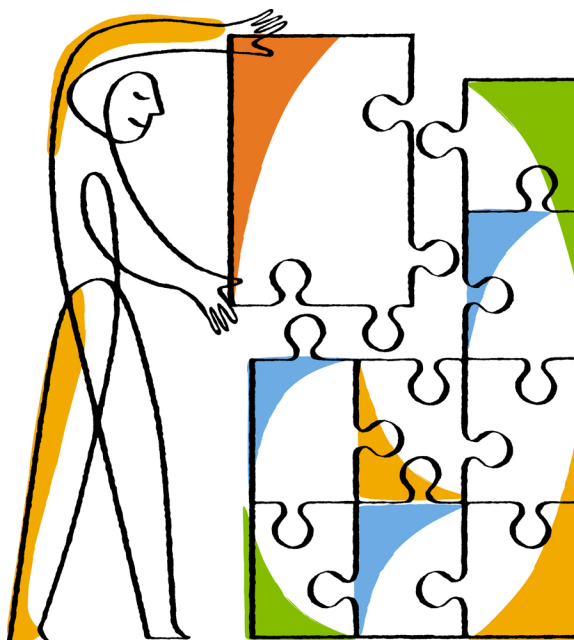




SnapProtect® Management Software 10.0 Service Pack 2B

Release Notes



NetApp, Inc.
495 East Java Drive
Sunnyvale, CA 94089
U.S.

Telephone: +1(408) 822-6000
Fax: +1(408) 822-4501
Support telephone: +1 (888) 463-8277
Web: www.netapp.com
Feedback: doccomments@netapp.com

Part number: 215-07764_A0_ur003
July 2013

Contents

SnapProtect Release Notes	5
SnapProtect Overview	5
New features	6
Important caution	8
Known issues and corrective actions	9
Auxiliary copies of Snapshot copies are not deleted after retention period is complete	9
Browsing and restoring from the primary Snapshot copy by using deferred indexing fails	9
Changing user password in CommCell console fails	10
Differential backup job fails if the database is set to read-only	10
External relationships are imported as two datasets	11
Failed, killed, or cancelled auxiliary job does not delete the provisioned volume ...	11
Full restore of the NFS data from vault destination to the original location (in-place) fails	12
Hyper-V in-place restore fails	12
Incremental snap backup failure for NAS client	12
Indexing fails using GPT-formatted Windows VMDKs	13
SnapProtect backup fails after modifications in vCenter credentials	13
Index processing fails on MediaAgent due to index cache error	14
Metadata collection fails for virtual machine	14
MetroCluster single file restore from a mirror copy fails	15
Mounting Snapshot copies fails if ESX proxy is a part of VMware cluster	15
OSSV backup retry count unaffected by registry key entry	15
Restore operation from a tertiary storage system fails with an internal software error	16
Restore operation triggers two jobs in DataFabric Manager Server	16
SnapProtect backups hang at the scan phase if automount is enabled on Linux Systems	16
SnapMirror tape backup fails	17
SnapMirror tape backup restore window does not display restricted volumes	17
SnapProtect does not back up mount points	17

SnapProtect does not delete relationships automatically when sub-client is deleted	17
SnapProtect updates fail but succeed on retry	18
SQL backup may fail in a clustered environment	18
Virtual machine restore in MS Hyper-V does not restore NICS	18
LUNs manually mounted through Virtual Server Agent get automatically unmounted	19
Known limitations	20
Documentation changes	21
Changes to information about upgrade from SnapProtect 9.0 (any Service Pack) to SnapProtect 10.0 Service Pack 2B	21
Copyright information	22
Trademark information	23
How to send your comments	24

SnapProtect Release Notes

You should read the SnapProtect release notes to learn about new and changed features, known issues and corrective actions, and known limitations in SnapProtect 10.0 Service Pack 2B.

SnapProtect Overview

SnapProtect software is a robust backup and recovery solution that manages Snapshot copies and replication, accelerates backup and recovery speed, and maximizes storage efficiency.

SnapProtect software integrates rapid Snapshot copy technology with a single management console for all your backup, recovery, and replication jobs. It is a complete disk-to-disk-to-tape solution in application-aware or virtualized environments. SnapProtect software manages Snapshot copies on NetApp FAS and V-Series primary storage, replication to FAS and V-Series secondary and tertiary storage, and tape creation. It provides management, storage provisioning, cataloging, and granular recoverability for NetApp application data, file data for NAS, file data in LUNs, and data in virtualized environments.

About the SnapProtect 10.0 Service Pack 2B release:

SnapProtect 10.0 Service Pack 2B is a major release and the first major upgrade of SnapProtect since May 2011. SnapProtect version 10.0 introduces several key features including NAS live browse, deferred indexing, Oracle and SQL database cloning, multi-threaded Virtual Server Agent, block level incremental backups for SnapMirror to tape and many other capabilities.

New features

You should be aware of the new features in SnapProtect 10.0 Service Pack 2B.

- **NAS live browse from Snapshot copies**
SnapProtect enables NAS live browse for browsing and restoring content such as files and folders directly from a NAS Snapshot copy without having to index or catalog the contents of the Snapshot copy. You can specify the Snapshot copy (primary or secondary) from which you can browse and restore files and folders directly.
- **Deferred Indexing**
SnapProtect allows indexing operation to be performed at a later time, thus completely eliminating its impact on production activities. This feature enables decoupling of the backup and indexing processes and provides added flexibility while creating backup schedules. You can specify the Snapshot copy (primary or secondary) on which to perform the indexing.
Note: Browsing and search capability within the catalog is available only after the index is created.
- **Cloning of Microsoft SQL and Oracle databases**
You can clone backups (Snapshot copies) of Microsoft SQL and Oracle databases by using NetApp's efficient volume cloning capability. The cloning operation allows you to duplicate large databases in a short period of time. Once the database is cloned, it can be attached to the same or any existing SQL and Oracle server to perform operations such as test or development and analytics.
- **Multi-threaded Virtual Server Agent (VSA)**
You can take application consistent VMware backups of multiple virtual machines simultaneously to accelerate your backup operations.
- **VMware datastore exclusion from backups**
You can exclude datastores from VMware backups. A common use case for this capability is exclusion of the page files that are stored in a separate datastore and need not be backed up.
- **Extended retention for Snapshot copies**
You can extend the retention period of your backups based on the hourly, daily, weekly, monthly or yearly schedules. This is in addition to the basic retention period available for the backup copies.
- **SnapProtect backup for Oracle on Windows server**
SnapProtect supports backup for Oracle databases deployed on Windows servers. SnapProtect support for Oracle covers different types of database configurations such as file system, ASM, and raw databases.
- **SnapProtect backup for Lotus Notes on Windows platform**
SnapProtect supports backup for Lotus Notes versions 8.0.x and 8.5.x on Windows.
- **Block level incremental backup for SnapMirror tape for 7- Mode**
SnapProtect supports block level incremental backups for SnapMirror to tape operations.
- **Selective Vault Copy**

You can select a particular Snapshot copy for SnapVault backup operations to be performed hourly, daily, weekly, monthly and so on. This feature is applicable for a vault copy only and not applicable for a mirror copy.

- Oracle log management or truncation.

You can perform log truncation or log management when using Oracle with SnapProtect.

For more information about the new features, see [*SnapProtect Books Online- Release Highlights*](#) in Getting Started page.

Important caution

You should be aware of the important caution that affects SnapProtect 10.0 Service Pack 2B.

Upgrade from SnapProtect 9.0 (any Service Pack) to SnapProtect 10.0 Service Pack 2B is not supported. If you want to upgrade from SnapProtect 9.0 (any Service Pack) to SnapProtect 10.0, contact technical support.

A CommServe database configuration check is required before you upgrade from SnapProtect 9.0 to 10.0. Contact technical support using your SnapProtect serial number.

Known issues and corrective actions

You must be familiar with the known issues in SnapProtect 10.0 Service Pack 2B and corrective actions for them.

Auxiliary copies of Snapshot copies are not deleted after retention period is complete

Cause	Snapshot copies are not deleted although the retention period is over. Even though the retention is aged out of the SQL database, the HTTP threads remain high on the storage system and the Snapshot copies will not be deleted.
Corrective action	To resolve this issue, set the OnCommand Unified Manager server option <code>snapDeltaMonitorEnabled</code> to No .

Browsing and restoring from the primary Snapshot copy by using deferred indexing fails

In a backup job running deferred indexing, browsing and restoring from primary Snapshot copy fails.

Cause	If you change the default value of Copy Precedence from 1 to any other number in CommServe, browsing and restoring from the primary Snapshot copy fails for a backup job that is running deferred indexing.
Corrective action	<ul style="list-style-type: none"> • In the CommCell browser, go to the Client Properties of the MediaAgent you want to restore. • Select Advanced. • Go to Additional Settings and select Add. • In the name field, enter RestoreCopyPrecedence. • In the category field, select NAS. • In the type field, select INTEGER. • In the value field, enter the precedence of the copy you want to restore from. To determine the precedence of the copy, go to the Storage Policy Properties and select Copy Precedence.

Changing user password in CommCell console fails

Changing user password in CommCell console fails with the following error message: Received Error: Password Verification Failure for logged in User

Cause While installing SnapProtect, if user password is left blank, changing the password at a later time fails.

Corrective action

1. In Windows command line, use C-drive as the SnapProtect base directory.
For example, `C:\Program Files\NetApp\SnapProtect\Base`
2. Run the following command:**qlogin**
3. Log in with user name as admin.
4. Press **Enter** for the password.
5. Run the following command:**qmodify galaxypassword -u username-p New Password**
For example, **qmodify galaxypassword -u admin -p admin123**

Differential backup job fails if the database is set to read-only

When a differential backup job is performed on a database set to read-only, the backup job fails. The following error message is displayed: Backup chain is broken.

Cause A differential backup job fails if the database is set to read-only mode.

Corrective action

1. Do not set the database to read-only mode.
2. Create sub-clients by clearing the **Disable Log Consistency Check** check box.
To disable log consistency:
 - a. Right-click on the sub-client.
 - b. Select Properties menu.
 - c. Select the SQL Settings tab.
 - d. Select the **Disable Log Consistency Check** checkbox.
3. Run the full and differential backups again.
4. If the same error occurs, select the **Disable Log Consistency Check** checkbox on the sub-client.

5. Run the full and differential backups again.
6. Restore the database and check the same source database content and accessibility.

External relationships are imported as two datasets

External primary-mirror-vault relationships might be imported as two datasets, but should be imported as one relationship under a single datastore.

Cause External primary-mirror-vault relationships should be imported as one relationship under a single dataset. However, if one of the qtrees does not have a SnapVault relationship in the mirror volume, the primary-mirror-vault relationships might be imported as two datasets. For example, the relationship might be imported as one dataset for the primary-mirror relationship and another dataset for the mirror-vault relationship.

Corrective action

1. Manually create a relationship for the qtrees that does not have a SnapVault relationship in the mirror volume.
2. During the import operation, edit the .xml file to combine the SnapVault and SnapMirror relationships into one primary-mirror-vault relationship.
After the import, OnCommand Unified Manager server creates the relationships for the qtrees that do not have a SnapVault relationship in the mirror volume.

Failed, killed, or cancelled auxiliary job does not delete the provisioned volume

SnapProtect creates volumes for vaults and mirror relationships on the destination, resulting in an increase in the number of mark-deleted objects because OnCommand Unified Manager continues to clear the backup and thereby causes the job to continue.

Cause Failed, killed, or cancelled auxiliary jobs are not deleted in the provisioned volume. The job continues to run, attempting to perform the operation without any way to clear the backup from the CommServe instance database or the OnCommand Unified Manager databases.

Corrective action None. You must perform the cleanup manually. The process for cleaning up mark-deleted objects that were discovered but have been marked as deleted by the OnCommand Unified Manager monitor process is manual at this time.

Full restore of the NFS data from vault destination to the original location (in-place) fails

Full restore of the NFS data from the vault destination to the original location (in-place) fails with the following error: `Error while reading pipeline buffer from MediaAgent.`

Cause	When you include <code>.snapshots</code> folder in the browse and restore window during restore of NFS data, full restore of NFS data from vault destination to original location fails.
Corrective action	Use NAS iData agent to backup or restore the NFS mounts points. If Linux iData agent is used to backup the NFS mount points, exclude <code>.snapshots</code> folder selection while performing restore operation.

Hyper-V in-place restore fails

Issue	A Hyper-V in-place restore operation fails.
Cause	This issue occurs because Hyper-V cannot overwrite an existing virtual machine.
Corrective action	Turn off and delete the existing virtual machine, and then restore the virtual machine to the same place.

Incremental snap backup failure for NAS client

Incremental snap backup for primary Snapshot copies might occasionally fail for the NAS client with the error: `UpdateIndex index processing failed.`

Cause	The index is updated during a full backup, resolving the problem. However, this full backup takes some time to process, depending on the total number of files being backed up.
Corrective action	Run the full backup instead of the incremental backup.

Indexing fails using GPT-formatted Windows VMDKs

When Windows VMDKs are GPT formatted, you might be unable to index your backup.

Cause	Windows VMDKs must be MBR formatted.
Corrective action	Reformat the Windows VMDK.

SnapProtect backup fails after modifications in vCenter credentials

When log in credentials for new vCenter is changed, the SnapProtect CommServe database is updated for that vCenter only. The SnapProtect backup fails with logs showing old user name.

Cause	The ESX host has multiple iSCSI initiators, SnapProtect might attempt to use an iSCSI initiator that has no connection to the storage system for indexing.
Corrective action	<p>Create a registry entry value to specify the ESX iSCSI initiator to be used for indexing. This resolves the indexing issue, but the registry entry does not support multiple ESX proxy servers. This registry key is a global value on the MediaAgent.</p> <ul style="list-style-type: none"> • SnapProtect backup location (Windows): HKEY_LOCAL_MACHINE \SOFTWARE\CommVault Systems\Galaxy\Instance<xxx>\iDataAgent • SnapProtect backup location (UNIX): /etc/CommVaultRegistry/Galaxy/Instance<xxx>/iDataAgent/.properties • NetWare: Not Applicable • Key: sSNAP_UseINITIATOR (optional) • Value: iSCSI initiator name; where iSCSI initiator is the name of the host computer. • Value type: String • Value: Valid range not applicable • Default value: None created in client computer • Description : This registry key is used to specify the iSCSI or FC (Fibre Channel) address to be used for snapshots. By default, the value for the FC or iSCSI initiator address will be detected. • Additional Information: N/A • Applies to: SnapProtect Backup

Index processing fails on MediaAgent due to index cache error

The UpdateIndex process fails on a MediaAgent with the following error message: Index processing failed on MediaAgent - this may be due to index cache full or corrupt.

Cause	There is not enough space to accommodate the index cache.
Corrective action	<ol style="list-style-type: none"> 1. On the MediaAgent, run Registry Editor. 2. Create DWORD registry value MediaAgent/nNASFORCEDDELETE. 3. Set value to 1. 4. Run the incremental backup job, and note the Job ID. 5. Remove the registry value. 6. Run another incremental backup job, and note the Job ID. <p>By reverting the registry key, the incremental backup job should complete successfully. By default, deleting the item that was not backed up is treated as an error. The registry key treats the situation as a warning and allows job to proceed.</p>

Metadata collection fails for virtual machine

When the disk cluster size is less than 1024 bytes, metadata collection fails for virtual machines. You can only perform a complete restore for these disks. You cannot browse or perform a file restore.

Cause	When the disk cluster size is less than 1024 bytes, the metadata collection fails.
Corrective action	<ol style="list-style-type: none"> 1. Check the cluster size by using the following command: <pre>fsutil fsinfo ntfs infor x:\</pre> where <i>x</i> is the drive letter or the volume. 2. Run the same command on every volume in the virtual machine. 3. Verify that all volumes are formatted as NTFS partitions.

MetroCluster single file restore from a mirror copy fails

In a MetroCluster environment, a SnapProtect restore job fails in a cluster failover on disaster (CFOD) failover state when restoring a single file from mirrored data to a different location.

Cause	This issue might occur when the following sequence of operations occurs: <ol style="list-style-type: none"> 1. F1 is a stand-alone file server that is the source. 2. File servers F2 and F3 are in a MetroCluster environment and are the destination. 3. The partner file server is taken over in a MetroCluster CFOD failover state. 4. A restore operation of a single file to a different location on SnapProtect fails.
Corrective action	Mount the Snapshot copy and restore manually.

Mounting Snapshot copies fails if ESX proxy is a part of VMware cluster

When Snapshot copies are mounted on the ESX proxy within the VMware cluster, the mounting operation fails.

Cause	When mounting Snapshot copies on an ESX proxy that is not a part of the VMware cluster, the datastore is removed. This happens before the virtual machine releases the VMDK file that is being indexed.
Corrective action	Move the ESX proxy out of the VMware cluster. The ESX proxy must be a stand-alone system.

OSSV backup retry count unaffected by registry key entry

The registry key *nSvRetr* for retry count is not honored for an existing Open Systems SnapVault (OSSV) relationships on a Windows platform.

Cause	OSSV transfers fail after the first retry, even after the retry count is increased using the registry key <i>nSvRetr</i> .
Corrective action	None. Be aware of the behavior when performing an OSSV backup.

Restore operation from a tertiary storage system fails with an internal software error

Issue	An attempt to restore files from a tertiary SnapProtect storage system fails.
Cause	This issue occurs when job-retention settings on the secondary SnapProtect storage system are inadequate.
Corrective action	Add the secondary storage system as a client and set the copy precedence for the restore operation to tertiary.

Restore operation triggers two jobs in DataFabric Manager Server

A SnapProtect restore job in a cluster failover on disaster (CFOD) failover state triggers two restore jobs in the DataFabric Manager Server. However, the data is restored correctly.

Cause	<p>This issue might occur when the following sequence of operations occurs:</p> <ol style="list-style-type: none">1. F1 is a stand-alone file server that is the source.2. File servers F2 and F3 are in a MetroCluster environment and are the destination.3. The partner file server is taken over in a MetroCluster CFOD failover state.4. A SnapProtect restore operation triggers two restore jobs in DataFabric Manager. However, the data is restored correctly.
Corrective action	No corrective action is needed.

SnapProtect backups hang at the scan phase if automount is enabled on Linux Systems

SnapProtect backups of Linux file system using Linux iData Agent hang at the scan phase if automount is enabled.

Cause	Commserve and Linux iData Agent on Linux File System are using different versions.
Corrective action	Disable automount on the Linux system.

SnapMirror tape backup fails

A SnapMirror tape backup from a SnapVault auxiliary copy fails if the volume has multiple qtrees.

Cause	The volume has multiple qtrees.
Corrective action	None. Avoid volumes with multiple qtrees.

SnapMirror tape backup restore window does not display restricted volumes

During a SnapMirror tape backup, the restore window does not list restricted volumes.

Cause	After restricting the volume, the restore window does not display the restricted volumes for the selection.
Corrective action	Manually enter the restore volume path in the restore window.

SnapProtect does not back up mount points

When you back up a volume, SnapProtect does not back up the mount point of the logical volume. For example, if /vol/volA is mounted on /vol, then SnapProtect does not back up the /vol/volA mount point as part of /vol backup.

Cause	The default sub-client on Linux physical boxes do not index the partition (except root).
Corrective action	To back up the mount point of the logical volume, you must create a sub-client for each partition.

SnapProtect does not delete relationships automatically when sub-client is deleted

SnapProtect does not automatically delete the relationships when the sub-client is deleted.

Cause	SnapProtect does not delete relationships automatically because deleting relationships causes backups to get deleted and the customer will not be able to perform a restore at a later time.
Corrective action	SnapProtect does not delete the relationships as part of sub-client deletion. Users must manually delete the relationships.

SnapProtect updates fail but succeed on retry

In a MetroCluster environment, a SnapProtect update job fails in a cluster failover on disaster (CFOD) failover state but succeeds during the automatic retry.

Cause	This issue might occur when the following sequence of operations occurs: <ol style="list-style-type: none">1. F1 is a stand-alone file server that is the source.2. File servers F2 and F3 are in a MetroCluster environment and are the destination.3. The partner file server is taken over in a MetroCluster CFOD failover state.4. A SnapProtect update operation on an existing policy fails.
Corrective action	Enable the retry option on SnapProtect, then start the update job again.

SQL backup may fail in a clustered environment

Cause	Moving or deleting an SQL database in a cluster causes the subsequent backup to fail because the database ID could not be found.
Corrective action	Add the moved or deleted database to the "do not backup" list in the sub-client properties.

Virtual machine restore in MS Hyper-V does not restore NICS

When backing up a virtual machine and restoring it along with the NICS information, the virtual machine is not connected to any network and `.ipconfig` command does not return any result.

Cause	When performing a backup or restore of a virtual machine with NICS information, by default the NICS information is not restored.
Corrective action	See the Books Online Hyper-V Backup Troubleshooting page for detailed instructions.

LUNs manually mounted through Virtual Server Agent get automatically unmounted

When a user manually mounts LUNs on virtual machine through Virtual Server Agent, the LUNs get automatically unmounted if Snap Mining operations are initiated.

Cause When Virtual Server Agent (VSA) is connected to a disk, LUNs that are manually mounted through VSA time out within 10 minutes if no activity is detected. The VSA does not maintain the LUNs beyond the default threshold.

When using Snap Mining for Exchange, VSA either communicates directly to the hardware array using iSCSI or implements a proxy. If a proxy is implemented, it must be a physical machine connected to a FC/iSCSI interface. This leaves Snap Mining operations completely independent of VSA. Therefore, VSA unmounts the LUNs that are mounted manually.

Corrective action LUNs should be mounted automatically when a Snap Mining job is initiated. The LUN will be unmounted once the signal is sent back that the data has been secured.

Known limitations

You should be aware of certain known limitations that affect SnapProtect 10.0 Service Pack 2B.

- The VMware Raw Device Mapping (RDM) support includes the following limitations:
 - RDM data cannot be protected by using the Virtual Server Agent (VSA).
RDM data can only be protected by using a file system or application agent within the guest operating system.
 - RDM can only be configured in physical compatibility modes.
Virtual compatibility modes are not supported.
 - Client must establish iSCSI connection from client to NetApp array as a communications link for creating a Snapshot copy.
Data path links are not supported.
 - Only client direct attached iSCSI is supported.
- Renaming volumes and updating datasets from within SnapProtect is not currently supported.
- Searching for all versions of files that have been backed up is not currently supported.

Documentation changes

You should be aware of the documentation changes or corrections to SnapProtect 10.0 Service Pack 2B.

Changes to information about upgrade from SnapProtect 9.0 (any Service Pack) to SnapProtect 10.0 Service Pack 2B

There are some changes to the existing information about upgrade from SnapProtect 9.0 (any Service Pack) to SnapProtect 10.0 Service Pack 2B in Books Online.

Upgrade from SnapProtect 9.0 (any Service Pack) to SnapProtect 10.0 Service Pack 2B is not supported. If you want to upgrade from SnapProtect 9.0 (any Service Pack) to SnapProtect 10.0, contact technical support.

A CommServe database configuration check is required before you upgrade from SnapProtect 9.0 to 10.0. Contact technical support using your SnapProtect serial number.

Copyright information

Copyright © 1994–2013 NetApp, Inc. All rights reserved. Printed in the U.S.

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. 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

NetApp, the NetApp logo, Network Appliance, the Network Appliance logo, Akorri, ApplianceWatch, ASUP, AutoSupport, BalancePoint, BalancePoint Predictor, Bycast, Campaign Express, ComplianceClock, Cryptainer, CryptoShred, CyberSnap, Data Center Fitness, Data ONTAP, DataFabric, DataFort, Decru, Decru DataFort, DenseStak, Engenio, Engenio logo, E-Stack, ExpressPod, FAServer, FastStak, FilerView, Flash Accel, Flash Cache, Flash Pool, FlashRay, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexSuite, FlexVol, FPolicy, GetSuccessful, gFiler, Go further, faster, Imagine Virtually Anything, Lifetime Key Management, LockVault, Mars, 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, Snap Creator, SnapDirector, SnapDrive, SnapFilter, SnapIntegrator, SnapLock, SnapManager, SnapMigrator, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapSuite, SnapValidator, SnapVault, StorageGRID, StoreVault, the StoreVault logo, SyncMirror, Tech OnTap, The evolution of storage, Topio, VelocityStak, 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.

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 www.ibm.com/legal/copytrade.shtml.

Apple is a registered trademark and QuickTime is a trademark of Apple, Inc. in the United States and/or other countries. Microsoft is a registered trademark and Windows Media is a trademark of Microsoft Corporation in the United States and/or other countries. RealAudio, RealNetworks, RealPlayer, RealSystem, RealText, and RealVideo are registered trademarks and RealMedia, RealProxy, and SureStream are trademarks of RealNetworks, Inc. in the United States and/or other countries.

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

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

NetApp, Inc. NetCache is certified RealSystem compatible.

How to send your comments

You can help us to improve the quality of our documentation by sending us your feedback.

Your feedback is important in helping us to provide the most accurate and high-quality information. If you have suggestions for improving this document, send us your comments by email to doccomments@netapp.com. To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

You can also contact us in the following ways:

- NetApp, Inc., 495 East Java Drive, Sunnyvale, CA 94089 U.S.
- Telephone: +1 (408) 822-6000
- Fax: +1 (408) 822-4501
- Support telephone: +1 (888) 463-8277