
</tr>
<tr>
<td>cf.takeover.use_mcrc_file</td>
<td>Sets the system to use the /etc/mcrc file rather than the /etc/rc file to configure partner interfaces upon takeover. Applies to MetroCluster configurations only.</td>
<td>off</td>
<td>7.3.2</td>
</tr>
<tr>
<td>cifs.audit.liveview.allowed_users</td>
<td>Specifies the user or group of users who can access audit records using the LiveView feature.</td>
<td>on</td>
<td>7.3.1</td>
</tr>
<tr>
<td>cifs.ipv6.enable {on</td>
<td>off}</td>
<td>Enables or disables CIFS over IPv6.</td>
<td>off</td>
</tr>
<tr>
<td>cifs.LMCompatibilityLevel</td>
<td>Sets the storage system's minimum security level (that is, the minimum level of the security tokens that the storage system accepts from clients).</td>
<td>1</td>
<td>7.3</td>
</tr>
<tr>
<td>cifs.perfmon.allowed_users</td>
<td>Specifies users or groups (in addition to Administrators) that are allowed to view performance data using Microsoft Perfmon.</td>
<td>no entry (allows access only to Administrators)</td>
<td>7.3.3</td>
</tr>
<tr>
<td>cifs.smb2.client.enable</td>
<td>Enables or disables the storage system's SMB 2.0 protocol client capability.</td>
<td>off</td>
<td>7.3.1</td>
</tr>
<tr>
<td>cifs.smb2.enable</td>
<td>Enables or disables the SMB 2.0 protocol.</td>
<td>off</td>
<td>7.3.1</td>
</tr>
<tr>
<td>cifs.smb2.durable_handle.enable</td>
<td>Enables or disables SMB 2.0 durable handles.</td>
<td>on</td>
<td>7.3.1</td>
</tr>
<tr>
<td>cifs.smb2.durable_handle.timeout</td>
<td>Specifies the SMB 2.0 durable handle timeout value.</td>
<td>16m</td>
<td>7.3.1</td>
</tr>
<tr>
<td>cifs.smb2.signing.required</td>
<td>Enables or disables the requirement that clients sign SMB 2.0 messages.</td>
<td>off</td>
<td>7.3.1</td>
</tr>
<tr>
<td>Option</td>
<td>Purpose</td>
<td>Default value or example</td>
<td>Release introduced</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>--------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>flexcache.deleg.high_water</td>
<td>Controls the number of outstanding delegations allowed by the origin volume. Do not modify this option unless instructed to do so by technical support.</td>
<td>90</td>
<td>7.3.1</td>
</tr>
<tr>
<td>flexcache.deleg.low_water</td>
<td>Controls the number of outstanding delegations allowed by the origin volume. Do not modify this option unless instructed to do so by technical support.</td>
<td>50</td>
<td>7.3.1</td>
</tr>
<tr>
<td>flexscale.enable</td>
<td>Enables or disables FlexScale functionality. If your storage system does not have the Performance Accelerator Module, this option enables or disables Predictive Cache Statistics (PCS).</td>
<td>off</td>
<td>7.3</td>
</tr>
<tr>
<td>flexscale.lopri_blocks</td>
<td>Controls whether low-priority user data blocks are cached by FlexScale.</td>
<td>off</td>
<td>7.3</td>
</tr>
<tr>
<td>flexscale.normal_data_blocks</td>
<td>Controls whether normal user data blocks should be cached by FlexScale.</td>
<td>on</td>
<td>7.3</td>
</tr>
<tr>
<td>flexscale.pcs_high_res</td>
<td>Controls the sampling rate of the Predictive Cache Statistics (PCS).</td>
<td>off</td>
<td>7.3.2</td>
</tr>
<tr>
<td>flexscale.pcs_size</td>
<td>Controls the size of the cache emulated by PCS.</td>
<td>Automatically set by PCS based on the system memory.</td>
<td>7.3.2</td>
</tr>
<tr>
<td>fpolicy.multiple_pipes</td>
<td>Enables multiple open instances of the SMB named pipe on an FPolicy server.</td>
<td>on</td>
<td>7.3.2</td>
</tr>
<tr>
<td>ftpd.ipv6.enable</td>
<td>Enables or disables FTP over IPv6.</td>
<td>off</td>
<td>7.3.1</td>
</tr>
<tr>
<td>httpd.ipv6.enable</td>
<td>Enables or disables HTTP and HTTPS over IPv6.</td>
<td>off</td>
<td>7.3.1</td>
</tr>
<tr>
<td>interface.blocked.mgmt_data_traffic</td>
<td>Blocks or allows data traffic on the management interface, e0M.</td>
<td>off for systems upgraded from an earlier release; on for new systems</td>
<td>7.3.6</td>
</tr>
<tr>
<td>Option</td>
<td>Purpose</td>
<td>Default value</td>
<td>Release introduced</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>---------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>ip.v6.enable</td>
<td>Enables or disables IPv6 on the storage system.</td>
<td>off</td>
<td>7.3.1</td>
</tr>
<tr>
<td>ip.v6.ra_enable</td>
<td>Enables or disables the router-advertised address autoconfiguration for IPv6.</td>
<td>on</td>
<td>7.3.1</td>
</tr>
<tr>
<td>nfs.always.deny.truncate</td>
<td>Controls whether NFSv2 and NFSv3 clients can truncate files in UNIX qtrees that are also opened from a CIFS client with DENY write permissions.</td>
<td>on</td>
<td>7.3.6</td>
</tr>
<tr>
<td>nfs.ifc.rcv.low</td>
<td>Specifies the NFS TCP flow control low water mark. Data ONTAP stops flow control when the TCP packet data goes below this threshold.</td>
<td>33170</td>
<td>7.3.1</td>
</tr>
<tr>
<td>nfs.ifc.rcv.high</td>
<td>Specifies the NFS TCP flow control high water mark. Data ONTAP starts flow control when the TCP packet data goes above this threshold.</td>
<td>98910</td>
<td>7.3.1</td>
</tr>
<tr>
<td>nfs.ipv6.enable</td>
<td>Enables or disables NFS over IPv6.</td>
<td>off</td>
<td>7.3.1</td>
</tr>
<tr>
<td>nfs.max_num_aux_groups</td>
<td>Specifies the maximum number of auxiliary UNIX groups that a user can be a member of.</td>
<td>32</td>
<td>7.3.1</td>
</tr>
<tr>
<td>nfs.thin_prov.ejuke</td>
<td>Specifies whether the NFS server forces a client to retry a request by breaking the connection or by sending NFSERR_JUKEBOX (NFSv3) or NFS4ERR_DELAY (NFSv4). Does not affect NFSv2.</td>
<td>off</td>
<td>7.3.1</td>
</tr>
<tr>
<td>nfs.v3.snapshot.active.fsid.enable</td>
<td>Determines whether the FSID of objects in a snapshot matches the FSID of the active file system for NFSv3.</td>
<td>on</td>
<td>7.3.4</td>
</tr>
<tr>
<td>nfs.v4.snapshot.active.fsid.enable</td>
<td>Determines whether the FSID of objects in a snapshot matches the FSID of the active file system for NFSv4.</td>
<td>off</td>
<td>7.3.4</td>
</tr>
<tr>
<td>raid.disktype.enable</td>
<td>Enables certain disk types to be mixed with an aggregate.</td>
<td>off</td>
<td>7.3.1</td>
</tr>
<tr>
<td>Option</td>
<td>Purpose</td>
<td>Default value or example</td>
<td>Release introduced</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>--------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>replication.logical.reserved_transfers</td>
<td>Specifies the number of reserved transfers for SnapMirror volumes.</td>
<td>0</td>
<td>7.3</td>
</tr>
<tr>
<td>replication.volume.reserved_transfers</td>
<td>Specifies the number of reserved transfers for SnapMirror and SnapVault qtrees.</td>
<td>0</td>
<td>7.3</td>
</tr>
<tr>
<td>rlm.snmp.traps</td>
<td>Enables or disables the SNMP traps for only the RLM.</td>
<td>on</td>
<td>7.3</td>
</tr>
<tr>
<td>security.passwd.rootaccess.enable</td>
<td>Enables or disables root access to the storage system.</td>
<td>on</td>
<td>7.3</td>
</tr>
<tr>
<td>semi-sync</td>
<td>For semi-synchronous SnapMirror configurations, this option is used instead of the outstanding parameter and provides a recovery point objective of approximately 10 seconds.</td>
<td></td>
<td>7.3</td>
</tr>
<tr>
<td>sftp.dir_override</td>
<td>Sets the override path for the user’s home directory.</td>
<td>“” (null)</td>
<td>7.3.2</td>
</tr>
<tr>
<td>sftp.enable</td>
<td>Enables the SSH File Transfer Protocol (SFTP).</td>
<td>off</td>
<td>7.3.2</td>
</tr>
<tr>
<td>shelf.atfcx.auto.reset.enable</td>
<td>Enables automatic storage expansion unit power-cycling for AT-FCX shelves with the required power supply and storage expansion unit firmware version.</td>
<td>auto</td>
<td>7.3.1</td>
</tr>
<tr>
<td>shelf.esh4.auto.reset.enable</td>
<td>Enables automatic storage expansion unit power-cycling for ESH4 storage expansion unit with the required power supply and storage expansion unit firmware version.</td>
<td>off</td>
<td>7.3.1</td>
</tr>
<tr>
<td>snaplock.autocommit_period</td>
<td>Sets the autocommit time delay.</td>
<td>none</td>
<td>7.3.1</td>
</tr>
<tr>
<td>snaplock.compliance.write_verify</td>
<td>This option is used to verify all disk writes to SnapLock Compliance volumes. It is used when immediate verification of the recording process is required.</td>
<td>off</td>
<td>7.3.1</td>
</tr>
<tr>
<td>snaplock.log.default_retention</td>
<td>Specifies a default retention policy for a secure log file.</td>
<td>6m</td>
<td>7.3.1</td>
</tr>
<tr>
<td>Option</td>
<td>Purpose</td>
<td>Default value or example</td>
<td>Release introduced</td>
</tr>
<tr>
<td>--------</td>
<td>---------</td>
<td>--------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>snaplock.log.maximum_size</td>
<td>This option specifies the maximum size for a secure log before the file is closed and a new log file is generated for use by the secure logging infrastructure.</td>
<td>10m</td>
<td>7.3.1</td>
</tr>
<tr>
<td>snapvault.nbu.archival_snap_default</td>
<td>Sets the default value for the nbu_archival_snap_vol option on new volumes.</td>
<td>on</td>
<td>7.3.1</td>
</tr>
<tr>
<td>snapvault.ossv.compression</td>
<td>Enables or disables the compression feature globally for Open Systems SnapVault relationships.</td>
<td>off</td>
<td>7.3.1</td>
</tr>
<tr>
<td>snapvault.snapshot_for_dr_backup</td>
<td>Enables you to specify the Snapshot copy to use for updating the destination system when backing up a volume SnapMirror destination using SnapVault.</td>
<td>vsm_base_only</td>
<td>7.3.5</td>
</tr>
<tr>
<td>ssl.v2.enable</td>
<td>Enables or disables SSLv2.</td>
<td>on</td>
<td>7.3.4</td>
</tr>
<tr>
<td>ssl.v3.enable</td>
<td>Enables or disables SSLv3.</td>
<td>on</td>
<td>7.3.4</td>
</tr>
<tr>
<td>tls.enable</td>
<td>Enables the Transport Layer Security (TLS) protocol.</td>
<td>off</td>
<td>7.3.2</td>
</tr>
<tr>
<td>tftp.max_connections</td>
<td>Controls the maximum number of concurrent TFTP connections served by the storage system.</td>
<td>8</td>
<td>7.3.3</td>
</tr>
<tr>
<td>wif.failover.link_degraded</td>
<td>If set to on and one or more of the links off in the active multimode vif fails, a failover to a multimode vif that has a higher aggregate bandwidth will occur.</td>
<td>off</td>
<td>7.3.1</td>
</tr>
</tbody>
</table>
### Changed options in Data ONTAP 7.3

Options have been modified to improve network and storage resource management.

For each option, the following table gives this information:
- The change in the option
- The location of documentation about the option
- The Data ONTAP 7.3 release in which the change was introduced

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Change</th>
<th>Release introduced</th>
</tr>
</thead>
<tbody>
<tr>
<td>autosupport.mailhost</td>
<td>The default value for this option has been changed from an empty string to mailhost.</td>
<td>7.3.2</td>
</tr>
<tr>
<td>cifs.max_mpx</td>
<td>The default value for this option has been changed to 255.</td>
<td>7.3.4</td>
</tr>
<tr>
<td>flexscale.max_io_qdepth</td>
<td>This option has become obsolete.</td>
<td>7.3.2</td>
</tr>
<tr>
<td>ip.tcp.protocol.offload.enable</td>
<td>This option has become obsolete.</td>
<td>7.3.2</td>
</tr>
<tr>
<td>iscsi.max_connections_per_session</td>
<td>The value for use_system_default has been changed from 4 to 32.</td>
<td>7.3</td>
</tr>
<tr>
<td>nfs.ifc.rcv.high</td>
<td>Beginning with Data ONTAP 7.3.1.1L1, the value of this option is automatically adjusted when the value of the nfs.tcp.recvwindowsize option is changed.</td>
<td>7.3.1.1L1</td>
</tr>
<tr>
<td>nfs.ifc.rcv.low</td>
<td>Beginning with Data ONTAP 7.3.1.1L1, the default value for this option has increased.</td>
<td>7.3.1.1L1</td>
</tr>
<tr>
<td>nfs.v4.setattr_acl_preserve</td>
<td>Beginning in Data ONTAP 7.3.3, this option has been removed.</td>
<td>7.3.3</td>
</tr>
<tr>
<td>nlm.cleanup.timeout</td>
<td>The default value for this option has changed from 5 seconds to 100 milliseconds.</td>
<td>7.3.1</td>
</tr>
<tr>
<td>timed.max_skew</td>
<td>This option has been deprecated.</td>
<td>7.3.2</td>
</tr>
<tr>
<td>timed.proto</td>
<td>The rtc and the rdate parameters of this option have been deprecated.</td>
<td>7.3.2</td>
</tr>
<tr>
<td>timed.sched</td>
<td>This option has been deprecated.</td>
<td>7.3.2</td>
</tr>
<tr>
<td>Command</td>
<td>Change</td>
<td>Release introduced</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>timed.window</td>
<td>This option has been deprecated.</td>
<td>7.3.2</td>
</tr>
</tbody>
</table>
Replaced or removed commands in Data ONTAP 7.3

The `software install` command is deprecated in Data ONTAP 7.3.1 and will not be supported in future release families. Use the `software update` command instead to update from Data ONTAP 7.2 and later releases.

**Note:** If you are upgrading from a Data ONTAP 7.1.x release, you must use the `software install` command.
SnapMirror commands that become obsolete in Data ONTAP 8.0

Starting with Data ONTAP 8.0, the snapmirror store and snapmirror retrieve commands will no longer be available.

These commands are used to perform the following tasks:
- Copy a volume to local tape and continue the backup on subsequent tapes if necessary
- Restore a volume from local tape
- Initialize a SnapMirror destination from tape

In Data ONTAP 8.0, these commands will be replaced with the smtape backup and smtape restore commands. Documentation on the smtape backup and smtape restore commands will be available in the supported release.

Note: If you use scripts that have any of these commands, you must modify your scripts with the updated commands before running them in Data ONTAP 8.0.
Requirements for running Data ONTAP 7.3.6

You can use this information to verify the storage systems and firmware needed to run Data ONTAP 7.3.6 and, in particular, to use it to create active/active configurations (formerly known as clusters).

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 7.3.5.

The following models of storage systems are supported:

- N3300, N3400 and N3600 storage systems
- N3700
- N5000 series systems
- N6000 series systems
- N6200 series systems
- N7000 series systems

Note: All of the storage systems listed above can be configured in active/active pairs.

Maximum total capacity supported

For information about each storage system model's capacity and maximum volume size, see the IBM System Storage N series Introduction and Planning Guide.
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 drive
- disk storage expansion unit and ESH

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 2.

Note: The latest system firmware is included with Data ONTAP upgrade packages. For more information, see the Data ONTAP Upgrade 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 2.

Note: New disk firmware is sometimes included with Data ONTAP upgrade packages. For more information, see the Data ONTAP Upgrade Guide.

Storage expansion unit firmware

For information about the latest 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 2.
**Storage systems that support Multipath Storage**

To configure Multipath Storage, which provides redundancy for the path from each controller to every storage expansion unit in the configuration and is the preferred cabling method, you need to have a supported storage system, storage expansion units and modules.

Multipath Storage is supported on the following N series storage systems and storage expansion units:
- All N series systems except the N3700 storage systems

**Note:** While Multipath adds value to a stretch MetroCluster environment, it is not necessary in a fabric-attached MetroCluster configuration because multiple paths already exist.

The only gateway systems that support native storage expansion units are N7000, N6200, N6000 and N5000 series gateways. Therefore, they are the only gateway models for which Multipath Storage applies on gateway systems. On each node in an active/active configuration of gateway systems using native storage expansion units, you must configure the `fc-non-array-adapter list` environment variable for the first storage expansion unit on a new loop to the gateway system.

**Note:** Setting the `fc-non-array-adapter list` environment variable is not required on gateway systems configured with EXN3000 or EXN3500 storage expansion units.
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 2 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.

Requirements for gateway fabric-attached MetroCluster configurations

Gateway fabric-attached configurations require in-order delivery of FC-VI traffic.

If the FC-VI traffic is not delivered in order, there are problems with cluster takeover. For example, each node might be up and running but the results of the cf status command might show cluster takeover disabled or might be cycling cluster takeover disabled and cluster takeover enabled.

See the Gateway MetroCluster Guide for information about the circumstances when you need to configure switches, hardware, or both to support in-order delivery of FC-VI traffic.
Important cautions

Before deploying 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” on page 113
- “Manageability cautions” on page 112
- “Network protocol cautions” on page 121
- “Block access protocol cautions” on page 122
- “Data protection cautions” on page 125
- “Storage management cautions” on page 131
Manageability cautions

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

- "Issues in certificate MD5 signature collision vulnerability"

Issues in certificate MD5 signature collision vulnerability

To enhance security, starting with Data ONTAP 7.3.5, Data ONTAP uses the SHA256 mensagemdigest algorithm to generate digital certificates (including CSRs and root certificates) on the storage system.

Data ONTAP 7.3.4 and earlier releases use the MD5 mensagem-digest algorithm to generate 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 certificate signing requests (CSRs) further signed by a certificate authority (CA) using SHA256 or SHA1.
Upgrade and revert cautions

If you are upgrading to Data ONTAP 7.3 or reverting from 7.3 to an earlier release, you should review these issues, and if any apply in your environment, take appropriate action.

For more information about these cautions, see the Data ONTAP Upgrade Guide.

- “New FlexVol volume space requirements when upgrading from a release earlier than Data ONTAP 7.3”
- “If you are upgrading a system that includes FlexCache volumes” on page 116
- “If you have been using the flex_cache license” on page 117
- “If you are performing a nondisruptive upgrade on a system with VMware ESX Server hosts” on page 115
- “If you are upgrading an N6000 or N6200 series storage system in an iSCSI environment” on page 114
- “If you are upgrading an N5500 storage system” on page 116
- “If you are upgrading an N3300 system running Data ONTAP 7.2.2L1” on page 117
- “New RLM firmware and its upgrade requirements” on page 115
- “BMC firmware upgrades for N3300, N3400 or N3600 storage systems” on page 117
- “If you are using SharedStorage” on page 117
- “If you are upgrading to a 4 Gb HBA in a SAN environment” on page 118
- “If you are upgrading from a 2 Gb onboard port to a 4 Gb adapter in a SAN environment” on page 118
- “Requirements for reverting to a Data ONTAP release with a lower maximum capacity” on page 119
- “If you are reverting to a previous release and you use large ACLs under NFSv4” on page 119
- “If you revert a system that has an FC 1062 or FC 1065 Ethernet card installed” on page 120

New FlexVol volume space requirements when upgrading from a release earlier than Data ONTAP 7.3

Upgrading to Data ONTAP 7.3 or later from an earlier release will cause existing FlexVol volumes to require more free space from their containing aggregate.

Data ONTAP 7.3 includes an improvement to free space accounting. As a result, existing FlexVol volumes reserve additional space, resulting in a loss of 0.5% of free space.
**Attention:** You should ensure that all systems upgrading to Data ONTAP 7.3 have at most 96 percent used space in their aggregates. If there is insufficient free space in an aggregate to satisfy the increased requirement from its FlexVol volumes, the space guarantee for one or more volumes in that aggregate could be disabled.

For more information, see the *Data ONTAP Upgrade Guide*.

### Determining system capacity and space guarantees

If you suspect that your system has almost used all of its free space, or if you use thin provisioning, you should check the amount of space in use by each aggregate. If any aggregate is 97 percent full or more, do not proceed with the upgrade and follow the steps below.

1. Check your system's capacity by entering the following command:
   ```
   df -A
   ```

   **If the capacity field shows...** | **Then...**
   --- | ---
   96% or less for all aggregates | You can proceed with your upgrade to Data ONTAP 7.3; no further action is required.
   97% or more for any aggregate | Continue to plan your upgrade with the `aggrSpaceCheck` tool listed in Step 2.

2. Download the Aggregate Space Checker (`aggrSpaceCheck`) from the IBM N series support website, which is accessed and navigated as described in “Websites” on page 2.

   After downloading the Aggregate Space Checker, use the tool's Reference Guide to install and use it to assess the free space requirements for your system in Data ONTAP 7.3 and later releases. If you do not have sufficient free space, the tool will recommend a course of action to ensure a successful upgrade.

After using this tool and completing the upgrade, make sure that your space guarantees are configured according to your requirements.

**If you are upgrading an N6000 or N6200 series storage system in an iSCSI environment**

If you are running iSCSI traffic on your N6000 series storage system and you are upgrading from Data ONTAP version 7.3 or earlier to version 7.3.5, you will no longer be able to run iSCSI traffic on the e0M interface.

In addition, if you revert from Data ONTAP version 7.3.5, the e0M interface remains disabled for iSCSI traffic by default as follows:
- Target portal group configuration related to e0M may change.
- e0M interface may be removed from the iSCSI access list configuration.
• c0M interface is disabled for iSCSI traffic.

**New RLM firmware and its upgrade requirements**

RLM firmware versions 4.0 and later require a different layout on flash media. You must ensure that you are running the latest 3.1.x RLM firmware to enable the transition to the new layout, then update to the 4.0 or later firmware.

You must be running the latest 3.1.x to update to 4.0. If you are running a firmware version earlier than 3.1, you must first perform an intermediate update to the latest 3.1.x firmware, then update from 3.1 to 4.0 in a separate operation.

**Attention:** Regardless of whether you update RLM firmware from the Data ONTAP CLI or the RLM CLI, do not update directly from a firmware version earlier than 3.1 to 4.0 or later. Doing so will corrupt the RLM flash device.

If you are updating to version 4.0 or later from the Data ONTAP CLI, you must run the `rlm update` command with the `-f` advanced option. Further updates do not require the advanced option.

If you are updating RLM firmware from the RLM CLI, you can use the normal procedure.

**Note:** Beginning with Data ONTAP 7.3.3, the RLM supports IPv6. To send RLM traffic over IPv6, you must be running RLM version 4.0 and IPv6 must be enabled on the storage system.

If you do not plan to send RLM traffic over IPv6 on Data ONTAP 7.3 releases, it is not required to update RLM firmware to 4.0 or later. However, firmware version 4.0 includes other enhancements, and it is a best practice to be running the latest firmware on your RLM.

For information about installing and updating the RLM firmware, see the *Data ONTAP Upgrade Guide*.

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

**If you are performing a nondisruptive upgrade on a system with VMware ESX Server hosts**

Before performing a nondisruptive upgrade on storage systems exporting data over NFS to VMware ESX Server hosts, you should verify that your clients’ NAS components are correctly configured. This verification will help ensure that VMware guest operating systems do not experience service disruption during the upgrade.
In particular, the following parameters should be set correctly:

- NFS Heartbeat parameters on the ESX Server
- Timeout values for SCSI disks on guest operating systems

It is also highly recommended that the file systems using virtual machine disk format (VMDK) on Windows be correctly aligned with the storage systems' WAFL file system.

For more information about verifying and updating these configurations, see the Data ONTAP Upgrade Guide.

**If you are upgrading a system that includes FlexCache volumes**

Before upgrading a system that includes FlexCache volumes, verify that the `convert_ucode` volume option is set to `off` for all FlexCache volumes. Failure to turn the `convert_ucode` volume option off before upgrading could cause a system panic.

**If you are upgrading an N5500 storage system**

As of Data ONTAP 7.3.3, the threshold limits for the NVRAM5 battery sensor have changed for the N5500 storage systems. Before initiating an upgrade to Data ONTAP 7.3.3 or later, you must ensure that the NVRAM5 battery sensor reading for your N5500 storage system is within the new threshold limits.

The following are the new threshold limits for the N5500 storage system NVRAM5 battery sensor:

- Critical low: 3649 mV
- Warning low: 3849 mV
- Warning high: 4250 mV
- Critical high: 4250 mV

If the current NVRAM5 battery sensor reading is not between 3849 mV (warning low) and 4250 mV (warning high), the system will fail to boot the new image during the nondisruptive upgrade to Data ONTAP 7.3.3 or later.

1. To display the current sensor state, reading, and threshold limits for all sensors, including the sensor information for the NVRAM5 battery, enter the following command:

   `environment head list-sensors`

   **Example**

   The following example shows the NVRAM5 battery sensor output from an N5500 system:
Note: The NVRAM5 battery sensor state might show normal even if the reading does not conform to the new threshold limits.

2. If the current reading of the NVRAM5 battery sensor is not between 3849 mV (warning low) and 4250 mV (warning high), perform one of the following steps:
   - If the current NVRAM5 battery reading is lower than 3849 mV, allow the charge on the battery to reach full voltage before proceeding with the upgrade.
   - If the battery is faulty, replace the battery before proceeding with the upgrade.

If you have been using the flex_cache license
You should install the flexcache_nfs license before upgrading to Data ONTAP 7.3 and later releases. If you do not install the flexcache_nfs, your FlexCache volumes will not work until you install the license.

If you are using SharedStorage
The SharedStorage functionality is not available in Data ONTAP 7.2 and later releases. If you are using SharedStorage in an earlier Data ONTAP release and you want to continue using it, do not upgrade to Data ONTAP 7.2 or later.

If you need to upgrade to Data ONTAP 7.2 or later and you must continue to use SharedStorage, please contact IBM technical support.

If you are upgrading an N3300 system running Data ONTAP 7.2.2L1
If you configured aggregates larger than 8 TB on an N3300 storage system running Data ONTAP 7.2.2L1, you cannot use the nondisruptive method to upgrade to any later release; you must use the standard upgrade method.

For more information about N3300 storage systems' storage capacity, see the IBM System Storage N series Introduction and Planning Guide.

BMC firmware upgrades for N3300, N3400 or N3600 storage systems
This Data ONTAP release includes new firmware for the Baseboard Management Controller (BMC). If you have not already installed BMC version 1.2, you should install the new BMC firmware immediately after upgrading.

For information about updating the BMC firmware, see the Data ONTAP Upgrade Guide.
If you are upgrading to a 4 Gb HBA in a SAN environment

If you attempt to run a N5000, N6000 or N7000 series system with a 4 Gb HBA in an unsupported cfmode, the 4 Gb HBA is set to offline and an error message is displayed.

You must change the cfmode to `single_image` or `standby` cfmode before upgrading. Only `single_image` and `standby` cfmodes are supported with the new 4 Gb Fibre Channel host bus adapters (HBAs) on N5000, N6000 and N7000 series storage systems.

In addition, Data ONTAP does not allow changing from a supported cfmode to an unsupported cfmode with the 4 Gb HBA installed on these systems.

If you are upgrading from a 2 Gb onboard port to a 4 Gb adapter in a SAN environment

If you have an N5000, N6000 or N7000 series system in a SAN environment and you are upgrading from a 2 Gb onboard port to a 4 Gb adapter, you must stop the FCP service and reconfigure the onboard port before installing the 4 Gb adapter. Failure to do so might result in a storage system panic and lost data.

**Note:** When you upgrade from the onboard ports to the 4 Gb HBAs, the World Wide Port Names (WWPNs) will change, which requires that you reconfigure any UNIX hosts with the newly assigned WWPNs.

You must reconfigure the 2-Gb onboard port before installing a 4-Gb adapter.

1. Stop the FCP service by entering the following command:
   ```
   fcp stop
   ```
   The FCP service is stopped and all target adapters are taken offline.

2. Set the onboard FC ports to unconfigured:
   ```
   fcadmin config -t unconfig <ports>
   ```
   **Example:**
   ```
   fcadmin config -t unconfig 0b 0d
   ```
   The onboard FC ports are unconfigured.

3. Ensure the cfmode is set to `single_image` or `standby`.
4. Shut down the storage system.
5. Install the 4 Gb adapter according to the instructions provided with the adapter.
6. Power on the storage system.
Requirements for reverting to a Data ONTAP release with a lower maximum capacity

When you revert to an earlier Data ONTAP release, your storage system must conform to the maximum capacity limitations of the earlier release. If you upgraded your system to a release that supports greater capacities and you configured storage to utilize the new capacities, you must reconfigure your system to the lower capacity limits before you revert. If you don't reconfigure in this way, the storage system will not boot up following the revert process until the excess capacity has been disconnected.

To access any storage in excess of system limits, you must disconnect it from the system you are reverting. Excess capacity must be disconnected for relocation to a different storage system in a way that allows aggregates to remain intact.

The system to which storage is relocated must meet the following requirements:

- It has spare capacity room to accommodate the relocated storage.
- It is running the same or a later Data ONTAP release as the system where the disks are currently installed.
- It is running a Data ONTAP release that supports the relocated disks.

For more information about physically moving aggregates, see the *Data ONTAP Storage Management Guide*.

For more information about maximum capacity limits for a given Data ONTAP release, see *IBM System Storage N series Introduction and Planning Guide*.

If you are reverting to a previous release and you use large ACLs under NFSv4

If you are running NFSv4 and use large ACLs, you can run the *pre_revert_acl* script to replace the large ACLs so that Data ONTAP does not replace them with a default ACL during the reversion.

In Data ONTAP 7.3 and later, you can have more than 192 ACEs per ACL in NFSv4. However, in releases earlier than Data ONTAP 7.3, the maximum number of ACEs was 192. Therefore, when you revert Data ONTAP 7.3 and later to a release earlier than Data ONTAP 7.3, Data ONTAP automatically replaces large ACLs (those with more than 192 ACEs) with a default ACL. To mitigate any concerns associated with the setting of this default ACL, IBM provides a Perl script called *pre_revert_acl*.

Before doing the revert, you should run the *pre_revert_acl* script from an NFS client with root permissions over all the exports of the storage system (or
This script works by mounting each export of the storage system, iterating over all the directories and files under that export, and listing the files that have large ACLs (ACLs with more than 192 ACEs). Optionally, the script can also replace the large ACL on each file with an ACL that you provide.

If you are not running NFSv4 on your system, you can ignore the ACL-related message displayed at the time of revert.

**If you revert a system that has an FC 1062 or FC 1065 Ethernet card installed**

Data ONTAP 7.3.2 and later releases support FC 1062 and FC 1065 10-Gigabit Ethernet cards. You must remove these cards before reverting to a previous release.
Network protocol cautions

If you use FilerView to manage network interfaces or if your network configuration includes a vif, you should review these issues and take appropriate action before upgrading.

For more information about these issues, see the Data ONTAP Network Management Guide.

- "If you use a vif that is named "vip"
- "If your system uses ATM for network connectivity"

If you use a vif that is named "vip"

Beginning in Data ONTAP 7.2, the string "vip" is reserved for private virtual interfaces. If you have configured a vif (a feature that implements link aggregation) named "vip" on your storage system in an earlier release, you must rename that vif if you want upgrade your system to Data ONTAP 7.2.1 or later.

If you keep "vip" as the name of a vif and you upgrade to Data ONTAP 7.2.1 or later, the interface status of the vif named "vip" will be set to down and the interface will be unavailable for network traffic.

For more information about creating a vif or renaming a vif, see the Data ONTAP Upgrade Guide Network Management Guide.

Renaming a vif

You can use the vif command to correct the interface name before upgrading to Data ONTAP 7.2.1 or later.
1. Bring down the vif by entering the following command:
   `ifconfig vip down`
2. Destroy the vif by entering the following command:
   `vif destroy vip`
3. Recreate the vif and give it a different unique name, entering the following command:
   `vif create new_vif_name`

If your system uses ATM for network connectivity

ATM is no longer supported in Data ONTAP 7.3 and later releases. If your system uses ATM for network connectivity, do not upgrade to Data ONTAP 7.3 or later.
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 Block Access Management Guide for iSCSI and FC.

- “Identical WWPNs can occur on both nodes in a cluster”
- “If jumpers J3 and J4 on 2 Gbps Fibre Channel target expansion are in positions 2 and 3”
- “If you use Solaris 10 and the Emulex Fibre Channel Adapter driver” on page 123
- “If an iSCSI target HBA fails” on page 123
- “If you use the automatic sizing feature on thinly provisioned LUNs when snap reserve is set to a non-zero value” on page 123

Identical WWPNs can occur on both nodes in a cluster

If a system and its disks are disconnected from its partner and then connected to a different partner, it is possible (though rare) that both systems can end up with the same WWPN. This problem exists only with systems in single_image cfmode.

If this situation occurs, the systems can behave as if they are both primary systems or both secondary systems, causing each system to compute identical WWPNs for its target ports. As a result, hosts will experience problems trying to access these duplicate ports in the fabric.

If you deploy ALUA on storage systems with FCP or iSCSI

If you deploy the T10 Asymmetric Logical Unit Access (ALUA) standard for SCSI on Fibre Channel or iSCSI enabled storage systems, ensure your host supports ALUA before enabling it. Enabling ALUA for a host that does not support ALUA can cause host failures during controller failover.

If jumpers J3 and J4 on 2 Gbps Fibre Channel target expansion are in positions 2 and 3

When Data ONTAP panics because it has entered an illegal state, all Fibre Channel target expansion adapters shut down. However, the lasers on the 2 Gbps target expansion adapters (model FC 1019) will sometimes remain on. This situation can cause the host to mistakenly perceive that the storage system is still running.

The workaround for this problem is to change the position of jumpers J3 and J4 on the adapter from positions 2 and 3 to positions 1 and 2, respectively.
If you use Solaris 10 and the Emulex Fibre Channel Adapter driver

If you are using Solaris 10 and the Emulex Fibre Channel Adapter driver, you need to upgrade to the 2.30j version driver or later before you upgrade to Data ONTAP 7.3 or later.

For more information, see the Sun solution 231581 "Completing the SCSI Command When There is a Data Underrun Error Condition May Result in Data Integrity Issues" located at:

sunsolve.sun.com/search/document.do?assetkey=1-66-231581-1

If an iSCSI target HBA fails

If your iSCSI target HBA fails, the iSCSI initiators connected to this HBA might time out, prompting the following error message on the storage system:
iSNAP.fw.Crashed.

The timeout on the iSCSI initiators might be caused by HBA firmware defects, hardware failure, or device driver defects.

Note: If MPIO is configured on the hosts, I/O should be re-routed as expected, preventing any disruption in service.

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 where a configuration requires snap reserve to be set 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.

Considerations

Using the automatic sizing feature is required because the space from deleted snapshots can only be used to fulfill snapshot space requests. Furthermore, autodelete will not begin until the snap reserve is exceeded.

Example

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 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 Data Protection Online Backup and Recovery Guide.

- “SnapLock Compliance volume upgrade requirement”
- “Issues in SnapLock interaction with active/active configuration”
- “Issues in moving SnapLock disks” on page 126
- “Issues in booting a system running Data ONTAP 7.3.1 with the first release of Data ONTAP 7.3” on page 126
- “Issues in upgrading to Data ONTAP 7.3 if you have SnapLock volumes” on page 126
- “If you upgrade systems running FPolicy” on page 127
- “Issues in reverting to Data ONTAP 7.3 if you have SnapLock volumes” on page 127
- “If you are reverting to a previous release that does not support deduplication with SnapLock volumes” on page 127
- “If you use SnapLock Compliance and FlexClone copies” on page 128
- “Limitation of SnapLock for SnapVault relationship” on page 128
- “If you use DataFabric Manager to manage SnapMirror or SnapVault relationships between vFiler units” on page 128
- “If you revert to a prior release, for a SnapMirror destination with volumes using deduplication or clone operations” on page 129
- “If you are reverting to a previous release and you use deduplication” on page 130

SnapLock Compliance volume upgrade requirement

If your storage system is running Data ONTAP 7.3.1 or later versions of Data ONTAP 7.3 and you have SnapLock Compliance volumes, you must upgrade the storage system to Data ONTAP 7.3.5.

Issues in SnapLock interaction with active/active configuration

SnapLock volumes cannot be created in an active/active configuration if one node is running on the first release of Data ONTAP 7.3 and the other node is running on Data ONTAP 7.3.1. This is because the first release of Data ONTAP 7.3 does not support SnapLock.

For more information, see Data ONTAP Archive and Compliance Management Guide.
Issues in moving SnapLock disks

If SnapLock disks are moved to a storage system that is running the first release of Data ONTAP 7.3, the system will halt. This happens because SnapLock is not supported in the first release of Data ONTAP 7.3.

However, if you move the SnapLock disks to a storage system that is running Data ONTAP 7.3.1, the system continues to be operational. If the SnapLock disks are recognized by the Data ONTAP 7.3.1 storage system, the storage system will bring the disks online.

Issues in booting a system running Data ONTAP 7.3.1 with the first release of Data ONTAP 7.3

If your storage system is running Data ONTAP 7.3.1 with SnapLock volumes and you attempt to boot the system with the first release of Data ONTAP 7.3, the system will halt. This happens because SnapLock is not supported in the first release of Data ONTAP 7.3.

To recover from such a halt, perform one of the following steps:

- Reboot the system in Data ONTAP 7.3.1.
- Remove the SnapLock disks from the system and continue to boot using the first release of Data ONTAP 7.3. You should immediately attach the removed SnapLock disks to a Data ONTAP system that supports SnapLock.

Issues in upgrading to Data ONTAP 7.3 if you have SnapLock volumes

If you have SnapLock volumes in your storage system and you upgrade from an earlier release family (such as a Data ONTAP 7.2 release) to the Data ONTAP 7.3 release family by booting the system with the first release of Data ONTAP 7.3, the system will halt. The halt will occur in the very early boot phase (much before any on-disk structure is updated). This happens because SnapLock is not supported in the first release of Data ONTAP 7.3.

To recover from this halt, perform one of the following steps:

- Reboot the system in the previous release which supported SnapLock. (For example, if you are upgrading from Data ONTAP 7.2.5.1, boot the system with Data ONTAP 7.2.5.1.)
- Remove the SnapLock disks from the system and continue to boot with the first release of Data ONTAP 7.3.

Note: You should immediately attach the removed SnapLock disks to a Data ONTAP system that supports SnapLock.

However, if you upgrade from an earlier release that supports SnapLock to Data ONTAP 7.3.1, which also supports SnapLock, the bootup and upgrade process will proceed normally and the system will be fully operational.
If you upgrade systems running FPolicy

If your system includes directories created or modified with NFS and you've configured FPolicy to scan files in these directories, FPolicy functionality might not be available during all or part of the upgrade process.

When you upgrade to Data ONTAP 7.2, Inode To Pathname (I2P) information is reinitialized on each existing volume on your system. FPolicy file screening will not take place in these directories until the I2P initialization process is completed.

For more information about I2P reinitialization, see the Data ONTAP Upgrade Guide.

Issues in reverting to Data ONTAP 7.3 if you have SnapLock volumes

SnapLock is not supported in the first release of Data ONTAP 7.3. Therefore, when reverting a storage system that contains SnapLock volumes to Data ONTAP 7.3 release family, you need to be aware of certain issues.

You can successfully revert to any release in the Data ONTAP 7.3 family even if your system contains SnapLock volumes. However, if you boot such a system with the first release of Data ONTAP 7.3, the system will halt. The list of SnapLock disks causing the system to halt will be listed on the console.

To recover from such a halt, perform one of the following steps:

• Reboot the system using a Data ONTAP release that supports SnapLock.
• Remove the SnapLock disks from the storage system. You will then be able to boot up using the first release of Data ONTAP 7.3.

Note: You should immediately attach the removed SnapLock disks to a Data ONTAP system that supports SnapLock.

If you boot a storage system containing SnapLock volumes in Data ONTAP 7.3.1, the system will boot up normally and continue to be operational.

If you are reverting to a previous release that does not support deduplication with SnapLock volumes

Beginning with Data ONTAP 7.3.1, deduplication is supported on SnapLock volumes.

However, if deduplication is enabled on a SnapLock volume and you attempt to revert to a Data ONTAP release that does not support deduplication on SnapLock volumes, you will see the following error message:

Volume "volname" cannot be reverted because SIS has been enabled on it. You must undo SIS on this volume before continuing with the revert.
To avoid or recover from this situation, contact technical support.

**If you use SnapLock Compliance and FlexClone copies**

You should avoid making a FlexClone copy when using SnapLock Compliance.

A FlexClone copy is a writable point-in-time image of a FlexVol volume or another FlexClone copy. A FlexClone copy allows users to make duplicate copies of data without risk of modifying the original copy or using additional storage for the duplicate copy.

There are two reasons for not making FlexClone copies when using SnapLock Compliance:

- The new clone cannot be deleted until the retention periods of all files contained in the original SnapLock Compliance FlexVol volume have expired. While there is no additional storage penalty involved with the cloning of a SnapLock Compliance FlexVol volume, it does count against the maximum number of traditional and flexible volumes available on the system until the retention dates for all files in the parent FlexVol volume expire and the parent volume can be deleted.

- The clone results in a second copy of compliance data that the archival application does not know exists. When the original file reaches the expiration of its retention date, the archival application will delete the copy it knows about on the parent SnapLock Compliance FlexVol volume, but not the copy contained in the clone. The result is an unwanted duplicate copy.

**Limitation of SnapLock for SnapVault relationship**

Beginning with Data ONTAP 7.3.1, you cannot have a SnapLock for SnapVault relationship between the SnapLock Compliance source and SnapLock Compliance destination volumes.

If you upgrade the storage system to Data ONTAP 7.3.1 or later, you must ensure that the destination for SnapLock for SnapVault relationship is not a SnapLock Compliance volume. If the destination volume is a SnapLock Compliance volume, the SnapVault update fails.

For more information, see *Data ONTAP Archive and Compliance Management Guide*.

**If you use DataFabric Manager to manage SnapMirror or SnapVault relationships between vFiler units**

For Data ONTAP 7.2 and later, SnapMirror and SnapVault relationships can be created using vFiler units. However, DataFabric Manager 3.4 and earlier releases cannot use vFiler units for managing SnapMirror and SnapVault relationships.
As a result, you might encounter the following issues:

- If the `snapvault.access` and `snapmirror.access` options on the source system allow access only to the destination vFiler unit, then the relationship creation, scheduled backups, on-demand backups, SnapMirror updates, and SnapMirror resync processes from DataFabric Manager fail, and you receive an error message: request denied by source filer, check access permissions on source.
  
  **Workaround:** To allow access to the destination hosting storage system, set the `snapmirror.access` and `snapvault.access` options on the source system.

- If the `ndmpd.preferred_interfaces` option is not specified on the source hosting system, then the backups from DataFabric Manager might not use the correct network interface.
  
  **Workaround:** Enable the `ndmpd.preferred_interfaces` option on the source hosting system.

- The backups and SnapMirror updates from DataFabric Manager fail and you receive the error message source unknown. This occurs when both of these conditions are met:
  
  - A relationship between two vFiler units is imported into DataFabric Manager by auto-discovery or is added manually.
  
  - The destination hosting system is not able to contact the source vFiler IP address.

  **Workaround:** Ensure that the host name or IP address of the source system that is used to create relationships can be reached from the destination hosting system.

**If you revert to a prior release, for a SnapMirror destination with volumes using deduplication or clone operations**

For systems in a SnapMirror relationship, the destination storage system should use a Data ONTAP release identical to or later than that used by the source.

In releases prior to Data ONTAP 7.3.1, when replicating volumes with deduplication, the nearline personality license was required on the destination storage system. However, for Data ONTAP 7.3.1 it is not essential to enable the nearline personality license on the destination for replicating such volumes. Therefore, if you revert from Data ONTAP 7.3.1 to a prior release, ensure that the nearline personality license is enabled on the destination storage system. Otherwise, after the revert operation, volume SnapMirror updates will fail for any volumes on the source that use deduplication.

**Note:** When using SnapMirror to replicate volumes that use deduplication or clone operations, the destination storage system should support deduplication.
For more information about the nearline personality license and the storage systems that support deduplication, see the Data ONTAP Data Protection Online Backup and Recovery Guide.

**If you are reverting to a previous release and you use deduplication**

In Data ONTAP 7.3 and later, the deduplication metadata for a volume is located outside the volume, in the aggregate. Therefore, when you revert from Data ONTAP 7.3 to a previous release that supports deduplication, the deduplication metadata is lost during the revert process.

The existing data in the volume will retain the space savings from the deduplication operations performed earlier. However, the new data written to the volume after the revert process will obtain space savings through deduplication within the new data only, and not from the data that existed before the revert process.

To use deduplication for all the data within the volume, and thus obtain higher space savings, use the `sis start -s` command. This command rebuilds the deduplication metadata for all the data in the volume. This process can take several days, depending on the size of the logical data in the volume.

**Attention:** Before using the `sis start -s` command, ensure that the volume has sufficient free space to accommodate the addition of the deduplication metadata. The deduplication metadata uses about 1-3 percent of the logical data size in the volume.
Storage management cautions

If you are migrating data to a new system or configuring FlexVol volumes, you might need to familiarize yourself with these storage management issues.

For more information about these issues, see the Data ONTAP Storage Management Guide.

- "If you are replacing traditional volumes with FlexVol volumes"
- "If you see unexpected warnings and messages regarding FlexVol volumes"

If you are replacing traditional volumes with FlexVol volumes

FlexVol volumes have different best practices, optimal configurations, and performance characteristics from those of traditional volumes. Make sure you understand these differences by referring to the FlexVol volume documentation, and deploy the configuration that is optimal for your environment.

For detailed information about configuring flexible volumes and aggregates, see the Data ONTAP Storage Management Guide.

If you see unexpected warnings and messages regarding FlexVol volumes

If an aggregate is unexpectedly taken offline because of a hardware failure, for example if you have an aggregate on a loop and the loop fails, you might see unexpected warnings and messages. Data ONTAP assigns a unique file system identifier (FSID) to every flexible volume on a system. Data ONTAP cannot check the FSIDs of offline flexible volumes. Data ONTAP does detect the possibility of FSID conflict and issues warnings and messages alerting you to the possibility of duplicate FSID creation.

During the time the aggregate is offline you may see warnings and messages during operations such as these:

- Creating a new flexible volume, including by cloning
  In this case, you will see a warning. You can override the warning, but if you do, you might see additional problems. If possible, do not create new FlexVol volumes until after you bring the offline aggregate back on line.

- Bringing a flexible volume online
  Before the flexible volume is brought online, Data ONTAP checks the FSID. If there is a duplicate FSID, you see the following message:
  `vol online: FSID marked invalid because it already exists. Unable to bring volume 'volname' online`
  The volume does not come online. You cannot override this warning.

- Accessing of a volume by a vFiler unit
You might see a message from the vFiler unit about a volume being in an unexpected state. The volume reported might not be an offline volume. NFS clients will not be able to access the reported vFiler volume.

You can fix this problem by first taking the volume offline using the following command:

```
vol offline volname
```

Then bring the volume back online using the following command:

```
vol online volname
```
Known problems and limitations

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

- “Manageability issues” on page 134
- “File access protocol issues” on page 136
- “Network protocol issues” on page 143
- “Block access protocol issues” on page 146
- “Data protection issues” on page 149
- “Storage resource management issues” on page 156
- “Third-party storage issues” on page 160
- “Active/active configuration issues” on page 161
Manageability issues

You might have to familiarize yourself with some issues related to manageability in this release.

- “Issues with exportfs commands in non-interactive SSH sessions”
- “vFiler DR configuration with the snapmirror.checkip.enable option on fails, if SnapMirror fails to authenticate destination IPv6 address”
- “No IPv6 support for AutoSupport e-mail notifications” on page 135
- “AutoSupport option settings” on page 135
- “Change in sysstat -x command output” on page 135
- “RLM configuration is not saved if the RLM’s Ethernet cable is not connected” on page 135

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`

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 Data Protection Online Backup and Recovery Guide.

No IPv6 support for AutoSupport e-mail notifications

IBM does not provide a global unicast IPv6 address for AutoSupport e-mail notifications to be sent from the storage system to technical support. Therefore, a dual IPv4/IPv6 configuration mode is required for storage systems that use Autosupport.

AutoSupport option settings

In Data ONTAP 7.3.2, two AutoSupport options of the option command cannot be enabled, and two others cannot be disabled.

The autosupport.local.nht_data.enable and autosupport.local.performance_data.enable options cannot be enabled. The autosupport.local.nht_data.enable option should send an AutoSupport message containing health test disk data to the "autosupport.to" list. The autosupport.local.performance_data.enable option should send the weekly performance AutoSupport message to the "autosupport.to" list.

The autosupport.nht_data.enable and autosupport.performance_data.enable options cannot be disabled. The autosupport.nht_data.enable option sends an AutoSupport message containing health test disk data to technical support. The autosupport.performance_data.enable option sends weekly performance AutoSupport messages to technical support.

Change in sysstat -x command output

In Data ONTAP 7.1 and later releases, the DAFS column is no longer displayed in the sysstat -x command output.

Note that any scripts that currently depend on sysstat -x command output might need to be revised.

RLM configuration is not saved if the RLM's Ethernet cable is not connected

If the RLM's Ethernet cable is not connected when you use the rlm setup command to configure the RLM, after connecting the cable you must rerun rlm setup.
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 File Access and Protocols Management Guide.

- “Order of steps when enabling SSL for LDAP traffic”
- “FPolicy quota and user reports show incorrect file size” on page 137
- “Failed CIFS connections due to signature mismatch” on page 137
- “Configuring user mapping for a default user quota with CIFS not enabled could severely degrade performance” on page 137
- “Configuring user mapping for a default user quota with CIFS not enabled could severely degrade performance” on page 137
- “Excessive pending CIFS authentication requests can cause service disruption” on page 138
- “Empty CIFS/SMB2.x change notifications” on page 138
- “Correction to required FPolicy screening requests” on page 139
- “FPolicy file extension issue on revert” on page 139
- “FPolicy compatibility issue in NFSv4 environments” on page 139
- “Limitations in the naming of FPolicy policies” on page 140
- “Some Group Policy Objects (GPOs) are applied differently on storage systems than on Windows systems” on page 140
- “Client notification messages in Windows domains require NetBIOS” on page 140
- “Unsupported Windows features in the file serving environment” on page 140
- “Configuration issue for clients that mount NFS shares using a non-reserved port” on page 141
- “NFSv4 client compatibility” on page 141
- “Unicode character 0x0080 is not supported” on page 141
- “The FTP server does not support Unicode characters” on page 141
- “No IPv6 support in FPolicy” on page 142

Order of steps when enabling SSL for LDAP traffic

Before you enable SSL for LDAP by setting the `ldap.ssl.enable` option to on, you must first install a root certificate. If you install the root certificate after enabling this option, you must disable and reenable this option for the storage system to read the certificate.
FPolicy quota and user reports show incorrect file size

The file size information displayed in FPolicy quota and user reports is incorrect.

This issue can occur if you register a file policy with the option size_and_owner set to true, and then register another file policy with the option size_and_owner not set. The last file policy registration without the option removes the global parameter for size_and_owner information. As a result, Data ONTAP sends incorrect information.

To avoid this issue, ensure that you register all file policies with the option size_and_owner set to true.

Failed CIFS connections due to signature mismatch

If you enable SMB signing, existing CIFS connections might fail due to signature mismatch.

To avoid this issue, use the cifs terminate command to shut down the CIFS server and ensure that all existing CIFS connections are terminated before enabling SMB signing. After enabling SMB signing, use the cifs restart command to restart the CIFS server.

Configuring user mapping for a default user quota with CIFS not enabled could severely degrade performance

If you configure user mapping for a default user quota on a storage system for which CIFS is not enabled, a later attempt to delete a qtree could result in significantly degraded performance. This could happen whether CIFS was never enabled on that storage system or CIFS was enabled but later disabled.

You are at risk for this issue if your /etc/quotas file contains lines like these:

```plaintext
QUOTA_PERFORM_USER_MAPPING_ON
...
* user0/vol1/vol1i 50G
...
QUOTA_PERFORM_USER_MAPPING_OFF
```

In this case, you must remove or comment out these user mapping directives from your /etc/quotas file and reinitialize quotas before disabling CIFS. After you reenable CIFS, you can reinstate the user mapping directives and reinitialize quotas again.

Temporarily disabling and then reenabling CIFS for a brief maintenance window is unlikely to cause this issue.
Excessive pending CIFS authentication requests can cause service disruption

If domain controllers become unavailable to a vFiler unit, pending CIFS authentication requests accumulate on the storage system. If the issue is not resolved, this can prevent other vFiler units on the storage system from successfully completing CIFS authentication requests.

Because a vFiler unit shares system resources with other vFiler units that are on the storage system, pending CIFS authentication requests for a vFiler unit could affect resources available to other vFiler units.

Data ONTAP enables you to monitor pending CIFS authentication requests and take corrective action if needed. It generates SNMP traps in the following situations:

- The amount of pending CIFS authentication requests reaches 50 percent of total possible requests
- The pending authentication requests drop down under 10 percent, meaning within a normal range again

For information about SNMP, see the Data ONTAP Network Management Guide.

Empty CIFS/SMB2.x change notifications

CIFS/SMB2.x clients connected to the storage system might request to be notified about changes to a particular directory. In certain situations, the notifications that Data ONTAP returns are empty.

Data ONTAP collects all notifications that occur within 500 milliseconds after an event is generated to avoid subsequent change notify requests for every single such event. If the maximum capacity of the buffer that is allocated to hold these notifications is reached, Data ONTAP responds with an empty notification.

To work around this issue, you can decrease the time period for accumulating events. This reduces the chance of maxing out the buffer and receiving empty change notifications.

To decrease the time period, enter the following command:

```
setflag smb_boxcar_expire_ms time
```

`time` is the length of the time period in milliseconds.
By reducing this time period, Data ONTAP returns change notification responses quicker and with fewer events per response. While this might not completely eliminate empty notifications, a properly reduced time period reduces them significantly.

Due to the reduced number of events returned with each change notification response, clients have to send more change notify requests to obtain all events.

**Correction to required FPolicy screening requests**

Beginning with the Data ONTAP 7.2.2 release, if the required option is on and the FPolicy server cannot be contacted, the client request is denied.

In earlier Data ONTAP releases, required FPolicy file screening did not work as expected if an FPolicy server could not be contacted. If a file policy was set to require screening (using the required option of the fpolicy options command) for a particular file type, but the FPolicy server could not be contacted (because of an internal error), client requests to access the files controlled by the file policy were still allowed to be completed.

**FPolicy file extension issue on revert**

Starting with Data ONTAP 7.2, the file name extension length supported by FPolicy for screening is increased to 260 characters. However, if you added longer extensions to the list of extensions to be screened in Data ONTAP and you then revert to an earlier version, the file names with the long extensions will not be screened by FPolicy after revert. It is recommended that you check your FPolicy extension list before reverting.

**FPolicy compatibility issue in NFSv4 environments**

If you are running an FPolicy for Data ONTAP based application in NFSv4 environments, you must upgrade the FPolicy application to support NFSv4.

Beginning in Data ONTAP 7.3, FPolicy supports NFSv4. Previously, FPolicy did not support NFSv4 and NFSv4 requests were not passed on to any FPolicy-based application.

Although FPolicy now supports NFSv4, the FPolicy-based application might not. If an application without NFSv4 support receives notice of NFSv4 file operations (such as file OPEN and CLOSE events), these file operations might appear as UNKNOWN events to the application and generate error messages.

To avoid these compatibility problems, you should upgrade any FPolicy-based applications to support NFSv4.
Limitations in the naming of FPolicy policies

Beginning with Data ONTAP 7.3, a file policy name can consist of only Unicode characters. No special characters other than the underscore (_) or the hyphen (-) are allowed in the policy name.

If you upgrade the system from an earlier release, and FPolicy used a policy name with a special character, FPolicy will continue to use the special characters in that policy name. However, FPolicy will not allow the creation of new policies with names containing special characters other than the underscore (_) or the hyphen (-). In addition to not allowing the special characters in new policy names, FPolicy truncates the names that contain a "." (dot) in them, by dropping the characters after and including the "." (dot). Any options configured on this policy will be lost after the upgrade.

For example, a policy with the name, abc.xyz, is created in Data ONTAP 7.2. After you upgrade to Data ONTAP 7.3, the policy name changes to abc only. The options configured on this policy (abc.xyz) are also lost.

Some Group Policy Objects (GPOs) are applied differently on storage systems than on Windows systems

Data ONTAP 7.1 and later releases support Group Policy Objects (GPOs) that are relevant to storage system management. However, Event Log and Audit (Local Policies) GPOs are applied differently on IBM storage systems than on Windows systems.

The application differences occur because the underlying logging and auditing technologies are different. Audit GPOs are applied to storage systems by mapping and setting corresponding Data ONTAP options. The effect of mapping these options is similar, but not identical, to Audit policy settings. For more information, see the Data ONTAP File Access & Protocols Management Guide.

Client notification messages in Windows domains require NetBIOS

The Windows client notification feature used for client messaging and shutdown notices 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.

Unsupported Windows features in the file serving environment

This release does not support every available Windows feature.

For example, this release does not support the following Windows features:
• Encrypted File System (EFS)
• Logging of NT File System (NTFS) events in the change journal
• Microsoft File Replication Service (FRS)
• Microsoft Windows Indexing Service
• Remote storage through Hierarchical Storage Management (HSM)
• Local user account creation from the User Manager or Microsoft Manager Console
• Quota management from Windows 2000 clients
• Windows 2000 quota semantics
• The LMHOSTS file
• NT File System (NTFS) native compression

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 lower than 1024) to mount the NFS shares.

NFSv4 client compatibility

When your NFSv4 clients are in a different domain than your device is in, you might need to enter the client domain name as the value for the Data ONTAP option nfs.v4.id.domain in order to provide mapping for file ownership and group membership.

For more information about mapping options, see RFC 3530 and your client operating system documentation.

If you have any client using NFSv4 that needs to access a storage system, ensure that the Data ONTAP option nfs.v4.enable is set to on. In new installations, this option is set to off by default.

Unicode character 0x0080 is not supported

If you attempt to create or rename a file or directory from a CIFS client with a name that contains the Unicode character 0x0080, an error will appear.

The FTP server does not support Unicode characters

The FTP server does not support Unicode characters; thus, file names containing Unicode characters, including Japanese characters, will be displayed in FTP clients with alternate characters used in place of Unicode characters.
No IPv6 support in FPolicy
Starting with Data ONTAP 7.3.1, IPv6 is supported on storage systems. However, FPolicy does not support IPv6.
Network protocol issues

If your storage systems are configured for Brocade switches, TOE devices, VLANs, NIS, or IPsec, you might need to familiarize yourself with current network protocol issues.

For more information about these issues, see the Data ONTAP Network Management Guide.

- “FC 1062 interface on an N3600 storage system fails if the configuration settings are changed”
- “Authentication failure when IPsec is used with Kerberos”
- “The ping6 usage message is incorrect”
- “TOE is disabled” on page 144
- “No IPv6 support for RIP and IPsec” on page 145
- “Do not use vlan delete -q with ipsec” on page 145
- “Enable caching with NIS lookup” on page 145
- “Potentially reduced performance for IPsec traffic” on page 145

FC 1062 interface on an N3600 storage system fails if the configuration settings are changed

If you have an FC 1062 network interface card on an N3600 storage system, you must not change the status of the network interface or modify the network interface settings.

The FC 1062 interface uses the configuration settings in the /etc/rc file. If you try to change the settings of this network interface after system boot, the interface stops responding and becomes inaccessible. In such cases, you must enter the commands to modify the interface settings (for example, IP address, MTU, flow control) in the /etc/rc file and reboot the storage system for these configurations to take effect.

Authentication failure when IPsec is used with Kerberos

When IPsec is used with Kerberos authentication, certain Windows clients might face issues connecting to the storage system. If you encounter this issue and have to use Kerberos in your environment, contact technical support. If you do not have to use Kerberos, you can use preshared key authentication.

For more information about configuring preshared key authentication, see the Data ONTAP Network Management Guide.

The ping6 usage message is incorrect

In the command-line interface, the ping6 command usage lists the -f option. However, Data ONTAP does not support the -f option of the ping6 command.
Single-mode vif does not fail over correctly

Sometimes, the underlying network interface in a single-mode vif does not fail over correctly to the specified interface. In such cases, the vif status is down. To resolve this issue, you should verify the flags field in the `vif status` command output.

Possible scenarios when the vif does not fail over correctly are as follows:

- The switch connected to the interface is turned off and then turned on
- Underlying links of the vif are unplugged and then plugged in

The cause for this behavior can be that some flags were not reset properly after the underlying interface was plugged back in (although the interface is configured to the up status). You can verify the status of the vif by checking the flags field in the `vif status` command output.

For example, in the following output, the flags field is not set for the interface eo0:

```
    system> vif status vif0
    default: transmit 'IP Load balancing', VIF Type 'multi_mode', fail 'log'
    vif0: 1 link, transmit 'none', VIF Type 'single_mode' fail 'default'
    VIF Status Up Addr_set
    up:
    e0a: state up, since 31Dec2008 11:35:08 (00:39:16)
    mediatype: auto-1000t-fd-up
    flags: enabled
    input packets 706738, input bytes 110244559
    output packets 705879, output bytes 108626114
    output probe packets 345968, input probe packets 342950
    up indications 6, broken indications 7
    drops (if) 0, drops (link) 29
    indication: up at 31Dec2008 11:35:08
    consecutive 2129806, transitions 14
    down:
    e0b: state down, since 31Dec2008 11:35:08 (00:39:16)
    mediatype: auto-1000t-fd-up
    flags: enabled
    input packets 4120296422, input bytes 11094841698426
    output packets 3543747818, output bytes 13576720461678
    output probe packets 354968, input probe packets 343739
    up indications 6, broken indications 6
    drops (if) 0, drops (link) 20
    indication: broken at 30Dec2008 17:28:08
    consecutive 2129804, transitions 13
```

If the flag field for any network interface constituting the vif is not set, you should try unplugging and plugging in the interface link repeatedly until the flags field shows enabled in the `vif status` command output.

TOE is disabled

In Data ONTAP 7.3.2, TOE functionality is disabled by default. There is no adverse effect on the performance of your storage system because TOE is disabled. However, if you want to enable TOE, contact technical support.
No IPv6 support for RIP and IPsec
RIPng, an extension of RIPv2 for support of IPv6, is not supported currently in Data ONTAP. Also, Data ONTAP does not support IPsec over IPv6.

Do not use vlan delete -q with ipsec
If you delete VLAN interfaces when IPsec is enabled, delete them one by one. Do not use the `vlan delete -q` command.

Enable caching with NIS lookup
If you use NIS for group lookup services, disabling NIS group caching can cause severe degradation in performance.

Whenever you enable NIS lookups (`nis.enable`), it is recommended that you also enable caching (`nis.group_update.enable`). Failure to enable these two options together could lead to timeouts as CIFS clients attempt authentication.

Potentially reduced performance for IPsec traffic
Data ONTAP 7.1 and later releases do not support hardware-assisted IPSec encryption and instead only uses software encryption.

If your storage system includes hardware-assisted encryption, and you use IPSec encryption for high volumes of traffic, you might see reduced throughput for the IPSec encrypted traffic.
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 Block Access Management Guide for iSCSI and FC.

- “Disks offline in Windows 2008 after a standard upgrade”
- “option lun.partner_unreachable.default-partner.behavior: Value must be ‘drop’, ‘error’, or ‘start’” error message periodically displays
- “FCoE adapters may fail to come online if the FCP service is stopped and started too quickly” on page 147
- “Brocade 200E switch speed must be set manually” on page 147
- “Ongoing cfmode support” on page 148
- “cfmode restrictions for 8-Gb target expansion adapters” on page 148

Disks offline in Windows 2008 after a standard upgrade

During a standard upgrade to Data ONTAP 7.3.3, LUNs are assigned new revision numbers. Windows Server 2008 software interprets the LUNs with new revision numbers as new disks and sets them offline; this status is shown in Windows 2008 management interfaces after the upgrade. Windows Server 2003 ignores the LUN revision number.

You can work around this problem using the nondisruptive upgrade method, which allows the LUN revision numbers to retain their previous version. You can also bring the disks online after the upgrade using Windows disk management tools or SnapDrive functionality.

"option lun.partner_unreachable.default-partner.behavior: Value must be 'drop', 'error', or 'start'" error message periodically displays

Even though the value of option lun.partner_unreachable.default-partner.behavior is set to drop, this error message periodically displays on the system console.

Data ONTAP periodically reads the value for this option from the registry.local file on disk. Unless the option is explicitly set, the value on the registry.local file remains as unknown.

To remedy this problem, force the change in the registry.local file by issuing the following command:

```
option lun.partner_unreachable.default-partner.behavior drop
```
FCoE adapters may fail to come online if the FCP service is stopped and started too quickly

The first-generation Qlogic 8432 FCoE adapter takes some additional time to bring online and take offline. As a result, if you stop the FCP service and restart it too quickly, the adapter may fail to come online.

To avoid this problem, wait a few seconds before restarting the FCP service.

Note: This problem will be addressed in the next generation of FCoE adapters.

Brocade 200E switch speed must be set manually

Note: The Brocade 200E switch is equivalent to the IBM SAN16B-2 switch.

When set with link speed auto-negotiation, Brocade 200E switches do not always attain maximum expected connection speeds with attached devices.

By default, both Brocade 200E (4 Gbps) switch ports and host bus adapters (HBAs) are set to negotiate connection link speeds automatically. However, link speed auto-negotiation between 200E Switch ports and HBAs might not always result in the maximum expected connection speed, thus degrading performance. As an example, an expected 4-Gbps link might only carry traffic at 2 Gbps.

To avoid this problem, do not use the link speed auto-negotiation feature on the Brocade 200E switch. Instead, manually set individual 200E switch ports at the desired maximum link speed that matches the connected device's speed capability.

Note: This problem might also affect connections between Brocade 200E switches and other devices, such as Fibre Channel adapters and storage expansion units. For this reason, you should manually set the Brocade 200E switch speed for connections to all devices.

Setting Brocade 200E switch speed manually

You can use the Brocade switch console interface to configure link speed settings.

1. Enter the following command at the switch console to manually set the speed:
   ```
   portCfgSpeed port_number speed_level
   ```

2. Enter the following command at the switch console to verify the link speed:
   ```
   switchshow
   ```
Ongoing cfmode support

The only supported cfmode for new installations starting with the Data ONTAP 7.3 release is `single_image`.

If you are upgrading to Data ONTAP 7.3 from a prior release, follow these guidelines:

- On legacy systems, including N3700 storage systems, you can continue to use other cfmodes that are supported on your systems. You can freely change from one supported cfmode to any other supported cfmode on these systems.
  
  See “How to manage FCP with active/active configurations” in the Data ONTAP Block Access Management Guide for iSCSI and FC for the list of supported cfmodes by storage system model.

- On N3300 and N3600 storage systems, and N5000, N6000 and N7000 series systems, you can continue to run the existing cfmode after upgrading. If you change to `single_image` cfmode, you cannot revert to other cfmodes.
  
  See Changing the Cluster cfmode Setting in Fibre Channel SAN Configurations for instructions on upgrading to `single_image` cfmode.

cfmode restrictions for 8-Gb target expansion adapters

8-Gb target expansion adapters support only `single_image` cfmode.

However, 8-Gb initiators can connect to all targets, regardless of speed, in whatever cfmode the target supports.

For more information about cfmode restrictions, see the Data ONTAP Block Access Management Guide for iSCSI and FC.
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 Data Protection Online Backup and Recovery Guide and the Data ONTAP Data Protection Tape Backup and Recovery Guide.

- “Data transfer speed reduces when LSI Logic 1030 Ultra320 SCSI HBA is used with tape drives (FC 1024)”
- “Data recovery using SnapVault or SnapMirror for a qtree with LUN clones” on page 150
- “Using SnapVault for NetBackup to protect applications” on page 150
- “SnapVault for NetBackup is not supported with Symantec Veritas NetBackup 6.5” on page 151
- “Changes to deduplication usage with SnapVault for NetBackup” on page 151
- “NetBackup managed SnapVault is unavailable” on page 151
- “Limitations when using SnapVault with vFiler units” on page 151
- “SnapVault cannot be enabled on vFiler units when SnapLock for SnapVault relationships are present in vFiler0” on page 153
- “Compatibility with SnapDrive and SnapManager” on page 153
- “Synchronous SnapMirror not supported for volumes with deduplication” on page 153
- “Creating more than 64 mirrored aggregates might impair disaster recovery” on page 153
- “The N series Management Console data protection capability 3.7 does not perform optimally with deduplication” on page 153
- “Improved sequential read performance for deduplicated FlexVol volumes” on page 153
- “Volumes with deduplication are disabled after a nondisruptive upgrade” on page 154
- “SnapVault issues in cascaded configurations” on page 154
- “Suboptimal space savings with deduplication when 16 GB Performance Acceleration Module is installed” on page 155

Data transfer speed reduces when LSI Logic 1030 Ultra320 SCSI HBA is used with tape drives (FC 1024)

The LSI Logic 1030 Ultra320 SCSI HBA (FC 1024) on storage systems fails to achieve 320 MBps speed with tape drives. To achieve 320 MBps speed with an...
LSI Logic 1030 Ultra320 SCSI HBA (FC 1024), you must set the new boot argument `mptscsi-U320fix?` to true in the boot environment.

**Data recovery using SnapVault or SnapMirror for a qtree with LUN clones**

You can use SnapVault to perform an in-place restore for a source qtree, from the destination qtree. However, if the source qtree has LUN clones, in-place restore is not supported. The use of `snapmirror resync` for restoring data to a source qtree with LUN clones is also not supported.

On replicating qtrees with LUN clones, each LUN clone within the qtree is stored as a LUN within the destination qtree. This applies to both SnapVault and qtree SnapMirror. Therefore, when you recover data from such a destination qtree, the original LUN clones would be restored as complete LUNs.

**SnapVault**

To recover data from the destination qtree using SnapVault, you can use one of the following options for a qtree with LUN clones.

- Delete the LUN clones within the source qtree, and then perform an in-place restore, using the `snapvault restore` command.

  **Note:** If you attempt an in-place restore for a qtree with LUN clones, the system displays the following error message.

  Qtree has lun clones

- Restore the data to a new qtree, by using the `snapvault restore` command.

  **Attention:** For a qtree with LUN clones, ensure that the volume has enough free space to store the LUN clones as complete LUNs before you initiate data recovery using SnapVault or qtree SnapMirror.

**Qtree SnapMirror**

In case of qtree SnapMirror, to recover data for a qtree with LUN clones, you can replicate the destination qtree to a new qtree.

**Note:** If you attempt to recover data from the destination to a source qtree with LUN clones, using a `snapmirror resync` operation, the system displays the following error message:

cannot resync as qtree has one or more lun clones

Abort resync

For more information about restoring data using SnapVault and SnapMirror, see the *Data ONTAP Data Protection Online Backup and Recovery Guide*.

**Using SnapVault for NetBackup to protect applications**

Starting with Data ONTAP 7.3.1, new SnapVault for NetBackup configurations for protecting applications are not supported.
All currently installed SnapVault for NetBackup solutions based on Data ONTAP 7.2 or Data ONTAP 7.3 continue to be fully supported for protecting data in applications such as Oracle, Microsoft SQL Server, Sybase, and IBM DB2.

SnapVault for NetBackup support for protecting applications is limited to customers who are already using SnapVault for NetBackup.

**SnapVault for NetBackup is not supported with Symantec Veritas NetBackup 6.5**

Due to a software problem with Symantec Veritas NetBackup 6.5, SnapVault for NetBackup does not work with NetBackup 6.5. Symantec has fixed this problem in NetBackup 6.5.1 and later. SnapVault for NetBackup works with NetBackup 6.0MP5 or NetBackup 6.5.1 and later.

**Changes to deduplication usage with SnapVault for NetBackup**

Data ONTAP 7.3.1 and later no longer support deduplication for use with SnapVault for NetBackup. This change applies to both structured (database) and unstructured (file) data types.

<table>
<thead>
<tr>
<th>Data type</th>
<th>Through SnapVault for NetBackup only</th>
<th>Post-replication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unstructured (file system)</td>
<td>Yes, automatic inline block-sharing</td>
<td>No</td>
</tr>
<tr>
<td>Structured (application)</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

The SnapVault for NetBackup specific inline block sharing feature, which provides deduplication support for file data only, continues to be supported, and is not affected by this change. Deduplication in a non-SnapVault for NetBackup configuration (for example, NetBackup shared or flexible disk option) remains supported and is not affected by this change.

**NetBackup managed SnapVault is unavailable**

Starting with the release of Data ONTAP 7.3, configuring and managing SnapVault replication between primary and secondary storage using Symantec VERITAS NetBackup is no longer available. NetBackup management for SnapVault replication remains available and supported when used with versions of Data ONTAP earlier than 7.3.

**Limitations when using SnapVault with vFiler units**

There are certain limitations when using SnapVault with vFiler units. These limitations apply to all Data ONTAP releases that support vFiler units.

The management of SnapVault secondary (creation or modification of SnapVault relationships and schedules at the SnapVault secondary) is only
supported from the default vFiler unit (vfiler0). The management of
SnapVault secondary is not supported from a nondefault vFiler context. If the
volume containing the SnapVault destination qtree is owned by a nondefault
vFiler unit, the SnapVault secondary needs to be managed through the default
vFiler unit (vfiler0).

Table 1. vFiler unit support with SnapVault secondary volumes

<table>
<thead>
<tr>
<th>Management of SnapVault secondary volume</th>
<th>Ownership of SnapVault secondary volume</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default vFiler unit (vfiler0)</td>
<td>Nondefault vFiler unit</td>
</tr>
<tr>
<td>Default vFiler unit (vfiler0)</td>
<td>Yes</td>
</tr>
<tr>
<td>Nondefault vFiler unit</td>
<td>Yes</td>
</tr>
<tr>
<td>Nondefault vFiler unit</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The management of SnapVault primary in a vfiler context is supported.

Table 2. vFiler unit support with SnapVault primary volumes

<table>
<thead>
<tr>
<th>Management of SnapVault primary volume</th>
<th>Ownership of SnapVault primary volume</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default vFiler unit (vfiler0)</td>
<td>Nondefault vFiler unit</td>
</tr>
<tr>
<td>Default vFiler unit (vfiler0)</td>
<td>Yes</td>
</tr>
<tr>
<td>Nondefault vFiler unit</td>
<td>Yes</td>
</tr>
<tr>
<td>(From a nondefault vFiler context, you can only manage volumes owned by that nondefault vFiler unit.)</td>
<td></td>
</tr>
</tbody>
</table>

DataFabric Manager support for the management of vFiler unit relationships

DataFabric Manager supports the management of SnapVault relationships for
volumes through the default vFiler (vfiler0) context only. When using
DataFabric Manager, the following limitations apply for SnapVault
relationships involving nondefault vFiler units.

- You can only view SnapVault relationships configured through the default
vFiler unit (vfiler0). You cannot view any SnapVault relationships
configured through nondefault vFiler units.
- You can configure new SnapVault relationships for a volume only through
the default vFiler unit (vfiler0), even if the volume belongs to a nondefault
vFiler unit.
SnapVault cannot be enabled on vFiler units when SnapLock for SnapVault relationships are present in vfiler0

When you create SnapVault relationships for SnapLock secondary volumes in vfiler0, you also manually set the snapvault.lockvault_log_volume option to the name of a SnapLock for SnapVault log volume. After this option is set, SnapVault cannot be enabled on any vFiler units on the storage system. For more information about the snapvault.lockvault_log_volume option, see the na_snapvault(1) man page.

Compatibility with SnapDrive and SnapManager

This version of Data ONTAP is not supported by all versions of N series software for Windows clients. Before installing or upgrading to this version of Data ONTAP, make sure that the SnapManager and SnapDrive versions you are running or plan to install are compatible with this release.

Synchronous SnapMirror not supported for volumes with deduplication

Volumes using deduplication cannot be replicated using synchronous SnapMirror.

Creating more than 64 mirrored aggregates might impair disaster recovery

If you create more than 64 mirrored (or SyncMirror) aggregates per storage system (or per node in a mirrored cluster or MetroCluster), an out-of-date plex might be brought back online after some types of failures.

To avoid bringing an out-of-date plex back online, do not create more than 64 mirrored aggregates per system, even though Data ONTAP does not prevent you from doing so.

The N series Management Console data protection capability 3.7 does not perform optimally with deduplication

Integration with deduplication does not work optimally with Protection Manager 3.7 because the retention of Snapshot copies causes deduplicated blocks to be locked within the Snapshot copies. In this case, deduplication savings will be limited

Do not use Protection Manager 3.7 on volumes that have deduplication enabled.

Improved sequential read performance for deduplicated FlexVol volumes

In Data ONTAP 7.2.6 and later releases of the Data ONTAP 7.2 release family, and in Data ONTAP 7.3.1, the performance of sequential read operations on large deduplicated VMDK files has improved.

In VMware environments, the VMDKs are created with a large number of duplicate blocks. This results in a high number of shared blocks after running
deduplication. Therefore, applications that perform large sequential read operations, such as dump, have low throughput when run on VMDK files.

Highly shared blocks are efficiently cached and read from the in-memory cache instead of the disk every time. This caching improves the sequential read performance on VMDK files.

**Volumes with deduplication are disabled after a nondisruptive upgrade**

In an active/active configuration with a two-node cluster, when one node performs a nondisruptive upgrade to Data ONTAP 7.3 or Data ONTAP 7.3.1 from a release prior to the Data ONTAP 7.3 release family, the nodes are updated sequentially. Deduplication is disabled for the volumes on the second node that is upgraded.

If the takeover storage system has been upgraded to Data ONTAP 7.3 or Data ONTAP 7.3.1, and assumes the functions of the “failed” partner while it is being upgraded, deduplication is disabled on the volumes belonging to the “failed” node running the earlier release.

After the takeover, deduplication schedules set in the earlier release are reset on those volumes.

After both the nodes have been upgraded, deduplication has to be reenabled and deduplication schedules reconfigured for each volume impacted.

You can use the `sis status` command to view the deduplication status of the volume, and the `sis on` command to enable deduplication.

You can use the following command to check deduplication schedules:
```
• sis config
```

You can use the following command to set deduplication schedules:
```
• sis config -s schedule path
```

**Note:** Before you start performing a nondisruptive upgrade, make a list of volumes enabled with deduplication and their schedule so that they can be reconfigured after the nondisruptive upgrade is complete.

**Note:** Upgrades within the same Data ONTAP release family (minor nondisruptive upgrade between Data ONTAP 7.3 and Data ONTAP 7.3.1) does not disable deduplication.

**SnapVault issues in cascaded configurations**

You might encounter a disruption in service during SnapVault operations involving cascaded configurations.
A disruption in service during a SnapVault operation might occur during one of the following scenarios:

- While using SnapVault to protect a volume SnapMirror destination or while using volume SnapMirror to protect a SnapVault destination, if any of the volumes in the cascade is a SnapLock volume, you might encounter a disruption in service.

- Starting with Data ONTAP 7.3.2, if you are using SnapVault schedules to backup qtrees in a volume SnapMirror destination volume and if you have not configured the corresponding SnapVault primary schedules on the volume SnapMirror primary volume, SnapVault backups can fail.

**Suboptimal space savings with deduplication when 16 GB Performance Acceleration Module is installed**

When you run a deduplication scan by using the `sis start -s` command on a volume with existing data and with the 16-GB Performance Acceleration Module installed, you obtain suboptimal space savings.
Storage resource management issues

If you have configured quotas or if you are using FlexVol volumes on N series systems, you might have to familiarize yourself with these storage resource management issues.

For more information about these issues, see the Data ONTAP Storage Management Guide.

- "Configuring user mapping for a default user quota with CIFS not enabled could severely degrade performance" on page 137
- "After changing the port assigned to ACP, a reboot is required to regain use of the original port" on page 157
- "DataFabric Manager requires a patch to view the 2 TB disks" on page 157
- "The all keyword for the aggr add command is not yet implemented" on page 157
- "Moving disks to a system running an earlier version of Data ONTAP could cause disk identification issues" on page 157
- "Data ONTAP can silently select varying disk sizes when enlarging or creating an aggregate" on page 157
- "Qtree quotas might prevent explicit quotas from overriding the default" on page 159
- "Adding a FlexCache origin volume to a vFiler unit might cause caching system to panic" on page 159

Configuring user mapping for a default user quota with CIFS not enabled could severely degrade performance

If you configure user mapping for a default user quota on a storage system for which CIFS is not enabled, a later attempt to delete a qtree could result in significantly degraded performance. This could happen whether CIFS was never enabled on that storage system or CIFS was enabled but later disabled.

You are at risk for this issue if your /etc/quotas file contains lines like these:

```
QUOTA_PERFORM_USER_MAPPING ON
...
user@/vol/vol1 50G
...
QUOTA_PERFORM_USER_MAPPING OFF
```

In this case, you must remove or comment out these user mapping directives from your /etc/quotas file and reinitialize quotas before disabling CIFS. After you reenable CIFS, you can reinstate the user mapping directives and reinitialize quotas again.

Temporarily disabling and then reenabling CIFS for a brief maintenance window is unlikely to cause this issue.
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.

The df -S command is not supported in Data ONTAP 7.3.3

In Data ONTAP 7.3.3, the df - S command is not supported.

DataFabric Manager requires a patch to view the 2 TB disks

For the Data Fabric Manager (DFM) to view the 2TB disks, you must install the DFM patch 4.0D23 on your DFM server. Contact N series support to obtain this patch.

The all keyword for the aggr add command is not yet implemented

The all keyword for the -g option of the aggr add command, which should cause Data ONTAP to fill all existing RAID groups before creating any new ones, has no effect.

Moving disks to a system running an earlier version of Data ONTAP could cause disk identification issues

If you remove a disk from a storage system running Data ONTAP 7.3 or later and place it into a storage system running an earlier version of Data ONTAP, the software disk ownership information is incorrect and might prevent Data ONTAP from identifying or correctly assigning the disk.

The disk identification issues cannot be solved except by returning the disk to the original storage system and removing the software disk ownership information using the more recent version of Data ONTAP.

To avoid causing disk identification issues, always use the recommended procedure for removing a data disk, which includes removing the software disk ownership information from the disk before removing it.

For more information, see the Data ONTAP Storage Management Guide.

Note: Gateway systems support disks starting with Data ONTAP 7.3. Therefore, you cannot move a disk from a gateway system to a gateway system running a version of Data ONTAP earlier than 7.3.

Data ONTAP can silently select varying disk sizes when enlarging or creating an aggregate

If disks or array LUNs of varying size are present in your storage system, relying on automatic disk selection can result in unexpected sizes being selected by Data ONTAP.
When you create a new aggregate or add storage to an existing aggregate using automatic disk selection, Data ONTAP selects disks or array LUNs based on various criteria including size, speed, and checksum type. To ensure that the selected disks or array LUNs are the size you want, specify the disk or array LUN size when creating or increasing the size of an aggregate.

For more information, see the na_aggr(1) man page.

**Adding disks when varying sized disks are in use**

When you have disks of different sizes available, always specify the disk size when creating or adding to an aggregate.

To specify the disk size when you add a disk to an aggregate, enter the following command:

`aggr add aggr_name num_disks @ size`

**Example**

For example, to add four 635-GB disks to aggr1, enter the following command:

`aggr add aggr1 4@635G`

**Discovering what disks Data ONTAP will automatically select**

To list which disks would be selected, use the `-n` option for the `aggr create` or `aggr add` command.

When you use the `-n` option, the disks that would be selected automatically, if you created an aggregate or added to an aggregate, are displayed. The creation or addition is not performed. If the selected disks are not what you intended, you can specify a disk list when you enter the `aggr create` or `aggr add` command.

To list the disks that would be selected for an `aggr create` command, enter the following command:

`aggr create aggr_name -n disk_list`

**Example**

For example, to list the disks that would be used for the creation of the newaggr aggregate using eight automatically selected disks, enter the following command:

`aggr create newaggr -n 8`
Qtrees with quotas applied, the override will not apply within those qtrees unless you also apply the override explicitly for those qtrees.

If you have a default user or group quota on a volume, and you want to override that default quota for a particular user or group, note this issue: If you also have one or more qtree quotas on that volume, the explicit quota might not take precedence over the default quota within those qtrees as expected.

**Overriding default qtree quotas**

To avoid quota precedence problems, you can override the default quota on the qtrees that have a quota.

Suppose you have the following `/etc/quotas` file:

```
#Quota target type disk files thold sdisk sfile
#----------- ---- ---- ----- ----- ----- ----- 
*          user@/vol/vol1 16K
14717      user@/vol/vol1 1M
/vol/vol1/mytree tree 10M
```

The presence of the qtree quota causes all users, including user 14717, to be limited to 16 KB of space in the mytree qtree.

To override quota precedence, add the following line to the quota file to enable overriding the qtree quota with an volume-wide quota of 1 MB:

```
14717 user@/vol/vol1/mytree 1M
```

User 14717 is now able to use 1 MB of space anywhere in vol1.

**Adding a FlexCache origin volume to a vFiler unit might cause caching system to panic**

If you attempt to add a FlexCache origin volume with existing FlexCache cache volumes to a vFiler unit using either the `vfiler create` or `vfiler add` command, the systems that contain the FlexCache cache volumes might panic.

To avoid this issue, destroy all FlexCache volumes backed by the origin volume before adding the origin volume to a different vFiler unit.

**Known problems and limitations**

159
Third-party storage issues

When Data ONTAP uses third-party storage, issues can occur with the switches and storage arrays in the configuration.

- “Exceeding the maximum number of assigned devices results in a panic”
- “No support for REP with zone checksum type array LUNs”
- “Limitation on EMC CX storage array LUN numbering”

Exceeding the maximum number of assigned devices results in a panic

If more than 256 array LUNs from a specific storage array target port to a specific gateway FC initiator port are assigned to a gateway system, the gateway system panics when you try to boot it.

No more than 256 array LUNs from a specific storage array port to a specific gateway FC initiator port should be assigned (in the Data ONTAP configuration) to a gateway system. This is a Data ONTAP limitation. 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

If you assigned more than 256 LUNs from the same storage array target port to the gateway system, you must remove ownership of enough of the array LUNs so that no more than 256 array LUNs from the same target port to the same gateway FC initiator are assigned to the gateway system.

No support for REP with zone checksum type array LUNs

RAID Error Propagation (REP) is not supported with volumes and aggregates that contain zone checksum type array LUNs.

Limitation on EMC CX storage array LUN numbering

If you are not using Storage Groups on your CX storage array, do not assign LUN numbers greater than 254 to array LUNs for gateway systems.

If you are not using Storage Groups, the CX storage array might not present internal LUNs numbers greater than 254 to your gateway system. If this occurred, the gateway would not be able to see those array LUNs.

If you are using Storage Groups, the CX storage array automatically assigns internal LUN numbers lower than 255.
Active/active configuration issues

If you are using the `cf.takeover.on_network_interface_failure` option, you might need to familiarize yourself with this active/active configuration issues.

For more information about these issues, see the *Data ONTAP Active/Active Configuration Guide*.

- “Re-creating mirrored aggregates when the base Snapshot copy is deleted”
- “If takeover is enabled for network interface failure, automatic giveback should be disabled” on page 163

Re-creating mirrored aggregates when the base Snapshot copy is deleted

You might not be able to resynchronize the aggregates after the disaster site node is recovered. In a disaster scenario in a MetroCluster configuration, the base Snapshot copy of an aggregate might get deleted due to Snapshot copy autodelete feature. In such a case, perform level-0 resynchronization between the aggregates.

1. Verify that your aggregates and volumes are operational and mirrored by entering the following command:

   ```
   aggr status
   ```

   If the aggregates are not in mirroring relationship, the disaster aggregate is displayed with an outof-date status.

2. Re-create the mirrored aggregates by entering the following command for each aggregate that was split:

   ```
   aggr mirror aggr_name -v disaster_aggr
   aggr_name is the aggregate on the surviving site's node.
   disaster_aggr is the aggregate on the disaster site's node.
   ```

<table>
<thead>
<tr>
<th>If there is...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>A common Snapshot copy</td>
<td>The aggregate <code>aggr_name</code> rejoins with <code>disaster_aggr</code></td>
</tr>
<tr>
<td>No common Snapshot copy</td>
<td>It displays an error message. Go to Step 3.</td>
</tr>
</tbody>
</table>

3. Delete the affected aggregate by entering the following command:

   ```
   aggr destroy disaster_aggr
   ```

   The `disaster_aggr` is the name of the aggregate at the disaster site.

4. Re-create the mirrored aggregates by entering the following command for the aggregate that was split:

   ```
   aggr mirror aggr_name
   ```

   The `aggr_name` is the aggregate at the surviving site.
Example:
The following example shows the command and status output of reestablishing the mirroring relationship between the plexes.

First, determine the aggregates that are not in mirroring relationship. In this, the aggr1(1) is not in mirroring relationship.

<table>
<thead>
<tr>
<th>Aggr State</th>
<th>Status</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>trad online</td>
<td>raid_dp, trad</td>
<td>resync</td>
</tr>
<tr>
<td></td>
<td>32-bit</td>
<td></td>
</tr>
<tr>
<td>aggr0 online</td>
<td>raid_dp, aggr</td>
<td>root</td>
</tr>
<tr>
<td></td>
<td>mirrored</td>
<td></td>
</tr>
<tr>
<td>aggr1 online</td>
<td>raid_dp, aggr</td>
<td></td>
</tr>
<tr>
<td></td>
<td>32-bit</td>
<td></td>
</tr>
<tr>
<td>aggr1(1) failed</td>
<td>raid_dp, aggr</td>
<td>out-of-date</td>
</tr>
</tbody>
</table>

Note: Note: The node at the surviving site is called filer1; the node at the disaster site is called filer2.

Next, re-create the mirrored aggregates.

Next, destroy the aggregate of the disaster site.

Next, re-create the mirroring relation between the two sites.

Verify that the synchronous mirrors of the MetroCluster configuration is reestablished.
If takeover is enabled for network interface failure, automatic giveback should be disabled

If you set the `cf.takeover.on_network_interface_failure` option to on to enable automatic failover on network interface failures, ensure that you have the `cf.giveback.auto.enable` option set to off.

If the `cf.giveback.auto.enable` option is set to on, a network interface failure could result in a continuous series of takeovers and givebacks until the network interface problem is resolved.
Changes to published documentation

Some information about the Data ONTAP 7.3 release family 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 Archive and Compliance Management Guide” on page 166
- “Changes to the Data ONTAP Commands Manual Page Reference” on page 167
- “Changes to the System Administration Guide” on page 177
- “Changes to the Storage Management Guide” on page 175
- “Changes to the Data Protection Online Backup and Recovery Guide” on page 168
- “Changes to the Data ONTAP Data Protection Tape Backup and Recovery Guide” on page 170
- “Changes to the File Access and Protocols Management Guide” on page 171
- “Changes to the MultiStore Management Guide” on page 173
- “Changes to the Upgrade Guide” on page 180
- “Change to the Gateway Implementation Guide for native storage expansion units” on page 182
- “Array LUN sizing with 2 TB disks is not documented in all Gateway Implementation Guides” on page 183
Changes to the Archive and Compliance Management Guide

New information has become available since the previous revision of the Data ONTAP Archive and Compliance Management Guide.

- “Correction to creating SnapLock traditional volumes”
- “Changes to cross-references to SnapLock information”
- “Integration of third-party applications with SnapLock feature”

Correction to creating SnapLock traditional volumes

The “Creating SnapLock traditional volumes” topic incorrectly lists the option `-v` for creating a SnapLock traditional volume.

The correct CLI command to create a SnapLock traditional volume is as follows:

```
vol create trad_vol -L snaplock_type ndisks [@disksize]
```

Changes to cross-references to SnapLock information

Starting with Data ONTAP 7.3.1, the SnapLock feature is explained in Data ONTAP Archive and Compliance Management Guide. The cross-references to SnapLock in Data ONTAP System Administration Guide and Data ONTAP Storage Management Guide incorrectly reference the Data ONTAP Data Protection Online Backup and Recovery Guide.

Integration of third-party applications with SnapLock feature

Starting with Data ONTAP 7.3.6, information about integrating third-party applications with the SnapLock feature by using Manage ONTAP SDK is provided in Data ONTAP Archive and Compliance Management Guide.
Changes to the Data ONTAP Commands Manual Page Reference

New information has become available since the previous revision of the Data ONTAP Commands: Manual Page Reference. You can access the current Data ONTAP man pages by using the man command at the storage system command line or by using FilerView.

You can view man pages in the following ways:
- At the storage system command line, by entering man command_or_file_name
- From the FilerView main navigational page

The na_ping6(1) man page lists incorrect options

The -a option and its sub-options listed in the na_ping6(1) man page are not supported in Data ONTAP. The -s option in the na_ping6(1) man page is incorrect. Instead, you must use the -d option to specify the data packet size with the ping6 command.
Changes to the Data Protection Online Backup and Recovery Guide

New information has become available since the previous revision of the Data ONTAP Data Protection Online Backup and Recovery Guide.

- “Single file reversion to or from symbolic links using SnapRestore not supported”
- “Syntax entry correction in the snapmirror.conf file”

Single file reversion to or from symbolic links using SnapRestore not supported

You cannot perform single file reversion to or from symbolic links using SnapRestore. This information is not included in the "Reverting a file to a selected Snapshot copy" topic in the Data ONTAP Data Protection Online Backup and Recovery Guide.

Syntax entry correction in the snapmirror.conf file

In the section titled "Enabling compression for a SnapMirror transfer" in the Data ONTAP Data Protection Online Backup and Recovery Guide, the syntax entry in the snapmirror.conf file that is required for enabling compression and the corresponding examples are incorrect.

The incorrect syntax entry for enabling compression in Step 3 is as follows:

`connection_name:src_vol dst_system:dst_vol compression=enable - * * * *`

The correct syntax entry for enabling compression is:

`connection_name:src_vol dst_system:dst_vol compression=enable * * * *`

The incorrect syntax entry in the example of step 3 is as follows:

`conxn_1:src_vol dst_system:dst_vol compression=enable - * * * *`

The correct syntax entry in the example of Step 3 is as follows:

`conxn_1:src_vol dst_system:dst_vol compression=enable * * * *`

The incorrect syntax entry in the "Compression for a multipath SnapMirror relationship" example is as follows:

`connection_name:src_vol dst_system:dst_vol compression=enable - * * * *`

The correct syntax entry in the "Compression for a multipath SnapMirror relationship" example is as follows:
Changes to the Data ONTAP Data Protection Tape Backup and Recovery Guide

Some additional information about tape backup features has become available since the previous revision of the Data ONTAP Data Protection Tape Backup and Recovery Guide.

- “Limitations of incremental dump backup”
- “Backing up data to tape using NDMP services”

Limitations of incremental dump backup

In the section titled "What increment chains are" in the Data ONTAP Data Protection Tape Backup and Recovery Guide, the limitations of incremental backup are not applicable in Data ONTAP 7.3.3 and later releases.

Backing up data to tape using NDMP services

Back up data to tape using NDMP services has been moved to the Data ONTAP Data Protection Tape Backup and Recovery Guide.

For more information about backing up data to tape using NDMP services, see the Data ONTAP Data Protection Tape Backup and Recovery Guide.
Changes to the File Access and Protocols Management Guide

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

- Corrections to various SFTP topics
- Correction for disabling virus scanning
- Enhancements to NFS access cache management on page 47

Corrections to various SFTP topics

Some corrections have been made to topics in the section Managing the Secure File Transfer Protocol (SFTP).

- Clarified the SFTP authentication style format for NTLM by adding the following statements: To authenticate using NTLM with a domain user account, you must specify the username in the format domain\username.
To authenticate using NTLM with a local user account, you must specify the username in the format storagesystem_hostname\username.
- Updated the topic Enabling or disabling SFTP user home directory restrictions to state correctly that by default the option sftp.dir_restriction is set to off.
- Corrected the commands in the topic Enabling or disabling SFTP user home directory restrictions:

<table>
<thead>
<tr>
<th>If you want SFTP user home directory restrictions to be...</th>
<th>Then enter the following command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>options sftp.dir_restriction on</td>
</tr>
<tr>
<td>Disabled</td>
<td>options sftp.dir_restriction off</td>
</tr>
</tbody>
</table>

- Corrected the commands in the topic Enabling or disabling the overriding of UNIX permissions:

<table>
<thead>
<tr>
<th>If you want overriding of UNIX permissions to be...</th>
<th>Then enter the following command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>options sftp.override_client_permissions on</td>
</tr>
<tr>
<td>Disabled</td>
<td>options sftp.override_client_permissions off</td>
</tr>
</tbody>
</table>

Correction for disabling virus scanning

The section about enabling or disabling virus scanning lists the incorrect option for disabling virus scanning of read-only files that a client opens. The correct option is -novscanread and the full CLI command to disable virus scanning of read-only files is as follows:
cifs shares -change sharename -novscanread

Enhancements to NFS access cache management

Beginning in Data ONTAP 7.3.6, the `exportfs` command includes updated options for managing entries in the NFS access cache.

The `-c` option of the `exportfs` command has been updated to take multiple IP addresses as arguments. This enables verification of current export rights for multiple clients in one operation.

The `-f` option of the `exportfs` command now includes a `-n` parameter, which allows you to flush access cache entries that correspond to a specific host.

For more information, see the `exportfs(1)` man page and the *Data ONTAP File Access and Protocols Management Guide.*
Changes to the MultiStore Management Guide

There are some changes to the existing content of the Data ONTAP MultiStore Management Guide.

- "Corrections to the SnapVault support on vFiler units"
- "Correction to HTTP licensing information for online migration of vFiler units" on page 174

Corrections to the SnapVault support on vFiler units

The sections "Where to enter SnapVault commands" and "Features and limitations of the snapvault command" have some incorrect information about interoperability between SnapVault and MultiStore.

Where to enter SnapVault commands

The following existing content is incorrect: Commands entered on a nondefault vFiler unit makes changes on or displays information only about that specific vFiler unit.

This content is corrected as follows: Some commands entered on a nondefault vFiler unit make changes on or display information only about that specific vFiler unit—for example, snapvault status and snapvault snap sched.

Features and limitations of the snapvault command

The following existing content is incorrect:

The features of the snapvault command when used in a MultiStore context are as follows:

- Additional SnapVault licenses are not required. vFiler units use the same source and destination licenses as the physical storage systems.
- The SnapVault feature can be turned on and off independently on each vFiler unit.
- The snapvault.access and snapvault.enable options can be changed independently on each vFiler unit.
- Each vFiler unit has its own snapvault.conf file in the /etc directory.
- SnapVault relationships established between vFiler units are maintained across vFiler unit migration.

This content is corrected as follows:

The features of the snapvault command when used in a MultiStore context are as follows:
• Additional SnapVault licenses are not required. vFiler units use the same source and destination licenses as the physical storage systems.
• The SnapVault feature can be turned on and off independently on each vFiler unit.
• The snapvault.access and snapvault.enable options can be changed independently on each vFiler unit.

**Correction to HTTP licensing information for online migration of vFiler units**

The "Licenses required for online migration" topic incorrectly states that HTTP must be licensed on the source and the destination storage systems to perform online migration of vFiler units. The corrected content is: You must enable httpd.admin.enable option on the source and destination storage systems for online vFiler unit migration.
Changes to the Storage Management Guide

New information has become available since the previous revision of the Data ONTAP Storage Management Guide.

- "Maximum size of deduplicated and non-deduplicated volumes in N6200 series storage systems"
- "Disk sanitization limitations"
- "Space guarantees and CIFS"
- "Requirements when creating a qtree quota" on page 176
- "ACP example output shows incorrect IP addresses" on page 176

Maximum size of deduplicated and non-deduplicated volumes in N6200 series storage systems

You need to be aware of the maximum volume size supported for N6200 series storage systems, with and without deduplication.

<table>
<thead>
<tr>
<th>Model</th>
<th>Maximum size of volume without deduplication (TB)</th>
<th>Maximum size of volume with deduplication (TB)</th>
<th>Total data size of volume with deduplication (TB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>N6210</td>
<td>16</td>
<td>4</td>
<td>20</td>
</tr>
<tr>
<td>N6240</td>
<td>16</td>
<td>16</td>
<td>32</td>
</tr>
<tr>
<td>N6270</td>
<td>16</td>
<td>16</td>
<td>32</td>
</tr>
</tbody>
</table>

Disk sanitization limitations

The topic titled "Disk sanitization limitations" incorrectly states that disk sanitization cannot be performed on more than one SES disk at the same time.

In fact, you can sanitize both SES disks in the same ESH storage expansion unit at the same time. However, if you do so, you will see errors on the console about access to that storage expansion unit. While the SES disks are being sanitized, storage expansion unit warnings (for example, temperature) will not be reported.

Space guarantees and CIFS

The topic titled "What space guarantees are" correctly warns against using a space guarantee of none for volumes being accessed using CIFS. However, the same is true for space guarantees of file.

Writes to a volume with a space guarantee of file could fail. Because write errors are unexpected in a CIFS environment, do not set the space guarantee to file for volumes accessed using CIFS.
Requirements when creating a qtree quota

The topic titled "How quotas work with users and groups" states that when you apply a user or group quota to a qtree, you must also define a quota for that user or group for the qtree's containing volume. This is incorrect; no such requirement exists.

ACP example output shows incorrect IP addresses

The IP addresses shown in the example showing the output of the storage show acp command shows ACP configured to use public IP addresses. This is incorrect; you should use private IP addresses when configuring ACP.

The example should read as follows:

```
Example
For example, if you select e0P as the interface for ACP traffic, 192.168.0.0 as the ACP domain, and 255.255.252.0 as the network mask for the ACP subnet, the storage show acp command output looks similar to the following example:
my-sys-1> storage show acp
Alternate Control Path: enabled
Ethernet Interface: e0P
ACP Status: Active
ACP IP address: 192.168.2.61
ACP domain: 192.168.0.0
ACP netmask: 255.255.252.0
ACP Connectivity Status: Full Connectivity
<table>
<thead>
<tr>
<th>Shelf Module</th>
<th>Reset Cnt</th>
<th>IP address</th>
<th>FW Version</th>
<th>Module</th>
</tr>
</thead>
<tbody>
<tr>
<td>7a.001.A</td>
<td>002</td>
<td>192.168.0.145</td>
<td>01.05</td>
<td>IOM6</td>
</tr>
<tr>
<td>7a.001.B</td>
<td>003</td>
<td>192.168.0.146</td>
<td>01.05</td>
<td>IOM6</td>
</tr>
<tr>
<td>7c.002.A</td>
<td>000</td>
<td>192.168.0.206</td>
<td>01.05</td>
<td>IOM6</td>
</tr>
<tr>
<td>7c.002.B</td>
<td>001</td>
<td>192.168.0.204</td>
<td>01.05</td>
<td>IOM6</td>
</tr>
</tbody>
</table>
```
Changes to the System Administration Guide

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

• “Changes to the supported OpenSSH client versions”
• “Changes to storage system configuration backup and restore”
• “Changes to the instructions on editing the /etc/rc file” on page 178
• “Corrections for root FlexVol volume size requirement” on page 179

Changes to the supported OpenSSH client versions

The SSH protocol section of the Data ONTAP System Administration Guide has updated information for OpenSSH client versions that Data ONTAP supports.

Data ONTAP supports the following SSH clients:
• OpenSSH client versions 4.0p1 and 4.4p1 on UNIX platforms
• SSH Communications Security client (SSH Tectia client) version 6.0.0 on Windows platforms
• Vandyke SecureCRT version 6.0.1 on Windows platforms
• PuTTY version 0.6.0 on Windows platforms
• F-Secure SSH client version 7.0.0 on UNIX platforms

To enhance security, OpenSSH client version 3.8p1 is no longer supported because it does not contain the latest security fix.

Changes to storage system configuration backup and restore

The Data ONTAP System Administration Guide has updated information about the backup and restore of a storage system configuration.

• The section about storage system configuration backup and cloning is amended with the following information:
  When you back up a storage system configuration, the following files are backed up for the storage system and the default vFiler unit (vfiler0):
  – System-specific configuration files, for example, /etc/rc
  – System-specific registry options
  – Volume configuration
  – vfiler0-specific configuration, for example, /etc/quotas, /etc/hosts, /etc/ usermap.cfg, /etc/nsswitch.conf, and /etc/hosts.equiv
  – vfiler0-specific registry options, for example, NFS, CIFS, ndmpd, and NIS
  If you have configured vFiler units, when you back up the configuration of a vFiler unit, the following files in the vFiler unit are backed up:
- vFiler-specific configuration files, for example, /etc/quotas, /etc/hosts, /etc/usermap.cfg, /etc/nsswitch.conf, and /etc/hosts.equiv
- vFiler-specific registry options, for example, NFS, CIFS, ndmpd, and NIS

vFiler configuration is backed up or restored only for the vFiler unit on which the config dump or config restore command is run.

- The section about restoring a storage system configuration is amended with information in Step 3 below:
  1. Enter the following command:
     config restore [-v] config_file
     -v enables you to restore volume-specific configuration files, as well as storage systemspecific configuration files.
  2. Reboot the system to run commands in the /etc/rc file.
  3. If you use quotas for any volumes owned by a non-default vFiler unit (a vFiler unit other than vfiler0), ensure that the quotas are in the desired state (on or off) for those volumes. The quotas state for volumes owned by a non-default vFiler is not restored when you restore a system configuration.

Changes to the instructions on editing the /etc/rc file

The instructions on editing the /etc/rc file in the Data ONTAP System Administration Guide have updated information.

The procedure for editing the /etc/rc file is amended with information in Step 3 below:
  1. Make a backup copy of the /etc/rc file.
  2. Edit the /etc/rc file.

    Note: Do not add CIFS commands to /etc/rc. Doing so can cause problems when the storage system boots if CIFS is not fully initialized or the commands cause deadlocks between the /etc/rc file and CIFS.
  3. Ensure that entries in the /etc/rc file are listed in the following order:
     hostname system_name
     ifgrp commands
     vlan commands
     ifconfig commands
     vfiler commands
     route commands
     [any other commands]
  4. Save the edited file.
  5. Reboot the storage system to test the new configuration.
     If the new configuration does not work as you want, repeat Step 2 through Step 4.
Corrections for root FlexVol volume size requirement

The size requirement for root FlexVol volumes on some systems has changed.

In the section titled Size requirement for root FlexVol volumes in the Data ONTAP System Administration Guide, the table is amended with the following information:

<table>
<thead>
<tr>
<th>Storage system model</th>
<th>Minimum root FlexVol volume size</th>
</tr>
</thead>
<tbody>
<tr>
<td>N6070</td>
<td>40 GB</td>
</tr>
<tr>
<td>N6210</td>
<td>17 GB</td>
</tr>
<tr>
<td>N6240</td>
<td>22 GB</td>
</tr>
<tr>
<td>N6270</td>
<td>44 GB</td>
</tr>
</tbody>
</table>
Changes to the Upgrade Guide

New information about various topics has become available since the previous revision of the Data ONTAP Upgrade Guide.

- Additional preparation for nondisruptive upgrades
- Additional requirement for AT-FCX storage expansion unit firmware upgrades

Additional preparation for nondisruptive upgrades

The procedures in "Preparing for nondisruptive upgrades" have been supplemented with four new steps.

The following steps should be inserted after the existing Step 1 ("Ensure that your HA pair is optimally configured and functioning correctly").

1. Ensure that network ports are up and functioning correctly by entering the following command:
   ```
   ifconfig -a
   ```

   **Example**

   For each interface, you see a display similar to the following:

   ```
   e0a: flags=0x2f4c867<UP,BROADCAST,RUNNING,MULTICAST,TCPCKSUM,LINK_UP>
   mtu 1500
   inet 192.9.200.41 netmask 0xffffff00 broadcast 192.9.200.255
   partner e0a 192.9.200.42
   ether 00:0c:29:56:54:7e (auto-1000t-fd-up) flowcontrol full
   ```

   For each interface that serves data traffic, ensure that each of the following is true:

   a. The interface has a partner that also serves data; that is, the partner is not an e0M or e0P interface.

   b. The link to the partner is up.

   c. The mtu, mediatype, and flowcontrol parameter settings are the same for both partners.

2. If you have edited the /etc/rc file, ensure that entries are listed in the following order:
   ```
   hostname system_name
   ifgrp [commands]
   vlan [commands]
   ifconfig [commands]
   vfiler [commands]
   route [commands]
   [any other commands]
   ```

3. If your systems include e0M management interfaces, ensure that they are serving only management traffic on a dedicated management LAN or that they are configured down.
If an e0M interface is serving management traffic, it should be partnered with another e0M interface.
For more information about e0M configuration, see the *Data ONTAP System Administration Guide*.

4. If your systems include e0P interfaces for controlling SAS disk shelves, ensure that they are connected only to a private ACP network or that they are configured down.
e0P interfaces should not be partnered.
For more information about ACP configuration, see the *Data ONTAP Storage Management Guide*.

**Additional requirement for AT-FCX storage expansion unit firmware upgrades**

The topic "Service availability during storage expansion unit firmware updates" currently lists two requirements for updating AT-FCX storage expansion unit firmware nondisruptively: minimum firmware version and MultiPath Storage configuration. There is an additional requirement that Data ONTAP 7.3.2 or later be running.

The first row of the table should read as follows:

<table>
<thead>
<tr>
<th>Module</th>
<th>Storage expansion unit model</th>
<th>System downtime required?</th>
</tr>
</thead>
<tbody>
<tr>
<td>AT-FCX</td>
<td>EXN1000</td>
<td>With Multipath Storage, firmware version 37, and Data ONTAP 7.3.2 or later: No Without Multipath Storage: Yes</td>
</tr>
</tbody>
</table>

After the table, the AT-FCX information should also be updated to state that you cannot perform a Data ONTAP NDU under the following circumstances:

- AT-FCX disk shelves are attached to your system and one or more of the following is true:
  - You have not verified that the latest AT-FCX firmware version is running.
  - A Data ONTAP release earlier than 7.3.2 is running.
  - AT-FCX version 36 or earlier is running.
  - MultiPath Storage is not configured.
Change to the Gateway Implementation Guide for native storage expansion units

Always check the shipping date of your AT-FCX modules if you are unsure that they meet the disk type requirements.

The Gateway Implementation Guide for Native Storage Expansion Units contains a statement on page 65 that implies you should check the version of AT-FCX modules only if you are moving a storage expansion unit from an N series system to a gateway system. In fact, you should always check the version of the AT-FCX modules if you are unsure if they meet the requirements for disk types that gateway supports. The information on page 65 should read as follows:

Note: Only AT-FCX modules shipped in December 2005 or later are supported. If you are unsure whether your module is the correct version, see the Data ONTAP Active/Active Configuration Guide for the procedure for checking the version of the AT-FCX module.
Array LUN sizing with 2 TB disks is not documented in all Gateway Implementation Guides

Starting with Data ONTAP version 7.3.3, 2 TB drives are supported on arrays configured with gateway systems. These larger drives increase the maximum usable size supported for array LUNs.

Not all of the Gateway Implementation Guides have been updated to include the supported maximum array LUN sizes. To calculate the maximum array LUN sizes supported with the 2 TB drives, double the maximum usable value that is provided for array LUNs with Data ONTAP 7.3.2. The maximum usable values are provided in the "Guidelines for array LUN sizing" section of the Gateway Implementation Guides.
Copyright and trademark information

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

Copyright information

Copyright © 1994 - 2011 NetApp, Inc. All rights reserved. Printed in the U.S.A.

Portions copyright © 2009, 2011 IBM Corporation. All rights reserved.

US Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

No part of this document covered by copyright may be reproduced in any form or by any means, graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system, without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.
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](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:

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.