Technical Report

SnapDrive 6.2 for Windows Best Practices

SnapDrive for Windows Team, NetApp
March 2010 | TR-3828

SIMPLIFYING AND AUTOMATING STORAGE AND DATA MANAGEMENT FOR WINDOWS ENVIRONMENTS

NetApp® SnapDrive® for Windows® simplifies management of business-critical information with its advanced server-based storage virtualization, helps businesses respond quickly to growth by providing the ability to expand storage on the fly with no downtime, speeds backup and restore of data in seconds with integrated Snapshot™ technology, and provides increased availability by performing online cloning and replication of production data without causing any downtime. This document details the best practices for deploying and using SnapDrive 6.2 for Windows.

TABLE OF CONTENTS

1 INTRODUCTION

This technical report is a best practices guide for NetApp storage systems using the SnapDrive for Windows solution. It also offers recommendations on various configuration options available with the solution and guidelines for when and where to use the options.

1.1 PURPOSE AND SCOPE

The success or failure of any software or infrastructure deployment hinges on making the proper design and architecture decisions up front. The goal of this guide is to provide guidelines for deploying and using SnapDrive for Windows with a NetApp storage appliance and any supporting software.

1.2 INTENDED AUDIENCE

This guide is intended for storage and server administrators and experts managing storage provisioning and Snapshot copies for NetApp storage systems by using the SnapDrive for Windows solution. NetApp recommends that users refer to the following documents before using this guide:

- SnapDrive for Windows Installation and Administration Guide
- SnapDrive for Windows Release Notes
- Technical Overview of NetApp SnapDrive
- NetApp Interoperability Matrix Tool
- Data ONTAP System Administration Guide
- Block Access Management Guide for iSCSI and FC for your release of Data ONTAP®
- Host Utilities Installation and Setup Guide
- Fibre Channel and iSCSI Configuration Guide for Data ONTAP

A good understanding of Windows file system administration is necessary, as well as an understanding of FCP and iSCSI concepts. The recommendations in this document are guidelines to assist with configuration of SnapDrive for Windows.

2 OVERVIEW

SnapDrive for Windows is an enterprise-class storage and data management application that simplifies storage management and increases availability of application data. The key functionality includes error-free application storage provisioning, consistent data Snapshot copies, rapid application recovery, and the ability to easily manage data. SnapDrive for Windows complements the native file system and volume manager, and it integrates seamlessly with the clustering technology supported by the host operating system. SnapDrive for Windows is supported on the following operating systems.

- Windows Server® 2008 (x86, x64, or IA64)
- Windows Server 2008 Hyper-V™
- Windows Server 2008 Server Core
- Windows Server 2008 R2
- Windows Server 2003 SP2 Standard or Enterprise

2.1 KEY FEATURES

Following are the key features of SnapDrive for Windows:

- Enhances online storage configuration, LUN expansion and shrinking, and streamlined management.
- Supports connections of up to 168 LUNs.
- Integrates Data ONTAP Snapshot technology, which creates point-in-time images of data stored on LUNs.

- Works in conjunction with SnapMirror® software to facilitate disaster recovery from either asynchronously or synchronously mirrored destination volumes.
- Enables SnapVault® updates of qtrees to a SnapVault destination.
- Enables management of SnapDrive on multiple hosts.
- Enhances support on Microsoft® cluster configurations.
- Simplifies iSCSI session management.
- Enables technology for SnapManager® products.

For details about SnapDrive for Windows minimum host requirements, required hot fixes, and features, refer to the SnapDrive 6.2 for Windows Installation and Administration Guide.

2.2 SNAPDRIVE FOR WINDOWS DEPLOYMENTS

SnapDrive for Windows can be used either as a standalone product or as a part of other NetApp solutions. For example, it can be deployed along with SnapManager for Exchange, SnapManager for SQL Server®, and SnapManager for SharePoint®. In both types of deployments, SnapDrive for Windows serves as a tool to create and manage storage. It also takes storage backup and restores storage from those backups, using Snapshot technology. SnapDrive for Windows integrates with Windows Volume Manager and also works in clustering and multipathing deployments by using FCP and iSCSI transport protocols. For a complete list of supported platforms, refer to the NetApp Interoperability Matrix Tool.

3 NEW IN SNAPDRIVE 6.2

- **Dynamic addition and removal of pass-through disks:** Support for dynamically adding and removing pass-through disks on Hyper-V virtual machines.
- **SnapDrive for Windows File-Level Restore:** Administrators can use the SnapDrive command-line interface to restore one or more files on a LUN from its corresponding Snapshot copy.
- **Role-based access control with Operations Manager:** Role-based access control (RBAC) is used for user login and role permissions. RBAC allows administrators to manage groups of users by defining roles. This feature requires Operations Manager.
- **Microsoft Cluster Shared Volumes:** Support for Microsoft Cluster Shared Volumes using Windows Server 2008 R2.
- **Microsoft clusters using FC pass-through LUNs with VMware ESX 4.0:** Support for creating Microsoft clusters using FC RDM LUNs on Windows Server 2003 and on Windows Server 2008 systems with VMware® ESX 4.0.
- **VMware ESX iSCSI initiators:** Support for RDM LUNs using VMware ESX iSCSI initiators.

Some of these new features and other features are explained in detail in this guide. For a detailed list of new features, refer to the SnapDrive 6.2 for Windows Installation and Administration Guide.

4 INSTALLATION AND BASIC CONFIGURATION

SnapDrive 6.2 for Windows software can be obtained from the NOW™ (NetApp on the Web) site. For detailed installation instructions, see the SnapDrive 6.2 for Windows Installation and Administration Guide. Before installing SnapDrive for Windows, use the following checklists to avoid potential errors or delays during or after the installation.

4.1 CHECKLIST FOR STORAGE SYSTEM

Step	Action
1	Verify license on the storage system. Use the `license` command on the CLI, FilerView®, or System Manager to verify installed licenses: • FCP, iSCSI, or NFS license, depending on the configuration • FlexClone® • SnapRestore® • SnapMirror • SnapVault • MultiStore® (vFiler™ environment only)
2	Verify whether FCP or iSCSI is enabled on the storage system. Use `fcp status` or `iscsi status`. If the status is Disabled, start the service by using the following command: `fcp start` or `iscsi start`
3	Note the storage system target address by using the following command on the storage system CLI: • For FCP, run `fcp nodename` • For iSCSI, run `iscsi nodename`
4	Make sure that the Fibre Channel port on the NetApp storage system is configured as target, using the `fcadmin config` command. For details, refer to the Data ONTAP Storage Management Guide.
5	Enable, configure, and test RSH or SSH access on the storage system for administrative access. SSH is recommended because it is more secure. For detailed information about these tasks, refer to the Data ONTAP Storage Management Guide.

Note: Determine whether zoning is required and make sure that the zoning configuration of the switch is appropriate. For information about zoning, refer to the Fibre Channel and iSCSI Configuration Guide for Data ONTAP.

If problems are encountered in the FCP or iSCSI connectivity, use the nSANity program to get information about the problem. The nSANity program can be downloaded from the Toolchest section on the NOW site. Refer to section 4.2, “Checklist for Host before SnapDrive Installation,” for details.

BEST PRACTICE

By default, any IP interface on the storage system accepts iSCSI commands. To make sure that all iSCSI commands are processed by the appropriate interfaces, disable iSCSI processing on a particular Ethernet interface by using the following command:

```
iscsi interface disable <interface_name>
```

For example:

```
iscsi interface disable e0b
```

Note: Do not use this command while active iSCSI sessions are connected to the Ethernet interface, because this may disrupt active sessions. Active sessions must first be disconnected from the host; otherwise, the storage system generates a warning when the command is issued.

4.2 CHECKLIST FOR HOST BEFORE SNAPDRIVE INSTALLATION

Before using or installing SnapDrive for Windows, make sure that the minimum requirements are met and that all components such as the OS version, software pack, hot fixes, multipath solution, cluster solution, and so on are valid by referring to product support matrixes and product documentation.

Step	Action
1	**Determine whether the version of Windows is supported by SnapDrive for Windows:** To determine which version of Microsoft Windows is being run: 1. On the taskbar at the bottom of the screen, click Start and then click Run. 2. In the Run dialog box, enter `winver`. **Note:** If running Windows 2008, enter `winver` in the Search box. 3. Click OK. A dialog box displays the version of Windows being run.

2	**For FCP environment:**
	1. Check the SnapDrive for Windows supported Host Utility version from the NetApp Interoperability Matrix Tool.
	2. Verify that NetApp Host Utilities are present on the host:
	`C:\Program Files\NetApp\FCP Host Utilities\san_version.exe`
	3. If Host Utilities are not installed, download and install the correct version from the NOW site; see the Host Utilities Installation and Setup Guide to install (or upgrade) and configure Host Utilities.
	4. Identify the HBA adapters on the host and verify that the ports are enabled:
	`C:\Program Files\NetApp\FCP Host Utilities\hba_info.exe`
	
	For iSCSI environment:
	1. Check the SnapDrive for Windows supported Host Utility version from the NetApp Interoperability Matrix Tool.
	2. Verify that NetApp Host Utilities are present on the host:
	3. `C:\Program Files\NetApp\FCP Host Utilities\san_version.exe` If Host Utilities are not installed, download and install the correct version from the NOW site; see the Host Utilities Installation and Setup Guide to install (or upgrade) and configure Host Utilities.
	4. Identify the iSCSI initiator running on the Windows host:
	`C:\Program Files\NetApp\FCP Host Utilities\msiscsi_info.exe`
	
	Note: It is essential that:
	• The HBA and its utility software are installed properly
	• An iSCSI initiator is already installed on the system and is supported
	• All required hot fixes are installed on the host

BEST PRACTICES

Refer to the NetApp Interoperability Matrix Tool and check the following items:

- Confirm that SnapDrive for Windows supports the environment.
- For specific information about requirements, see

  SnapDrive 6.2 for Windows Installation and Administration Guide

  Fibre Channel and iSCSI Configuration Guide for Data ONTAP
- Always download the latest Host Utility Kit from the download section of the NOW site.
- NetApp recommends performing all procedures from the system console and not from a terminal service client.
- After completing the preceding checklist, see the steps in the SnapDrive 6.2 for Windows Installation and Administration Guide for details of how to install SnapDrive for Windows.
- Refer to the SnapDrive 6.2 for Windows Release Notes for the latest fixes, known issues, and documentation correction.

4.3 SNAPDRIVE FOR WINDOWS SERVICES

NetApp SnapManager products like SnapManager for Exchange, SnapManager for SQL Server, and SnapManager for SharePoint leverage SnapDrive for Windows to create application-consistent backups, perform fast restores, and create clones quickly.

For SnapDrive for Windows commands and APIs to work, the SnapDrive services must be running. The following table describes the services available in the SnapDrive for Windows installation.

Table 1) SnapDrive for Windows Services

Windows Service	Description of Service	Path to executable
SnapDrive	Manages and monitors NetApp SnapDrive	`C:\Program Files\NetApp\SnapDrive\SWSvc.exe`
SnapDrive Management Service	Manages SnapDrive in the local or remote system via CLI or GUI	`C:\Program Files\NetApp\SnapDrive\SDMgmtSvc.exe`

Note: Paths to SnapDrive executables are determined by the drive letter used when installing SnapDrive for Windows.

BEST PRACTICES

- The SnapDrive for Windows service account must have administrative rights on the host and must be a member of the storage system's local administrators group.
- Certain security policies set on the windows host or domain may cause SnapDrive service startup issues and errors.

For information about authentication requirements, refer to “Configuring Access for SnapDrive” in the SnapDrive 6.2 for Windows Installation and Administration Guide.

4.4 SETTING UP SNAPDRIVE TO COMMUNICATE TO A NETAPP STORAGE SYSTEM

Step	Action
1	**Verify the SnapDrive for Windows installation and version:** From the host with the SnapDrive installation: 1. Open the Microsoft Management Console (MMC). 2. Select the SnapDrive host.

	3. Select Help > About SnapDrive Management Snapping. .
2	**Check the network connectivity and DNS resolution from the host to storage system:** `ping <storage_system_IPaddress >`; `ping <storage_system_name>`
3	**Configure SnapDrive for Windows to use the preferred IP address for the storage controller.** For more information, refer to "Setting a Preferred IP Address" in the SnapDrive 6.2 for Windows Installation and Administration Guide.

4.5 INSTALLATION AND CONNECTIVITY ISSUES

Step	Action
1	Verify that configuration is supported on the NetApp Interoperability Matrix Tool.
2	Verify that the SnapDrive service account has appropriate credentials and privileges on both the host and the storage controller, has a working password, and can log in to the host and the storage controller.
3	Verify that all required services are enabled and started. SnapDrive requires the following: • Windows Management Instrumentation Service • Virtual Disk Service • Plug and Play Service • RPC Service
4	Check for any Windows local security policies that may interfere with connectivity or installation. From the host, select: Local Security Policies > Security Settings > Local Policies > User Rights Assignments
5	If in a cluster configuration, check the Windows firewall on the local node and all other nodes. Enable SnapDrive to communicate through the firewall. For details, refer to the SnapDrive 6.2 for Windows Installation and Administration Guide. or Disable the firewall. (Not recommended for security reasons.)
6	User credentials during installation should be in the domainname/username format.

5 SECURITY AND ACCESS CONTROL

SnapDrive for Windows offers the following levels of security:

- **HTTPS:** Allows all interactions with the storage system and host through the Data ONTAP interface, including sending the passwords in a secure fashion.
- **Access control:** Allows administrators to specify the operations that a host running SnapDrive for Windows can perform on a storage system. Access control permissions must be set individually for each host. The Storage Access Control Tool for SnapDrive on NOW (`storacl.exe`) can be used to set individual host access permissions or RBAC via Operations Manager. For information about Data ONTAP access control, refer to Role-Based Access Control for Data ONTAP 7G.

5.1 HTTPS

- For added security, use HTTPS instead of HTTP for host-to-storage-system communication. To use HTTPS:
  1. Configure and enable HTTPS on the storage system side:

a. SecureAdmin `setup ssl`

b. Options `ssl.enable on`

2. During SnapDrive installation, there is a prompt to configure default transport protocol as RPC, HTTP, or HTTPS. Transport protocols can also be set after installation with either of the following methods.

   a. `sdcli transport_protocol set -m MachineName -f StorageSystemName -type HTTPS -port 443 [-user UserName] [-pwd Password]`

      or

   b. Open Microsoft Management Console (MMC).Select the SnapDrive host and right-click for transport settings.

   Note: HTTPS is not supported with MultiStore.

BEST PRACTICE

For the highest level of security, use HTTPS as the communication method whenever possible.

For more information about general security best practices, refer to Best Practices for Secure Configuration of Data ONTAP 7G.

5.2 ACCESS CONTROL

BEST PRACTICE

NetApp recommends using Operations Manager for RBAC control, as described in section 5.4. In an environment where Operations Manager is not being used for RBAC, users can use the Storacl tool, found in the Toolchest on NOW.

Figure 1 show the flow of SnapDrive access control when RBAC has been configured with Operations Manager and Storacl.

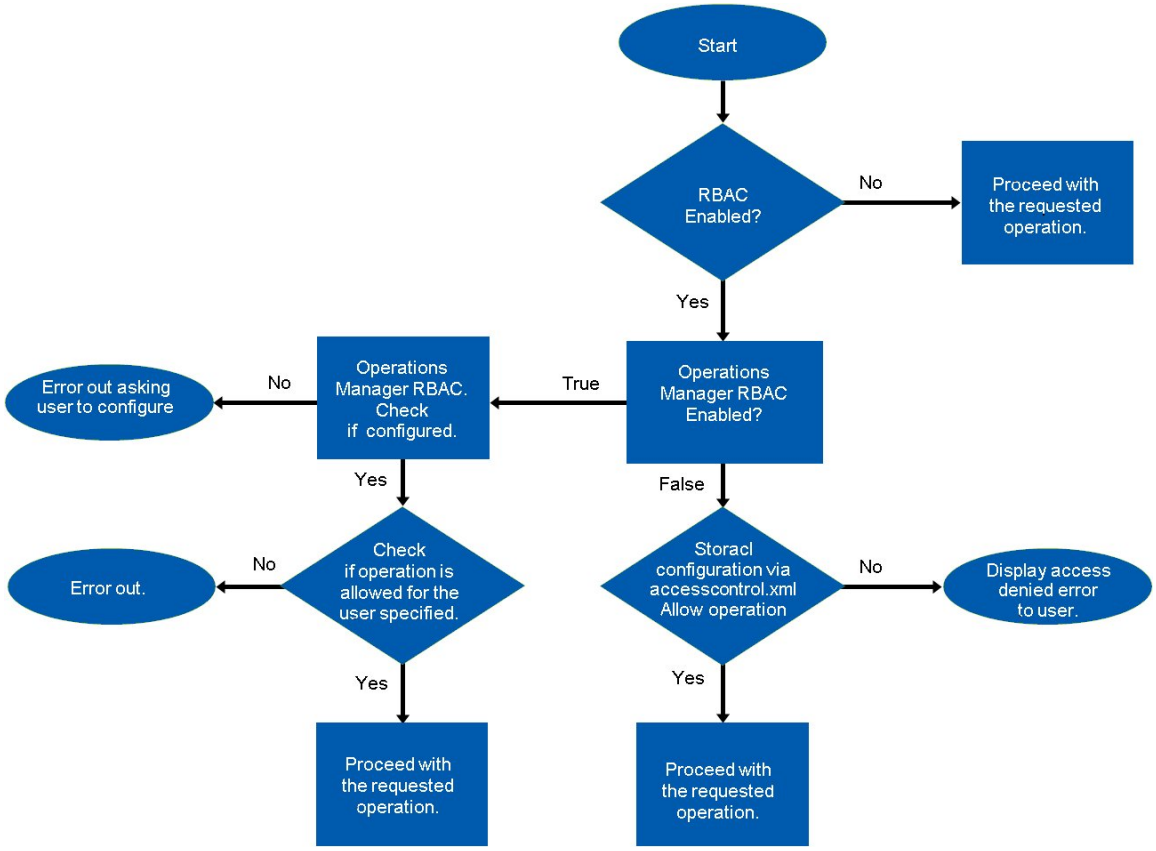

Figure 1) Flow of SnapDrive access control.

5.3 CONFIGURING ACCESS CONTROL WITH STORACL

Storacl gives storage administrators the ability to set access control for different users for different storage resources such as aggregates, volumes, qtrees, and LUNs on specific storage systems. Storacl also allows storage administrators to create settings for thin provisioning LUNs. For information about how to use the Storacl tool, see the Storage Access Control Guide.

5.4 CONFIGURING ROLE-BASED ACCESS CONTROL WITH OPERATIONS MANAGER

RBAC is implemented by using the Operations Manager infrastructure. SnapDrive 6.2 for Windows conforms to the policies set on Operations Manager. SnapDrive contacts Operations Manager to check for required permissions before proceeding with a given operation. If the policy does not exist, or if a deny policy is created, the operation produces an error message.

There are two methods of enabling RBAC for SnapDrive:

- RBAC can be enabled during initial SnapDrive via the installation wizard.
- If SnapDrive is already installed on the host, RBAC can be enabled via SDCLI.

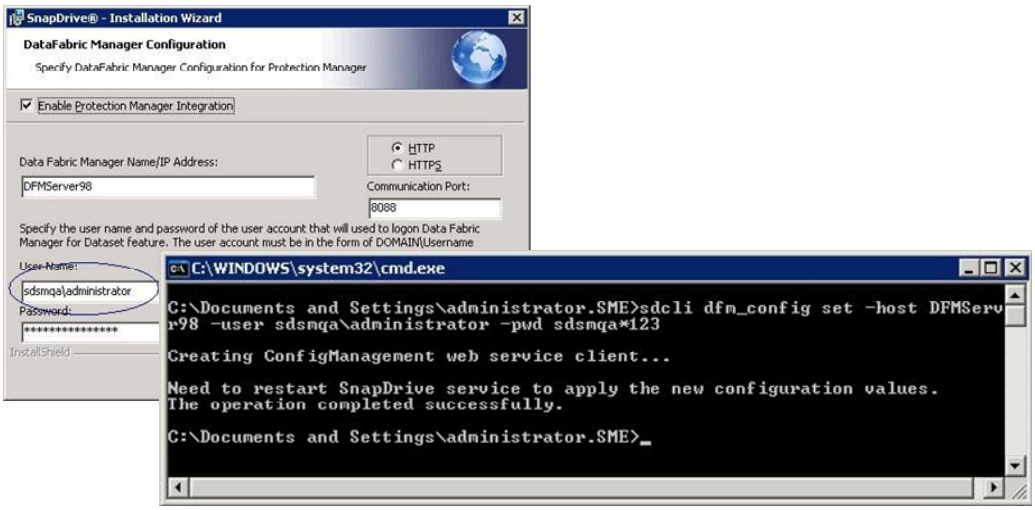

Figure 2) Enabling RBAC in SnapDrive.

Enable DFM RBAC on the storage system with the Storacl tool, found in the Toolchest on NOW.

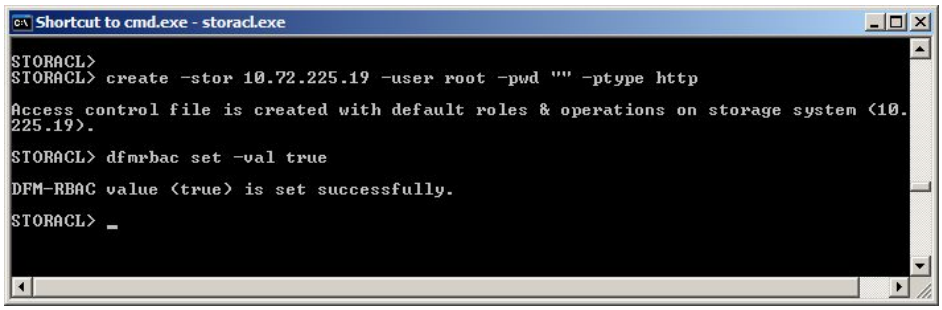

Figure 3) Enabling RBAC on the storage system.

Note: SnapDrive for Windows must be installed with the Operations Manager server settings, such as the OM server name and IP address, user name, and password.

To configure a SnapDrive for Windows RBAC user, select the SnapDrive for Windows user that will be used for RBAC (for example, DOMAIN\username).

The user must have the minimum capability of core access check over global group or (`global DFM.Core.AccessCheck`) in Operations Manager. The Operations Manager administrator configures the user with specific roles and capabilities according to resources and available operations. (For example, `global DFM.Database.Write` enables SnapDrive to refresh storage system entities on Operations Manager.)

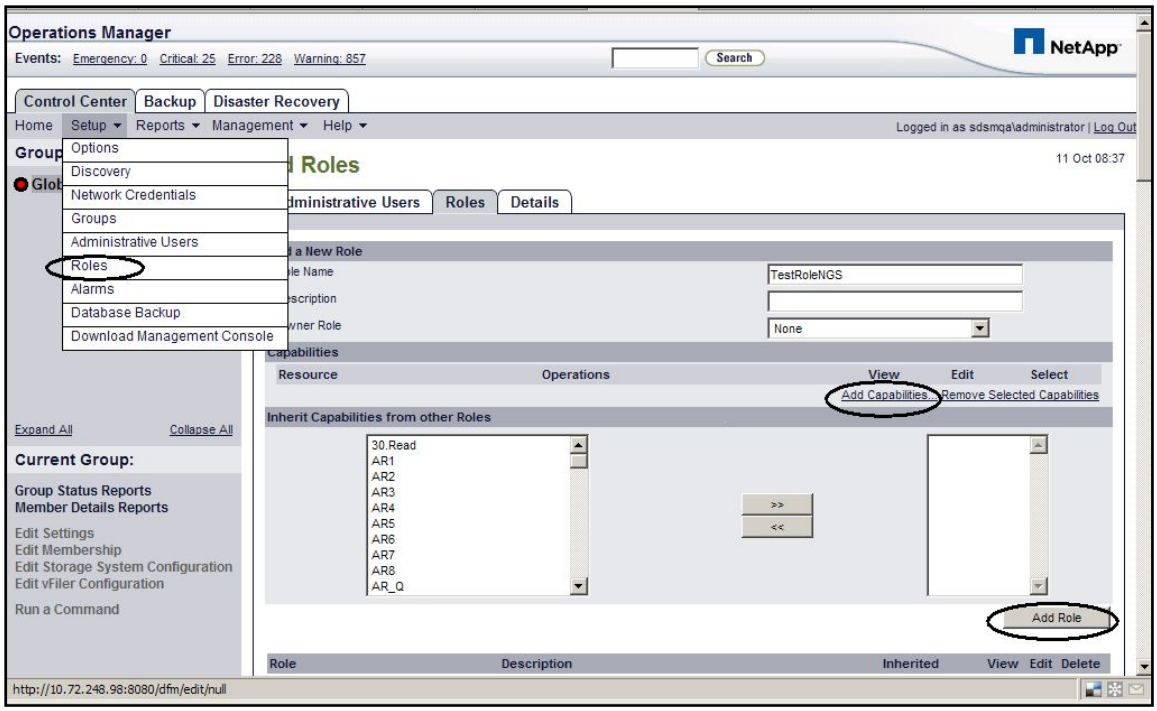

Figure 4) Roles and capabilities.

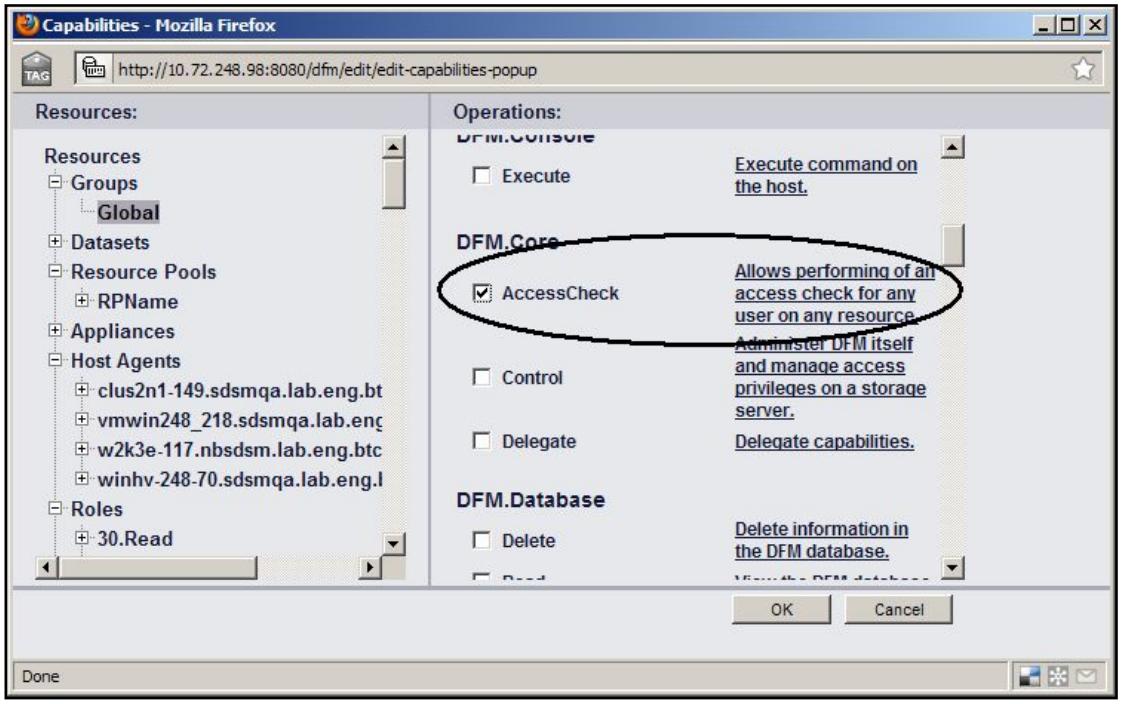

Figure 5) Enable AccessCheck for an user.

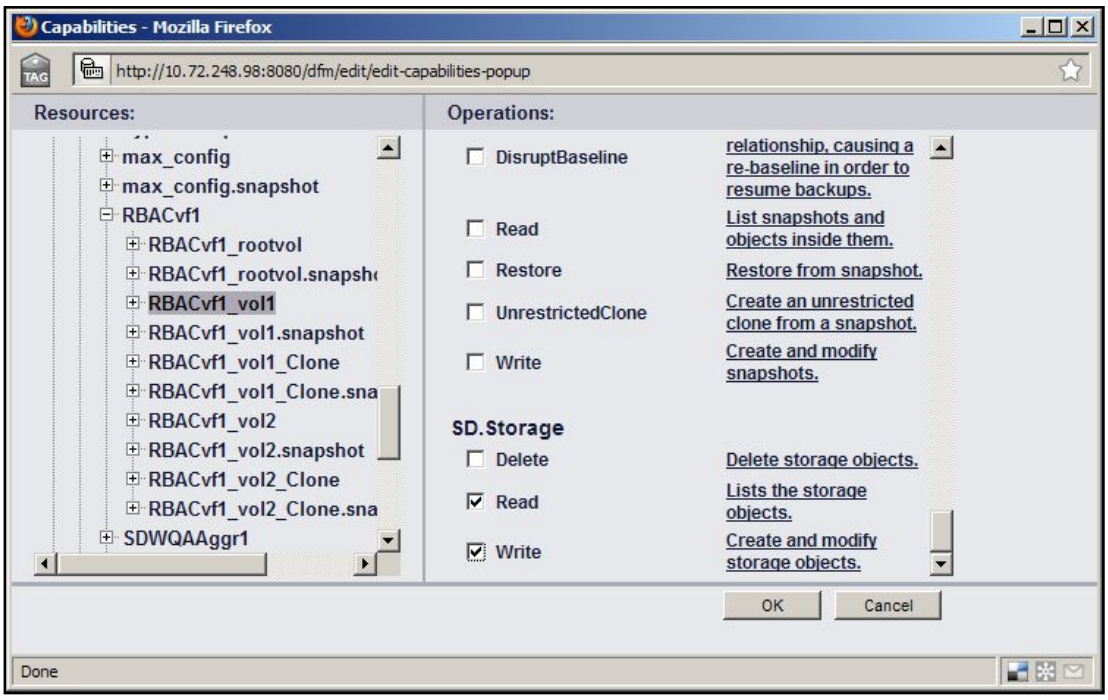

Figure 6) Enable Read, Write permissions for a user.

The Operations Manager administrator must grant capabilities to the invoker of SnapDrive in order to execute SnapDrive commands. For information about the mapping between various capabilities compared to commands, see the SnapDrive 6.2 for Windows Installation and Administration Guide.

Preconfigured roles simplify the task of assigning roles to users. The following table describes the predefined roles on the Operations Manager server.

Table 2) Available Roles on the Operations Manager server

Role Name	Description
`GlobalSDStorage`	Manage storage with SnapDrive for Windows
`GlobalSDConfig`	Manage configurations with SnapDrive for Windows
`GlobalSDSnapshot`	Manage Snapshot copies with SnapDrive for Windows
`GlobalSDFullControl`	Full use of SnapDrive for Windows

Table 3) SDW to RBAC role mapping

SDW operation	Operations Manager RBAC role capability
`disk create`	For LUNs inside volumes:{SD.Storage.Write, Volume} For LUNs inside Qtrees:{SD.Storage.Write, QTree}
`disk delete`	{SD.Storage.Delete, LUN}

`disk connect`
`disk disconnect`
`disk disconnect –f`
	{SD.Storage.Write, LUN}

`disk list`	{SD.Storage.Read, Volume}
`snap list`	{SD.SnapShot.Read, Volume}
`snap create`	{SD.SnapShot.Write, Volume}

`snap restore`	{SD.SnapShot.Restore, Volume}
`snap delete`	{SD.SnapShot.Delete, Volume}
`snap rename`	{SD.SnapShot.Write, Volume}
`snapvault archive`	{SD.SnapShot.Write, Secondary Volume}
`snapvault snapshot_delete`	{SD.SnapShot.Delete, Secondary Volume}
`snapvault snap_list`	{SD.SnapShot.Read, Secondary Volume}
`snapvault verify_configuration`	{SD.SnapShot.Read, Primary and Secondary Volume}
`snapvault rename`	{SD.SnapShot.Write, Secondary Volume)
`igroup create`	{SD.Config.Write, Storage System}
`igroup rename`	{SD.Config.Write, Storage System }
`igroup delete`	{SD.Config.Delete, Storage System }
`igroup list`	{SD.Config.Read, Storage System }
`snap mount`	For LUN clones in Volume: {SD.SnapShot.Clone, Volume} For LUN clones in QTree: {SD.SnapShot.Clone, QTree} For traditional volume clones: {SD.SnapShot.Clone, Storage System } For flex volume clones: {SD.SnapShot.Clone, Parent Volume} For flex volume clones which are split: {SD.SnapShot.Clone, Parent Volume }
`snapshot unmount`	For lun clones (lun resides in Volume or QTree): {SD.SnapShot.Clone, Volume} For volume clones: {SD.SnapShot.Clone, Parent Volume}
`volume create`	{SD.Storage.Write, Aggregate}
`volume rename`	{SD.Storage.Write, Volume}
`volume delete`	{SD.Storage.Delete, Volume}
`volume list`	{SD.Storage.Read, Aggregate }
`aggregate list`	{SD.Storage.Read, Storage System }

6 STORAGE PROVISIONING

SnapDrive for Windows allows administrators to create, delete, map, unmap, shrink, and grow LUNs on a storage system and to connect to LUNs that already exist on the storage system. If administrators have to perform these tasks without SnapDrive for Windows, they must be performed manually. SnapDrive for Windows simplifies these tasks by reducing the time and probable errors of the manual process.

Note: Although SnapDrive for Windows can create storage by using a minimum of options, NetApp recommends that users understand the default values and use them appropriately.

Proper sizing is crucial to avoiding volume-full conditions that can adversely affect the environment. Properly sizing aggregates, volumes, and LUNs depends on various aspects of the environment.

BEST PRACTICES

- Do not create LUNs on the root storage system volume `/vol/vol0`.
- For better Snapshot copy management, do not create LUNs on the same storage system volume if those LUNs have to be connected to different hosts.
- If multiple hosts share the same storage system volume, create a qtree on the volume to store all LUNs for the same host.

- SnapDrive for Windows allows administrators to shrink or grow the size of LUNS. Never expand a LUN from the storage system; otherwise, the Windows partition will not be properly expanded.
- Make an immediate backup after expanding the LUN so that its new size is reflected in the Snapshot copy. Restoring a Snapshot copy made before the LUN was expanded will shrink the LUN to its former size.
- Do not have LUNs on the same storage system volume as other data; for example, do not place LUNs in volumes that have CIFS or NFS data.
- Calculate LUN size according to application-specific sizing guides and calculate for Snapshot usage if Snapshot copies are enabled.
- Depending on the volume or snap reserve space available, use the option `volume auto grow` or `snap auto delete` to avoid a volume-full condition due to poor storage sizing.

For information about calculating the size of the storage system volume, refer to the Fibre Channel and iSCSI Configuration Guide for Data ONTAP or search the Technical Reports Library for application-specific documentation.

6.1 VOLUME AND LUN SIZING

A volume running out of space can affect the host's ability to write to a LUN, which can cause severe problems. Proper space management can prevent such problems by planning ahead and proactively monitoring the storage. When planning or sizing LUNs, consider LUN growth rate and rate of change to estimate when a volume will run out of space.

For example, Figure 7 illustrates the type of information and assumptions that you might make about LUN growth for a specific environment.

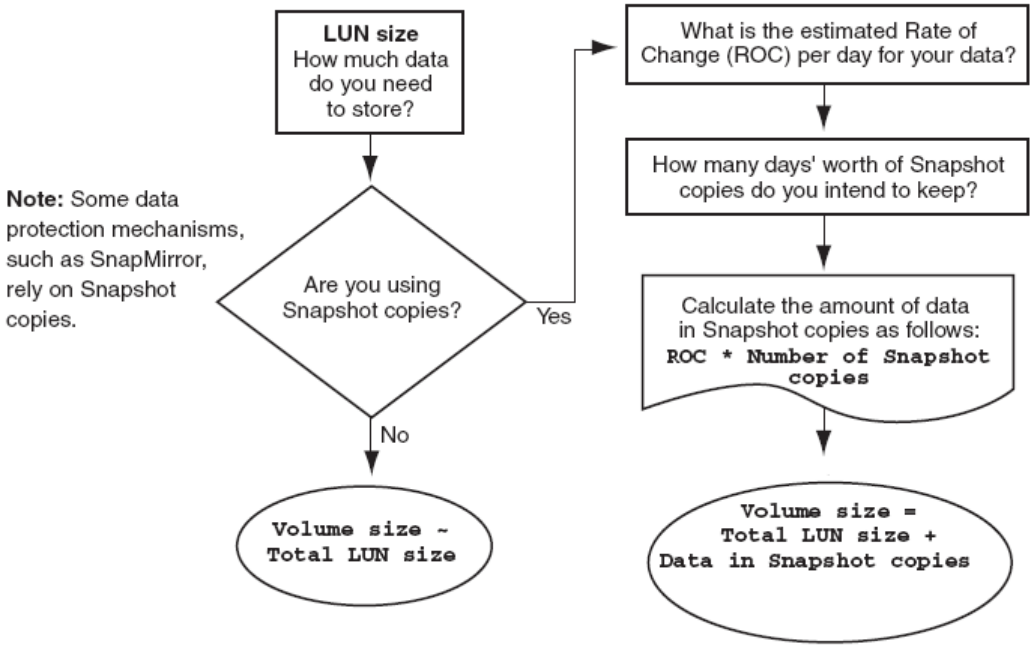

Figure 7) Information and assumptions about LUN growth.

BEST PRACTICE

For best practice guidelines in sizing environments, refer to application-specific best practices and also to the Block Access Management Guide for iSCSI and FC for your release of Data ONTAP.

6.2 THINLY PROVISIONED ENVIRONMENTS

SnapDrive allows administrators to overprovision storage, over what is physically available. Administrators can configure SAN attached servers with LUNs large enough to meet customer needs, and on the storage side they can increase physical disk hardware as required, providing better storage investments.

Advantages of thin provisioning:

- Less storage is required initially when buying a new storage system.
- More servers per storage system provide a greater level of consolidation.
- An application server's total disk capacity can be over-allocated, providing good ROI.
- Monitoring storage space is critical in thin provisioned environments; otherwise, available storage space can be exhausted, causing application down time. One method of protection in this kind of environment is to use the Snapshot Autodelete and Volume Auto-grow features. For information about these features, refer to the Data ONTAP System Administration Guide.

In conjunction with SnapDrive, the Storacl tool allows the creation of thin provisioned LUNs on storage. The Storacl tool allows disabling LUN reservation and creating thin provisioned LUNs with a maximum size of 16TB. The Storacl tool can be downloaded from the Toolchest on NOW.

To enable or disable LUN space reservation, follow these steps:

1. Check the current LUN space reservation policy by using the following command:

   ```
   spacereserve get -vol <volume name> [-stor <storage system> -user <Root
   userName> -pwd <password> -port HTTPsPortNumber>
   ```

   Result: If no policy has been set, "File is not found on the storage system." is returned. Otherwise, an output such as "Volume Path:volume_name Space reservation:false" or "Volume Path:volume_name Space reservation:true" is returned, depending on whether the LUN space reservation is set to Disabled or Enabled.

2. Enable or disable LUN space reservation:

   ```
   spacereserve set -vol <volume name> -val <true|false> [-stor <storage
   system> -user <Root userName> -pwd <password> -port <HTTPsPortNumber>
   ```

Note: The `spacereserve set` command creates a file named `ThinProvision.xml` on the `/etc` folder of the storage system. SnapDrive always checks this file before creating a new LUN on a volume to determine whether LUN space reservation should be enabled for the new LUN.

BEST PRACTICE

For best practice guidelines in thinly provisioned environments, refer to Thin Provisioning in a NetApp SAN or IP SAN.

6.3 STORAGE PROVISIONING IN A MULTISTORE ENVIRONMENT

SnapDrive can manage LUNs on MultiStore units when using the iSCSI protocol. SnapDrive does not distinguish between a physical storage system and a MultiStore unit. Therefore there are no changes in the SnapDrive commands. Also, SnapDrive for Windows does not support FCP when connecting to LUNs on the MultiStore unit.

For details about SnapDrive for Windows MultiStore support, refer to the SnapDrive 6.2 for Windows Installation and Administration Guide.

7 SPACE MANAGEMENT AND FRACTIONAL RESERVATIONS

Data ONTAP uses space reservation to guarantee writes to a LUN or to overwrite data on a LUN. When a LUN is created, Data ONTAP reserves enough space in the traditional or flexible volume so that write operations to those LUNs do not fail due to lack of disk space. Other operations, such as making a Snapshot copy or creating new LUNs, can succeed only if there is enough available unreserved space.

BEST PRACTICE

Actively monitor data in the volume by using the `df -r` command to make sure that overwrite reserve space is not exhausted.

For information about calculating the size of the storage system volume, refer to the Block Access Management Guide for iSCSI and FC for your release of Data ONTAP.

7.1 FRACTIONAL RESERVE

For information about calculating fractional reserve, refer to the Block Access Management Guide for iSCSI and FC for your release of Data ONTAP.

BEST PRACTICES

Use caution when changing the fractional reserve value to a value less than 100%, because when space is fully consumed, the write operation fails and that disrupts the environment.

Do not modify fractional reserve:

- Unless there is a mechanism to monitor fractional reserve or volume and aggregate available space. SnapDrive for Windows does not provide this functionality.
- If there are multiple LUNs in a volume and each LUN has a different rate of change, an estimate must be made of the overall volume size and the combined fractional reserve setting based on the average rate of change of all the LUNs.
- Snapshot Autodelete and/or Volume Autosize should be used when setting fractional reserve to a value less than 100%.

8 SNAPSHOT COPY MANAGEMENT

SnapDrive for Windows integrates with NetApp Snapshot copy technology to make stored data reliable to host applications. Offering the ability to create and manage Snapshot copies from the host makes SnapDrive for Windows especially valuable to users.

Snapshot copies record the state of the blocks in the file system at a given time and provide read-only access to that image of the file system. SnapDrive for Windows enables the creation, restoration, and deletion of Snapshot copies of the file system and the cloning of storage entities from Snapshot copies. For information about the commands used to perform these tasks, refer to the SnapDrive 6.2 for Windows Installation and Administration Guide.

SnapDrive for Windows Snapshot copies are widely used because of the following advantages:

- Host-consistent Snapshot copies (restorable copy)
- Faster restore time
- Create backups of larger amounts of data much faster

8.1 SNAPSHOT COPY MANAGEMENT

For Data ONTAP 7.1 and later, SnapDrive uses the LUN-clone-split-restore method for SnapRestore operations. This has the limitation that Snapshot copy creation on the volume is not allowed until the LUN-clone-split operation is completed. Therefore NetApp recommends monitoring LUN cloning status from the

storage system CLI by using the `LUN clone split status` command before initiating SnapRestore operations from SnapDrive.

SnapDrive for Windows also allows administrators to connect to Snapshot copies, enabling them to connect to replicated copies of the existing data.

Here are two example scenarios in which the cloning feature might be used:

- When there is an available update for the application running on the storage system LUNs, to make sure that the updated software runs satisfactorily before using it in production.
- To create a copy of LUNs on the NetApp storage system that can be mounted on the same host or on a different host to separate the upgrade and testing processes. After the new application update, the Snapshot LUN file can be destroyed and the update can be performed on the production storage system during scheduled maintenance.

.

If FlexClone is licensed on the storage controller and all other prerequisites have been met, SnapDrive uses FlexClone volume technology to connect to LUNs in a Snapshot copy. To use FlexClone, a FlexClone license is required. No separate license is required for creating LUN clones. For more information about FlexClone and LUN clones, refer to the Data ONTAP 7.3 Storage Management Guide.

BEST PRACTICE

Disable automatic Snapshot copy creation on the storage system for the volume on which the LUNs are created and set the Snapshot space reserve to 0 by using the following commands on the storage system; then delete any existing Snapshot copies.

- `vol options <vol-name> nosnap {on | off}`
- `snap reserve <vol_name> 0`
- `snap delete <vol_name>`

For information about Snapshot management best practices, refer to the SnapDrive 6.2 for Windows Installation and Administration Guide or the Data Protection Online Backup and Recovery Guide.

8.2 CONSISTENT SNAPSHOT COPIES

Making Snapshot copies in a SAN environment differs from doing so in a NAS environment in one very fundamental way: In a SAN environment, the storage system does not control the state of the file system.

SnapDrive for Windows is tightly integrated with the Windows operating system, which can create and restore consistent Snapshot copies for file system data. This is possible with SnapDrive for Windows because all data in the NTFS file system is flushed to disk when creating the Snapshot copy. Snapshot copies are useful only when they can be successfully restored. Snapshot copies of a single storage system volume that contains all the LUNs in the host file system are always consistent, provided that the file system supports the freeze operation. But if the LUNs in the host file system span different storage system volumes or storage systems, then the copies may not be consistent unless they are made at exactly the same time across different storage system volumes or storage systems and they can be restored successfully.

Example: Microsoft Exchange server requires multiple LUNs for different types of data such as the LOGS and DB LUN. Microsoft Exchange best practices also note that these LUNs should reside on different volumes.

```
sdcli snap create -fs /mnt/fs_multi_vol -snapname snap1
```

BEST PRACTICE

The following guides describe tools that are tightly integrated with SnapDrive for Windows and the Windows application. Use the various Windows application-specific tools for application-consistent Snapshot copies.

- SnapManager for Microsoft Exchange: Best Practice Guide

- SnapManager for Microsoft SQL Server: Best Practice Guide
- SnapManager for Microsoft SharePoint: Best Practice Guide
- SnapManager for Microsoft Hyper-V: Best Practice Guide

For more information, refer to the NOW site or the Technical Reports Library.

8.3 SNAPSHOT COPY SPACE MANAGEMENT

Snapshot copy backups occur in a matter of seconds, and each copy typically consumes only the amount of data that has changed since the previous copy was created. Thus Snapshot copies consume minimal disk space, while at the same time providing up to 255 online point-in-time images.

The amount of disk space consumed by an individual Snapshot copy is determined by the following two factors:

- The rate at which the data changes within the active file systems. The data change can be in megabytes per second or megabytes per hour.
- The amount of time that elapses between creation of Snapshot copies.

BEST PRACTICES

- Disable automatic Snapshot copy creation on the storage system for the volume on which the LUNs are created.
- Periodically check the Snapshot copies and delete old copies that could unnecessarily occupy space.
- Because users make several Snapshot copies, NetApp recommends naming the copies in a manner that indicates their usage.

8.4 SNAP RESERVE

Data ONTAP reserves a default of 20% of volume space to be available for files to use. This is because Snapshot copies need space, which they consume in the snap reserve area. By default, after the snap reserve area is filled, the Snapshot copies start to take space from the general volume. Because of WAFL® technology, snap reserve does not reserve specific physical blocks; rather, it is a logical space accounting mechanism. For more information about snap reserve, refer to the Block Access Management Guide for iSCSI and FC for your release of Data ONTAP.

BEST PRACTICE

NetApp recommends setting the snap reserve value to 0% for space reserved LUNs. This is because the scheduled Snapshot copies created by the storage controller do not capture the LUN in a consistent state. Setting the snap reserve to 0% allows all of the volume space to be usable by the LUNs in the volume. This simplifies management of the environment because the volume can hold all of the LUNs and the Snapshot data for the volume.

9 RESTORING A SNAPSHOT COPY

SnapDrive for Windows 6.2 includes the following methods for restoring a Snapshot copy:

- Rapid LUN Restore (LUN clone split)
- Volume-based Snapshot copy restore
- File Level Restore (FLR)—available with Data ONTAP 7.1 and later

SnapDrive for Windows uses the LUN clone split method of LUN restore in the GUI. Both volume-based Snapshot restores and file-level restore are available only via the SnapDrive command line utility (`sdcil.exe`).

For more information about Snapshot management, refer to the SnapDrive 6.2 for Windows Installation and Administration Guide or the Data Protection Online Backup and Recovery Guide.

9.1 USING FILE-LEVEL RESTORE BASED SNAPRESTORE

Use the following command to restore a file using the file-based SnapRestore method:

```
sdcli snap restore [-m <MachineName>] {-d <MountPoint> -s <SnapshotName>} ||
{ -flr [-copy] {-s <SnapshotName> -files <filepath>[...] }+ }


MachineName         - Optional. If not provided will use local machine
SnapshotName        - Name of the backup snapshot from which to restore
-flr                - Selects file level restore
-copy               - Optional - this is the option to force copy-restore
-files              - Means the filepath args are files to restore
filepath            - List of "destination" filepath, including the mount point
detailssnapname snap_name [-force [-noprompt]] [{-reserve | -noreserve}] [-vbsr
[preview|execute]]
```

Example:

```
sdcli snap restore –flr –s snapshotname –files m:\files\file.txt
```

BEST PRACTICES

- SnapDrive enables data consistency of files restored from consistent Snapshot copies. However, application consistency is outside the function of SnapDrive for Windows. Files restored by using a file-level restore operation may result in application inconsistency. Use file-level restoration with caution, following the recommended practices for the operating system or applications using the files.
- If there are newer Snapshot copies that were created after the Snapshot copy being used to restore from, it is a best practice to replicate those Snapshot copies to a secondary storage system by using SnapVault and then perform the file-based SnapRestore operation.

10 COMPLEMENTARY SOLUTIONS

There are various complementary solutions that use SnapDrive technology in data protection, backups, disaster recovery, and data availability for the environment This section gives a few examples of common scenarios. For information about specific solutions, consult a NetApp technology specialist.

10.1 DATA PROTECTION

NetApp tools such as SnapRestore, SnapMirror, SnapVault, SyncMirror®, MetroCluster, and Operations Manager are just a few examples of NetApp technology that can be used in conjunction with SnapDrive to create an enterprise-wide data protection policy.

For specific data protection best practices, refer to the NOW site or the Technical Reports Library. The following documents also offer in-depth knowledge about data protection using SnapDrive:

- Disaster Recovery Support for DataFabric Manager Data Using SnapDrive
- SnapVault Disk to Disk Backup on Windows Environment
- SnapMirror Sync and SnapMirror Semi-Sync Overview and Design Considerations
- SnapMirror Async Overview and Best Practices Guide
- iSCSI Multipathing Possibilities on Windows with Data ONTAP

10.1 CLUSTERING

SnapDrive for Windows is available in both physical and virtual environments and integrates with Microsoft Cluster Server, Windows failover clustering, VMware MSCS, and Hyper-V MSCS. For information about how to set up clustering on the different platforms, refer to the NOW site or the SnapDrive 6.2 for Windows Installation and Administration Guide.

BEST PRACTICE

Windows has an optional quorum resource called Majority Node Set (MNS) that does not require a disk on a shared bus for the quorum device. In this type of deployment, all nodes of the MNS cluster set must have SnapDrive installed and they must be able to communicate with all nodes and storage controllers involved in the cluster set.

10.2 SNAPMANAGER

As stated in section 8.2, SnapDrive for Windows enables users to create file-system-consistent Snapshot copies on NetApp storage. SnapManager tools enable application-specific consistency and use SnapDrive for Windows for its underlying technology to create Snapshot copies on NetApp storage. This tight integration of SnapDrive and application awareness has made SnapManager one of the most popular tools for making and managing backups for Microsoft Exchange, SQL Server, SharePoint, and Hyper-V in a NetApp storage environment. All of the SnapManager products rely on SnapDrive for Windows to execute all backup and restore commands on the storage system.

For information about specific application best practices and SnapManager, refer to the NOW site or the Technical Reports Library. The following documents also offer in-depth knowledge for specific application environments:

- SnapManager for Microsoft Exchange: Best Practice Guide
- SnapManager for Microsoft SQL Server: Best Practice Guide
- SnapManager for Microsoft SharePoint: Best Practice Guide
- SnapManager for Microsoft Hyper-V: Best Practice Guide
- SnapManager 2.0 for Virtual Infrastructure Best Practices Guide

10.3 VIRTUALIZATION

Virtual infrastructures are vital solutions for enterprise environments that are looking for operational efficiency, cost effectiveness, and flexibility. SnapDrive for Windows offers support for environments that use VMware virtualization and also Microsoft Hyper-V technology. The following document also offers in-depth knowledge for virtualized environments:

- Best Practices for File System Alignment in Virtual Environments

VMWARE SPECIFIC ENVIRONMENTS

The following links provide in-depth knowledge about VMware environments:

- NetApp and VMware Virtual Infrastructure 3 Storage Best Practices
- NetApp and VMware vSphere Storage Best Practices
- SnapManager 2.0 for Virtual Infrastructure Best Practices Guide

HYPER-V SPECIFIC ENVIRONMENTS

The following links provide in-depth knowledge about Hyper-V environments:

- NetApp Implementation Guide for Microsoft Virtualization
- NetApp Storage Best Practices for Microsoft Virtualization
- SnapManager for Microsoft Hyper-V: Best Practice Guide

For information about best practices for virtualized environments, refer to the NOW site or search the Technical Reports Library for the specific application.

11 FOR MORE INFORMATION

- Review the SnapDrive 6.2 for Windows Release Notes for additional information such as limitations, upgrade information, fixed issues, known issues, and documentation corrections.
- Visit SnapDrive Frequently Asked Questions.
- Visit the NOW site for Technical Assistance & Documentation.
- Download the latest software from Software Downloads.
- Talk to your peers and other experts by visiting the NetApp Communities.
- Get free instructor-led training sessions to help you in "Getting Started with Software Packs."