Abstract
# TABLE OF CONTENTS

1  Executive Summary .................................................................................................................. 4
   1.1  Purpose and Scope ............................................................................................................... 4
   1.2  Audience .......................................................................................................................... 4

2  SnapCenter .................................................................................................................................. 4
   2.1  SnapCenter Architecture ............................................................................................... 5
   2.2  SnapCenter Features ........................................................................................................ 6
   2.3  SnapCenter Server Requirements .................................................................................. 6

3  Database Storage Layout ......................................................................................................... 7
   3.1  Setting Up Microsoft SQL Server Database Storage Layout with SnapCenter .............. 7
   3.2  Setting Up the Database Layout in a Virtual Environment ............................................. 8

4  Upgrading from SnapManager to SnapCenter Plug-In for Microsoft SQL Server .............. 10
   4.1  Upgrade Methodology ..................................................................................................... 10
   4.2  General Recommendations for SnapCenter Server ...................................................... 10

5  Backup Best Practices ............................................................................................................. 11
   5.1  Using Resource Group to Back Up Multiple Databases ................................................. 12
   5.2  Best Practices for Setting Up Log Backup .................................................................... 13
   5.3  Improving Verification Performance After Database Backup .................................. 13
   5.4  Sizing Consideration for SnapVault/SnapMirror ......................................................... 15
   5.5  Considerations for a Large Number of Small- to Large-Size Databases .................... 15

6  Restore Best Practices ............................................................................................................ 17
   6.1  ONTAP Restore Mechanism ......................................................................................... 17
   6.2  Restore Scenario for Storage Layout for SnapCenter ................................................ 17
   6.3  Restore Database to Alternate Host Option .................................................................. 20

7  Cloning Best Practices ........................................................................................................... 21
   7.1  Using Clone to Create a Database Copy ....................................................................... 21
   7.2  Managing a Clone Copy ................................................................................................. 21
   7.3  Managing Clone Copies in Hybrid Scenarios ............................................................... 22
   7.4  Additional Clone Guidelines ......................................................................................... 23

8  Microsoft SQL Server Deployment for Advanced Setup ................................................... 24
   8.1  Policy setting consideration for Microsoft SQL Server Always On Availability Groups .............................................................. 24
   8.2  Managing SQL Server and SnapCenter Backups for Asymmetric LUN Mapping in Windows Clusters .............................................................. 25

9  Performance and Benchmarking ............................................................................................. 25
9.1 Lab Setup 1 Using NetApp Storage FAS 8020 ................................................................. 25

10 Conclusion ............................................................................................................................. 26

Where to Find Additional Information .................................................................................. 26

Version History ......................................................................................................................... 27

LIST OF TABLES
Table 1) SnapCenter Server requirements. .................................................................................. 6
Table 2) SnapCenter restore mechanism. .................................................................................... 20

LIST OF FIGURES
Figure 1) SnapCenter architecture ............................................................................................ 5
Figure 2) Database layout for VMware using VMDK with NFS datastores. .............................. 9
Figure 3) Creating single Snapshot copy in ONTAP ................................................................. 12
Figure 4) Configuring the log directory. ...................................................................................... 13
Figure 5) Configuring the verification server. ............................................................................. 14
Figure 6) Storage layout for large databases on LUNs ................................................................. 18
Figure 7) Storage layout for small- to medium-size databases on LUNs. .................................... 18
Figure 8) Storage layout for large databases on VMDKs. ............................................................ 19
Figure 9) Storage layout for small to medium databases on VMDKs. ......................................... 19
Figure 10) Copy of cloned volume. .............................................................................................. 22
Figure 11) High-level overview of a small-scale hybrid architecture. ......................................... 23
Figure 12) Backing up databases in an availability group. ......................................................... 24
Figure 13) Availability group architecture .................................................................................. 25
1 Executive Summary

As data volume and the number of databases increase, maintaining recovery time objectives (RTOs) and recovery point objectives (RPOs) and managing the backup operation is crucial to enterprise applications. Providing efficient manageability for standalone and SQL always-on instances, meeting the need for on-demand availability of database copies, and ensuring that the storage space is not occupied with redundant copies are all requirements of data protection products.

SnapCenter 4.1 helps you modernize data protection, leveraging NetApp ONTAP® technologies to achieve RTO and RPO and more efficient database backup.

1.1 Purpose and Scope

Designing an optimal data protection and restore process is a crucial task. Improper design can lead to longer backup and restore time, sprawling backup jobs, complicated and lengthy restore mechanisms, unnecessary consumption of redundant spaces, and other similar scenarios.

This document discusses tactically deploying the database files, offloading some of the background process to alternative instances, grouping backup resources, and other best practices.

The best practices and recommendations described in this guide enable database architects and storage administrators to plan a highly available and easy-to-manage Microsoft SQL Server environment and to meet stringent service-level agreements (SLAs).

1.2 Audience

This guide assumes that you understand Microsoft SQL Server storage architecture and the administration and data protection concepts of backup and restore, and that you have a working knowledge of the following subjects:

- NetApp ONTAP data management software
- NetApp SnapCenter scalable software for application-consistent data protection
- Microsoft SQL Server

To determine configuration compatibility across the NetApp stack, see the NetApp Interoperability Matrix Tool (IMT).

The best practices for NetApp SnapCenter data protection presented in this document focus exclusively on Microsoft SQL Server 2008 and Windows Server 2008 R2 SP1 and later.

2 SnapCenter

SnapCenter is NetApp’s next-generation data protection software for tier 1 enterprise applications. SnapCenter, with its single-pane-of-glass management interface, automates and simplifies the manual, complex, and time-consuming processes associated with the backup, recovery, and cloning of multiple databases and other application workloads.

SnapCenter leverages technologies, including NetApp Snapshot™ copies, SnapMirror® replication technology, SnapRestore® data recovery software, and FlexClone® thin cloning technology, that allow it to integrate seamlessly with technologies offered by Oracle, Microsoft, SAP, VMware, and MongoDB across FC, iSCSI, and NAS protocols. This integration allows IT organizations to scale their storage infrastructure, meet increasingly stringent SLA commitments, and improve the productivity of administrators across the enterprise.
2.1 SnapCenter Architecture

SnapCenter is a centrally managed web-based application that runs on a Windows platform and remotely manages multiple servers that must be protected.

Figure 1 shows the high-level architecture of the NetApp SnapCenter Server.

Figure 1) SnapCenter architecture.

The SnapCenter Server has an HTML5-based GUI as well as PowerShell cmdlets and APIs. The SnapCenter Server is high-availability (HA) capable out of the box, meaning that if one SnapCenter host is ever unavailable for any reason, then the second SnapCenter Server can seamlessly take over and no operations are affected.

The SnapCenter Server can push out plug-ins to remote hosts. These plug-ins are used to interact with an application, a database, or a file system. In most cases, the plug-ins must be present on the remote host so that application- or database-level commands can be issued from the same host where the application or database is running.

To manage the plug-ins and the interaction between the SnapCenter Server and the plug-in host, SnapCenter uses SM Service, which is a NetApp SnapManager® web service running on top of Windows Server Internet Information Services (IIS) on the SnapCenter Server. SM Service takes all client requests such as backup, restore, clone, and so on.

The SnapCenter Server communicates those requests to SMCore, which is a service that runs colocated within the SnapCenter Server and remote servers and plays a significant role in coordinating with the SnapCenter plug-ins package for Windows. The package includes the SnapCenter plug-in for Microsoft Windows Server and SnapCenter plug-in for Microsoft SQL Server to discover the host file system, gather database metadata, quiesce and thaw, and manage the SQL Server database during backup, restore, clone, and verification.
SnapCenter Virtualization (SCV) is another plug-in that manages virtual servers running on VMWare and that helps in discovering the host file system, databases on virtual machine disks (VMDK), and raw device mapping (RDM).

2.2 SnapCenter Features

SnapCenter enables you to create application-consistent Snapshot copies and to complete data protection operations, including Snapshot copy-based backup, clone, restore, and backup verification operations. SnapCenter provides a centralized management environment, while using role-based access control (RBAC) to delegate data protection and management capabilities to individual application users across the SnapCenter Server and Windows hosts.

SnapCenter also includes the following key features:

- A unified and scalable platform across applications and database environments and virtual and nonvirtual storage, powered by the SnapCenter Server
- Consistency of features and procedures across plug-ins and environments, supported by the SnapCenter user interface
- RBAC for security and centralized role delegation
- Application-consistent Snapshot copy management, restore, clone, and backup verification support from both primary and secondary destinations (NetApp SnapMirror and SnapVault®)
- Remote package installation from the SnapCenter GUI
- Nondisruptive, remote upgrades
- A dedicated SnapCenter repository for faster data retrieval
- Load balancing implemented using Microsoft Windows network load balancing (NLB) and application request routing (ARR), with support for horizontal scaling
- Centralized scheduling and policy management to support backup and clone operations
- Centralized reporting, monitoring, and dashboard views
- SnapCenter 4.1 now also supports data protection on Microsoft SQL Server 2017 on Microsoft Windows Server

2.3 SnapCenter Server Requirements

Table 1 shows the minimum requirements for installing SnapCenter Server and plug-in on a Windows server.

Table 1) SnapCenter Server requirements.

<table>
<thead>
<tr>
<th>Components</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum CPU count</td>
<td>4 cores/vCPUs</td>
</tr>
<tr>
<td>Memory</td>
<td>Minimum: 8GB</td>
</tr>
<tr>
<td></td>
<td>Recommended: 32GB</td>
</tr>
<tr>
<td>Storage space</td>
<td>Minimum space for installation: 10GB</td>
</tr>
<tr>
<td></td>
<td>Minimum space for repository: 20GB</td>
</tr>
<tr>
<td>Supported operating systems</td>
<td>Windows Server 2012</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2012 R2</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2016</td>
</tr>
</tbody>
</table>
Components | Requirement
---|---
Software packages | .NET 4.5.2 or later
| Windows Management Framework 4.0 or later
| PowerShell 4.0 or later

For latest version compatibility and other plug-in information, refer to the NetApp Interoperability Matrix Tool.

### 3 Database Storage Layout

This section describes considerations when setting up the storage layout.

#### 3.1 Setting Up Microsoft SQL Server Database Storage Layout with SnapCenter

The best practices for designing and deploying Microsoft SQL Server with NetApp storage systems are explained in the document TR:4590 Best Practice Guide for Microsoft SQL Server with ONTAP.

SnapCenter best practice considerations for Microsoft SQL Server database layout are aligned with the suggested Microsoft SQL Server deployment. SnapCenter supports backup only of user databases that reside on a NetApp storage system. Along with the performance benefit of segregating user database layout into different volumes, SnapCenter also has a large influence on the time required to back up and restore. Separate volumes for data and log files significantly improves the restore time as compared to a single volume hosting multiple user data files. Similarly, user databases with I/O-intensive applications might experience increased backup time. Sections 5 and 6 of this document explain backup and restore practices.

When backing up databases with SnapCenter, take the following considerations into account:

- Databases with I/O intensive queries throughout the day should be isolated in different volumes and eventually have separate jobs to back them up.
- Large databases and databases that have minimal RTO should be placed in separate volumes for faster recovery.
- Small to medium-size databases that are less critical or that have fewer I/O requirements should be consolidated into a single volume. Backing up a large number of databases residing in the same volume results in fewer Snapshot copies to be maintained. NetApp also recommends consolidating Microsoft SQL Server instances to use the same volumes to control the number of backup Snapshot copies taken.
- Create separate LUNs to store full text-related files and file-streaming-related files.
- Assign a separate LUN for each instance to store Microsoft SQL server log backups. The LUNs can be part of the same volume.
- System databases store database server metadata, configurations, and job details; they are not updated frequently. System databases and tempdb should be placed in separate drives or LUNs. Do not place system databases in same volume as user databases. User databases have different backup policies and the frequency of user database backups is not same as for system databases.
- In the case of Microsoft SQL Server AG setup, the data and log files for replicas should be placed in an identical folder structure on all nodes.

#### Best Practices

The following are NetApp recommendations on volume design for optimal performance:

- Allocate at least 10% available free space in an aggregate.
• Use flexible volumes to store Microsoft SQL Server database files, and don’t share volumes between hosts.
• Use NTFS mount points instead of drive letters to bypass the 26-drive letter limitation in Microsoft Windows Server.

  **Note:** When using volume mount points, NetApp recommends giving the volume label the same name as the mount point.

• Configure a volume auto size policy, when appropriate, to help prevent out-of-space conditions.
• When the SQL Server database I/O profile consists mostly of large sequential reads, such as with decision support system workloads, enable read reallocation on the volume. Read reallocation optimizes the blocks for better performance.
• Set the Snapshot copy reserve value in the volume to zero for ease of monitoring from an operational perspective.
• Disable storage Snapshot copy schedules and retention policies. Instead, use the SnapCenter for SQL Server plug-in to coordinate Snapshot copies of the Microsoft SQL Server data volumes.
• Microsoft SQL Server uses the system database `tempdb` as a temporary workspace, especially for I/O intensive database consistency checker (DBCC) `CHECKDB` operations. Therefore, place this database on a dedicated volume with a separate set of spindles. In large environments where volume count is a challenge, you can consolidate `tempdb` into fewer volumes and store it in the same volume as other system databases. This procedure requires careful planning. Data protection for `tempdb` is not a high priority because this database is re-created every time the SQL Server is restarted.
• Place user data files (.mdf) on separate volumes because they are random read/write workloads. It is common to create transaction log backups more frequently than database backups. For this reason, place transaction log files (.ldf) on a separate volume or VMDK from the data files so that independent backup schedules can be created for each. This separation also isolates the sequential write I/O of the log files from the random read/write I/O of data files and significantly improves Microsoft SQL Server performance.

### 3.2 Setting Up the Database Layout in a Virtual Environment

For database layout in a virtual environment, NetApp recommends an approach similar to that outlined in the previous section. However, there are additional points to be considered when data files reside on VMDK or RDM. SnapCenter supports database files on virtual disk only in the case of VMware.

  **Note:** For other hypervisor environments, such as Hyper-V, SnapCenter is supported only for database files residing on NetApp storage connected with the iSCSI protocol.

**Virtual Disk on VMFS**

VMware virtual machines typically include a set of files in two given formats: virtual machine file system (VMFS) or RDM. Both formats enable you to access the virtual machine’s disk (VMDK), but they differ in approach to storage, and VMware recommends VMFS for the majority of VMs. With VMFS, the VMDK files also hold the data, whereas with RDM the data is stored on an external disk system. VMFS holds disk data from multiple VMs; RDM does not. VMFS was designed specifically to support virtualization.

Although RDM is sometimes recommended for I/O-intensive operations, with VMFS a storage volume can support one or many VMs. This volume can change without affecting network operations. Because they share storage volumes, VMs are easier to manage, and resource utilization remains high. Various ESXi servers can read and write to the file system at once, because it stores information at the block level.

**Best Practices**

The following are NetApp recommendations for VMDK:
• Use separate VMDKs for primary (.mdf) and log (.ldf) files for user databases. These VMDKs must reside in a datastore placed on a separate volume from the volume containing the system databases and the operating system VMDKs.

• Use separate VMDKs for system databases (master, model, and msdb). These VMDKs must reside in a datastore placed on a separate volume from the volume that contains user databases and the operating system VMDKs.

• Use separate VMDKs for the tempdb database.

• Data files (tables and indexes) are the primary files that are used by the Microsoft SQL Server storage engine. Each database might have multiple files and should be spread across multiple VMDKs.

• Don’t share volumes and datastores between different Windows Server machines.

**Note:** Whether it’s a single database file or multiple database files in the same volume, a database restored in VMDK with VMFS includes mount and copy restore.

**Virtual Disk on NFS**

ESXi can access a designated NFS volume located on a NAS server, mount the volume, and use it for its storage needs. You can use NFS volumes to store and boot virtual machines in the same way that you use VMFS datastores.

ESX 5.0 and later support up to 256 NFS datastores. The default value is 8, but this can be increased to the maximum number that is specific to the version of ESX or ESXi being used.

**Best Practices**

The following are NetApp recommendations for NFS datastores:

• Use one NFS datastore for multiple system databases from multiple instances.

• Use one NFS datastore per user database and user log; alternatively, separate the user database and the user log on different NFS datastores.

• Do not define a default gateway for the NFS storage network.

• Make sure that each NFS datastore is connected only once from each ESX or ESXi server by using the same NetApp target IP address on each ESX or ESXi server.

*Figure 2)* Database layout for VMware using VMDK with NFS datastores.
The database storage design has the following characteristics:

- To restore a single database in a VMDK that is also holding a single database, SnapCenter performs Single File SnapRestore to recover the data file and log. For example, recovering DB1 from the Figure 2 layout is a faster process. Single File SnapRestore is explained in section 6.1.
- When placing multiple database files and logs in single VMDK, restoring a single database includes mount and copy restore, as shown in DB2 and DB3 in Figure 2.

**Note:** NetApp recommends using hypervisor settings with NFS or iSCSI protocol if there are no RDMs or VMDKs (VMFS) in the environment.

### 4 Upgrading from SnapManager to SnapCenter Plug-In for Microsoft SQL Server

This section outlines the considerations for upgrading from NetApp SnapManager management software to SnapCenter plug-in for Microsoft SQL server.

#### 4.1 Upgrade Methodology

The SnapManager product is at the end of lifecycle support and no new features or patches are scheduled to be released. NetApp recommends upgrading SnapManager to SnapCenter 4.1, if you have not already done so.

Follow these steps to migrate SnapManager to SnapCenter:

1. Install the SCSQL plug-in alongside SMSQL.
2. Get the current backup schedule information of SMSQL from the PowerShell cmdlet `Get-SmSchedule`.
3. Create a new policy-based scheduled backup in SCSQL.
4. Use the following cmdlet to disable SMSQL schedules:

   ```powershell
   Get-SmSchedule -Hostname <hostname> -PluginCode SMSQL -DisableCurrentGenSchedule
   ```

5. Continue to run backup jobs from SCSQL until the backup copies are deleted from SMSQL as per the retention policy.
6. Once all the old backups are deleted from SMSQL, uninstall SMSQL.


#### 4.2 General Recommendations for SnapCenter Server

Follow these steps while configuring SnapCenter Server or adding host to install plugins.

1. Enable the hypervisor global settings for iSCSI disks connected to VMs.
2. When adding the Windows cluster host in SnapCenter, make sure that Add All Hosts in the Cluster or DAG is checked

3. Verify that the SVM short names are resolvable from all the plug-in hosts and the SC server. Resolve the SVM short name by adding the DNS entry or the etc\hosts entry.

4. Uninstall SnapCenter plug-ins from the SnapCenter GUI only.

5  Backup Best Practices

This section describes various scenarios to configure backup policies that should help you recover databases with ease and minimal downtime, while avoiding last-minute challenges.

Consider the following before configuring backup policy:

- Do you need full backup of databases and log backups of databases?
- List the RPOs for your production and nonproduction systems.
  - In SnapCenter terms, RPO can be identified as the backup frequency; that is, how frequently you want to schedule the backup to reduce the loss of data, up to a few minutes. SnapCenter doesn't stop you from scheduling backups as often as every 5 minutes; however, backup might not complete within 5 minutes during peak transactions or when the rate of change of data is unusually high in the given time. The best practice is to schedule frequent transaction log backups rather than full backups.
  - NetApp recommends scheduling Snapshot copies from only one source, either from SnapCenter or directly from ONTAP storage, to avoid reaching the Snapshot limit of 255 copies per volume or breaching Snapshot retention on ONTAP 9.3 and earlier versions. NetApp recommends backing up from SnapCenter, because it provides application-consistent backup.

  **Note:** In ONTAP 9.4 and later, the Snapshot copy limit is extended to 1,024.

  - There are numerous approaches to handling RPOs and RTOs. One alternative to this backup approach is to have separate backup policies of data and logs with different intervals. For example, schedule log backups at intervals of 15 minutes and data backups at intervals of 24 hours from SnapCenter.
  - If you have a disaster recovery requirement, list the RPO and RTOs in the event of disaster of the entire site or storage or compute host.
- List the retention requirements.
  - How long do you want to retain these backups, based on the category of backups (hourly, daily, weekly, monthly)? If you want to protect the Snapshot copies for the long term, you can create a SnapVault destination. You can tag these backups in various categories such as hourly, daily, weekly, and monthly and set retention periods for the them. SnapVault might not be an exact
replacement for tape or cloud, but it can address the backup needs for the near long term (maximum around 7 years).

- Do you want to verify and validate each backup for compliance or auditing needs?
  - The verification can be enabled in the policy and activated during the implicit resource group creation. You can verify the backups from primary or secondary disaster recovery or from vault storage. You can also perform deferred verification by scheduling it from either GUI or CLI. In the verification process, FlexClone is used to clone the database volumes, mount them on the host, and run the Microsoft SQL Server `DBCC CHECKDB` process across the mounted FlexClone volumes.

5.1 Using Resource Group to Back Up Multiple Databases

Resource groups were introduced with SnapCenter. The advantage of having a resource group is to have federated backup, as in SnapManager. If a Microsoft SQL Server instance is hosting multiple databases (100 or more) that are residing on the same large volumes, SnapCenter doesn’t create separate Snapshot copies for each database. Instead, it optimizes the Snapshot copies with a single application-consistent copy for that volume. In this way, SnapCenter reduces the number of Snapshot copies in ONTAP and a consistent point-in-time backup is available.

The other advantage of using resource groups is that you can group multiple instances or databases across different instances to reduce the number of jobs to be managed and monitored.

**Note:** Snapshot copies are created separately per host per volume.

Resource groups help to reduce storage overhead and to control the number of Snapshot copies.

Figure 3 is an example of an instance hosting multiple databases on the same volume (SC01040006500_5_MDML_Data_Log_Vol). The screenshot shows a single Snapshot being created in ONTAP each time the Snapshot is taken by using the resource group.

![Figure 3) Creating single Snapshot copy in ONTAP.](image)

**Best Practice**

Use resource groups for backup configuration for Snapshot optimization and number of jobs to be managed.
5.2 Best Practices for Setting Up Log Backup

Transaction log backup provides point-in-time recovery, which helps to achieve a defined recovery point objective (RPO). SnapCenter provides the ability to perform and manage log backup files, which helps in recovering the complete database from SnapCenter automatically without any manual intervention.

Create a host log directory (for SnapCenter) on a dedicated FlexVol® volume in which SnapCenter copies transaction logs. Set the log directory path based on the following scenarios:

- If a Microsoft SQL Server instance is running as a standalone instance, configure the host log directory for each instance in the green box highlighted in Figure 4.
- In the case of AG, configure the host log directory for each node in the green box.
- When configuring the host log directory for failover cluster instance (FCI) including the AG running under FCI, configure the host log directory in the blue box, selecting the correct Microsoft SQL Server instance. Also verify that the drive selected for the log directory is also part of the cluster disk group under the Microsoft SQL Server role.

![Figure 4) Configuring the log directory.](image)

**Best Practice**

NetApp recommends backing up the transaction log from SnapCenter so that during the restoration process, SnapCenter can read all of the backup files and restore in sequence automatically.

5.3 Improving Verification Performance After Database Backup

The verification process is greatly improved in SnapCenter by executing the processes in parallel. This is an advantage in a consolidated environment where there are multiple databases running on the same instance. For business criticality, the verification process can be offloaded to an alternate server.

The verification process for databases is enabled from the Configure plug-in for SQL Server section on the Host tab, as shown in Figure 5. You can configure a maximum job count, which translates to the number of verification jobs executed for that Microsoft SQL Server instance. For example, if the maximum job count is set to 3, and the SC job is backing up an instance with 9 databases and 3 verification instances are selected, then multiple verification jobs are created, and each job has a set of databases. After job creation, the tasks are distributed to selected instances for verification and the number of jobs that each instance can execute.
The following scenario has a Microsoft SQL Server Instance with 20 small databases. Here are the use cases.

1. Consider one instance for verification; maximum job count = 1.

   Total time taken was 00:02:30. The process takes more time because one job was created to sequentially execute the verification job.

2. Consider three instances, including the primary instance, for verification; maximum job count = 3. Jobs were distributed across various servers, reducing the time for verification.
Total time taken was 00:1:04

- Configure additional instances for verification when you have a large number of databases that take longer to perform a consistency check. You must also consider those instances that are less utilized, have little effect on performance, and support equal or higher versions or editions as compared to the primary instance.
- Set the maximum job count to more than 1 to run the verification jobs in parallel within an instance.

### 5.4 Sizing Consideration for SnapVault/SnapMirror

Correctly sizing a SnapVault/SnapMirror solution is an important step in the design phase to make sure that backups complete within a planned backup window, RPOs are met, and user I/O performance is not adversely affected. There are many variables that must be considered when sizing a SnapVault and SnapMirror solution.

- **Disk space.** The SnapVault/SnapMirror secondary, or target, must be sized so that adequate disk space is available to retain all of the planned backups. This space can be estimated fairly accurately by using known information about the primary data and the required RPOs. This calculation is independent of the systems used. To calculate the required disk space on the SnapVault/SnapMirror target, you need to gather the following information: the size of the primary data; the daily, weekly, and monthly data change rates; the number of daily, weekly, and monthly backup copies to be kept; and the space savings that can be anticipated by using NetApp deduplication and compression.
- **Data throughput.** It is also important to size a SnapVault/SnapMirror solution so that data can be transferred fast enough to complete backups in the time available. To do this, first determine how much data, on average, is transferred in a SnapVault/SnapMirror incremental update and how much time must be allotted to complete the backup, then use these numbers to determine the required data throughput in units such as megabytes per second. If you have multiple SnapVault/SnapMirror relationships, remember to consider the size of all the backups that must be completed during a given backup window. Once the required data throughput speed is determined, an appropriate NetApp FAS or AFF system can be selected that can handle the data speed required.
- **Client I/O.** Another factor to consider when sizing is how the SnapVault/SnapMirror processes affect the other workloads running on a system. Clients generally experience more latency with a greater number of concurrent SnapVault/SnapMirror streams. If a large number of transfers must take place during a given backup window, it is usually best to stagger the updates so that they don't all run at the same time and cause unacceptable latency to clients. For example, if 80 relationships must update within a 10-hour window and it is determined that, on average, eight concurrent updates can finish in 1 hour, then a transfer schedule can be created that starts eight new updates every hour during the given 10-hour window.

**Note:** When sizing a SnapVault/SnapMirror solution, an acceptable client I/O latency threshold should first be established. Then determine what the client I/O latency effect might be for a specific configuration, given the system being used, the type of dataset to be backed up, and the number of concurrent transfers needed to complete all backups within the given window.

### 5.5 Considerations for a Large Number of Small- to Large-Size Databases

- SnapCenter can back up large numbers and sizes of databases in an instance or group of instances within a resource group. The size of a database is not a major factor in backup time. Duration of backup varies depending on the number of LUNs per volume, the load on Microsoft SQL Server, the total number of databases per instance, and especially the I/O bandwidth and usage.
- When configuring the policy to back up databases from an instance or resource group, you must restrict the maximum databases backed up per Snapshot copy to 100 per host. Verify that the total number of Snapshot copies does not exceed 255 copies per the limit set in ONTAP 9.3 or the 1024 Snapshot limit in ONTAP 9.4.
• Schedule backups during off-peak times so that the backup process does not affect the applications that have a minor wait time.
• I/O usage plays an important part in the backup process. The backup process waits for quiescing until all the I/O operations on a database are completed. Such databases with highly intensive I/O operation should be deferred to another backup time or should be isolated from other backup jobs to avoid affecting other resources in same resource group that are scheduled for backup.

Example
For an environment that has six Microsoft SQL Server hosts, hosting 200 databases per instance, assuming four LUNs per host and one LUN per volume, set the full backup policy with max databases backed up per Snapshot copy to 100.

200 databases on each instance are laid out as 200 data files distributed equally on two LUNs and 200 logfiles distributed equally on two LUNs, which is 100 files per LUN and per volume.

Schedule three backup jobs by creating three resource groups, each grouping two instances that include total 400 databases.

Running all three backup jobs in parallel backs up 1,200 databases simultaneously but depending on the server load and I/O usage, the start and end times of each instance vary. A total of 24 Snapshot copies are created in this case.

Along with the full backup, NetApp recommends configuring transaction log backups for critical databases. Validate that the database property is set to full recovery model.

Refer to the SnapCenter Data Protection Guide for Microsoft SQL Server to configure log backup: https://library.netapp.com/ecm/ecm_download_file/ECMLP2846075.

Best Practices
• Do not include the tempdb database in a backup because the data it contains is temporary. Place tempdb on a LUN or an SMB share that is in a storage system volume where Snapshot copies are not created.
• Always run SCSQL backups during off-peak hours to avoid affecting the performance of regular user activity.
• Microsoft SQL Server instances with high I/O intensive applications should be isolated in different backup jobs to reduce the overall backup time for other resources.
• Limit the set of host to be backed up simultaneously to 10 and stagger the remaining set of host backups to avoid simultaneous processing.
• Preferably use the Microsoft SQL Server instance name in the resource group instead of multiple databases, because when new databases are created in Microsoft SQL Server instance, SnapCenter automatically considers a new database for backup.
• If you change the database configuration, such as changing the database recovery model to full recovery model, perform a backup immediately to allow up-to-the-minute restores.
• SCSQL cannot automatically restore transaction log backups created by using the SQL Server Management Studio against an SCSQL full backup of a database. The transaction log files created by SQL Server Management Studio have the default extension .trn, and a transaction log backup created by SnapCenter has the extension .trb. However, a full database backed up from SCSQL can continue to restore log backup files from Microsoft SQL Server Management Studio.
• When cloning FlexVol volumes, make sure that there is sufficient space for the clone metadata.
• Create a separate policy to manage and backup system databases at least once a week.
• The verification server must be connected to the NetApp storage system where the backup Snapshot copies are located. The connectivity can be Fibre Channel (FC), Fibre Channel over Ethernet (FCoE),
or iSCSI. It is not required for the connectivity of the verification server to the NetApp storage to match the connectivity of the production Microsoft SQL Server host.

- Make sure that SCSQL backups on VMDK use a verification server that is running on a virtual machine only

**Note:** SnapCenter does not allow VM and Microsoft SQL Server applications to be backed up together. They are backed up separately.

## 6 Restore Best Practices

This section describes the ONTAP restore mechanism and restore best practices.

### 6.1 ONTAP Restore Mechanism

ONTAP provides the following restore mechanisms, which SnapCenter uses.

#### Single File SnapRestore

Single File Snap Restore (SFSR) is a fast mode of restore in which the process restores a complete LUN in a volume from a Snapshot copy to the read-write mode. A LUN is treated as a single file in a volume and, during the single file restore process, SnapCenter replaces the current working copy of the LUN with a Snapshot copy. In short, SFSR is a realignment of pointers to the blocks of time when the Snapshot copies were taken.

**Note:** The SFSR process works only if the data files reside on a disk connected with iSCSI protocol or VMDKs on NFS only.

#### SubLUN

The SubLUN process restores a range of bytes in the underlying LUNs associated with the files being restored. For example, a Microsoft SQL Server instance might be hosting multiple user databases over the same LUN. Restoring a user database file from the LUN without touching other files is a partial restoration, which in turn must restore a specific range of bytes from the LUN.

SubLUN restore is more time-consuming than the SFSR process, but it is still faster than regular copy-restore process.

**Note:** The SubLUN process works if the data files reside on a disk connected with the iSCSI protocol and compression is not enabled on the volume.

#### Mount and Copy Restore

An alternative restore option available from ONTAP, mount and copy restore is the traditional way of restoration. If the SFSR and subLUN processes are not viable, then SnapCenter selects the traditional approach of mounting the volume and copying the files to the target host and attaching the databases. This is obviously a time-consuming process. In the case of log file restoration, SnapCenter might choose to access the shared path, if it was provided by the end user, to restore the logs, thus eliminating the process to copy the log files. During the mount and copy restore process, temporary storage is visible for brief time until the required files are copied, and then it is removed. Depending on the restoration scenario and architecture deployed, SnapCenter picks up the restoration mechanism. Section 6.2 describes how the restore mechanism is determined based on the storage layout.

### 6.2 Restore Scenario for Storage Layout for SnapCenter

With reference to the suggested storage layout in [SnapCenter 4.1 – Data Protection Guide for Microsoft SQL Server](https://www.netapp.com), this section describes the restoration path for each scenario.
Case 1: Storage Layout for Large Databases on LUNs

Figure 6) Storage layout for large databases on LUNs.

In this scenario, each data file of a database is stored in a separate iSCSI or FC LUN. When the database needs to be restored, SnapCenter identifies whether all the data files residing on the LUN are associated with single database to be restored and then uses the SFSR mechanism to restore the LUNs of the database from Snapshot copy.

Case 2: Storage Layout for Small- to Medium-Size Databases on LUNs

Figure 7) Storage layout for small- to medium-size databases on LUNs.

Multiple databases are stored in an iSCSI or FC LUN. In this case, when a single database must be restored, SnapCenter identifies the range of bytes used in the LUN for that database. SnapCenter uses the SubLUN mechanism to restore a range of bytes to restore a database.
Case 3: Storage Layout for Large Databases on VMDKs

Figure 8) Storage layout for large databases on VMDKs.

In this case, database files reside on the VMware VMDK files of VMFS. SnapCenter cannot recover VMFS as it does for LUN as a file. SnapCenter uses the mount and copy restore method of mounting the copy of the volume as VMDK and then copying the files to the desired location to perform database restoration by attaching the database.

Case 4: Storage Layout for Small to Medium Databases on VMDKs

Figure 9) Storage layout for small to medium databases on VMDKs.

SnapCenter cannot extract the range of bytes used for Microsoft SQL Server data files residing on VMDK on VMFS. Similar to Case 3, SnapCenter uses the mount and copy restore method of mounting the copy of volume as VMDK and then copying the files to the desired location to perform database restoration by attaching the database.

Table 2 shows the restore mechanism used by SnapCenter for various use cases.
Table 2) SnapCenter restore mechanism.

<table>
<thead>
<tr>
<th>Server</th>
<th>Scenario</th>
<th>In-Place Restore</th>
<th>Restore Alternate Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Single DB spread across single or multiple LUNs/volume (no other data files on volume)</td>
<td>SFSR</td>
<td>Mount &amp; copy restore</td>
</tr>
<tr>
<td>2</td>
<td>Single DB restore from single LUN hosting multiple data files</td>
<td>SubLUN (single DB restore)</td>
<td>Mount &amp; copy restore</td>
</tr>
<tr>
<td>3</td>
<td>Single DB restore in VMDK on VMFS; single files or multiple files present on disk</td>
<td>Mount &amp; copy restore</td>
<td>Mount &amp; copy restore</td>
</tr>
<tr>
<td>4</td>
<td>Single DB restore having files in multiple VMDKs (VMFS)</td>
<td>Mount &amp; copy restore</td>
<td>Mount &amp; copy restore</td>
</tr>
<tr>
<td>5</td>
<td>Single DB restore from VMDK on NFS; no other files present</td>
<td>SFSR</td>
<td>Mount &amp; copy restore</td>
</tr>
<tr>
<td>6</td>
<td>Single DB restore having files in multiple VMDKs (NFS)</td>
<td>Mount &amp; copy restore</td>
<td>Mount &amp; copy restore</td>
</tr>
<tr>
<td>7</td>
<td>VM hosted on Hyper-V (only iSCSI supported)</td>
<td>Based on #1 or 2</td>
<td>Based on #1 or 2</td>
</tr>
<tr>
<td>8</td>
<td>Different reseed scenarios like reseeding from local copy in the same location</td>
<td>Based on #1,2,3,4,5,6</td>
<td>Mount &amp; copy restore</td>
</tr>
<tr>
<td>9</td>
<td>Restoring DB to public cloud (Azure, AWS) — iSCSI connected storage only</td>
<td>--</td>
<td>Mount &amp; copy restore</td>
</tr>
<tr>
<td>10</td>
<td>In case of server/instance rebuild (different host in case original server is affected by virus)</td>
<td>--</td>
<td>Mount &amp; copy restore</td>
</tr>
<tr>
<td>11</td>
<td>In case of server/instance rebuild (with same configuration/setup, including name)</td>
<td>SFSR</td>
<td>--</td>
</tr>
<tr>
<td>12</td>
<td>Restoration from vCenter to another vCenter group (only for VMDK)</td>
<td>Not supported</td>
<td>Not supported</td>
</tr>
<tr>
<td>13</td>
<td>Restoration from vCenter to another vCenter group (iSCSI)</td>
<td>--</td>
<td>Mount &amp; copy restore</td>
</tr>
<tr>
<td>14</td>
<td>DB restoration from VM to physical instance (only iSCSI supported)</td>
<td>--</td>
<td>Mount &amp; copy restore</td>
</tr>
</tbody>
</table>

6.3 Restore Database to Alternate Host Option

This restore operation is similar to the restore operation in Microsoft SQL Server Management Studio. Large databases might take longer to perform restore due to its streaming process. The best practice is to set a timeout value to avoid backup failure at the end. The default setting is 3 hours or 10800000 milliseconds.

Generally a 1.5TB database restore takes around 9 hours. NetApp recommends setting the following timeout value in the SMCoreServiceHost.exe.config file located in the plug-in server in C:\Program Files\NetApp\SnapCenter\SMCore\.
Search for the keyword RESTTimeout and change

```xml
<add key=RESTTimeout value=10800000 />
```
to

```xml
<add key=RESTTimeout value=32400000 />
```
to set 9 hours restoration timeout value. If the database is too large and you expect it to take more time to restore, then set the restore time accordingly (in milliseconds).

**Best Practices**

- Alter the RESTTimeout value setting before restoring a large database.
- If the volume is not accessible in an alternate host, use the Custom Log Directory option when restoring the database with Restore to Alternate Host. This helps to read log backup files directly from the given location rather than mounting the directory.

7 Cloning Best Practices

7.1 Using Clone to Create a Database Copy

- To restore a database to another location in the development or test environment, or to create a copy for analysis purposes, the best practice is to leverage cloning methodology to create a copy of the database on the same instance or an alternate instance.
- Cloning databases of 500GB on iSCSI disks hosted on an FAS environment typically takes about 5 minutes. After that, the user can perform all the required read/write operations on the database.
- A database can be cloned in two ways:
  - By creating a clone from the latest backup.
  - By using clone lifecycle management (CLM), so that the latest copy is made available on the secondary instance.
- Together with resource group, CLM can clone a single database or multiple databases in the same instance. Starting with SnapCenter 4.1, CLM is supported for both standalone and failover cluster instances (FCI).
- You can perform a clone split later during the off-peak period or maintenance window to isolate the clone copy from the Snapshot copy and avoid any dependency on either of them in future. Refer to section 6.3 to set the restoration timeout value to help large databases do a complete clone split.

**Note:** The split operation takes approximately the same length of time that a restore operation might take.

SnapCenter allows you to mount the clone copy on the required disk to maintain the format of folder structure on the secondary instance and continue to schedule backup jobs.

**Best Practice**

- If possible, consider using a database clone instead of restoring, because it reduces the time to restore, the load on storage to perform I/O operations, and space utilization.
- For recurring database restoration jobs, schedule a CLM job from SnapCenter. This reduces the overhead of managing the job from Microsoft SQL Server to perform stream backup and restore.

7.2 Managing a Clone Copy

As described earlier, cloning is a simpler and faster process to restore databases. Managing clones is a necessary task to make sure that there are no ghost entries or orphaned storage in the SnapCenter inventory.
The clone copies are created by SnapCenter, so SnapCenter maintains the list of copies. Forcibly deleting the database from Microsoft SQL Server can keep the drives on the secondary host redundant and unaccounted for.

Figure 10 shows the copy of a cloned volume from the NetApp System Manager link. The volume is orphaned because of dropping the database from the Microsoft SQL Server command window, leaving the logical drive empty and unused.

**Figure 10) Copy of cloned volume.**

NetApp recommends deleting such clone copy databases from SnapCenter or else cleaning periodically to avoid redundancy from the discovery list.

Following is the alternate workaround to delete such orphaned volumes:

- Expand the database resource details from SnapCenter to view the backup topology and backup summary.

Following is a workaround to clean the entry from SnapCenter if the database is dropped from Microsoft SQL Server Management Studio and volumes are deleted from ONTAP:

- Identify the clone and delete it by selecting the Force checkbox.

**Best Practice**

Always delete the clone copy of a database from SnapCenter.

**7.3 Managing Clone Copies in Hybrid Scenarios**
SnapCenter supports clone and restore of a Microsoft SQL Server database onto another hypervisor. Whether it is on-premises Hyper-V VM’s, or VM’s hosted on public cloud like Azure and AWS, cloning is possible if the source and target disk are mapped with the iSCSI protocol. A Microsoft SQL Server host running on an Azure or AWS infrastructure can be added as a host to SnapCenter and perform the task.

Figure 11 is a high-level overview of a small-scale hybrid architecture, with SnapCenter managing servers on premises and in the cloud. ONTAP Cloud is used as secondary storage for replication. Hyperscalers like AWS and Azure, which offer a flexible compute resource, leverage NetApp Private storage (NPS) for storage through cloud-connected colocation facilities, such as Equinox, by which data can remain private outside the cloud.

Figure 11) High-level overview of a small-scale hybrid architecture.

7.4 Additional Clone Guidelines

- You should have created a backup of the database using SnapCenter.
- For the clone operation to be successful, verify that the aggregate used by the Microsoft SQL Server database is included in the SVMs list of assigned aggregates.
- The clone can be created on the same host as that of the source database. When creating the clone on an alternate host, verify that the alternate host meets the following requirements:
  - SnapCenter plug-in for Microsoft Server should be installed on the alternate host.
  - The clone host should be able to discover LUNs from primary or secondary storage.
- If you are cloning from primary storage or secondary (vault or mirror) storage to an alternate host, make sure that an iSCSI session is established between the secondary storage and the alternate host, or that it is zoned properly for FC.
- If you are cloning from vault or mirror storage to the same host, make sure that an iSCSI session or FC zoning is established between the vault or mirror storage and the Microsoft SQL Server host.
- If you are cloning in a virtualized environment, confirm that an iSCSI session is established between the primary or secondary storage and ESX server hosting the alternate host, or that it is zoned properly for FC.
  - Same or higher Microsoft SQL Server version or edition as the source database host.
  - Clone lifecycle management can be used to schedule recurring cloning processes.
8  Microsoft SQL Server Deployment for Advanced Setup

8.1  Policy setting consideration for Microsoft SQL Server Always On Availability Groups

SnapCenter provides various settings for protecting databases in the availability group (AG). The data protection policy set through SnapCenter overrides the settings on Microsoft SQL Server AG property. One such property is the reseeding AG database. In case of database corruption on either of the nodes, databases can be recovered faster by restoring them from locally available backup.

NetApp recommends backing up databases from all available nodes for faster recovery on each node. Figure 12 shows the setting to back up databases in AG on all available node. The settings are visible while configuring the policy.

Figure 12) Backing up databases in an availability group.

Reseeding the database does not require you to rebuild the AG configurations. To restore the database and add it back to AG, navigate to SnapCenter > Resources > Databases, click Reseed, and select the database.

Note: The Reseed option is available only on Microsoft SQL Server AG running on a Windows failover cluster instance.

With SnapCenter 4.1, the SQL AG database Reseed and Restore operations access other replicas’ log backups as network share instead of mounting the storage.
Best Practice
NetApp recommends backing up databases from all available nodes so that the Reseed operation can be performed across all nodes.

8.2 Managing SQL Server and SnapCenter Backups for Asymmetric LUN Mapping in Windows Clusters

The SnapCenter plug-in for Microsoft SQL Server supports discovery of Asymmetric LUN Mapping (ALM) configuration for Microsoft SQL Server high availability and disaster recovery. Such architectures are usually designed to achieve business continuity in case of disaster, when nodes of Windows clusters can failover to another data center by using AG.

Figure 13) Availability group architecture.

In Figure 13, the architecture is supported with AG between two subsets of FCI or between a subset of FCI and a single node. This setup is useful when one-to-many FCI subsets on the production site are mapped to one node on the secondary site with databases residing on the respective drives. This setup helps in a many-to one-relationship where minimal servers are present at the disaster recovery location.

The best practice is to have same mount point or drive letter across nodes in different data centers within same Windows Server failover cluster (WSFC). Having the same drive letter helps the reseeding to work without having to alter the restore location.

Note: Provisioning is not supported in ALM kind of architecture.

9 Performance and Benchmarking

The data described in this section shows the scale of plug-ins that SnapCenter Server can handle. SnapCenter server has capacity to handle more plugins. Performance and benchmarks are subject to lab setup.

9.1 Lab Setup 1 Using NetApp Storage FAS 8020

SC Server Configuration:

<table>
<thead>
<tr>
<th>OS Server</th>
<th>Memory</th>
<th>Processors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 2012 R2</td>
<td>16GB</td>
<td>4 cores</td>
</tr>
</tbody>
</table>
Plug-In Configuration:

<table>
<thead>
<tr>
<th>SCSQL Plug-ins</th>
<th>SCO Plug-ins</th>
<th>Databases</th>
<th>DB size</th>
<th>Protection</th>
<th>SVMs</th>
</tr>
</thead>
<tbody>
<tr>
<td>60</td>
<td>20</td>
<td>1,200</td>
<td>Up to 2TB</td>
<td>SnapVault</td>
<td>60</td>
</tr>
</tbody>
</table>

Resource Groups 40

LUNs Per host 6

LUN/Volume Mapping 1:1

Schedules and Workflows:

- Daily backup: Full backup with SnapVault/SnapMirror update with inline verification (once per day)
  - 10 concurrent backups scheduled
- Log-only backup for every 6 hours
- On-demand clone (clone from backup)

Workflow Timing:

<table>
<thead>
<tr>
<th>Server</th>
<th>Workflow</th>
<th>Scale</th>
<th>Timing</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Full + log backup with inline verification (SM and SV update)</td>
<td>200 DBs/10 Hosts</td>
<td>11 mins</td>
</tr>
<tr>
<td>2</td>
<td>Restore a SQL database (SnapRestore/SFSR)</td>
<td>1TB</td>
<td>&lt;1 min</td>
</tr>
<tr>
<td>3</td>
<td>Restore a SQL database (SubLUNFileClone)</td>
<td>1TB</td>
<td>6 mins</td>
</tr>
<tr>
<td>4</td>
<td>Backup with verification</td>
<td>1TB</td>
<td>4 hours 40 mins</td>
</tr>
<tr>
<td>5</td>
<td>Clone from backup</td>
<td>1TB</td>
<td>&lt;2 mins</td>
</tr>
</tbody>
</table>

10 Conclusion

Microsoft SQL Server is an enterprise-class product. Multiple configuration options are available to suit most of customer needs. NetApp storage and data management software is built in a similar fashion, giving the flexibility to manage Microsoft SQL Server in a manner that best meets customer business requirements. With high-performance, easy-to-manage storage systems, robust software offerings and efficient data protection solution, NetApp offers flexible storage and data management solutions to support Microsoft SQL Server.

Where to Find Additional Information

To learn more about the information described in this document, refer to the following documents and/or websites:

- SnapCenter 4.1 Concepts Guide
  [https://library.netapp.com/ecm/ecm_download_file/ECMLP2846073](https://library.netapp.com/ecm/ecm_download_file/ECMLP2846073)
• SnapCenter 4.1 Data Protection Guide for Microsoft SQL Server
  https://library.netapp.com/ecm/ecm_download_file/ECMLP2846075
• SnapCenter 4.1 Administration Guide
  https://library.netapp.com/ecm/ecm_download_file/ECMLP2846072
• Best Practice Guide for Microsoft SQL Server with ONTAP
  TR:4590 - Best Practice Guide for Microsoft SQL Server with ONTAP
• Steps to backup Snap Vault
• SnapCenter Software Resources
  https://mysupport.netapp.com/info/web/ECMP12509262.html
• SnapCenter Documentation Center
  http://docs.netapp.com/ocsc-40/index.jsp
• Product Documentation
• NetApp Documentation Centers
  https://mysupport.netapp.com/info/web/ECMLP2557637.html

Version History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Document Version History</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 1.0</td>
<td>August 2018</td>
<td>Initial Release</td>
</tr>
</tbody>
</table>
Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer’s installation in accordance with published specifications.

Copyright Information

Copyright © 2018 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.

Data contained herein pertains to a commercial item (as defined in FAR 2.101) and is proprietary to NetApp, Inc. The U.S. Government has a non-exclusive, non-transferrable, non-sublicensable, 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).

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.