TABLE OF CONTENTS

1 Introduction ........................................................................................................................................... 4
  1.1 Objective ......................................................................................................................................... 4
  1.2 Audience .......................................................................................................................................... 4

2 SnapProtect Solution Overview .......................................................................................................... 4

3 SnapProtect Sizing Considerations .................................................................................................... 5

4 SnapProtect for vSphere ..................................................................................................................... 6
  4.1 Validated Lab Design ....................................................................................................................... 7

5 RPO and RTO Requirements ............................................................................................................... 9

6 Configure SnapProtect for vSphere Backups ..................................................................................... 10

7 Configure vSphere Backups ................................................................................................................ 11

8 Create a Mirror Copy or a Vault Copy ............................................................................................... 19
  8.1 Resource Pools .............................................................................................................................. 19
  8.2 Create an Auxiliary Snapshot Copy .............................................................................................. 19

9 Configure Restore Options ................................................................................................................ 24
  9.1 Datastore Types and Restore Requirements ............................................................................... 24
  9.2 Configure a Restore ....................................................................................................................... 25

10 Configure Backups to Tape or to a Cloud Appliance ....................................................................... 29
  10.1 Configure Tape Backups ............................................................................................................. 29
  10.2 Configure AltaVault Backups ..................................................................................................... 33

11 SnapProtect and vSphere Disaster Recovery ................................................................................... 34

Appendix: Backup Test Validation ........................................................................................................ 34

References ............................................................................................................................................... 35

LIST OF TABLES
Table 1) Storage layout .......................................................................................................................... 7
Table 2) LUN information ....................................................................................................................... 7
Table 3) vSphere network configuration ................................................................................................. 8
Table 4) RPO requirements and design considerations ......................................................................... 9
Table 5) RTO requirements and design considerations ......................................................................... 9
Table 6) Validation test results ............................................................................................................... 35
LIST OF FIGURES

Figure 1) SnapProtect solution architecture. ...........................................................................................................5
Figure 2) D2D2T architecture on a VMware vSphere environment. ...........................................................................7
Figure 3) vSphere network design layout. ....................................................................................................................8
Figure 4) Resource pools in Unified Manager. ............................................................................................................19
Figure 5) SVM associations to create an auxiliary copy in SnapProtect. .................................................................19
1 Introduction

NetApp® SnapProtect® software offers centralized backup management of IT infrastructures through a single pane of glass. NetApp Integrated Data Protection technologies are the backbone of this architecture. NetApp SnapVault® software manages backup and long-term retention use cases, and NetApp SnapMirror® software manages disaster recovery. The solution delivers application-consistent NetApp Snapshot® backup and recovery that supports all major enterprise applications, including Oracle Database, Microsoft SQL Server, and Microsoft Exchange. NetApp SnapProtect also supports backup and recovery of virtualization environments running hypervisors such as VMware vSphere and Microsoft Hyper-V.

1.1 Objective

This document describes the SnapProtect with VMware vSphere solution and explains key features of Snapshot backup and recovery for vSphere. Backup and recovery are performed by using NetApp technologies such as SnapVault and SnapMirror within the NetApp Data ONTAP® operating system. This document also describes backup and recovery best practices for the SnapProtect with VMware vSphere solution.

1.2 Audience

The audience for this document includes sales engineers, field consultants, professional services personnel, IT managers, partner engineers, and customers who want to deploy the SnapProtect for VMware vSphere solution.

2 SnapProtect Solution Overview

The SnapProtect solution has the following high-level components:

- **SnapProtect server.** Functions as a single pane of glass for unified management.
- **NetApp OnCommand® Unified Manager.** Enables automated storage provisioning.
- **NetApp FAS controllers.** Provide Snapshot backups integrated with NetApp data protection technologies.
- **Third-party storage or direct-attached storage.** Can be backed up through SnapProtect for Open Systems.
- **iData agents.** Provide client communication and application consistency.

Figure 1 shows the architecture of the SnapProtect solution.

**Note:** For more information about the components of the solution, see TR-3920: NetApp SnapProtect Management Software Solution Overview.
3 SnapProtect Sizing Considerations

Sizing a SnapProtect deployment for application backups typically depends on the following factors:

- **CommServe sizing.** CommServe is the master server of your backup infrastructure. The CommServe server ties together the elements of the CommCell configuration and includes several tools for managing and administering the CommCell component. The CommServe server communicates with all agents in the CommCell component to initiate data protection, management, and recovery operations. Similarly, the server communicates with media agents when the media subsystem requires management. The CommServe server maintains a database that contains all the information related to the CommCell component. For more information about CommServe, see System Requirements – CommServe.

- **Storage sizing.** Storage sizing typically depends on how you define sizing for the vSphere environment and sizing for backups. SnapProtect creates backups by using Snapshot technology, and it leverages Data ONTAP SnapVault and SnapMirror replication technologies in the back end to protect data. Storage sizing for secondary and tertiary backup targets depends on the backup topology in use.

  **Note:** For assistance with sizing storage for your vSphere environment and backups, contact your NetApp sales representative.

- **vSphere sizing.** VMware ESXi supports three types of storage configurations for connecting to shared storage arrays: VMware Virtual Machine File System (VMFS) datastores, network-attached storage (NAS) datastores, and raw device mappings (RDMs). Sizing for a vSphere environment depends on a large number of parameters, but the type of workloads running in the virtual infrastructure and the performance requirements are usually the primary sizing criteria. For more information about vSphere storage best practices and performance guidelines, see the following documents:
  - Performance Best Practices for VMware vSphere 5.5
  - TR-3749: NetApp Storage Best Practices for VMware vSphere

- **SnapVault sizing.** The Rapid SnapVault/OSSV Space Estimator sizing tool can help you calculate how much storage is required on your secondary and tertiary targets, considering backup schedules,
growth, and retention. SnapProtect is integrated with OnCommand Unified Manager, which automatically provisions secondary volumes for SnapVault and SnapMirror targets. For SnapVault sizing, the most important consideration is how much storage, or how many disks, you should buy to accommodate backups. Volume sizing is intelligently managed by Unified Manager.

- **OnCommand Unified Manager sizing.** OnCommand Unified Manager is an important part of the SnapProtect solution. OnCommand Unified Manager 5.x is used for Data ONTAP 7-Mode deployments, and OnCommand Unified Manager 6.x is used for clustered Data ONTAP deployments. Unified Manager is the interface between CommServe and Data ONTAP, and it is used to provision volumes in the secondary target. Sizing for Unified Manager depends on the number of storage nodes and the number of relationships between SnapVault and SnapMirror that a single instance of Unified Manager can manage. CommServe offloads auxiliary-copy operations to Unified Manager. Therefore, Unified Manager must be sized as a separate entity.

**Note:** For more information about sizing requirements for Unified Manager or for assistance with accurately sizing the solution, contact your NetApp sales representative.

- **Tape backup sizing.** Disk or tape backups of applications are considered streaming backups. Sizing for these backups depends on the following factors:
  - Backup size
  - Retention policy (daily, weekly, or monthly)
  - Storage capacity of the tape or disk

NetApp recommends that you create backup copies on tape or disk by using either a SnapVault or SnapMirror destination. NetApp also recommends that you create these copies from a proxy client so that the production environment is not affected by these performance-intensive tasks.

## 4 SnapProtect for vSphere

SnapProtect offers the following unique capabilities that distinguish it from other applications used to back up vSphere environments:

- Ability to create a point-in-time Snapshot copy of the data used for backups
- Rapid protection of the vSphere environment without overhead on the production virtualization infrastructure
- Integration with the Virtual Server Agent to allow the array to perform backups in minutes, even with a large number of virtual machines (VMs)
- A dedicated ESXi server that works as a proxy for data movement, removes utilization on the production servers, and provides file and folder recovery from the secondary storage tier

Figure 2 depicts the disk-to-disk-to-tape (D2D2T) architecture for a vSphere environment. D2D2T backups leverage SnapVault or SnapMirror technologies, and they back up data to tape or to NetApp AltaVault® (formerly known as SteelStore) storage, a cloud-integrated, streaming-based storage appliance.

NetApp recommends deploying vSphere on the NFS protocol. This best practice allows better management of Snapshot copies and enables you to leverage the array-based restore capabilities of NetApp SnapRestore® technology, which is referred to as the hardware revert capability in the SnapProtect GUI.

**Note:** The hardware revert feature is available only for vSphere VMs hosted on NFS mounts.
4.1 Validated Lab Design

The VMware vSphere environment used for the validation of this solution was set up according to the guidelines described in TR-3749: NetApp Storage Best Practices for VMware vSphere. Table 1 and Table 2 present configuration details of the validated lab design.

Table 1) Storage layout.

<table>
<thead>
<tr>
<th>Cluster</th>
<th>Storage Virtual Machine (SVM)</th>
<th>Aggregate</th>
<th>Volume</th>
<th>Volume Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>SP_Cluster</td>
<td>VMware_SVM</td>
<td>aggr1</td>
<td>vol1</td>
<td>1500GB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>aggr1</td>
<td>vol2</td>
<td>1500GB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>aggr2</td>
<td>vol3</td>
<td>9000GB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>aggr2</td>
<td>vol4</td>
<td>2000GB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>aggr2</td>
<td>vol5</td>
<td>1200GB</td>
</tr>
</tbody>
</table>

Table 2) LUN information.

<table>
<thead>
<tr>
<th>Tier</th>
<th>Purpose</th>
<th>Protected by SnapProtect?</th>
<th>LUN Information</th>
<th>LUN Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tier 1 (iSCSI datastore)</td>
<td>OS partition for app VMs with RDM</td>
<td>Yes</td>
<td>1 x 1000GB + 1 x 500GB</td>
<td>1500GB</td>
</tr>
<tr>
<td>Tier 2 (NFS datastore)</td>
<td>OS partition for app VMs with GI</td>
<td>Yes</td>
<td>1 x 1000GB + 1 x 500GB</td>
<td>1500GB</td>
</tr>
</tbody>
</table>
Datastore layout planning is critical for the design of the backup architecture. VMs across tier 1, 2, and 3 datastores can be mapped to the respective subclients and policies in the SnapProtect backup workflows. Workflows in the validated lab design were configured in the following way:

- Tier 1 datastores: Configured for SnapVault every 4 hours and for SnapMirror every 15 minutes.
- Tier 2 datastores: Configured for SnapVault every 24 hours and for SnapMirror every 8 hours.
- Tier 3 datastores: Configured for SnapVault daily and for SnapMirror weekly.

Table 3 and Figure 3 describe the network design of the vSphere environment tested in the lab.

Table 3) vSphere network configuration.

<table>
<thead>
<tr>
<th>vSwitch</th>
<th>NIC</th>
<th>Teamed Interfaces</th>
<th>VM Port Group/VMKernel Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>vSwitch0</td>
<td>vmnic0</td>
<td>Active</td>
<td>Management</td>
</tr>
<tr>
<td></td>
<td>vmnic1</td>
<td>Active</td>
<td></td>
</tr>
<tr>
<td>vSwitch1</td>
<td>vmnic2</td>
<td>Not teamed</td>
<td>iSCSI1/NFS1</td>
</tr>
<tr>
<td></td>
<td>vmnic3</td>
<td>Not teamed</td>
<td>iSCSI2/NFS2</td>
</tr>
<tr>
<td>vSwitch2</td>
<td>vmnic4</td>
<td>Active</td>
<td>vMotion</td>
</tr>
<tr>
<td></td>
<td>vmnic5</td>
<td>Active</td>
<td></td>
</tr>
<tr>
<td>vSwitch3</td>
<td>vmnic6</td>
<td>Active</td>
<td>VM network</td>
</tr>
<tr>
<td></td>
<td>vmnic7</td>
<td>Active</td>
<td></td>
</tr>
</tbody>
</table>

Figure 3) vSphere network design layout.

Server Network Interfaces

Management NICs

SAN/NFS NICs

vMotion NICs

VM Network NICs
5 RPO and RTO Requirements

Data corruption and total site failures are two of the many catalysts for data recovery. Understanding your organization’s recovery point objective (RPO) and recovery time objective (RTO) can help you mitigate data loss.

The RPO for VM data corruption on a production server is 15 minutes at a minimum. For an entire site failure, SnapProtect can provide up to a 30-minute RPO. SnapProtect is not an ideal solution for continuous data protection because the minimum RPO that you can achieve is 15 minutes.

Note: To accurately schedule the creation of Snapshot copies, remember to account for data change rates, CPU utilization workloads on the controllers, and the amount of network bandwidth available for replication.

Note: Be sure to test and validate the RPO and RTO requirements defined for your infrastructure before stating them in your disaster recovery (DR) documents.

For VMware vSphere environments running on NFS, data is restored to its previous state in seconds. Array-based restore technologies, such as SnapRestore (hardware revert) and single-file SnapRestore, are enabled by SnapProtect for these types of restore operations.

Note: SnapRestore is available only for recovery from primary Snapshot copies.

VMs hosted on VMFS datastores employ a copy-based restore mechanism for recovery. The time it takes for this type of restore operation (that is, the RTO) depends mainly on network infrastructure limits.

Table 4 lists RPO time frames and design considerations for restoring VM data with SnapProtect.

<table>
<thead>
<tr>
<th>RPO (min)</th>
<th>Recommended Disk Type</th>
<th>Recommended Number of VMs per Subclient</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>SSD</td>
<td>200</td>
</tr>
<tr>
<td>30</td>
<td>15k RPM/10k RPM disks</td>
<td>150</td>
</tr>
<tr>
<td>60</td>
<td>7k RPM disks</td>
<td>100</td>
</tr>
</tbody>
</table>

To obtain the time frames reported in Table 4, we used the following settings in lab tests:

- Multithreading enabled (max. 10). Ten parallel VMware snapshots were invoked inside a vCenter Server per datastore. By default, the maximum number of concurrent VMware snapshot operations is set to 3, but you can modify this value with the registry key `VwDatastoreSnapThreadCount`; the value is set on the Virtual Server Agent (VSA).
- Snapshot workflow without indexing.
- VMs grouped per datastore so that they are part of a single subclient.

In a vSphere environment, the SnapProtect backup process involves first creating a VMware snapshot. The workflow then makes a NetApp Snapshot copy of the VMs to be backed up before the SnapProtect backup job completes. The time it takes to create a VMware snapshot is longer if you use slower disks. In critical environments, NetApp recommends using faster disks for backups to complete in less time.

Table 5 lists RTO time frames and design considerations for restoring VM data with SnapProtect.

<table>
<thead>
<tr>
<th>RTO</th>
<th>Transport Mode</th>
<th>Datastore Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Faster RTOs</td>
<td>Array-based restore (hardware revert)</td>
<td>NFS</td>
</tr>
<tr>
<td>Slower RTOs</td>
<td>NBD/SAN (streaming-based)</td>
<td>SAN (iSCSI/FC/FCoE)</td>
</tr>
</tbody>
</table>
Restoring a SnapProtect backup is faster when VMs are stored in an NFS datastore. The SnapProtect hardware revert feature rapidly restores VMs placed on NFS datastores to their original location or to an alternate location. Hardware revert uses SnapRestore technology to restore VMs and can be used only with NFS datastores.

In a storage area network (SAN) environment, hardware revert is not supported. Restores in a SAN environment must be copy based.

**Note:** RPO and RTO requirements depend on backup scheduling and retention policies.

## 6 Configure SnapProtect for vSphere Backups

To configure SnapProtect for vSphere backups, complete the following steps:

1. **Install SnapProtect.**
   
   **Note:** For information about how to install SnapProtect and test the installation, see [SnapProtect Pre-Deployment Test – Windows](#).

2. **Select New Client > Virtualization > VMware vCenter** to add the vCenter Server credentials.

3. **Enter the vCenter Server host name and the credentials associated with the vCenter Server.** Select a VSA proxy and click OK.
Note: The proxy server is the server on which VSA is installed. To distribute the load, you can configure multiple VSAs, but you must associate a single VSA proxy to each subclient. You can install VSA only on the Windows platform. For more information, see Deployment – SnapProtect for VMware.

The biggest design consideration for VSA is that it sits as close as possible to the vCenter Server to avoid traffic on the WAN. If you have multiple vCenter Servers at different sites, you must typically deploy the media agent and VSA at each site. Configure a proxy ESXi server at the subclient level or datastore level to override the default settings. When backing up vSphere data to tape at a remote site, add the registry key sProxyESX to the remote VSA proxy. Doing so specifies the IP address or host name of the remote proxy ESXi server that will handle mount operations.

7 Configure vSphere Backups

To configure vSphere backups, complete the following steps:

1. From the SnapProtect GUI, create a subclient under the VMware Virtual Server client. Right-click defaultBackupSet and select All Tasks > New Subclient.
   
   Note: For detailed information about creating subclients, see Basic Configuration – SnapProtect for VMware.

2. In the General tab of the Subclient Properties dialog box, enter a name for the subclient.

3. Click the Content tab. Click Browse and select the VMs that you want to protect. You can select VMs individually or the datastore in which they reside.
NetApp recommends that you select the datastore because it maps to a volume on the storage system. Later you can define the minimum number of Snapshot copies for the volume per backup.
4. Click the Storage Device tab and select a storage policy. If no storage policy is available, you can create one by using the Create Storage Policy wizard.

5. Click the SnapProtect Operations tab to set the proxy ESXi server.
   The proxy ESXi server is used in mount operations to perform indexing. The proxy ESXi server must be managed by the vCenter Server, but it cannot be a member of any vSphere cluster.
**Note:** For SnapProtect operations, because mounting and indexing are performance-intensive tasks, NetApp recommends that you keep the proxy ESXi server out of the production cluster. You can select a separate proxy for the backup copy (tape backup). If you do not select a separate proxy, the default proxy used for backups will also be used for tape backups.
6. Click the Advanced Options tab to select the proxy ESXi server for mount and indexing operations.
7. Click the Backup Options tab to select application-aware backups, if applicable, for Exchange or SQL Server by using VSA.
8. Click the Filters tab to select a filter that fits your requirements.

9. Click OK.

10. To disable or enable granular recovery, you can access the Enable Granular Recovery option from two locations in the SnapProtect GUI:
– Right-click the subclient and select Backup > Advanced.

– Under Schedule Policies, select Add New Schedule > Backup Options > Advanced.
Note: Building an index for granular recovery is a time-consuming task. NetApp strongly recommends that you disable granular recovery. If granular recovery is necessary, distribute the VMs across multiple subclients and schedules so that the indexing operation does not overload the ESXi server and the vCenter Server at the same time.

The live browse feature is used in the back end to perform granular recovery of files and folders that have not been previously indexed. The granular recovery option is the old indexing method employed before the inclusion of the live browse capability in SnapProtect. The old method does not support anything newer than ext3 on Linux platforms. If you enable granular recovery, you will never be able to perform a live browse against that backup job because the granular recovery setting cannot be changed after the backup is created.

8 Create a Mirror Copy or a Vault Copy

SnapProtect allows you to create a Snapshot copy (a mirror copy or a vault copy) on a secondary storage system for replication and DR purposes. Before you can create an auxiliary Snapshot copy of your data from the SnapProtect console, you must set up a resource pool and SVM associations on OnCommand Unified Manager.

8.1 Resource Pools

Resource pools are groups of aggregates that are created by the storage administrator through OnCommand Unified Manager to provide storage provisioning to partner applications for backup management. The target SVM is added as a resource pool in Unified Manager.

You might pool your resources based on attributes such as performance, cost, physical location, or availability. By grouping related resources into a pool, you can treat the pool as a single unit for monitoring and provisioning. The pool simplifies the management of these resources and allows more flexible and efficient use of the storage.

Figure 4 shows resource pools in the Unified Manager GUI and Figure 5 illustrates SVM associations.

Figure 4) Resource pools in Unified Manager.

Figure 5) SVM associations to create an auxiliary copy in SnapProtect.

8.2 Create an Auxiliary Snapshot Copy

To create an auxiliary Snapshot copy in SnapProtect, complete the following steps:
1. Right-click a storage policy in the SnapProtect GUI and select All Tasks > Create a New Snapshot Copy.

2. Depending on your requirements, select either the Mirror or the Vault/Backup workflow in the General tab of the Properties dialog box.
3. In the Copy Policy tab, select the source copy for the workflow that you selected in the General tab.

**Note:** In a cascade relationship, SnapProtect does not support the primary-vault-mirror topology (Snapshot copy > SnapVault > SnapMirror). Therefore, the source copy for a mirror copy cannot be a vault copy; it must be a primary snap copy. But for a vault copy, the source copy can be either a primary snap copy or a mirror copy.
4. In the Provisioning tab, select a provisioning policy for the workflow that you selected in the General tab.

Note: The SnapVault Destination provisioning policy with deduplication and compression enables storage efficiency on the secondary storage system.
5. Initiate the Snapshot copy operation. Right-click the storage policy and select All Tasks > Run Auxiliary Copy.

6. In the General tab, select a copy to run and verify that different schedules are configured for each copy in the cascade.
7. In the Job Initiation tab, select the Schedule option to configure a schedule for creating auxiliary copies.

9 Configure Restore Options

Configure Restore Options

Restore operations in SnapProtect have different characteristics and requirements depending on the type of datastore that hosts the VMs to be restored.

9.1 Datastore Types and Restore Requirements

For VMs hosted on an NFS datastore, restore operations have the following requirements:

- You can restore an entire datastore or VM either by volume-based SnapRestore or single-file SnapRestore (hardware revert):
  - Selecting a datastore initiates a volume-based SnapRestore operation.
  - Selecting an individual VM and VM files initiates a single-file SnapRestore operation.
- To perform granular recovery of individual files and folders within the VM, index the data by enabling the granular recovery option. Otherwise, use live browse to perform such restores.
- The proxy ESXi server must be able to access all production datastores through NFS.
For VMs hosted on an FC datastore, restore operations have the following requirements:

- All restores are copy based.
- To configure the entire workflow of a copy-based restore on a SAN, ensure that the VSA proxy is installed on a physical server with an FC host bus adapter (HBA) and logged in to the SAN.
- The proxy ESXi server must be able to access all production datastores through FC.

For VMs hosted on an iSCSI datastore, restore operations have the following requirements:

- All restores are copy based and performed over iSCSI.
- The VSA proxy must be logged in through an iSCSI session to the SVMs that host the datastore.
- For ESXi servers with an enabled FC HBA, the default path for mount operations is the FC path. Force the server to use the iSCSI path by adding the registry `nlscsiEnable` on the VSA.

### 9.2 Configure a Restore

You can initiate restore operations for all of the copies configured in your storage policy. To configure restore options, complete the following steps:

1. From the Storage Policy Properties dialog box, click the Copy Precedence tab to set the number for each restore copy.
2. Right-click the subclient and select Browse and Restore.
3. Click the Advanced Options tab to set the copy precedence.

4. Select a restore type for your VMs. To restore an entire VM at a given location, select the Full Virtual Machine option.
   
   **Note:** You have two options for restoring guest files and folders within the VM:
   
   - Use the live browse feature.
   - Enable the granular recovery option to build an index for the offline restore.
5. Select the VM or VMs that you want to restore and click Recover All Selected.

6. If you are using NFS datastores, select the Use Hardware Revert Capability checkbox.
**Note:** A hardware revert operation invokes either a single-file SnapRestore operation, which restores a single file from the Snapshot copy, or a volume-based SnapRestore operation, which reverts the entire volume to the Snapshot copy. For NetApp NFS configurations, a volume-based restore does the following:

- Reverts all data on the file server volume, not just the data that is associated with the Snapshot copy.
- Deletes all Snapshot copies that were created after the Snapshot copy to which you are reverting.

If you perform a volume revert on the source for a SnapVault or SnapMirror copy and the Snapshot copy to which you are reverting was created before the most recent Snapshot copy moved to the SnapVault or SnapMirror copy, then the SnapVault or SnapMirror copy operation no longer works.

**Note:** The hardware revert option makes the restore process faster. For VMFS datastores, you can perform only streaming-based restores because hardware revert is not supported.

7. If you are restoring an existing VM, select the Unconditionally Overwrite VM with the Same Name checkbox.

8. Select one of the following transport modes for this copy-based restore:
   - **Auto:** By default, the transport mode is network based.
   - **SAN:** If datastores are configured in a SAN environment, all the data transport happens in the SAN (FC or iSCSI).
   - **Hot Add:** The VSA is part of the same ESXi host on which the VM is hosted and restored.
   - **NBD:** The transport mode is network based over the LAN.

![Restore Options for All Selected Items](image-url)
10 Configure Backups to Tape or to a Cloud Appliance

You can back up data to tape, to a virtual tape library, or to an AltaVault appliance.

10.1 Configure Tape Backups

You can configure tape backups in two ways:

- **Server-to-storage-controller backup.** During a server-to-storage-controller backup, the tape library is connected to the controller and configured using NDMP.
- **System-to-server backup.** During a system-to-server backup, the tape library is connected to the media agent and configured as a generic SCSI device. This type of backup is also called a remote backup.

Configure Server-to-Storage-Controller Backup

To configure a server-to-storage-controller backup, complete the following steps:

1. Verify that the tape library is shared across a media agent and the storage node.
2. Configure the tape library by using an NDMP intercluster LIF on the storage node.
   
   Note: For more information about this task, see TR-4330: Cluster-Aware Backup Configuration for SnapProtect and Simpana.
3. From the SnapProtect GUI, right-click the storage policy and select Properties.
4. From the Storage Policy Properties dialog box, configure the Snapshot management rules:
   a. Click the Snapshot tab and select Enable Backup Copy.
   b. Select the Specify the Source Copy checkbox and then select Primary (Classic) Copy from the drop-down menu. This storage policy is usually configured for streaming backup operations.
   c. Click OK.
5. From the SnapProtect GUI, click the Storage Policies tab. Right-click the Primary (Classic) Copy storage policy and select Properties.
6. Click the Data Paths tab. Click Add to add the tape library to the policy.
7. Select the newly added tape library and click Set Default to set it as the default library.

8. Right-click the Primary (Classic) policy and select Change Data Path.
9. From the Drive Pool drop-down list, select the data path to NDMP and click OK to change the data path.

![Image of Change Data Path dialog box]

**Configure System-to-Server Backup**

To configure the tape library on the media agent by using the default settings, complete the following step:

1. Point the data path of the primary (classic) copy to the SCSI device on the media agent that is configured to run the backup.

   **Note:** For more information about this configuration, see the “Remote Backup” section of TR-4330: 
   Cluster-Aware Backup Configuration for SnapProtect and Simpana.

**10.2 Configure AltaVault Backups**

An AltaVault appliance can be connected to SnapProtect as a disk library through the CIFS protocol or the NFS protocol. To configure AltaVault backups, complete the following steps:

1. From the SnapProtect GUI, expand Storage Resources, right-click Libraries, and select Add > Disk Library.

2. Configure the disk library:
   a. Enter a name for the library.
   b. Select a media agent.
   c. Select Network Path.
   d. Enter a user name in the Connect As field.
   e. Enter and confirm the password.
   f. Browse to select a folder for the library.
   g. Click OK.
3. Right-click the Primary (Classic) policy and select Change Data Path. Change the data path to the newly added disk library for the primary (classic) copy in your storage policy and point the backups to the AltaVault appliance.

   **Note:** You must configure the AltaVault appliance to move data to the cloud. Because this data movement is not managed by SnapProtect, the AltaVault configuration is outside the scope of this document. For more information about how to configure AltaVault, see the NetApp SteelStore Solution Guide.

11 SnapProtect and vSphere Disaster Recovery

SnapProtect cannot orchestrate the entire disaster recovery (DR) workflow for vSphere. However, you can use SnapProtect to configure SnapMirror and then use the destination of the mirrored volumes to manually bring up vSphere at the DR location. Using scripts, a vSphere administrator can run the DR orchestration outside of SnapProtect.

The SnapMirror portion of the Site Recovery Manager integration can be implemented by SnapProtect. For more information about this integration, see TR-4264: Deploying VMware vCenter Site Recovery Manager 5 on Clustered Data ONTAP.

Appendix: Backup Test Validation

NetApp validated a cascade D2D2T backup and used the results of the validation test to create the best practices guidance provided in this report. We ran the validation test by using the configuration information listed in Table 1 and Table 2. The test consisted of the following high-level steps:

1. We created a primary Snapshot copy of the production vSphere environment.
2. Using SnapMirror, we created an auxiliary copy and mirrored it on the secondary storage.
3. From the mirrored destination, we used SnapVault to create another copy and stored it on the tertiary storage.
4. We then performed a backup copy operation and streamed it from the SnapVault destination to an AltaVault appliance and a tape library.

In short, we created the primary Snapshot copy of the production environment, mirrored it by using SnapMirror, stored it by using SnapVault, and streamed it to an AltaVault appliance. Table 6 presents the results of the validation test.

Table 6: Validation test results.

<table>
<thead>
<tr>
<th>SnapProtect Operation</th>
<th>Average Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Snapshot copy (100 VMs)</td>
<td>15 minutes</td>
</tr>
<tr>
<td>SnapMirror to secondary cluster (baseline) (5TB datastore)</td>
<td>8 hours</td>
</tr>
<tr>
<td>SnapMirror updates to secondary cluster at a data change rate of 3%</td>
<td>14 minutes</td>
</tr>
<tr>
<td>SnapVault baseline (5TB datastore)</td>
<td>8 hours</td>
</tr>
<tr>
<td>SnapVault updates at a data change rate of 10% per day</td>
<td>30 minutes</td>
</tr>
<tr>
<td>Restore and recovery (SnapRestore)</td>
<td>7 to 8 minutes</td>
</tr>
<tr>
<td>Restore and recovery from SnapVault destination (copy-based full restore)</td>
<td>Close to 9 hours</td>
</tr>
</tbody>
</table>

Note: When running a similar test, plan for 15 minutes of overhead from the native replication operation on Data ONTAP. The overhead might consist of the following elements:
- 5 minutes for the job start notification to OnCommand Unified Manager
- 5 minutes for the confirmation job run by Unified Manager (a one-time activity for provisioning storage on a secondary target)
- 5 minutes for the job completion notification from Unified Manager to the server running SnapProtect

References

This report references the following documents and resources:

- Deployment – SnapProtect for VMware
- Getting Started with User Administration and Security
- NetApp Interoperability Matrix Tool
  [http://support.netapp.com/matrix/mtx/login.do](http://support.netapp.com/matrix/mtx/login.do)
- NetApp SteelStore Solution Guide for CommVault Simpana
  [https://fieldportal.netapp.com/?oparams=278858](https://fieldportal.netapp.com/?oparams=278858)
- Performance Best Practices for VMware vSphere 5.5
  [https://www.vmware.com/pdf/Perf_Best_Practices_vSphere5.5.pdf](https://www.vmware.com/pdf/Perf_Best_Practices_vSphere5.5.pdf)
- Rapid SnapVault/OSSV Space Estimator
  [https://fieldportal.netapp.com/?oparams=65793](https://fieldportal.netapp.com/?oparams=65793)
- SnapProtect Software Binder
- Storage Policy – Getting Started
- System Requirements – CommServe
- TR-3749: NetApp Storage Best Practices for VMware vSphere
- TR-3920: NetApp SnapProtect Management Software Solution Overview
- TR-4264: Deploying VMware vCenter Site Recovery Manager 5 on Clustered Data ONTAP
- TR-4330: Cluster-Aware Backup Configuration for SnapProtect and Simpana
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 © 1994–2015 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52.227-19 (June 1987).

Trademark Information

NetApp, the NetApp logo, Go Further, Faster, AltaVault, ASUP, AutoSupport, Campaign Express, Cloud ONTAP, Clustered Data ONTAP, Customer Fitness, Data ONTAP, DataMotion, Fitness, Flash Accel, Flash Cache, Flash Pool, FlashRay, FlexArray, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexVol, FPolicy, GetSuccessful, LockVault, Manage ONTAP, Mars, MetroCluster, MultiStore, NetApp Insight, OnCommand, ONTAP, ONTAPI, RAID DP, RAID-TEC, SANtricity, SecureShare, Simplicity, Simulate ONTAP, Snap Creator, SnapCopy, SnapDrive, SnapIntegrator, SnapLock, SnapManager, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapValidator, SnapVault, StorageGRID, Tech OnTap, Unbound Cloud, WAFL, and other names are trademarks or registered trademarks of NetApp Inc., in the United States and/or other countries. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. A current list of NetApp trademarks is available on the web at http://www.netapp.com/us/legal/netapptmlist.aspx, TR-4456-0915