Technical Report

Backup and Recovery of IBM Rational ClearCase on NetApp Data ONTAP Operating in Cluster-Mode

Agnes Jacob, NetApp, and Michael Donati, IBM Rational
February 2012 | TR-4041

ABSTRACT

This technical report describes in detail the way to backup and recover IBM® Rational® ClearCase® data on NetApp® clustered storage solutions. It provides information on the critical ClearCase data that is important to protect and some basic procedures to perform backup and recovery. It also discusses a strategy to use for catastrophic events.

TABLE OF CONTENTS

LIST OF FIGURES

1 INTRODUCTION

IBM Rational ClearCase is a change and configuration management application that provides engineering development teams with the ability to manage and track versions of all types of files and directories used in software development. Key features of Rational ClearCase include version control, workspace and build management, and process configurability.

Data protection of ClearCase main repositories that store a company's intellectual property is important to the success of software development companies. It can be very costly when critical data that has been developed for months is lost due to user error, hardware, or catastrophic failure,

NetApp Data ONTAP® software operating in Cluster-Mode provides data protection solutions that eliminate or minimize data loss and keep ClearCase main repositories safe. NetApp Snapshot™ technology enables backups to be performed in minutes, reducing backup windows. Another benefit of quick backups is that they can be done frequently, enabling much more aggressive recovery point objectives (RPOs). NetApp SnapMirror® solutions simplify disaster recovery via an easy-to-implement and robust mirroring solution. Implementing NetApp SnapMirror significantly reduces risks for an organization and protects ClearCase data in the event of a catastrophic event.

1.1 SCOPE

This document is intended for use by individuals responsible for the backup and recovery of Rational ClearCase data on NetApp Cluster-Mode storage. It assumes that readers have experience with administration of NetApp Cluster-Mode solutions and IBM Rational ClearCase. It also assumes that the reader has read the following document for an understanding of ClearCase architecture and deployment options on NetApp Cluster-Mode storage: TR-4032: Deployment and Implementation Guide: IBM Rational ClearCase on NetApp Data ONTAP Operating in Cluster-Mode.

ClearCase data can be deployed on any NetApp storage protocol, including FC, iSCSI, NFS, CIFS, and even a hybrid configuration in which the database is on SAN and source pools are on NAS (only for VOBS in a UNIX® environment). This document provides methods and procedures for protecting ClearCase data on each of these storage protocols.

2 CRITICAL CLEARCASE DATA TO PROTECT

The most critical data to protect and preserve is in the ClearCase main repository, which is referred to as the Version Object Base (VOB). It contains all the files, directories, and metadata associated with the software development projects. The Views and registry data can be recreated; however, it is advisable to protect this data to save time in reconstruction. This section describes the contents of these repositories.

2.1 VERSION OBJECT BASE (VOB) STORAGE

The most important ClearCase component to back up is the Version Object Base, which is the central repository that contains all the files and directories under version control and the metadata associated with them. The VOB directory (.vbs) is comprised of the following components:

- Database (db)—A flat file database (based on Raima) that holds the metadata information for files and directories that are stored in the pools
- Source pool (s)—A pool that holds all versions of any file stored in the VOB
- Cleartext pool (c)—An internal cache of the most recently accessed versions of any text file in the VOB
- Derived pools (d)—These hold the binary files (usually the output of the build process using the clearmake tool) in the cache directory that allows files to be shared by multiple developers

Data loss must be kept to an absolute minimum for the VOB. Since developers need access to VOB data 24/7, the time it takes for backup and recovery should be short. The VOB database must be locked prior to backup and unlocked afterward. During the VOB lock, developers have only read access. Individual files within the VOB should never be recovered independently. All files within the VOB storage area must be recovered as a unit.

2.2 VIEW STORAGE

The View is a private developer workspace that is used to access the artifacts stored in the VOB. The contents of views, unlike that of VOBs, can usually be reconstructed easily and thus it is optional to back up views. However, regular backups of views can still be important, especially if users are not in the habit of checking in their work regularly to the main VOB repository. The View directory (*.vws) is composed of the following:

- Database (db)—ClearCase internal information
- View-private files (.s)—Checked-out files, unshared derived objects, and temporary files
- Configuration specification (config_spec)—Configuration specification file that contains rules related to the versions of the files that developers see or access in their workspace

2.3 REGISTRY

The ClearCase Registry contains information relating to the VOBs, Views, and client instances. It is a directory that holds flat files like vob_tag, vob_object, view_tag, and view_object. It does not reside on the NetApp storage system; however, it is advisable to create backups of these files. When there are numerous VOBs, Views, and client instances, it can be time consuming and difficult to recreate the registry.

3 NETAPP DATA PROTECTION SOLUTIONS

NetApp's data protection solutions provide ClearCase customers with a simplified and quick approach to backing up and recovering critical ClearCase data. These solutions were designed to improve the overall operational efficiency of backup and recovery.

3.1 NETAPP SNAPSHOT TECHNOLOGY

NetApp Snapshot technology provides the foundation for NetApp storage backup and recovery solutions like SnapRestore® and SnapMirror technologies. The NetApp WAFL® file system can copy versions of itself at a point in time. Each copy is referred to as a Snapshot copy. A NetApp Snapshot copy requires minimal disk space since it only maintains and copies the set of pointers to disk blocks containing the data and not the actual copy of the data blocks. Since Snapshot copies are copies of pointers to disk blocks, they can be created quickly. As a result, VOB lockout times are reduced. Snapshot copies are created at a volume level, and each volume has a .snapshot directory that is accessible and viewable by NFS and CIFS users. For the internals of NetApp Snapshot technology, please refer to the "Data ONTAP Cluster-Mode Data Protection Guide" for your particular release on the NetApp Support (NOW) site.

3.2 SNAPMIRROR

Having a disaster recovery site to protect ClearCase data minimizes data loss in the event of a catastrophic event at a main site. The NetApp Cluster-Mode SnapMirror solution creates an identical second set of data capable of replacing the primary set of ClearCase data if something happens to the primary. In addition, the solution is built on a replication engine that provides a more robust, scalable, and higher-performing data copy infrastructure. SnapMirror utilizes Snapshot technology by replicating the

image copy **asynchronously** from the source volume to the destination volume. There are two types of data protection mirrors:

- **Intracluster**—Mirrors within a cluster
- **Intercluster**—Mirrors to a different cluster in a different location

Intercluster SnapMirror should be used for disaster recovery of ClearCase data for greater protection. It provides a failover and giveback solution for volumes residing on different clusters. This type of solution protects against hardware failures, data center or floor failures, and site failures.

3.3 SNAPDRIVE

The NetApp SnapDrive® solution not only simplifies provisioning clustered storage but provides consistent Snapshot copies when backing up the file system. SnapDrive is available in Windows® and UNIX environments. It eases data backup so that data can be easily recovered if it is deleted or lost due to a failure. It uses Snapshot technology to create an image of the data on NetApp storage attached to the host.

3.4 TAPE BACKUP

NetApp's tape backup and restore solution uses Network Data Management Protocol (NDMP) versions 3 and 4, which efficiently maximize network bandwidth. NDMP-enabled commercial backup applications can be used to perform a dump backup or restore of ClearCase data. Protecting ClearCase data using NetApp's tape backup and restore solution is a Snapshot copy–based backup to tape. NetApp Cluster-Mode supports a dump engine for tape backup of an entire volume, an entire qtree or subtree, files, directories, and associated ACL information. It supports full and incremental backups.

4 BACKUP AND RECOVERY OF CLEARCASE DATA

Depending on the deployment of ClearCase on NetApp, backup steps will vary. But in all configurations, backup requires first locking the VOB, taking the Snapshot copy either through "snap create" or SnapDrive, and then unlocking the VOB. For backup of ClearCase views, there is no ClearCase locking mechanism to temporarily prevent users or developers from writing into the volumes. However, when using NetApp SnapDrive, SnapDrive locks the file system prior to taking the Snapshot copy so that no writes are lost.

When planning for backup and recovery there are two objectives to consider:

- Recovery Point Objective (RPO)—The amount of acceptable data loss
- Recovery Time Object (RTO)—The amount of time it takes to perform the recovery

Your criteria for the above objectives will depend on the type of backup and recovery you select:

- Online daily disk backups
- Tape backups
- Mirror disk backups

The next sections go through the procedures for online daily disk backup and restore of both ClearCase VOBs and Views. As for mirror disk backups and restores using SnapMirror, see the technical report called "TR-3999: SnapMirror Startup Guide for Data ONTAP 8.1 Operating in Cluster-Mode." It provides instructions for setting up SnapMirror relationships in NetApp Cluster-Mode, and thus this document does not cover these procedures. For detailed information on SnapMirror, please refer to the "Data ONTAP Cluster-Mode Data Protection Guide" for your particular release on the NetApp Support (NOW) site.

5 DATA LAYOUT CONSIDERATIONS

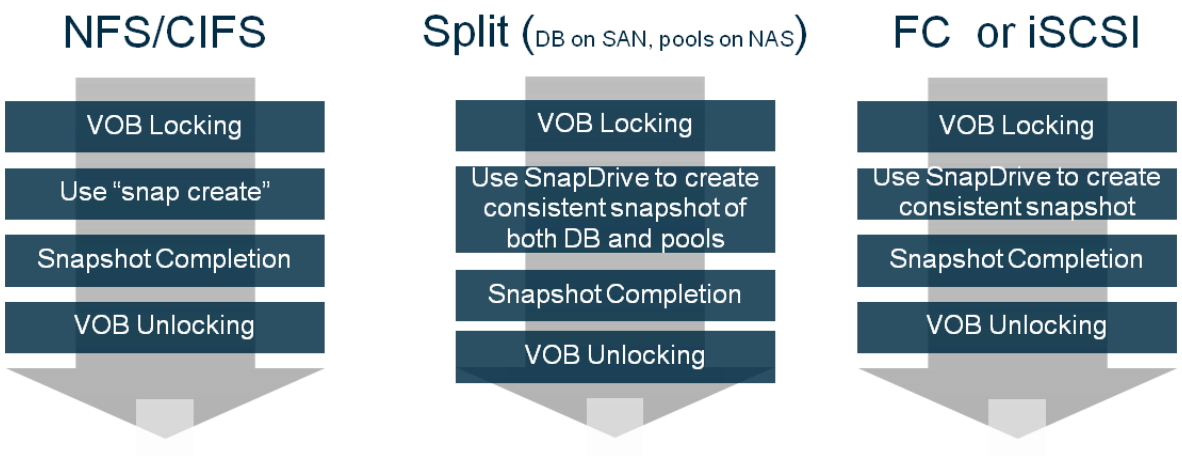
Data layout must be considered in order to have a good backup and recovery strategy. Create and lay out volumes with recovery and manageability in mind. Data layout considerations include the following.

- Use separate volumes for ClearCase VOB and View storage except when the VOBs are interdependent. Backups and restores are performed at a volume level. If all VOBs or Views were placed on one volume and only one of the VOBs or Views was corrupted, it would require all VOBs or Views residing in the volume to be restored together. It is unlikely that all VOBs or Views will be corrupted at the same time.
- For interdependent, administrative, and hyperlinked VOBs, place these related VOBs in one volume or create qtrees for each VOB. In some ClearCase environments, there may be interdependent, administrative, and hyperlinked VOBs. For instance, a VOB might be part of a group of VOBs that are connected by hyperlinks. Also, if Unified Change Management (UCM) VOBs and Rational ClearQuest (a bug-tracking tool) are in use, the databases of ClearCase and ClearQuest are likely to hold references to each other. The data and relationships of multiple related databases can be changed using operations such as join a project, make an activity, and deliver or rebase a stream. In addition, changes in Administrative VOB hierarchy, like creating a global type, can affect multiple VOBs with a single operation. Thus in these scenarios, NetApp advises placing the related VOBs into one volume or creating qtrees within one volume such that they can be locked and the backup and restore are consistent.

6 ONLINE DAILY DISK BACKUP AND RESTORE PROCEDURES

Depending on the deployment of ClearCase on NetApp, backup steps will vary. But all configurations require first locking the VOB, then taking the Snapshot copy either through “snap create” or SnapDrive, and then unlocking the VOB.

Figure 1) Backup procedure depending on deployment.



Restore procedures require stopping the ClearCase services, selecting which Snapshot copy to restore, and then restoring a Snapshot copy using SnapRestore or SnapDrive. The next subsections take you through the basic commands to perform backup and recovery on each type of deployment for an entire VOB or View stored on a volume. The ClearCase procedures and commands that are used in the next section are documented in the “ClearCase Administrator’s Manual.” NetApp assumes that readers have

some basic knowledge of ClearCase procedures and thus details of these procedures are not covered here.

6.1 BACKUP PROCEDURES

BACKUP OF VOB DEPLOYED ON NAS

Basic steps to perform a backup of VOBs deployed on NAS:

1) Get list of VOBs on VOB server:

   cleartool lsvob

2) Lock VOBs on VOB server:

   cleartool lock vob:<vobname>

3) Create Snapshot copy:

   snap create –vserver <vserver_name> -volume <vol_name> -snapshot <snapname>

4) Unlock VOB.

These steps can all be done via script. In order to have this set of commands within a script, one would need to have ssh access to the NetApp storage system without a password. In order to be able to ssh onto a NetApp system without a password, create an SSH public key on the server host and paste on the public key for the cluster Vserver and admin user. In UNIX, create an “admin” user and “admin” ssh onto the NetApp system. When the admin user first uses ssh on a NetApp system, a Digital Signature Algorithm (DSA) key is generated and placed in the home directory of the admin user performing the ssh, ~/.ssh/filename.pub. Copy and paste the key from this file using the following command:

```
cl_agnes_cmode::> security login publickey create –vserver
<Vserver_name> -username admin –index 0 –publickey <public_key>
```

After you successfully ssh onto the NetApp system without a password, you can use a script that parses the output of cleartool lsvob to lock the VOB and create a Snapshot copy of the volume holding the VOB and then unlock it. Please refer to the “Secure Administration Guide” on the NOW site to see how to create other users for administration.

BACKUP OF VOB DEPLOYED ON FC OR iSCSI USING SNAPDRIVE

SnapDrive is required to back up VOBs deployed on SAN in order to flush the host operating system buffers to storage and create a consistent Snapshot copy. For comprehensive instructions, please refer to the “SnapDrive for UNIX Guide” or the “SnapDrive for Windows Guide” on the NOW site. Following are quick steps to back up VOBs using SnapDrive on UNIX. We assume that the vsadmin user and the network interfaces for FC or iSCSI have been properly configured in Cluster-Mode.

SnapDrive Setup

1. Download and install the latest release of SnapDrive for UNIX from the NetApp Support site to the server hosts. Refer to the “SnapDrive for UNIX Guide” for complete instructions on how to install.
2. On the storage, set up the aggregate list:

   vserver modify -vserver test2 -aggr-list aggr_test

   vserver show -fields aggregate,aggr-list -vserver test2

   vserver aggregate aggr-list
   ------- --------- ---------

test2 aggr_test aggr_test

3. Get the logical interface IP addresses for the test2_mgmt:

```
cl_agnes_cmode::> net int show -vserver test2
 (network interface show)
        Logical   Status    Network          Current      Current Is
Vserver     Interface  Admin/Oper Address/Mask      Node         Port    Home
-----------     ----------      ---------- -  -----------------        -----------   ------- ----
test2
        test2_isan09 up/up    172.31.8.243/24    fas3170c-svl09 e4a     true
        test2_isan10 up/up    172.31.8.244/24    fas3170c-svl10 e4a     true
        test2_isan11 up/up    172.31.8.245/24    fas3170c-svl11 e4a     true
        test2_isan12 up/up    172.31.8.246/24    fas3170c-svl12 e4a     true
        test2_lif       up/up    172.31.8.241/24    fas3170c-svl09 e4a     false
        test2_mgmt   up/up    172.31.8.242/24    fas3170c-svl09 e4a     false
6 entries were displayed.
```

ON THE VOB SERVER:

4. Modify the snapdrive.conf file in the /opt/NetApp/snapdrive directory with the following settings:

```
use-https-to-filer="off"
multipathing-type="NativeMPIO"
enable-alua="on"
```

5. SnapDrive requires use of names instead of IP addresses. Thus, add in /etc/hosts for the IP address of the logical interfaces for the management IP address for the iSCSI management logical interface. For this example, it is set up to be test2_mgmt.

```
        # cat /etc/hosts | grep test2
172.31.8.242    test2
```

6. Configure snapdrive with test2 as the appliance name and enter the password for the vsadmin setup on the NetApp system:

```
# snapdrive config set vsadmin test2
        # snapdrive config list
        username    appliance name   appliance type
        ----------------------------------------
        vsadmin     test2          StorageSystem
```

7. Configure the management path:

   # snapdrive config set –mgmtpath test2 test2

   # snapdrive config list –mgmtpath

   system name management interface datapath interface

   ---

   test2 172.31.8.242 172.31.8.242

8. Once SnapDrive is configured, it can be used to create luns as well as create Snapshot copies of luns. In the following example, /lun2 is the NetApp lun and test2_snap4 is the name of the Snapshot copy.

   # snapdrive snap create -fs /lun2 -snapname test2_snap4

   To validate snapshot has been created on filer execute:

   cl_agnes_cmode::> snap show -vserver test2 -volume test2_vol

   ---Blocks---

   Vserver Volume Snap Size Total% Used%

   -------- ------- ---------- ------ -----

   test2 test2_vol test2_snap4 104KB 1% 43%

BACKUP OF VOB DEPLOYED ON HYBRID CONFIGURATION (DB ON SAN, POOLS ON NAS)

In order to back up a VOB deployed on a hybrid configuration, SnapDrive is required. In this scenario, take the previous steps for backing up FC and iSCSI and add the logical interface IP address of the data path to /etc/hosts and to the snapdrive config set.

Additional Steps

1. Edit /etc/hosts and add the IP address of the NAS logical interface for the data:

   # cat /etc/hosts | grep test2_nas

   172.31.8.241 test2_nas

2. Add test2, which is the management logical interface for iSCSI and test_nas to be part of the management path:

   snapdrive config set –mgmtpath test2 test2

   snapdrive config set –mgmtpath test2 test2_nas

   snapdrive config list –mgmtpath

   system name management interface datapath interface

   ---

   test2 172.31.8.242 172.31.8.242|172.31.8.241

3. When initiating the `snapdrive snap create` command, specify the file system of the VOB residing on the lun (/lun2) and on the NAS volume (/mnt/test):

   snapdrive snap create -unrelated -fs /lun2 /mnt /test -snapname test2_snap4

VIEW BACKUP

As previously mentioned, there is no ClearCase locking mechanism for Views that is similar to the VOBs'. However, SnapDrive can be used to facilitate the locking of the file system. SnapDrive as described in the

previous section can be used in a similar way for both SAN and NAS deployments of Views. It just requires specifying the file system drive letter or mount point to initiate the backup. If you do not need to protect all the data in the views, then you can do a simple `snap create` of the volume without using SnapDrive.

REGISTRY BACKUP

For backup of registry files and client_list.db, the directory can be zipped or simply copied to the SAN or NAS volume and backed up with the VOB or View. A cron job or Windows scheduler can be used to periodically copy these files to the appropriate directory or file system that resides on the SAN or NAS volume. It is best to add the zip of the registry and client list after you lock the VOBs.

6.2 RESTORE PROCEDURES

VOB RESTORE

The VOB restore uses Data ONTAP restore procedures and NOT the vob_restore provided with ClearCase. NetApp recommends shutting down the ClearCase services when doing a restore. In the following steps, vobstg is the name of the mount point of the volume, which in this example is an NFS volume. For VOBs deployed on SAN, the steps are the same; however, the mount command mounts the SAN volume instead of the NFS volume.

Steps to Restore

On the VOB server:

1. Shut down the ClearCase services on the VOB server:

   /opt/rational/clearcase/etc/clearcase stop

2. Unmount the volume of the VOB on the VOB server:

   # umount /vobstg

3. On the storage, get a list of the Snapshot copies that are available for restoring for the particular Vserver and volume that have the VOB data:

   cl_agnes_cmode::> snap show -vserver test2 -volume test2_vol

4. Use SnapRestore to restore the desired volume. The restore requires the advanced privilege level or higher:

   cl_agnes_cmode::> set -privilege advanced

   Warning: These advanced commands are potentially dangerous; use them only when

   directed to do so by NetApp personnel.

   Do you want to continue? {y|n}: y

   cl_agnes_cmode::*> volume snapshot promote -vserver test2 -volume test2_vol –snapshot test2_snap4

5. Remount the NFS volume on the VOB server:

   mount test2:/test2_vol /vobstg

6. Restart the ClearCase services on the VOB server:

   /opt/rational/clearcase/etc/clearcase start

Another option for restoring the VOB when the VOB is deployed on a NAS volume (NFS or CIFS) is to “cd” into the “.snapshot” directory of the mounted volume and copy the desired VOB directory (.vbs) to the

desired location. This option also requires that the ClearCase services be shut down and restarted during and after copying.

VIEW RESTORE

For a View deployed on a NAS volume, it is possible to restore individual files. It just requires going into the desired ".snapshot" directory on the server host and copying the file into the desired location. If the entire volume needs to be restored, do the following:

1. Unmount the volume on the View server host.
2. Select the desired Snapshot copy.
3. Use SnapRestore to do the restore on the storage.
4. Remount the restored volume.

For a View deployed on a LUN, restoring individual files requires using the lun clone of the Snapshot copy, mounting the clone on the server host, and copying the file to the desired location. If the entire lun needs to be restored, then use SnapDrive to restore the lun.

REGISTRY RESTORE

To restore the registry:

1. Shut down the ClearCase services on the registry server.
2. Mount the NAS volume on the registry server and "cd" to the .snapshot directory. Select the snapshot directory of files to restore.
3. Copy the registry files into the rgy directory.
4. Restart the ClearCase services on the registry server.

For registry files stored on a LUN, use a lun clone or use FlexClone® technology to clone the Snapshot copy, then mount the clone and copy the registry files into the rgy directory.

6.3 SNAPSHOT SCHEDULES

When volumes are created, Snapshot copy schedules are set up by default to automatically take hourly, weekly, and monthly Snapshot copies. Since locking and unlocking the VOB is required to back up a ClearCase VOB, the default scheduled snapshot policy should be disabled in one of the following ways.

- When the volume is created, set the snapshot-policy option to none. For example:

  vol create –vserver test –volume test_vol –aggregate aggr_test –size 20MB –state online –type RW –snapshot-policy none

- Modify the volume snapshot policy to none. For example:

  vol modify –vserver test –volume test_vol –snapshot-policy none

After the snapshot policy has been disabled on the storage, scripts to back up VOBs on the server host can be added to the cron job or Windows scheduler to periodically back up ClearCase VOBs.

7 TAPE BACKUP AND RESTORE

It is important in a ClearCase environment to minimize the backup window so that developers are not disrupted for a long period of time. Thus, it is necessary to keep locking of ClearCase VOB data at a minimum. Tape backups can take a longer time than disk backups, so NetApp recommends doing an offline tape backup of the Snapshot copy of the ClearCase data or volumes instead of an online tape backup. Performing tape backups of ClearCase data has some advantages, including:

- Tapes can be archived for a longer period of time.
- Tapes can be archived in a more secure location (such as underground vaults) than any machine.
- ClearCase data is stored in a stable physical medium. Having tape backups has some advantages.

NetApp tape backup solutions support NDMP-enabled commercial backup applications to perform a dump backup or restore. Refer to the NetApp Interoperability Matrix to verify if the NDMP client you plan to use is supported. For more information on tape backups, refer to the "Data Protection Tape Backup and Recovery Guide" for your particular release at the NetApp Support (NOW) site.

8 LIMITATIONS

NetApp Cluster-Mode data protection solutions do not yet support certain features. However, the following features will be supported in future releases of Data ONTAP operating in Cluster-Mode:

- Snapdrive for Unix for operating systems other than Linux will not be supported until NetApp Data ONTAP 8.1.1
- Qtree SnapMirror
- Synchronous SnapMirror
- SnapVault® technology

9 CONCLUSIONS

Protecting ClearCase data is important for safeguarding a company's investment in product development efforts. NetApp provides an array of data protection solutions that reduce risk for an organization and simplify the protection of ClearCase data.

10 REFERENCES

1. TR-4032: Deployment and Implementation Guide: IBM Rational ClearCase for NetApp Data ONTAP Operating in Cluster-Mode by Agnes Jacob and Michael Donati

2. IBM ClearCase Administration Guide: Backing Up Critical Rational ClearCase Data

3. Backup and Restore of IBM Rational ClearCase Data on NAS Devices by Bob McCullough and Maneesh Jain

4. ClearCase Backup and Recovery by Bob Fulwiler

NetApp and IBM provides no representations or warranties regarding the accuracy, reliability, or serviceability of any information or recommendations provided in this publication, or with respect to any results that may be obtained by the use of the information or observance of any recommendations provided herein. The information in this document is distributed AS IS, and the use of this information or the implementation of any recommendations or techniques herein is a customer's responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. This document and the information contained herein may be used solely in connection with the NetApp and IBM products discussed
in this document.

Go further, faster®

www.netapp.com