About dump engine for FlexVol volumes

ONTAP 9

NetApp
December 14, 2022

This PDF was generated from https://docs.netapp.com/us-en/ontap/tape-backup/data-backup-dump-concept.html on December 14, 2022. Always check docs.netapp.com for the latest.

Table of Contents

About dump engine for FlexVol volumes . . . 1
- About dump engine for FlexVol volumes . . . 1
- How a dump backup works . . . 1
- Types of data that the dump engine backs up . . . 2
- What increment chains are . . . 3
- What the blocking factor is . . . 4
- When to restart a dump backup . . . 4
- How a dump restore works . . . 6
- Types of data that the dump engine restores . . . 6
- Considerations before restoring data . . . 7
- Scalability limits for dump backup and restore sessions . . . 8
- Tape backup and restore support between Data ONTAP operating in 7-Mode and ONTAP . . . 8
- Delete restartable contexts . . . 9
- How dump works on a SnapVault secondary volume . . . 10
- How dump works with storage failover and ARL operations . . . 10
- How dump works with volume move . . . 11
- How dump works when a FlexVol volume is full . . . 12
- How dump works when volume access type changes . . . 12
- How dump works with SnapMirror single file or LUN restore . . . 12
- How dump backup and restore operations are affected in MetroCluster configurations . . . 12

About dump engine for FlexVol volumes

About dump engine for FlexVol volumes

Dump is a Snapshot copy based backup and recovery solution from ONTAP that helps you to back up files and directories from a Snapshot copy to a tape device and restore the backed up data to a storage system.

You can back up your file system data, such as directories, files, and their associated security settings, to a tape device by using the dump backup. You can back up an entire volume, an entire qtree, or a subtree that is neither an entire volume nor an entire qtree.

You can perform a dump backup or restore by using NDMP-compliant backup applications.

When you perform a dump backup, you can specify the Snapshot copy to be used for a backup. If you do not specify a Snapshot copy for the backup, the dump engine creates a Snapshot copy for the backup. After the backup operation is completed, the dump engine deletes this Snapshot copy.

You can perform level-0, incremental, or differential backups to tape by using the dump engine.

After reverting to a release earlier than Data ONTAP 8.3, you must perform a baseline backup operation before performing an incremental backup operation.

Related information

Upgrade, revert, or downgrade

How a dump backup works

A dump backup writes file system data from disk to tape using a predefined process. You can back up a volume, a qtree, or a subtree that is neither an entire volume nor an entire qtree.

The following table describes the process that ONTAP uses to back up the object indicated by the dump path:

Stage	Action
1	For less than full volume or full qtree backups, ONTAP traverses directories to identify the files to be backed up. If you are backing up an entire volume or qtree, ONTAP combines this stage with Stage 2.
2	For a full volume or full qtree backup, ONTAP identifies the directories in the volumes or qtrees to be backed up.
3	ONTAP writes the directories to tape.
4	ONTAP writes the files to tape.
5	ONTAP writes the ACL information (if applicable) to tape.

The dump backup uses a Snapshot copy of your data for the backup. Therefore, you do not have to take the volume offline before initiating the backup.

The dump backup names each Snapshot copy it creates as `snapshot_for_backup.n`, where `n` is an integer starting at 0. Each time the dump backup creates a Snapshot copy, it increments the integer by 1. The integer is reset to 0 after the storage system is rebooted. After the backup operation is completed, the dump engine deletes this Snapshot copy.

When ONTAP performs multiple dump backups simultaneously, the dump engine creates multiple Snapshot copies. For example, if ONTAP is running two dump backups simultaneously, you find the following Snapshot copies in the volumes from which data is being backed up: `snapshot_for_backup.0` and `snapshot_for_backup.1`.

When you are backing up from a Snapshot copy, the dump engine does not create an additional Snapshot copy.

Types of data that the dump engine backs up

The dump engine enables you to back up data to tape to guard against disasters or controller disruptions. In addition to backing up data objects such as a files, directories, qtrees, or entire volumes, the dump engine can back up many types of information about each file. Knowing the types of data that the dump engine can back up and the restrictions to take into consideration can help you plan your approach to disaster recovery.

In addition to backing up data in files, the dump engine can back up the following information about each file, as applicable:

- UNIX GID, owner UID, and file permissions
- UNIX access, creation, and modification time
- File type
- File size
- DOS name, DOS attributes, and creation time
- Access control lists (ACLs) with 1,024 access control entries (ACEs)
- Qtree information
- Junction paths

Junction paths are backed up as symbolic links.

- LUN and LUN clones

  You can back up an entire LUN object; however, you cannot back up a single file within the LUN object. Similarly, you can restore an entire LUN object but not a single file within the LUN.

  The dump engine backs up LUN clones as independent LUNs.

- VM-aligned files

Backup of VM-aligned files is not supported in releases earlier than Data ONTAP 8.1.2.

When a snapshot-backed LUN clone is transitioned from Data ONTAP operating in 7-Mode to ONTAP, it becomes an inconsistent LUN. The dump engine does not back up inconsistent LUNs.

When you restore data to a volume, client I/O is restricted on the LUNs being restored. The LUN restriction is removed only when the dump restore operation is complete. Similarly, during a SnapMirror single file or LUN restore operation, client I/O is restricted on both files and LUNs being restored. This restriction is removed only when the single file or LUN restore operation is complete. If a dump backup is performed on a volume on which a dump restore or SnapMirror single file or LUN restore operation is being performed, then the files or LUNs that have client I/O restriction are not included in the backup. These files or LUNs are included in a subsequent backup operation if the client I/O restriction is removed.

A LUN running on Data ONTAP 8.3 that is backed up to tape can be restored only to 8.3 and later releases and not to an earlier release. If the LUN is restored to an earlier release, then the LUN is restored as a file.

When you back up a SnapVault secondary volume or a volume SnapMirror destination to tape, only the data on the volume is backed up. The associated metadata is not backed up. Therefore, when you try to restore the volume, only the data on that volume is restored. Information about the volume SnapMirror relationships is not available in the backup and therefore is not restored.

If you dump a file that has only Windows NT permissions and restore it to a UNIX-style qtree or volume, the file gets the default UNIX permissions for that qtree or volume.

If you dump a file that has only UNIX permissions and restore it to an NTFS-style qtree or volume, the file gets the default Windows permissions for that qtree or volume.

Other dumps and restores preserve permissions.

You can back up VM-aligned files and the `vm-align-sector` option. For more information about VM-aligned files, see Logical storage management.

What increment chains are

An increment chain is a series of incremental backups of the same path. Because you can specify any level of backup at any time, you must understand increment chains to be able to perform backups and restores effectively. You can perform 31 levels of incremental backup operations.

There are two types of increment chains:

- A consecutive increment chain, which is a sequence of incremental backups that starts with level 0 and is raised by 1 at each subsequent backup.
- A nonconsecutive increment chain, where incremental backups skip levels or have levels that are out of sequence, such as 0, 2, 3, 1, 4, or more commonly 0, 1, 1, 1 or 0, 1, 2, 1, 2.

Incremental backups are based on the most recent lower-level backup. For example, the sequence of backup levels 0, 2, 3, 1, 4 provides two increment chains: 0, 2, 3 and 0, 1, 4. The following table explains the bases of the incremental backups:

Backup order	Increment level	Increment chain	Base	Files backed up
1	0	Both	Files on the storage system	All files in the backup path
2	2	0, 2, 3	Level-0 backup	Files in the backup path created since the level-0 backup
3	3	0, 2, 3	Level-2 backup	Files in the backup path created since the level-2 backup
4	1	0, 1, 4	Level-0 backup, because this is the most recent level that is lower than the level-1 backup	Files in the backup path created since the level-0 backup, including files that are in the level-2 and level-3 backups
5	4	0, 1, 4	The level-1 backup, because it is a lower level and is more recent than the level-0, level-2, or level-3 backups	Files created since the level-1 backup

What the blocking factor is

A tape block is 1,024 bytes of data. During a tape backup or restore, you can specify the number of tape blocks that are transferred in each read/write operation. This number is called the *blocking factor*.

You can use a blocking factor from 4 to 256. If you plan to restore a backup to a system other than the system that did the backup, the restore system must support the blocking factor that you used for the backup. For example, if you use a blocking factor of 128, the system on which you restore that backup must support a blocking factor of 128.

During an NDMP backup, the MOVER_RECORD_SIZE determines the blocking factor. ONTAP allows a maximum value of 256 KB for MOVER_RECORD_SIZE.

When to restart a dump backup

A dump backup sometimes does not finish because of internal or external errors, such as tape write errors, power outages, accidental user interruptions, or internal inconsistency on the storage system. If your backup fails for one of these reasons, you can restart it.

You can choose to interrupt and restart a backup to avoid periods of heavy traffic on the storage system or to avoid competition for other limited resources on the storage system, such as a tape drive. You can interrupt a

long backup and restart it later if a more urgent restore (or backup) requires the same tape drive. Restartable backups persist across reboots. You can restart an aborted backup to tape only if the following conditions are true:

- The aborted backup is in phase IV.
- All of the associated Snapshot copies that were locked by the dump command are available.
- The file history must be enabled.

When such a dump operation is aborted and left in a restartable state, the associated Snapshot copies are locked. These Snapshot copies are released after the backup context is deleted. You can view the list of backup contexts by using the `vserver services ndmp restartable backup show` command.

```
cluster::> vserver services ndmpd restartable-backup show
Vserver     Context Identifier                   Is Cleanup Pending?
----------- ------------------------------------ -------------------
vserver1 330e6739-0179-11e6-a299-005056bb4bc9 false
vserver1 481025c1-0179-11e6-a299-005056bb4bc9 false
vserver2 5cf10132-0179-11e6-a299-005056bb4bc9 false
3 entries were displayed.

cluster::> vserver services ndmpd restartable-backup show -vserver
vserver1 -context-id 330e6739-0179-11e6-a299-005056bb4bc9

                      Vserver: vserver1
            Context Identifier: 330e6739-0179-11e6-a299-005056bb4bc9
                   Volume Name: /vserver1/vol1
           Is Cleanup Pending?: false
            Backup Engine Type: dump
Is Snapshot Copy Auto-created?: true
                     Dump Path: /vol/vol1
   Incremental Backup Level ID: 0
                     Dump Name: /vserver1/vol1
     Context Last Updated Time: 1460624875
               Has Offset Map?: true
                 Offset Verify: true
       Is Context Restartable?: true
              Is Context Busy?: false
                  Restart Pass: 4
              Status of Backup: 2
            Snapshot Copy Name: snapshot_for_backup.1
          State of the Context: 7

cluster::>"
```

How a dump restore works

A dump restore writes file system data from tape to disk using a predefined process.

The process in the following table shows how the dump restore works:

Stage	Action
1	ONTAP catalogs the files that need to be extracted from the tape.
2	ONTAP creates directories and empty files.
3	ONTAP reads a file from tape, writes it to disk, and sets the permissions (including ACLs) on it.
4	ONTAP repeats stages 2 and 3 until all the specified files are copied from the tape.

Types of data that the dump engine restores

When a disaster or controller disruption occurs, the dump engine provides multiple methods for you to recover all of the data that you backed up, from single files, to file attributes, to entire directories. Knowing the types of data that dump engine can restore and when to use which method of recovery can help minimize downtime.

You can restore data to an online mapped LUN. However, host applications cannot access this LUN until the restore operation is complete. After the restore operation is complete, the host cache of the LUN data should be flushed to provide coherency with the restored data.

The dump engine can recover the following data:

- Contents of files and directories
- UNIX file permissions
- ACLs

  If you restore a file that has only UNIX file permissions to an NTFS qtree or volume, the file has no Windows NT ACLs. The storage system uses only the UNIX file permissions on this file until you create a Windows NT ACL on it.

  > If you restore ACLs backed up from storage systems running Data ONTAP 8.2 to storage systems running Data ONTAP 8.1.x and earlier that have an ACE limit lower than 1,024, a default ACL is restored.

- Qtree information

  Qtree information is used only if a qtree is restored to the root of a volume. Qtree information is not used if a qtree is restored to a lower directory, such as `/vs1/vol1/subdir/lowerdir`, and it ceases to be a qtree.

- All other file and directory attributes

- Windows NT streams
- LUNs
  - A LUN must be restored to a volume level or a qtree level for it to remain as a LUN.

    If it is restored to a directory, it is restored as a file because it does not contain any valid metadata.
  - A 7-Mode LUN is restored as a LUN on an ONTAP volume.
- A 7-Mode volume can be restored to an ONTAP volume.
- VM-aligned files restored to a destination volume inherit the VM-align properties of the destination volume.
- The destination volume for a restore operation might have files with mandatory or advisory locks.

  While performing restore operation to such a destination volume, the dump engine ignores these locks.

Considerations before restoring data

You can restore backed-up data to its original path or to a different destination. If you are restoring backed-up data to a different destination, you must prepare the destination for the restore operation.

Before restoring data either to its original path or to a different destination, you must have the following information and meet the following requirements:

- The level of the restore
- The path to which you are restoring the data
- The blocking factor used during the backup
- If you are doing an incremental restore, all tapes must be in the backup chain
- A tape drive that is available and compatible with the tape to be restored from

Before restoring data to a different destination, you must perform the following operations:

- If you are restoring a volume, you must create a new volume.
- If you are restoring a qtree or a directory, you must rename or move files that are likely to have the same names as files you are restoring.

> In ONTAP 9, qtree names support the Unicode format. The earlier releases of ONTAP do not support this format. If a qtree with Unicode names in ONTAP 9 is copied to an earlier release of ONTAP using the `ndmpcopy` command or through restoration from a backup image in a tape, the qtree is restored as a regular directory and not as a qtree with Unicode format.

> If a restored file has the same name as an existing file, the existing file is overwritten by the restored file. However, the directories are not overwritten.

To rename a file, directory, or qtree during restore without using DAR, you must set the EXTRACT environment variable to `E`.

Required space on the destination storage system

You require about 100 MB more space on the destination storage system than the amount of data to be restored.

> The restore operation checks for volume space and inode availability on the destination volume when the restore operation starts. Setting the FORCE environment variable to `Y` causes the restore operation to skip the checks for volume space and inode availability on the destination path. If there is not enough volume space or inodes available on the destination volume, the restore operation recovers as much data allowed by the destination volume space and inode availability. The restore operation stops when there is no more volume space or inodes left.

Scalability limits for dump backup and restore sessions

You must be aware of the maximum number of dump backup and restore sessions that can be performed simultaneously on storage systems of different system memory capacities. This maximum number depends on the system memory of a storage system.

The limits mentioned in the following table are for the dump or restore engine. The limits mentioned in the scalability limits for NDMP sessions are for the NDMP server, which are higher than the engine limits.

System memory of a storage system	Total number of dump backup and restore sessions
Less than 16 GB	4
Greater than or equal to 16 GB but less than 24 GB	16
Greater than or equal to 24 GB	32

> If you use `ndmpcopy` command to copy data within storage systems, two NDMP sessions are established, one for dump backup and the other for dump restore.

You can obtain the system memory of your storage system by using the `sysconfig -a` command (available through the nodeshell). For more information about using this command, see the man pages.

Related information

Scalability limits for NDMP sessions

Tape backup and restore support between Data ONTAP operating in 7-Mode and ONTAP

You can restore data backed up from a storage system operating in 7-Mode or running ONTAP to a storage system either operating in 7-Mode or running ONTAP.

The following tape backup and restore operations are supported between Data ONTAP operating in 7-Mode and ONTAP:

- Backing up a 7-Mode volume to a tape drive connected to a storage system running ONTAP
- Backing up an ONTAP volume to a tape drive connected to a 7-Mode system
- Restoring backed-up data of a 7-Mode volume from a tape drive connected to a storage system running ONTAP
- Restoring backed-up data of an ONTAP volume from a tape drive connected to a 7-Mode system
- Restoring a 7-Mode volume to an ONTAP volume

```
-   A 7-Mode LUN is restored as a LUN on an ONTAP volume.
-   You should retain the ONTAP LUN identifiers when
restoring a 7-Mode LUN to an existing ONTAP LUN.
```

- Restoring an ONTAP volume to a 7-Mode volume

An ONTAP LUN is restored as a regular file on a 7-Mode volume.

Delete restartable contexts

If you want to start a backup instead of restarting a context, you can delete the context.

About this task

You can delete a restartable context using the `vserver services ndmp restartable-backup delete` command by providing the SVM name and the context ID.

Steps

1. Delete a restartable context:

   `vserver services ndmp restartable-backup delete -vserver *vserver-name* -context -id *context_identifier*`.

```
cluster::> vserver services ndmpd restartable-backup show
Vserver     Context Identifier                   Is Cleanup Pending?
----------- ------------------------------------ -------------------
vserver1    330e6739-0179-11e6-a299-005056bb4bc9 false
vserver1    481025c1-0179-11e6-a299-005056bb4bc9 false
vserver2    5cf10132-0179-11e6-a299-005056bb4bc9 false
3 entries were displayed.

cluster::>
cluster::> vserver services ndmp restartable-backup delete -vserver
vserver1 -context-id 481025c1-0179-11e6-a299-005056bb4bc9

cluster::> vserver services ndmpd restartable-backup show
Vserver     Context Identifier                   Is Cleanup Pending?
----------- ------------------------------------ -------------------
vserver1    330e6739-0179-11e6-a299-005056bb4bc9 false
vserver2    5cf10132-0179-11e6-a299-005056bb4bc9 false
3 entries were displayed.

cluster::>"
```

How dump works on a SnapVault secondary volume

You can perform tape backup operations on data that is mirrored on the SnapVault secondary volume. You can back up only the data that is mirrored on the SnapVault secondary volume to tape, and not the SnapVault relationship metadata.

When you break the data protection mirror relationship (`snapmirror break`) or when a SnapMirror resynchronization occurs, you must always perform a baseline backup.

How dump works with storage failover and ARL operations

Before you perform dump backup or restore operations, you should understand how these operations work with storage failover (takeover and giveback) or aggregate relocation (ARL) operations. The `-override-vetoes` option determines the behavior of dump engine during a storage failover or ARL operation.

When a dump backup or restore operation is running and the `-override-vetoes` option is set to `false`, a user-initiated storage failover or ARL operation is stopped. However, if the `-override-vetoes` option is set to `true`, then the storage failover or ARL operation is continued and the dump backup or restore operation is aborted. When a storage failover or ARL operation is automatically initiated by the storage system, an active dump backup or restore operation is always aborted. You cannot restart dump backup and restore operations even after storage failover or ARL operations complete.

Dump operations when CAB extension is supported

If the backup application supports CAB extension, you can continue performing incremental dump backup and restore operations without reconfiguring backup policies after a storage failover or ARL operation.

Dump operations when CAB extension is not supported

If the backup application does not support CAB extension, you can continue performing incremental dump backup and restore operations if you migrate the LIF configured in the backup policy to the node that hosts the destination aggregate. Otherwise, after the storage failover and ARL operation, you must perform a baseline backup prior to performing the incremental backup operation.

For storage failover operations, the LIF configured in the backup policy must be migrated to the partner node.

Related information

ONTAP concepts

High Availability

How dump works with volume move

Tape backup and restore operations and volume move can run in parallel until the final cutover phase is attempted by the storage system. After this phase, new tape backup and restore operations are not allowed on the volume that is being moved. However, the current operations continue to run until completion.

The following table describes the behavior of tape backup and restore operations after the volume move operation:

If you are performing tape backup and restore operations in the…	Then…
storage virtual machine (SVM) scoped NDMP mode when CAB extension is supported by the backup application	You can continue performing incremental tape backup and restore operations on read/write and read-only volumes without reconfiguring backup policies.
SVM-scoped NDMP mode when CAB extension is not supported by the backup application	You can continue performing incremental tape backup and restore operations on read/write and read-only volumes if you migrate the LIF configured in the backup policy to the node that hosts the destination aggregate. Otherwise, after the volume move, you must perform a baseline backup before performing the incremental backup operation.

When a volume move occurs, if the volume belonging to a different SVM on the destination node has the same name as that of the moved volume, then you cannot perform incremental backup operations of the moved volume.

Related information

How dump works when a FlexVol volume is full

Before performing an incremental dump backup operation, you must ensure that there is sufficient free space in the FlexVol volume.

If the operation fails, you must increase the free space in the Flex Vol volume either by increasing its size or by deleting the Snapshot copies. Then perform the incremental backup operation again.

How dump works when volume access type changes

When a SnapMirror destination volume or a SnapVault secondary volume changes state from read/write to read-only or from read-only to read/write, you must perform a baseline tape backup or restore operation.

SnapMirror destination and SnapVault secondary volumes are read-only volumes. If you perform tape backup and restore operations on such volumes, you must perform a baseline backup or restore operation whenever the volume changes state from read-only to read/write or from read/write to read-only.

Related information

ONTAP concepts

How dump works with SnapMirror single file or LUN restore

Before you perform dump backup or restore operations on a volume to which a single file or LUN is restored by using SnapMirror technology, you must understand how dump operations work with a single file or LUN restore operation.

During a SnapMirror single file or LUN restore operation, client I/O is restricted on the file or LUN being restored. When the single file or LUN restore operation finishes, the I/O restriction on the file or LUN is removed. If a dump backup is performed on a volume to which a single file or LUN is restored, then the file or LUN that has client I/O restriction is not included in the dump backup. In a subsequent backup operation, this file or LUN is backed up to tape after the I/O restriction is removed.

You cannot perform a dump restore and a SnapMirror single file or LUN restore operation simultaneously on the same volume.

How dump backup and restore operations are affected in MetroCluster configurations

Before you perform dump backup and restore operations in a MetroCluster configuration, you must understand how dump operations are affected when a switchover or switchback operation occurs.

Dump backup or restore operation followed by switchover

Consider two clusters: cluster 1 and cluster 2. During a dump backup or restore operation on cluster 1, if a switchover is initiated from cluster 1 to cluster 2, then the following occurs:

- If the value of the `override-vetoes` option is `false`, then the switchover is aborted and the backup or restore operation continues.
- If the value of the option is `true`, then the dump backup or restore operation is aborted and the switchover continues.

Dump backup or restore operation followed by switchback

A switchover is performed from cluster 1 to cluster 2 and a dump backup or restore operation is initiated on cluster 2. The dump operation backs up or restores a volume that is located on cluster 2. At this point, if a switchback is initiated from cluster 2 to cluster 1, then the following occurs:

- If the value of the `override-vetoes` option is `false`, then the switchback is cancelled and the backup or restore operation continues.
- If the value of the option is `true`, then the backup or restore operation is aborted and the switchback continues.

Dump backup or restore operation initiated during a switchover or switchback

During a switchover from cluster 1 to cluster 2, if a dump backup or restore operation is initiated on cluster 1, then the backup or restore operation fails and the switchover continues.

During a switchback from cluster 2 to cluster 1, if a dump backup or restore operation is initiated from cluster 2, then the backup or restore operation fails and the switchback continues.

Copyright information

Copyright © 2022 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.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.